University of Sussex

Secure quantum-enhanced networks of remote sensors

Efficiently estimating remote parameters with information privacy and integrity

Sean William Moore

Submitted for the degree of Doctor of Philosophy

University of Sussex

November 2024

Declaration

I hereby declare that, unless otherwise indicated, the results presented in this thesis are the product of my own independent research, and that, to the best of my knowledge, all the relevant sources have been appropriately acknowledged. In addition, this thesis has not been and will not be submitted in whole or in part to another University for the award of any other degree. Some of these results have already been published or are available in a preprint:

- Sean W. Moore, Jacob A. Dunningham; Secure quantum remote sensing without entanglement. AVS Quantum Sci. 1 March 2023; 5 (1): 014406.
- Sean William Moore and Jacob A. Dunningham. Secure quantum-enhanced measurements on a network of sensors. 2024. arXiv: 2406.19285 [quant-ph].

I confirm that I am responsible for all of the calculations, both analytical and numerical, and the contents of both works and throughout this thesis. My co-author, Professor Jacob Dunningham, aided in conceptualising the novel secure quantum remote sensing protocols of sections 5.1 and 6.1, the use of multipass methods for enhancing information gain in section 5.2.3 and the disguised man in the middle attack of section 7.2.3. The remaining novel concepts and proofs of chapters 5, 6 and 7 are entirely of my own design. Furthermore, he provided invaluable support and guidance by discussing methodology, results and proposing changes to enhance the quality of the manuscripts.

Sean William Moore

UNIVERSITY OF SUSSEX

Sean William Moore, Doctor of Philosophy

Secure quantum-enhanced networks of remote sensors
Efficiently estimating remote parameters with information privacy and integrity

Summary

Quantum metrology and quantum communications are typically considered as distinct applications in the broader portfolio of quantum technologies. However, there are scenarios where combining the two is appropriate and advantageous. This thesis is a study of the methods used for secure quantum remote sensing and proposes novel protocols that ensure privacy and integrity of information when estimating parameters and functions of parameters at remote locations.

There are three novel protocols proposed. The first is for one party, Alice, to produce quantum states that are used by a remote party, Bob, to interact with and measure a parameter with the aim that only Alice may gain information about the parameter. It does not require entanglement or high dimensional states, using only phase sensitive qubits. This makes it simpler and more practical, providing a greater flux of information than existing protocols. The second protocol has many Bobs, each with their own parameter and Alice performs estimation of a function of those parameters. It is the first secure network protocol to provide privacy and estimation beyond the standard quantum limit for a function of parameters without using a separate quantum key distribution between parties. The final protocol adapts the communication method between Alice and each Bob for both of the previous protocols to protect against manipulation of their classical communications. It is the first secure quantum remote sensing protocol to integrate all of the security features into a single protocol and does not require classical authentication.

Like previous protocols, these are shown to be exponentially more likely to detect an attack on the privacy and integrity with each quantum state attacked. However, they are novel in providing a rigorous privacy limit in terms of the amount of information an eavesdropper attacking the quantum communication channel can obtain before being detected and are optimised for information gain while maintaining such a limit. Finally, they are shown to be significantly more robust in a photonic implementation than other cryptographic quantum protocols improving practicality, allowing a greater flux of information.

Acknowledgements

When I applied for my doctorate I placed more importance on who I would be working with than the specifics of the proposed project. I could not have made a better decision. In the last four years I have learned how unpredictable the direction and cadence of research can be, every new discovery opening a plethora of new directions and approaches. The part of my research that has been constant and unmovable is the support of my supervisor Jacob Dunningham. I could not imagine having a better relationship with any supervisor. Thank you, it has been a pleasure.

I am grateful to DSTL for providing the financial support for my doctorate and inviting me to several interesting events. Duleep Wickramasinghe, in particular, has been in regular contact, maintaining an interest in my progress. I am glad to have had his continual support as my research evolved in unexpected directions.

I have been at the University of Sussex a long time, spending 10 years as part of the department of mathematics and physics. My doctorate is the final chapter of journey starting as a first year undergraduate in 2014. The members of the department who had a positive influence on me are too many to count. Here, I will focus on those who had the greatest influence on my outlook and experience as a postgraduate researcher.

Andrea Banfi, who, after I had spent two years away from my studies as an undergraduate, supervised me for a project and reignited my passion for physics with his infectious personality. Robert Smith supervised me as a masters student and introduced me to numerical approaches to physics, with him I built skills and understanding outside of the standard curriculum that have proved invaluable in my approach to research. Sebastian Jaeger and Kathy Romer encouraged me take on numerous extra curricular roles during my doctorate from which I gained the soft skills that I was lacking and evolved as a person.

For the most part I have been in a small group with only my supervisor, Jacob, having an influence on my research. After a little over half of my doctorate I was approaching the end of my first body of work. I attended a conference on secure networks of quantum sensors at LIP6, Sorbonne University which had a profound influence on the direction of the rest of my research. I acknowledge the influence of all of the presenters at that

conference, Damian Markham and Majid Hassani in particular for organising it. Several months before the end of my doctorate my supervisor took on another PhD student, Luke Rhodes, who I have enjoyed working with. This initiated the final evolution in my role, going from being supervised to helping supervise another researcher and oversee a new project.

Over the course of my doctorate I have gone through easier and more difficult times, a lot has changed. This has been on a professional, societal and personal level. I have been fortunate to have the support of my supervisor, Jacob, as I, and for some things, we have had to adapt to these changes. The most important place to have support is at home. I could not have undertaken this journey without my fiancee, Solène. No matter what else is going on I have always had her to turn to for everything. Having her and our two dogs, Fidgy and Roxy, at home every day has been my favourite part of the last four years.

Contents

List of Tables

List of Figures

Greek symbols

$(\delta\phi)^2$ Dispersion of ϕ estimates.

Γ Weight of basis vectors of measurements performed by Eve in a photon splitting attack.

Λ Expected value of circular dispersion of posterior distribution for parameter drawn from circular uniform prior distributions.

Λ_A Alice's expected value of circular dispersion of posterior distribution for parameter drawn from circular uniform prior distributions drawn from the amount of data she decides to use.

Λ_E Eve's expected value of circular dispersion of posterior distribution for parameter drawn from circular uniform prior distributions drawn from the amount of data she gains before being detected.

Ξ Expected value of circular dispersion around true value of posterior distribution for a single set of parameters chosen at random from circular uniform distributions drawn from the distance between two points on a circle. Circular analogue of half the mean square error.

α Weighting of $|0\rangle$ basis vector in qubit (ch1) OR prior distribution hyperparameter (can also be a vector).

α_k Weighting of basis vector k in quantum state.

β Weighting of $|1\rangle$ basis vector in qubit.

$\boldsymbol{\nu}$ Weighting for linear function of parameters.

χ Initial state of .

χ_0 Shift in initial state of separable or entangled set of qubits their measurements away from $\sigma_x - \sigma_y$ basis, can be shared secret.

χ_j Initial state of the j^th qubit, can contain a shared secret.

δ A small number (ch1) OR dispersion of dispersion of following variable.

$\delta\phi$ A small shift in ϕ.

δa Dispersion of dispersion of following variable.

η Number of rounds Eve could gain information from before Alice detects her.

γ Phase of measurements performed by Eve in a photon splitting attack.

$\hat{\phi}$ Estimator of the phase of a qubit.

$\hat{\theta}$ Estimator of random variable θ.

λ An eigenvalue.

μ Number of independent measurements OR circular mean of distribution.

ν Circular standard deviation.

ϕ Phase of a qubit or applied to a qubit using a phase gate.

ρ Density operator for quantum state.

σ Linear standard deviation.

σ_x Pauli-X eigenstate.

σ_y Pauli-Y eigenstate.

σ_z Pauli-Z eigenstate.

θ Bloch sphere coordinate corresponding to the probabilities of the $|0\rangle$ and $|1\rangle$ eigenvalues for a qubit OR a random variable such as a function of phases $\theta = f(\phi)$ (sec2.4.3,ch6,7).

$\tilde{\epsilon}$ Shared secret between Alice and Bob added to phase.

φ Phase of a qubit measurement.

$\varphi_k(m)$ The k^{th} possible combination of m phases from the set $\vec{\phi}$.

ϑ Bloch sphere coordinate corresponding to the probabilities of the $|0\rangle$ and $|1\rangle$ eigenvalues for qubit measurement.

$\vec{\varphi}$ The set of all possible combination of phases from the set $\vec{\phi}$.

ξ Circular dispersion around true value of posterior distribution for single set of results for single set of parameters chosen at random from circular uniform distributions drawn from the distance between two points on a circle. Circular analogue of half the mean square error.

Number sets

$\bigcap$ Union of two sets.

$\bigcup$ Union of two sets.

$\forall$ For all.

$\in$ Member or a set.

$\mathbb{C}$ Complex number set.

$\mathbb{F}$ Set of Bobs that performed fidelity checks.

$\mathbb{M}$ Set of Bobs that performed parameter measurement.

$\mathbb{N}$ Natural number set.

$\mathbb{Q}$ Rational number set.

$\mathbb{R}$ Real number set.

Quantum states

$|0\rangle$ The eigenstate corresponding to the 0 quantum bit eigenvalue.

$|1\rangle$ The eigenstate corresponding to the 1 quantum bit eigenvalue.

$|E\rangle$ The state of an entangled ensemble of states.

$|S_b\rangle$ The state of the b^{th} qubit in a separable ensemble of states.

$|X\pm\rangle$ The Pauli-X eigenstates.

$|Y\pm\rangle$ The Pauli-Y eigenstates.

$|Z\pm\rangle$ The Pauli-Z eigenstates.

$|\alpha/\delta\rangle$ The squeezed coherent state.

$|\alpha\rangle_b$ A possible state of the qubit in the b^{th} Hilbert space, either $|\alpha\rangle_b = 0$ or $|\alpha\rangle_b = 1$ and $|\alpha\rangle_b \neq |\beta\rangle_b$.

$|\beta\rangle_b$ A possible state of the qubit in the b^{th} Hilbert space, either $|\beta\rangle_b = 0$ or $|\beta\rangle_b = 1$ and $|\beta\rangle_b \neq |\alpha\rangle_b$.

$|\chi_B\rangle$ A generalised GHZ state with B quanta entangled and a phase χ. When $B = 1$ this is a qubit state and $_1$ may be omitted from the notation.

$|\lambda_k\rangle$ A quantum state in the Hilbert space of the λ_k eigenstate.

$|\mathcal{R}\rangle$ A random qubit state.

$|\psi_{\mathcal{P}}\rangle$ A pure qubit state.

$|\psi\rangle$ Standard expression for a quanta in a superposition of states. Used to describe the quantum subject of the current discussion or an arbitrary quantum state.

$|k\rangle$ Quantum eigenstates with eigenvalues $k \in \mathcal{N}_0^+$. Also written $|j\rangle$ when using superposition of eigenstates.

Latin symbols

B Total number of Bobs.

Bi Circular bias.

$C_{\hat{X},X}$ Cost function for parameter X and its estimator $\hat{X}$.

$D(\theta\ \phi)$ Circular distance between angles ϕ and θ.

E Probability of Alice sending an ensemble of states to the Bobs that are entangled.

F Probability of performing a fidelity check.

F_{glo} Fisher information of global estimation strategy.

F_{loc} Fisher information of local estimation strategy.

L_a Symmetric logarithmic derivative.

M Probability of performing a parameter measurement.

M_m Number of bobs that perform measurement in a round.

N Number of rounds specific to discussion OR number of resources used.

$P_{coh}(k)$ Probability of their being k photons in a coherent state.

P_{sing} Probability of a man in the middle attack being detected in a single round.

S Probability of Alice sending an ensemble of states to the Bobs that are separable.

V Circular variance.

$\bar{R}$ Mean resultant length of directional distribution.

$\hat{P}(X)$ Quantum phase gate operator applying phase X.

$\hat{U}$ Unitary operator.

$\mathcal{B}$ Probability a mixed qubit is in a biased state.

$\mathcal{F}$ The quantum Fisher information. For multiple parameters this is a matrix with elements $\mathcal{F}_{ab}$ for parameter a and b. When discussing the single parameter quantum Fisher information for situation X this can be written $\mathcal{F}_X$.

$\mathcal{I}$ The classical Fisher information. For multiple parameters this is a matrix with elements $\mathcal{I}_{ab}$ for parameter a and b. When discussing the single parameter quantum Fisher information for situation X this can be written $\mathcal{I}_X$.

$\mathcal{L}$ Likelihood function.

$\mathcal{N}$ Normal distribution.

$\mathcal{P}$ Probability a mixed qubit is in the pure state intended.

$\mathcal{R}$ Probability a mixed qubit is in a random state.

$\mathcal{V}$ Linear variance.

$\mathcal{WN}$ Wrapped normal distribution.

$\vec{n}$ Set of measurement results corresponding to probabilities $\vec{p}$.

d_E Probability of a man in the middle attack being detected by an entangled state in a round.

d_S Probability of a man in the middle attack being detected by a separable state in a round.

d_X Probability of a man in the middle attack of type defined by the acronym X being detected if a fidelity check corresponding to the initial state is performed.

m Number of bobs that perform measurement in a round (ch6,7) OR number of passes in m-pass parameter estimation (ch5).

p Sometimes written P, a probability relevant to the discussion. $\vec{p}$ is a vector of probabilities for the family of categorical distributions.

u Probability of Eve being undetected when performing a man in the middle attack.

Acronyms

AQS Anonymous quantum sensing.

BB84 The Bennett-Brassard quantum key distribution algorithm first published in 1984.

Bin Binomial distribution.

E91 Ekert's entanglement quantum key distribution protocol first published in 1991.

Geo1 First form of geometric equation.

Geo2 Second form of geometric equation.

GHZ Greenberger–Horne–Zeilinger state.

IR Intercept and resend attack.

KARGRA Kamioka Gravitational Wave Detector.

LIGO Laser Interferometer Gravitational-Wave Observatory.

MIM Man in the middle attack.

MLE Maximum likelihood estimator.

Mn Multinomial distribution.

MR Measure and replace attack.

NB Negative binomial distribution.

NM Negative multinomial distribution.

QKD quantum key distribution.

SARG04 Quantum cryptography protocol published in 2004 by Valerio Scarani, Antonio Acín, Gregoire Ribordy, and Nicolas Gisin.

SP Spoofing attack.

SQRS Secure quantum remote sensing.

VIRGO Virgo interferometer.

XOR Exclusive or logic gate.

Glossary

Alice (SQRS) The party that produces initial quantum states in most SQRS protocols. She may also apply a phase parameter.

asymptotic limit (quantum metrology) In quantum metrology the asymptotic limit describes the amount of data for which it is highly statistically likely that the uncertainty of parameter estimators closely matches the asymptote. For well chosen estimators (for instance the MLE) this corresponds to near equality in the Cramér-Rao bound.

authentication protocol (cryptography) An authentication protocol is a cryptographic protocol specifically designed to assure different entities that they are communicating with authorised and/or specific entities..

Bayesian statistical inference A type of statistical inference in which Bayes' theorem is used to calculate a probability of a hypothesis, given prior evidence, and update it as more information becomes available.

Bell pair Bell's states are specific quantum states of two qubits that represent the simplest examples of quantum entanglement.

Bernoulli trial A random experiment with exactly two possible outcomes.

bias Statistical bias is a systematic tendency in which the methods for gathering and/or analysing data generate statistics that present a skewed or biased description of reality. The bias of an estimator is the difference between its expected value and the true value of the parameter.

Bloch sphere A geometrical representation of the pure state space of a qubit. Named after Felix Bloch.

Bob (SQRS) The party that measure final quantum states in most SQRS protocols. He may also apply a phase parameter.

Charlie (SQRS) A third party in some SQRS protocols. He may apply a phase parameter to quantum states.

circular statistics Circular or polar statistical distributions are probability distributions of a random variable whose values are angles, usually taken to be in a continuous 2π range.

classical Fisher information A way of measuring the amount of information that an observable random variable X carries about an unknown parameter ϕ of a distribution that models X.

cost function This function maps an event or set of values of some variable to a real number representing the cost associated with the event. In statistical inference the expected value of the cost function is used.

Cramér-Rao bound A lower bound on the variance of an unbiased parameter estimator with minimal prior information or large data.

cryptography The practice and study of techniques for secure communication and information storage in the presence of adversarial behaviour.

directional statistics The subdiscipline of statistics that deals with multidimensional data such as directions axes or rotations.

dispersion (statistics) The extent to which a distribution is stretched or squeezed.

entangled (quantum) states An ensemble of quantum states that cannot be described independently. Evolution and measurement of any of the entangled quanta affects the others.

equatorial plane of the Bloch sphere Plane of the Bloch sphere where states may be described as $\frac{1}{\sqrt{2}}(1, e^{i\phi})^T$, where ϕ is the phase, similar to a longitude.

Eve (SQRS) A malicious party in an SQRS protocol who may attack the protocol in various ways for various reasons. Synonymous with eavesdropper in classical cryptography.

frequentist statistical inference A type of statistical inference based in frequentist probability, which treats "probability" in equivalent terms to "frequency" and draws conclusions from sample-data only analysing the frequency of events in the data.

great circle The circular intersection of a sphere and a plane passing through the sphere's centre point. For instance, the equator and all lines of latitude.

grid approximation A Bayesian numerical method where a grid of possible values is used to compute an approximation to a posterior distribution.

Heisenberg limit The fundamental limit on estimation uncertainty due to the Heisenberg uncertainty principle. For single parameters, $\delta\phi \sim 1/N$.

hyperspherical coordinate system A coordinate system for an n-sphere, ($n \in \mathbb{N}^+$ the n-dimensional generalisation of the 1-dimensional circle and 2-dimensional sphere.

integrity (cryptography) The ability to avoid and detect changes made to information by an adversary.

key (cryptography) A piece of information which, when processed through a cryptographic algorithm, can encode and decode cryptographic data.

likelihood function A measure of how well a statistical model explains observed data by calculating the probability of seeing data under different parameter values of that model.

Markov chain A stochastic process describing a sequence of possible events in which the probability of each event occurring depends only on the state obtained in the previous event. Named in honour of Andrey Markov.

Matlab A programming language and numeric computing environment developed by MathWorks.

metrology The scientific study of measurement.

Monte Carlo methods A broad class of computational algorithms that rely on repeated random sampling to obtain numerical results.

multipass quantum metrology Quantum metrology techniques where probes interact with parameters multiple times or their interaction time is increased to increase the information gain.

non-orthogonal basis When two or more sets of quantum states are used where all of the states in each set are orthogonal but any two states from each set are not orthogonal. For sets $|\vec{\phi}\rangle$ and $|\vec{\psi}\rangle$, $\langle\phi_j|\phi_k\rangle = \langle\psi_j|\psi_k\rangle = 0 \forall j \neq k$ and $\langle\phi_j|\psi_k\rangle \neq 0 \forall j, k$..

orthogonal state Two quantum states, $|\phi\rangle$ and $|\psi\rangle$ are orthogonal then $\langle\phi|\psi\rangle = 0$. .

polarisation encoded photon Photons that hold parameter information in their polarisation state. For instance, phase information.

posterior distribution The posterior probability is a type of conditional probability that results from updating the prior probability with information summarized by the likelihood via an application of Bayes' rule.

prior distribution A prior probability distribution of an uncertain quantity, often simply called the prior, is its assumed probability distribution before some evidence is taken into account..

privacy (cryptography) The ability to keep information private from an adversary.

probability density function A function whose value at any given point in the set of possible values taken by the random variable can be interpreted as providing a relative likelihood that the value of the random variable would be equal to that sample. Often used to specify the probability of a continuous random variable falls within a particular range of values.

quantum Fisher information The quantum analogue of the classical Fisher information. It quantifies the amount of information that measurement of a quantum state could give about a parameter. For multiple parameters there is a quantum Fisher information matrix.

quantum noise Noise arising from the indeterminate state of matter in accordance with the fundamental principles of quantum mechanics. Specifically, the uncertainty principle and zero-point energy fluctuations.

separable (quantum) states An ensemble of quantum states that can be described independently. Evolution and measurement of one of the states does not affect the others.

single shot metrology Metrology using a single measurement.

spoofing (cryptography) An attack on a cryptographic protocol where the information is replaced with misleading information.

standard deviation A measure of dispersion of a distribution about it's mean. Defined in linear statistics for random variable X as $\sqrt{E[X^2] - (E[X])^2}$.

standard quantum limit A limit on some methods of quantum parameter estimation where the dispersion of an estimator evolves as $\delta\phi \sim 1/\sqrt{N}$ where N is the resource count. If $N = \mu$ the number of independent measurements this is equivalent to the shot-noise limit of classical statistics.

variance A measure of dispersion, the expected value of the squared deviation from the mean of a random variable.

Chapter 1

Introduction

Quantum technologies is a rapidly maturing field where the fundamental laws of quantum mechanics are used to build materials, systems and devices with various advantages over classical systems. Quantum physics demonstrates that the universe is indeterministic. All systems are in a potentially infinite superposition of states until measurement forces them to choose a single state, the probability of each choice can be predicted using quantum mechanics. The seemingly deterministic nature of classical physics is due to the instability of large quantum systems and the reduced probability of quantum effects on large quantum systems. Classical systems are too large to show quantum effects, they are built from so many quantum subsystems that due to the statistics of those subsystems appear deterministic [1, 2].

Three ways in which quantum mechanics are used to improve on classical technologies are: the use of the indeterministic nature of quantum states to perform calculations with more complex logic gates than classical computer [3], the use of quantum states to perform more efficient measurements [4] and the creation of systems secure against eavesdropping and tampering [5]. Each is used to bring a quantum mechanical advantage to computing, metrology and cryptography respectively. When more than one of these applications is required classical systems apply them sequentially. Quantum systems can perform more than one of these tasks concurrently. For instance secure quantum remote sensing [6–17] (SQRS) and blind quantum computing [18] bring aspects of security to quantum metrology and computing respectively.

Quantum information is the convergence of the fundamental laws of physics with information theory [19]. It has led to the development of new quantum technologies where the performance metrics of the devices are defined by fundamental physics. The development

of quantum information theory alone has been enough to stimulate new classical science and technologies. For instance, Grover's algorithm [20] reduces the computation requirement for a brute force attack on a cryptographic key from the $\mathcal{O}(N)$ evaluations required by a classical computer, where N is the key size, to $\mathcal{O}(\sqrt{N})$ on a quantum computer. So, post-quantum classical cryptographic methods are now used to protect against future large scale quantum computers.

Quantum computing uses manipulations of groups of quantum states similar to idealised states to perform calculations and algorithms that are not possible with classical computers. The most fundamental quantum state for all quantum information theory is the qubit, a quantum state that has two quantum numbers, labelled as 0 and 1. These can be thought of analogues to 0 and 1 of classical bits. However, as the qubit, which functions like a quantum bit in calculations, can be any superposition of these states, quantum computers can perform algorithms not possible with classical bits. A pure qubit state is represented

$$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle\,, \tag{1.1}$$

where $\alpha, \beta \in \mathbb{C}$ and $|\alpha|^2 + |\beta|^2 = 1$. In addition to solving some problems more efficiently than a classical computer [20–29], they are a powerful tool for the simulation of quantum systems [30–35]. Qubits are also important states in quantum metrology and cryptography.

The subject of this thesis is novel SQRS protocols that optimise information gain while ensuring information security. It brings information privacy and integrity to quantum metrology protocols using qubits. Privacy is the ability to keep information private from an adversary and integrity is the ability to avoid and detect changes made to information by an adversary. Chapter 2 introduces quantum metrology with a focus on the quantum states, parameter interaction and measurements for phase estimation integral to the main results of this thesis. Quantum metrology uses quantum states to improve on

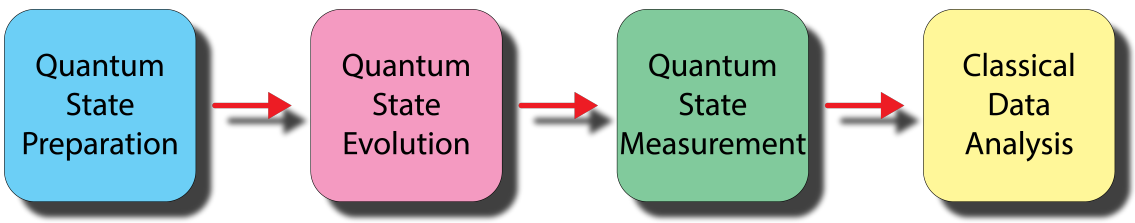

Figure 1.1: The four essential steps to any quantum metrology protocol.

classical metrology. It shares many of the same principles as quantum computing. However, rather than manipulating quantum states to perform calculations, metrology focuses on the inference of unknown quantum parameters. The steps of a quantum metrology

protocol are set out in figure 1.1. The first step to showing the effectiveness of a quantum metrology protocol is quantifying the information gain over classical protocols. In the large data limit, the quantum Fisher information matrix [36], with elements $\mathcal{F}_{ab}$ defined in chapter 2, is used as a measure of the amount of information held by quantum state about unknown parameters as a measure of the effectiveness of initial state creation and parameter interaction. A metrology protocol outputs classical information. Therefore, it relies on statistical inference for the analysis of that classical data and conversion to parameter estimates.

The classical Fisher information matrix [37], with elements $\mathcal{I}_{ab} \leq \mathcal{F}_{ab}$ also defined in chapter 2, is bounded from above by the quantum Fisher information and used as a measure of the effectiveness of data analysis of the data $\vec{x}$ resulting from the measurement protocol. The quantum,

$$(\delta a)(\delta b) \geq \frac{[\mathcal{F}^{-1}]_{ab}}{n} \geq \frac{1}{\mu \mathcal{F}_{ab}} \tag{1.2}$$

and classical Cramér-Rao bounds,

$$(\delta a)(\delta b) \geq \frac{[\mathcal{I}^{-1}]_{ab}}{n} \geq \frac{1}{\mu \mathcal{I}_{ab}}, \tag{1.3}$$

where $[X]^{-1}_{ab}$ is the ab index of the inverse of a matrix X and μ is the number of independent measurements, put a limit on the covariance of the estimators of parameters a and b. When $a = b$ it gives a lower bound on the variance of parameter a.

Entanglement and multiple interactions with parameters are effective ways of increasing information gain about a parameter that can give equivalent results when applied appropriately [38, 39]. Highly non-classical quantum states such as squeezed states [40] improve information gain on one parameter in quantum metrology protocols that measure two parameters with one being of more interest than the other. They do this by increasing δb which decreases δa. However, the focus on large data information gain means that statisticians must be aware of how attainable the asymptotic limit in which the results of the Fisher informations are useful. For instance, infinite precision states,

$$|\psi\rangle \propto (1-\delta)\,|0\rangle + \delta\,|\alpha/\delta\rangle\,, \tag{1.4}$$

where $|0\rangle$ is the vacuum state and $|\alpha/\delta\rangle$ is a squeezed coherent state, have infinite quantum Fisher information as $\delta \to 0$ and so would appear to offer perfect measurement precision with finite resources. However, a careful analysis shows that they also require infinite data, $\mu \to \infty$ to have equality in the Cramér-Rao bound [41] making the Fisher information a poor measure of practical information gain. More recently, there has been an increased

focus on measures of information gain that are not constrained by the same requirements as the Fisher informations [42], especially for limited data.

There are many scenarios where limited data information gain is important. For instance, in the search for gravitational waves Michelson interferometers are used at VIRGO, LIGO and KAGRA to detect variations in space-time on the surface of the Earth [43]. As gravitational waves travel through the Earth they cannot be measured indefinitely making it imperative that measurements and result analysis are well optimised for limited data.

SQRS is a scenario where the limited data information gain is very important. Since in these cases sending many pieces of information about a parameter being measured compromises its security, it is not sufficient to use information asymmetry with an eavesdropper in large data to quantify information privacy. Often this is qualified by ensuring that an eavesdropper is increasingly likely to be detected each time they attack. However, if the information gain before the eavesdropper is detected is not quantified then, the amount of information privacy has not been quantified.

Chapter 3 discusses the methods used for the final step of the metrology protocols in this thesis. It covers the methods of data creation, analysis and the analysis of limited data information gain. As this research is theoretical and the probabilities of events occurring are well defined the data is created numerically in simulations using pseudo-random number generators. The number of possible event combinations are very large so, Monte Carlo simulations are used to draw statistics of the information gain. The data analysis is performed using Bayesian statistical inference with circular statistics to account for the circular nature of phase parameters and their estimation in limited data scenarios with minimal prior information. Matlab codes to perform the calculations giving the most important numerical results in this thesis are available on two github repositories linked to the S-W-Moore account relevant to the articles most of the results in this thesis are drawn from [44, 45]. Using these methods chapters 5, 6 and 7 demonstrate the effectiveness of their SQRS protocols by optimising the protocol parameters for limited data information gain while bounding information privacy using a limit on the average information an eavesdropper can gain.

Quantum cryptography is the use of quantum states to protect the transfer of information. Most protocols use fundamental physics to augment the size of cryptographic keys while making it very unlikely for an eavesdropper to listen in without being detected [5]. This differs from classical cryptography that relies on pseudo random number generators for key enlargement [46, 47].

Security of systems is an increasingly large driver for the development of quantum information systems beyond the implementation of quantum key distribution. For some technologies, such as navigation and global positioning, improved metrology protocols are sufficient to solve security issues. There have been various proposals for satellite based systems with quantum advantages [48]. Some proposals are for improving the satellites system by using quantum enhanced measurements such as entangled photons for distance measurements and quantum timekeeping. However, there are many scenarios where it is not possible to connect to a satellite or doing so is undesirable for security purposes as it broadcasts the position publicly. Alternatively, security concerns could be solved by quantum passive positioning systems that do not rely on an external signal. Quantum enhancement has improved accelerometers and gyroscopes to the point that they can be used for long-term navigation systems without the need for satellites. Another passive system proposed uses magnetic maps [49].

Alternatively, applying cryptographic principles to metrology protocols can ensure SQRS. Chapter 4 provides a thorough review of cryptographic principles and how they have been applied to SQRS in the past. SQRS is a quantum metrology process where some party(ies) involved in quantum state preparation or measurement gain information about quantum parameter(s) held at any remote site(s) with information privacy and integrity. Information privacy ensures that the amount of information gain about the parameter(s) being protected by any parties not designated to gain it, such as an eavesdropper, is sufficiently limited. Information integrity ensures that noise or a malicious party is limited in how much they can manipulate the protocol to bias the estimation or reduce information gain without it being detected. The following are some examples where SQRS can prove useful by ensuring fidelity of measurements states and security against information being stolen or spoofed.

Quantum sensors are now being used for biomedical applications [50]. With medical data being very sensitive it is imperative that it is measured and stored securely against the data being stolen or tampered with. If someone used quantum sensors on a patient who is not present in the hospital it could be advantageous to use quantum mechanics to ensure security of the device measurements [13]. Such classical devices already exist for conditions such as diabetes where some patients carry blood sugar trackers. In this case the patient can be trusted to wear the device but not necessarily to track and truthfully report their blood sugar themselves. If a quantum device was being used in a similar way, quantum states could be used for the security in addition to the measurement.

There are also scenarios where measurement has been outsourced to remote parties that can be trusted to follow instructions but are not be using secure devices themselves or do not have the ability to prepare the quantum states required for measurement themselves. For example, interferometric synthetic-aperture radar which is used for various applications such as volcanology and ground subsidence for oil and water reservoir detection are performed with portable sensors that are brought to different geographic positions to send signals for measuring remote parameters and left without surveillance. Not producing the measurement states on site could greatly reduce the size weight and power requirements of measurement devices. However, on arrival it would be important to ensure that the quantum states are unchanged when the device arrives on site. A rival could manipulate the quantum states of unattended sensors, intercept signals and read results off an unattended device making it important that the measurement results from unattended sensors could only be interpreted by designated parties and could not be eavesdropped or spoofed without detection.

There are scenarios where a measurement signal can be easily intercepted but the results are to be kept secret. This could be a deep sea survey searching for resources beneath the sea floor or search and navigation radar where it might be advantageous to hide the act of measurement and its results.

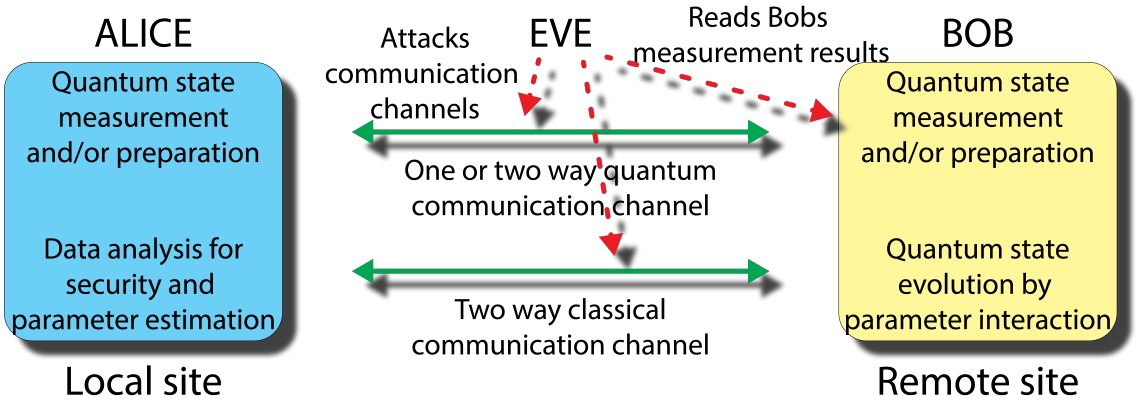

Figure 1.2: An illustration of two party SQRS scenarios. Quantum states are shared between two sites with the aim of one of the sites being able to estimate some parameter(s) held at the other site with information privacy and integrity. In other single site parameter scenarios the quantum state evolution is performed by a third party or it is dependent on both parties (such as a distance measurement). There are also muliple parameter scenarios where those parameters are held over several sites.

SQRS protocols have the potential to bring security determined by fundamental physics to many scenarios where measurement of parameters held at remote sites must be obtained.

For instance medical tests, volcanology, deep sea surveys, radar and many more. The essential principle of SQRS for two parties is demonstrated in figure 1.2. In many of these protocols, fidelity checking of quantum states is used to verify for man in the middle attacks whereby some agent between the two parties can intercept and manipulate the classical and quantum channels between them. The same state fidelity verification is equally useful for remote sensors with local state production and noise in quantum state transportation. The new protocols shown in this thesis bring improvements in practicality, measurement efficiency and security limits.

Chapter 5 introduces a novel two-party SQRS protocol that does not require entanglement and achieves significantly improved information gain compared to previous protocols. It also shows the protocol's effectiveness for parameter estimation with limited data and ability to perform estimation beyond the standard quantum limit.

When considering functions of parameters joint measurement using sequential probe interactions or entangled probes are known to provide significant advantage [38, 39, 51, 52]. When the parameters of interest are held in different locations, a quantum network of sensors [53–62] brings this measurement advantage. Secure quantum network metrology protocols have previously been developed for networks of clocks measuring the average of many measurements of the same phase to provide information integrity [6, 63], the identification of which nodes are in the presence of non-zero magnetic fields with information privacy [9] and the sum of remote phase parameters while maintaining privacy of individual parameters and integrity of their sum [15].

Many scenarios where SQRS, such as volcanology and radar, are used for measuring functions of parameters drawn from different locations. This could be done by using single phase SQRS in parallel and combining the results classically. However, if security is not required, networks of sensors can provide a significant measurement advantage for functions of parameters when an appropriate entangled state is shared between the probes.

In SQRS protocols, to effectively stop an eavesdropper from attacking the quantum channel with no chance of being detected, the measurement states that arrive at the remote site are chosen at random for fidelity checking or interaction with the local parameter. However, when distributing an entangled state over multiple nodes, every part of that state must be chosen for fidelity checking concurrently for it to be effective, reducing the net fidelity checking probability exponentially with the size of the network. When an entire entangled state is used for the estimation of a function of parameters there is a quantum measurement advantage but, if security is to be maintained, this forces a reduction in

flux rate making it impractical. This is exacerbated in limited data scenarios where the statistical variation in result counts and their accuracy further reduces the measurement accuracy and precision.

Chapter 6 introduces a new protocol for performing secure quantum enhanced measurement of linear functions of parameters. It is a hybrid protocol where some separable quantum states and some entangled quantum states are distributed over the networked sensors in an indistinguishable way. It has most of the measurement advantage of an insecure entangled network while maintaining security. It uses the same cryptographic principles as the two party protocol to ensure its security. As network size increases the security is increasingly due to the separable states and the information gain due to the entangled states.

The limited data estimation effectiveness demonstrated in chapters 5 and 6 shows that it is very important for an eavesdropper to be detected quickly. Chapter 7 gives more analytical security proofs for man in the middle attacks on the quantum communication channel. Furthermore, it introduces a new protocol with adaptations to Alice and Bob's communication methods that protects against manipulations of the classical communication channel. This could be applied to both of the previous protocols such that they can be used without classical communication authentication. An authentication protocol is a cryptographic protocol specifically designed to assure different entities that they are communicating with authorised and/or specific entities. With authentication instead encoded in the quantumness of the protocol, it is the first SQRS protocol to integrate features fulfilling all of the security requirements. The only requirement is a shared secret phase to be used as a quantum key.

This thesis brings together a wide variety of concepts from different scientific disciplines to produce novel results. These different sciences have different naming conventions for symbols. The thesis uses the all of the conventions that do not clash but must change a few to retain clarity. It also defines many variables specific to the thesis. In total there are a large amount of symbols used drawn from different sciences and complemented by those specific to the thesis. Therefore, the front matter contains lists of the different types of symbols used with a description of what they represent categorised by type. Furthermore, due to the large number of technical terms and abbreviations, there is a list of acronyms and a glossary.

Many of the key findings in the thesis are due to numerical calculations. Explanations of the numerical methods, how they function and why they are as they are, are

given throughout the main body where appropriate. Appendix A provides an alternative approach, it explains all of the numerical methods in a way that is implementation independent so that the reader can recreate the calculations without going through the entire main body. Otherwise, Matlab code for the main results can be found in two github repositories linked to the S-W-Moore account [44, 45] relevant to the articles most of the results in this thesis are drawn from [16, 17]. The full Matlab code is too long to be included in the main body of the thesis. However, the appendix does contain two different Matlab codes that have already been used to teach about the numerical methods used here; they demonstrate a variety of methods for simulating the metrology data and producing likelihood functions for the protocol in chapter 5.

This thesis proposes protocols that apply cryptographic principles to metrology for the purposes of estimating phase parameters at a remote site and linear functions of phase parameters over a network of remote sites with information integrity and optimised information gain for any given privacy limit. It shows how to gain quantum enhanced measurements of parameters held at remote sites and functions of parameters held at different remote sites using multiple passes, separable and entangled states as appropriate with limited data while maintaining security by maintaining sufficient information privacy and integrity to ensure information asymmetry and limits on the eavesdropper's information gain. These protocols have both quantum enhanced measurement, with information gain beyond the standard quantum limit, and security maintaining information privacy and integrity.

Chapter 2

Quantum metrology of phase parameters

This chapter introduces the conceptual framework of quantum metrology for phase parameters and functions of phase parameters. It gives analytical results that underpin the rest of the thesis such as optimal metrology protocols for large data information gain and their measurement result probabilities. It begins by setting out the notation and important results for the first three steps of any quantum metrology protocol for phase measurements with qubits, as illustrated in figure 1.1. Quantum state preparation, evolution and measurement are each discussed in their own section.

The state evolution and measurement sections also introduce the quantum and classical Fisher informations respectively. The quantum Fisher information is the standard measure of the maximum rate of information gain of quantum parameters in large data from many copies of a quantum state that depends on those parameters. The classical Fisher information is the standard measure of the rate of information gain about parameters from measurement results. The results in this chapter are used to set out the quantum metrology protocol that optimises the large data information gain of a single parameter used in chapter 5.

The final section of this chapter introduces the concepts of quantum enhanced measurements for a single parameter used in chapter 5. Then, it introduces quantum sensing networks and quantum enhanced measurements for functions of parameters giving initial results helpful for optimising the information gain in network scenarios used in chapter 6.

The final step of quantum metrology, the data analysis for parameter estimation is discussed in detail along with numerical methods of creating such data and analysing

limited data information gain in chapter 3.

2.1 Notation and quantum state preparation

In quantum information the Heisenberg picture of quantum mechanics is often used. From this perspective states are time-independent and their operators, such as observables, are time-dependent. This thesis uses Dirac notation and the matrix form for quantum states and operations. Any isolated physical system can be associated to a complex vector space or Hilbert space known as the state space. A pure quantum state is denoted by such a column vector. The Hilbert space denotes possible quantum numbers for a system such as energy level or polarisation. In Dirac notation, kets such as $|\psi\rangle$ denote the quantum state vector describing the state ψ in the relevant Hilbert space. Writing the K basis vectors of the Hilbert space as $|k\rangle$, then a pure quantum state is written in Dirac notation as $|\psi\rangle = \sum_{k=1}^{K} \alpha_k |k\rangle$, where $\alpha_k \in \mathbb{C}$ and $\sum_{k=1}^{K} |\alpha_k|^2 = 1$. Bras, the hermitian conjugate (complex conjugate of the transpose) of kets, $\langle\psi| = (|\psi\rangle)^\dagger = ((|\psi\rangle)^*)^T$ are row vectors. The inner product of two vectors $|\phi\rangle = \sum_{k=1}^{K} \phi_k \hat{k}$ and $|\psi\rangle = \sum_{k=1}^{K} \psi_k |k\rangle$ is $\langle\phi|\psi\rangle = \langle\phi|\psi\rangle = \sum_{k}^{K} = \phi_k^* \psi_k$. In particular $\langle\psi|\psi\rangle = 1$.

A quantum state evolves when it is acted on by an observable changing its state. This evolution is described by the Shrödinger equation, $i\hbar\frac{d|\psi\rangle}{dt} = \hat{H}|\psi\rangle$ where $\hat{H}$ is the Hamiltonian operator. Operators are square matrices specific to the Hilbert space and are used to describe the evolution of quantum states when interacting with observables. All observables have hermitian operators, $\hat{O} = \hat{O}^\dagger = (\hat{O}^*)^T$; they are their own conjugate transpose. This means that their eigenvalues are real ergo observable. The $\hat{}$ notation denotes an operator. A pure quantum state evolves when acted on by an operator, $|\psi_{\text{final}}\rangle = \hat{O}|\psi_{\text{initial}}\rangle$. A special operator is the identity $I = \text{diagonal}(1, ..., 1)$, often written without the $\hat{}$ notation, which does not change a quantum state.

2.1.1 Qubits

The most fundamental model for the state of a single quantum in quantum information is the qubit, a two level quantum system. The quantum numbers could represent a variety of states such as charge, energy level, spin, polarisation and number. The qubit Hilbert space used in quantum information is given by equation (1.1) where the eigenstates have been re-parameterised into the computational basis with eigenstates written as $\{|0\rangle, |1\rangle\}$. The eigenvalues 0 and 1 correspond to the binary classical bits rather than the physical realisation of the quantum system making all calculations applicable to all qubit states

regardless of the original eigenvalues or their order in the equations. A pure qubit state has two degrees of freedom that can be written in as spherical coordinates

$$|\psi_{\mathcal{P}}\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\phi}\,|1\rangle\,. \tag{2.1}$$

The spherical parameterisation models a pure state qubit having state somewhere on the surface of a sphere that uses $\{r = 1, \theta, \phi\}$, $\theta \in [0, \pi]$, $\phi \in [0, 2\pi)$ as the standard spherical coordinates with $|0\rangle$ and $|1\rangle$ as the north and south poles respectively. Pure states in higher dimensional systems with more than two Hilbert state spaces are modelled on higher dimensional hyperspheres with the degrees of freedom similarly aligning with the hyperspherical polar coordinates.

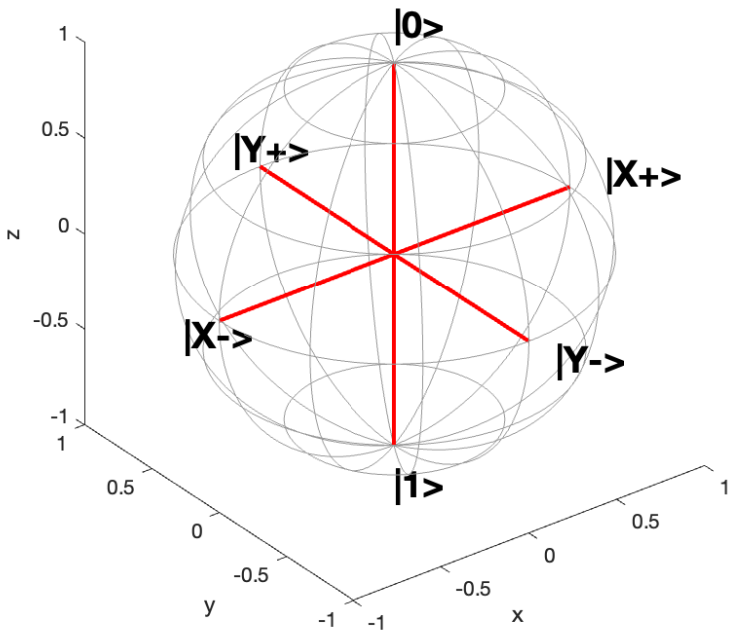

Figure 2.1: The Bloch sphere and the Pauli eigenstates.

In addition to recreating classical logic gates, a quantum system has additional logic gates available due to the topology of the Bloch sphere. Classical gates transform binary bits whereas quantum gates can move the state of qubits anywhere around the Bloch sphere. This allows for quantum computers to run a variety of algorithms allowing them to solve some problems much faster than classical computers.

In this thesis four of these quantum logic gates and their eigenfunctions are used a lot. They are shown in table 2.1. For a linear operator, such as a quantum logic gate, $\hat{O}$,

Operator	Matrix	eigenfunction 1	eigenvalue 1	eigenfunction 2	eigenvalue 2
Pauli-X (X)	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$	$\|X+\rangle = \frac{1}{\sqrt{2}}\binom{1}{1}$	+1	$\|X-\rangle = \frac{1}{\sqrt{2}}\binom{1}{-1}$	-1
Pauli-Y (Y)	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$	$\|Y+\rangle = \frac{1}{\sqrt{2}}\binom{1}{i}$	+1	$\|Y-\rangle = \frac{1}{\sqrt{2}}\binom{1}{-i}$	-1
Pauli-Z (Z)	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$	$\|Z+\rangle = \binom{1}{0}$	+1	$\|Z-\rangle = \binom{0}{1}$	-1
Phase (P(ϕ))	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\phi} \end{bmatrix}$	$\|Z+\rangle = \binom{1}{0}$	+1	$\|Z-\rangle = \binom{0}{1}$	$e^{i\phi}$

Table 2.1: Important single qubit gates, eigenfunctions and eigenvectors for quantum metrology and quantum cryptography in a standard Hilbert space.

eigenfunctions, $f = |\psi\rangle$, and their eigenvalues, $\lambda \in \mathbb{C}$ are defined as

$$\hat{O}f = \lambda f. \tag{2.2}$$

The Pauli matrices form three quantum logic gates. Their eigenfunctions will be used for initial states of qubits in some of the protocols discussed in this thesis. The Phase gate is used to apply phase parameters to states that will be measured in an effort to estimate them.

2.1.2 Mixed state qubits

A ket is used to represent a pure quantum state. A single quantum system can be in a superposition of different pure states; if there is a probability p_k of $|\psi\rangle$ being in $K > 1$ different pure states $|\psi_k\rangle$ then it is a mixed state. The density operator $\hat{\rho} = \sum_{k=1}^{K} p_k |\psi_k\rangle \langle\psi_k|$, often written without the hat as ρ, is an operator with position terms able to describe both mixed and pure states. If a quantum system is in state ρ_k with probability p_k then for the system $\rho = \sum_k p_k \rho_k$. The trace of a matrix is the sum of its diagonal elements. In particular $Tr(\rho) = 1$. A quantum state is pure if the square of its density matrix is equal to the density matrix $\rho^2 = \rho$ or equivalently, $Tr(\rho^2) = Tr(\rho) = 1$.

Unitary operators are such that $\hat{U}^\dagger \hat{U} = I$. The evolution of a closed quantum system is described by a unitary transformation changing the density operator

$$\rho' = \hat{U}\rho\hat{U}^\dagger. \tag{2.3}$$

In the presence of noise sources a qubit could be transformed to another state. For

instance, symmetric phase noise could be due to the uncertainty $\delta\phi$ for a qubit described by equation (2.1). Such noise could be represented as a qubit having a probability of being in a random state rather than a single specific pure state. This, and some other forms of noise, turn a qubit into an mixed state. The mixed state qubit model that is most relevant to this thesis is one where the qubit has a probability $\mathcal{P}$ of being in the pure state and $\mathcal{R}$ of having been replaced by a random state,

$$|\psi_m\rangle = \begin{cases} |\psi_{\mathcal{P}}\rangle & \text{with probability} \quad \mathcal{P} \\ |\mathcal{R}\rangle & \text{with probability} \quad \mathcal{R}\text{=1-}\mathcal{P} \end{cases} \tag{2.4}$$

where $|\mathcal{R}\rangle$ is a random qubit, equally weighted over all possible pure qubit states and $|\psi_{\mathcal{P}}\rangle$ is the pure qubit state given in equation (2.1). The density operator of such a mixed qubit state is

$$\rho = \mathcal{P}\rho_{\mathcal{P}} + \mathcal{R}\rho_{\mathcal{R}}. \tag{2.5}$$

This is expressed in terms of the density operator of a pure qubit

$$\rho_{\mathcal{P}} = \begin{pmatrix} \cos^2(\theta/2) & \frac{1}{2}\sin(\theta)e^{-i\phi} \\ \frac{1}{2}\sin(\theta)e^{+i\phi} & \sin^2(\theta/2). \end{pmatrix} \tag{2.6}$$

Any two states on opposite sides of the Bloch sphere have coordinates $\{\theta, \phi\}$ and $\{\pi - \theta, \phi + \pi\}$ (antipodal points on the Bloch sphere), therefore the density matrix when there is an equal chance of each state is

$$\begin{aligned} &\frac{1}{2}\rho(\{\theta,\phi\}) + \frac{1}{2}\rho(\{\pi-\theta,\phi+\pi\}) \\ &\quad = \frac{1}{2}\begin{pmatrix} \cos^2(\theta/2) + \cos^2((\pi-\theta)/2) & \frac{1}{2}\sin(\theta)e^{-i\phi} + \frac{1}{2}\sin(\pi-\theta)e^{-i(\phi+\pi)} \\ \frac{1}{2}\sin(\theta)e^{+i\phi} + \frac{1}{2}\sin(\pi-\theta)e^{+i(\phi+\pi)} & \sin^2(\theta/2) + \sin^2((\pi-\theta)/2) \end{pmatrix} \\ &\quad = \frac{1}{2}\begin{pmatrix} \cos^2(\theta/2) + \sin^2(\theta/2) & \frac{1}{2}\sin(\theta)e^{-i\phi} + \frac{1}{2}\sin(\theta)\left(-e^{-i\phi}\right) \\ \frac{1}{2}\sin(\theta)e^{+i\phi} + \frac{1}{2}\sin(\theta)\left(-e^{+i\phi}\right) & \sin^2(\theta/2) + \cos^2(\theta/2) \end{pmatrix} = \frac{1}{2}I \end{aligned} \tag{2.7}$$

The random qubit could be in any state around the Bloch sphere with equal probability. As each state can be paired with one on the opposite side of the sphere and each pair has the same density matrix, the average density matrix, that of a random state is the same as any pair on opposite sides of the sphere

$$\rho_{\mathcal{R}} = \frac{1}{2}I. \tag{2.8}$$

Restricting this to any great circle (circular intersection of a sphere and a plane passing through the sphere's centre point) of the Bloch the sphere provides the same result. A

change in coordinate system (and Hilbert space) can re-parameterised for any great circle to the equatorial plane

$$|\psi_{eq}\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\ e^{i\phi}\end{pmatrix}. \tag{2.9}$$

A random state restricted to any great circle averages to the same density function, $\rho_{\mathcal{R}} = \frac{1}{2}I$, as on the entire sphere. Therefore, the density matrix of a mixed state qubit is

$$\rho = \mathcal{P}\rho_{\mathcal{P}} + \frac{\mathcal{R}}{2}I = \begin{pmatrix}\mathcal{P}\cos^2(\theta/2) + \frac{\mathcal{R}}{2} & \frac{\mathcal{P}}{2}\sin(\theta)e^{-i\phi}\\ \frac{\mathcal{P}}{2}\sin(\theta)e^{+i\phi} & \mathcal{P}\sin^2(\theta/2) + \frac{\mathcal{R}}{2}\end{pmatrix} \tag{2.10}$$

Some noise sources can be asymmetric. In these cases it can be useful to break the density matrix into three parts, the noiseless pure state, $\rho_{\mathcal{P}}$, with probability $\mathcal{P}$, the biased pure state due to asymmetric noise, $\rho_{\mathcal{B}}$, with probability $\mathcal{B}$ and the random state due to symmetric noise, $\frac{1}{2}I$, with probability $\mathcal{R} = 1 - \mathcal{P} - \mathcal{B}$,

$$\rho = \mathcal{P}\rho_{\mathcal{P}} + \mathcal{B}\rho_{\mathcal{B}} + \frac{1-\mathcal{P}-\mathcal{B}}{2}I. \tag{2.11}$$

2.1.3 Composite systems

Composite systems are made from multiple distinct physical systems. These can be constructed from multiple Hilbert spaces by taking the tensor product of the different Hilbert spaces. For instance, the joint system for $|\psi_k\rangle$ with $k = 1, 2, ...K$ is $|\psi_1\rangle_1 \otimes |\psi_2\rangle_2 \otimes ... \otimes |\psi_K\rangle_K$. When there is no ambiguity over the Hilbert spaces in question this is written in the form $|\psi_1\psi_2...\psi_K\rangle$. When they describe or act over multiple Hilbert spaces, $|\psi\rangle$ and $\hat{O}$ become higher dimensional objects.

Entanglement describes composite systems where the state of multiple particles depend on each other. When particles are entangled, the measurement of any of subset of the particles affects the state of the other particles. For instance, two qubits can be entangled into any of the Bell states

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle + |11\rangle\right) \tag{2.12}$$

$$|\Phi^-\rangle = \frac{1}{\sqrt{2}}\left(|00\rangle - |11\rangle\right) \tag{2.13}$$

$$|\Psi^+\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \tag{2.14}$$

$$|\Psi^-\rangle = \frac{1}{\sqrt{2}}\left(|01\rangle + |10\rangle\right) \tag{2.15}$$

where $|xy\rangle = |x\rangle_X \otimes |y\rangle_Y$ notation is used due to it being clear what subsystems are being concatenated. Furthermore, a quantum state known as the the generalised GHZ state

made of B qubits is

$$|GHZ, B\rangle = \frac{|0\rangle^{\otimes B} + |1\rangle^{\otimes B}}{\sqrt{2}}. \tag{2.16}$$

The generalised GHZ state can be further generalised by allowing for the $|0\rangle_b$ and $|1\rangle_b$ to switch places for any b and treating it like a qubit in the Bloch sphere,

$$|\Psi\rangle = \cos(\theta/2) \prod_{b=1}^{B} |\alpha\rangle_b + \sin(\theta/2) e^{i\phi} \prod_{b=1}^{B} |\beta\rangle_b \,, \tag{2.17}$$

where $|\alpha\rangle_b, |\beta\rangle_b \in \{|0\rangle, |1\rangle\} \forall b$ and $|\alpha\rangle_b \neq |\beta\rangle_b \, \forall b$. The effect of noise on a pure entangled system of qubits such as this is identical to that of a single qubit where $\prod_{b=1}^{B} |\alpha\rangle_b$ is treated as $|0\rangle$ and $\prod_{b=1}^{B} |\beta\rangle_b$ as $|1\rangle$. A generalisation of the GHZ state restricted to the equatorial plane of the Bloch sphere in the Hilbert space of the entire entangled state of B qubits is particularly useful to chapter 6,

$$|\chi_B\rangle = \frac{|0\rangle^{\otimes B} + e^{i\chi} |1\rangle^{\otimes B}}{\sqrt{2}}, \tag{2.18}$$

where $|\alpha\rangle_b$ and $|\beta\rangle_b$ are re-parameterised as $|0\rangle_b$ and $|1\rangle_b$ respectively for all b corresponding to classical binary 0 and 1 bits instead of quantum numbers and χ represents the phase in the B dimensional Bloch hypersphere.

The Bell and GHZ states are all pure entangled states. Their subsystems are mixed states. The partial trace is used to split a density operator ρ^{AB} between two sets of Hilbert spaces A and B,

$$\rho^A = tr_B(\rho^{AB}), \qquad tr_B(|a_1\rangle \langle a_2| \otimes |b_1\rangle \langle b_2|) = |a_1\rangle \langle a_2| \, tr(|b_1\rangle \langle b_2|). \tag{2.19}$$

If the reduced density matrix is a pure state then the composite system is separable. If it is a mixed state then the composite system may be but is not necessarily entangled. All of the subsystems of the pure entangled states shown here are mixed with reduced density operator $I/2$, like a random qubit state.

Entanglement is not Binary. The Bell and GHZ-like states shown here are fully entangled. This thesis only uses fully entangled and fully separable states so, it doesn't discuss measures of the amount of entanglement. An example a partially entangled state is a mix of separable $|X+\rangle$ qubits, $|X+\rangle |X+\rangle$, with probability p and the Φ^+ entangled Bell state with probability $(1-p)$. Writing the two dimensional Hilbert space in matrix form as $(|00\rangle, |01\rangle, |10\rangle, |11\rangle)^T$ the density matrix for each pure state can be written

$$\rho(|X+\rangle |X+\rangle) = \frac{1}{4} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \qquad \rho(|\Phi^+\rangle) = \frac{1}{2} \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}. \tag{2.20}$$

Both are pure states with $\rho^2 = \rho$. However their mix,

$$\rho(\text{mixed}) = \frac{1}{4}\begin{pmatrix} 2-p & p & p & p \\ p & p & p & p \\ p & p & p & p \\ p & p & p & 2-p \end{pmatrix}, \tag{2.21}$$

is not pure,

$$\rho(\text{mixed})^2 = \frac{1}{16}\begin{pmatrix} 4-p^2+p^4 & 2p(1+p) & 2p(1+p) & 4p \\ 2p(1+p) & p & p & 2p(1+p) \\ 2p(1+p) & p & p & 2p(1+p) \\ 4p & 2p(1+p) & 2p(1+p) & 4-p^2+p^4 \end{pmatrix},$$

$$\rho(\text{mixed})^2 \neq \rho(\text{mixed}) \ \forall p \neq \{0,1\}. \tag{2.22}$$

2.2 Parameter interactions and quantum Fisher information

The quantum metrology present in this thesis is mostly phase metrology where the phase operator $P(\phi)$ shown in table 2.1 is used to evolve the Pauli-X, Y and Z eigenstates shown in the same table and GHZ states of the form shown in equation (2.18).

2.2.1 Phase encoding on qubits

The phase operator performs the following transformations on the single qubit eigenstates of table 2.1

$$P(\phi)\,|X\pm\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm e^{i\phi} \end{pmatrix} \qquad P(\phi)\,|Y\pm\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ \pm ie^{i\phi} \end{pmatrix} \tag{2.23}$$

$$P(\phi)\,|Z+\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad P(\phi)\,|Z-\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{2.24}$$

The phase gate does not change the state of the Z states, they are called phase insensitive. The X and Y states are evolved by the phase gate so they are called phase sensitive. Quantum states in the equatorial plane of the Bloch sphere can be described using the formalism

$$|\chi\rangle = |\chi_1\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\chi}\,|1\rangle\right), \tag{2.25}$$

where $\chi = 0, \pi$ correspond to the $|X\pm\rangle$ states respectively and $\chi = \pi/2, 3\pi/2$ correspond to the $|Y\pm\rangle$ states respectively. From now on χ will be used to represent the initial state phase of some separable or entangled qubit state in the equatorial plane and ϕ will be the

phase encoded by phase gates $P(\phi)$ onto those states. States of this form evolve with the phase gate,

$$P(\phi)\left|\chi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{i(\chi+\phi)}\left|1\right\rangle\right). \tag{2.26}$$

Applying multiple phase gates consecutively to a Hilbert space is equivalent to applying one phase gate for the sum of the phases,

$$\prod_{k=1}^{K} P(\phi_k)\left|\chi\right\rangle = P\left(\sum_{k=1}^{K}\phi_k\right)\left|\chi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{i(\chi+\sum_k \phi_k)}\left|1\right\rangle\right). \tag{2.27}$$

Multiple applications of the phase gate applies the same phase multiple times,

$$P(\phi)^{\otimes N}\left|\chi\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle + e^{i(\chi+N\phi)}\left|1\right\rangle\right). \tag{2.28}$$

In noisy scenarios the actual phase true of each probe $\tilde{\phi}_k$ can vary between each state that is encoded or be different from phase that should be measured. When this is asymmetric the expectation value is $\langle\tilde{\phi}\rangle = \frac{1}{K}\sum_{k=1}^{K}\tilde{\phi}_k \neq \phi$ it causes bias $\phi \to \phi + \delta\phi$. When it is symmetric, $\langle\tilde{\phi}\rangle = \phi, \exists\tilde{\phi}_k \neq \phi$, this is equivalent to the noisy phase operator transforming the pure qubit into a mixed qubit with non-zero probability of being the pure encoded qubit and non-zero probability of being a random qubit as shown by the density operator of equation (2.10). Generally, phase noise can cause both symmetric and asymmetric effects.

2.2.2 Composite systems and multiple phase encoding

Separable composite systems have the phase operator act on the individual Hilbert spaces. Entangled composite systems can perform a greater variety of parameter interactions. In particular, if the entangled qubits such as the equatorial plane restricted generalisation of the GHZ state in equation (2.18) is interacted on by phase gates, $P_b(\phi_b)$, then the net effect of the phase gates is a single gate acting on the entangled state with the sum of those parameters,

$$\prod_{b=1}^{B} P_b(\phi_b)\left|\chi_N\right\rangle = P_{\text{all b}}\left(\sum_{b=1}^{B}\phi_b\right)\left|\chi_N\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle^{\otimes N} + e^{i(\chi+\sum_b \phi_b)}\left|1\right\rangle^{\otimes N}\right), \tag{2.29}$$

giving the same result regardless of which particle(s) the P_b act on making it a single phase gate for the entire entangled state. This is useful when calculating functions of parameters where $\sum_b \nu_b\phi_b$ for $\nu_b \in \mathbb{R}\forall b$ can be encoded. A special case is when all of the ϕ_b are the same,

$$\prod_{b=1}^{B} P_b(\phi)\left|\chi_N\right\rangle = P_{\text{all b}}\left(B\phi\right)\left|\chi_N\right\rangle = \frac{1}{\sqrt{2}}\left(\left|0\right\rangle^{\otimes N} + e^{i(\chi+B\phi_b)}\left|1\right\rangle^{\otimes N}\right), \tag{2.30}$$

the estimation is of a multiple of the single parameter.

By having them act on any selection of the particles of an entangled state, a phase gate changes the state of the entire entangled state. For instance, if $N = 1$ and $B > 1$, a single qubit can be encoded with multiple phases or the same phase multiple times. This is used in chapter 5 for quantum enhancement. If $B = 1$ and $N > 1$ an entangled state can be encoded with a single phase. If $B = N$ this could represent an entangled state being distributed to be encoded with remote phases for quantum enhanced parameter estimation as in chapter 6.

2.2.3 Quantum Fisher information

The maximum amount of information that could be extracted from a quantum state is quantified using the quantum Fisher information matrix. It has the following properties [36]

1. $\mathcal{F}$ is real symmetric, $\mathcal{F}_{ab} = \mathcal{F}_{ba} \in \mathbb{R}$
2. $\mathcal{F}$ is positive semi-definite, $\mathcal{F} \geq 0$. If $\mathcal{F} > 0$ then $[\mathcal{F}^{-1}]_{aa} \geq 1/\mathcal{F}_{aa}$ for any a.
3. $\mathcal{F}$ is independent of a unitary operation acting on ρ but not the parameters, $\mathcal{F}(\rho) = \mathcal{F}(U\rho U^\dagger)$ for a $\vec{x}$-independent unitary operation U.
4. Conjugate systems, if $\rho = \otimes_k \rho_k(\vec{x})$, then $\mathcal{F}(\rho) = \sum_k \mathcal{F}(\rho_k)$.
5. Multiple systems, $\rho = \oplus_k \mu_k \rho_k(\vec{x})$ with μ_k a $\vec{x}$-independent weight, then $\mathcal{F}(\rho) = \sum_k \mu_k \mathcal{F}(\rho_k)$.
6. Convexity, $\mathcal{F}(p\rho_1 + (1-p)\rho_2) \leq p\mathcal{F}(\rho_1) + (1-p)\mathcal{F}(\rho_2)$ for $p \in [0, 1]$.
7. Mapping, if $\mathcal{F}$ is monotonic under a completely positive and trace preserving map Φ, $\mathcal{F}(\Phi(\rho)) \leq \mathcal{F}(\rho)$.
8. Basis change, if $\vec{y}$ is a function of $\vec{x}$, then $\mathcal{F}(\rho(\vec{c})) = J^T \mathcal{F}(\rho(\vec{y}))J$, where J is the Jacobian matrix, $J_{jk} = \partial y_j / \partial x_k$.

The general form of the quantum Fisher information matrix is

$$\mathcal{F}_{ab} := \frac{1}{2} Tr\left(\rho\{L_a, L_b\}\right) \tag{2.31}$$

where L_a and L_b are the symmetric logarithmic derivative for the parameters x_a and x_b determined by the equation,

$$\partial_a \rho = \frac{1}{2}\left(\rho L_a + L_a \rho\right). \tag{2.32}$$

For pure states the entries to the matrix are

$$\mathcal{F}_{ab} = 4Re\left(\langle\partial_a\psi|\partial_b\psi\rangle - \langle\partial_a\psi|\psi\rangle\langle\psi|\partial_b\psi\rangle\right). \tag{2.33}$$

The quantum Fisher information of the pure states in equations (2.1) and (2.17) are

$$\mathcal{F}_{\theta\theta} = 1 \qquad \mathcal{F}_{\phi\phi} = \sin^2(\theta) \qquad \mathcal{F}_{\theta\phi} = 0. \tag{2.34}$$

This indicates that the information gain of ϕ is dependent on the value of θ with an optimal information gain when $\theta = \pi/2$, the state being $\frac{1}{\sqrt{2}}(|0\rangle + e^{i\phi}|1\rangle)$ like those shown in table 2.1 and equations (2.12-2.17). This also indicates that there is no single measurement that can give information about θ and ϕ simultaneously, though it is possible to do so with multiple copies of a state and different measurements.

These results also apply to entangled qubits states of the form given in equation (2.17) by by choosing a computation basis such that $\prod_{b=1}^{B}|\alpha\rangle_b$ as $|0\rangle$ and $\prod_{b=1}^{B}|\beta\rangle_b$ as $|1\rangle$. This thesis is a study of the metrology of phase parameters on well defined initial states. Convention dictates that phase parameters to be estimated are labelled ϕ with estimates $\hat{\phi}$. So far, ϕ has been treated as the phase an arbitrary state in the Bloch sphere. To differentiate the initial quantum state and the phase to be estimated, from now on initial states in the equatorial plane of the Bloch sphere will be labelled $|\chi_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + e^{i\chi}|1\rangle^{\otimes N}\right)$ where χ is a known value. Then, a phase gate will be applied $P(\phi)|\chi_N\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle^{\otimes N} + e^{i(\chi+\phi)}|1\rangle^{\otimes N}\right)$ where ϕ is unknown. By the eighth property of the quantum Fisher information changing $\phi \to \chi + \phi$ does not the results in equations (2.34) and (2.36). By the same rule $\phi \to B\phi$ changes $\mathcal{F}_{\phi\phi} = B^2\sin^2(\theta)$.

The quantum Cramér-Rao bound is used as a measure of the covariance of parameter estimates

$$(\delta a)(\delta b) \geq \frac{[\mathcal{F}^{-1}]_{ab}}{\mu} \geq \frac{1}{\mu\mathcal{F}_{ab}} \tag{2.35}$$

where μ is the number of independent measurements and δa is a measure of the dispersion of the parameter a. For a single quantum state $\mu = 1$ due to the destructive effect of quantum measurement but, $\mu > 1$ can be achieved with multiple copies of parameters.

The Fisher information matrix for qubits is diagonal. Therefore, $[\mathcal{F}^{-}1]_{ab} = \mathcal{F}_{ab}^{-1}$ and the Cramér-Rao bounds for pure qubits defined by equation (2.1) are

$$\delta\phi \geq \frac{1}{\sqrt{\mu}} \qquad \delta\theta \geq \frac{1}{|\sin(\theta)|\sqrt{\mu}}. \tag{2.36}$$

2.3 Measurements and classical Fisher information

2.3.1 Quantum measurement

Quantum measurements are described by a collection of measurement operators $\{\hat{M}_m\}$. They satisfy the completeness equation,

$$\sum_m M_m^\dagger M_m = I, \tag{2.37}$$

which is such that it is possible to reach all possible directions of the relevant Hilbert space. If the quantum system is in a state $|\psi\rangle$ immediately before measurement, the probability of each measurement result, m, occuring is

$$P(m) = \langle\psi| M_m^\dagger M_m |\psi\rangle \tag{2.38}$$

and the state after measurement is

$$\frac{M_m |\psi\rangle}{\sqrt{\langle\psi| M_m^\dagger M_m |\psi\rangle}}. \tag{2.39}$$

Often, the act of measurement destroys the particle that is in the quantum state. However, the state itself is not necessarily destroyed. For example, when measuring a single photon with a photomultiplier tube, a photocathode converts the photon into an electron. If the measurement was for energy levels then, the energy of the produced electron is dependent on that of the incident photon. However, once the tube has converted this to a classical signal, the difference is not measurable.

When measuring a qubit the measurement operator acts over the same Hilbert space

$$M_m = \begin{pmatrix} \cos^2(\vartheta/2) & \frac{1}{2}\sin(\vartheta)e^{-i\varphi} \\ \frac{1}{2}\sin(\vartheta)e^{+i\varphi} & \sin^2(\vartheta/2) \end{pmatrix}, \tag{2.40}$$

resembling the density operator of a pure state qubit. This is called a projective measurement; it projects the quantum state into a Hilbert space with eigenstates M_+ and M_-, on opposite sides of the Bloch sphere (two antipodal points). The probability of a each result dependent on how close the quantum state is to the each eigenstate of that Hilbert space.

A set of measurement operators $\{M_+(\vartheta,\varphi), M_-(\pi/2 - \vartheta, \varphi + \pi)\}$ satisfies the completeness equation. They are equivalent to projection into the states $\langle M_+| = (\cos(\vartheta/2), \sin(\vartheta/2)e^{-i\varphi})$ and $\langle M_-| = (\sin(\vartheta/2), \cos(\vartheta/2)e^{-i(\varphi+\pi)})$. So, the measurement

probabilities can be calculated $P(\pm) = |\langle M_\pm | P(\phi)\psi\rangle|^2$. Therefore the probability of each result for phase encoded pure qubit states,

$$P(\phi)\,|\psi(\theta,\chi)\rangle = \cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i(\chi+\phi)}\,|1\rangle), \tag{2.41}$$

is,

$$\begin{aligned}
P(+|\phi, \text{pure qubit}) &= \left|(\cos(\vartheta/2), \sin(\vartheta/2)e^{-i\varphi}\begin{pmatrix}\cos(\theta/2)\\ \sin(\theta/2)e^{i(\chi+\phi)}\end{pmatrix}\right|^2 \\
&= \left|\cos(\vartheta/2)\cos(\theta/2) + \sin(\vartheta/2)\sin(\theta/2)e^{i(\chi+\phi-\varphi)}\right|^2 \\
&= \cos^2(\vartheta/2)\cos^2(\theta/2) + \sin^2(\vartheta/2)\sin^2(\theta/2) \\
&\quad + \cos(\vartheta/2)\cos(\theta/2)\sin(\vartheta/2)\sin(\theta/2)\left[e^{i(\chi+\phi-\varphi)} + e^{-i(\chi+\phi-\varphi)}\right] \\
&= \frac{1}{2}\left(1 + \cos(\theta)\cos(\vartheta) + \sin(\theta)\sin(\vartheta)\cos(\chi+\phi-\varphi)\right), \qquad (2.42) \\
P(-|\phi, \text{pure qubit}) &= \left|(\sin(\vartheta/2), \cos(\vartheta/2)e^{-i(\varphi+\pi)}\begin{pmatrix}\cos(\theta/2)\\ \sin(\theta/2)e^{i(\chi+\phi)}\end{pmatrix}\right|^2 \\
&= \left|\sin(\vartheta/2)\cos(\theta/2) + \cos(\vartheta/2)\sin(\theta/2)e^{i(\chi+\phi-\varphi)}\right|^2 \\
&= \sin^2(\vartheta/2)\cos^2(\theta/2) + \cos^2(\vartheta/2)\sin^2(\theta/2) \\
&\quad + \sin(\vartheta/2)\cos(\theta/2)\cos(\vartheta/2)\sin(\theta/2)\left[e^{i(\chi+\phi-\varphi)} + e^{-i(\chi+\phi-\varphi)}\right] \\
&= \frac{1}{2}\left(1 - \cos(\theta)\cos(\vartheta) + \sin(\theta)\sin(\vartheta)\cos(\chi+\phi-\varphi-\pi)\right), \\
&= \frac{1}{2}\left(1 - \cos(\theta)\cos(\vartheta) - \sin(\theta)\sin(\vartheta)\cos(\chi+\phi-\varphi)\right), \qquad (2.43)
\end{aligned}$$

Using only antipodal pairs of measurement operators on qubits is not a requirement. Any set of equally probable measurements spread evenly around one (minimum of two) or both (minimum of three) dimensions of the Bloch sphere suffice and many more could be devised.

When considering mixed states, it is appropriate to use the density operator to calculate the measurement probabilities. For a collection of quantum measurement operators $\{M_m\}$ that could apply to one or multiple Hilbert spaces and satisfy the completeness equation (2.37), the probability of measurement result m for mixed and pure states is

$$P(m) = tr(M_m^\dagger M_m \rho) \tag{2.44}$$

and the density matrix after measurement is

$$\frac{M_m \rho M_m^\dagger}{tr(M_m^\dagger M_m \rho)} \tag{2.45}$$

When the initial state is a mixed qubit, there is a probability $P(\text{pure qubit}) = \mathcal{P} \in [0,1]$ that it acts like a pure qubit and $P(\text{random qubit}) = \mathcal{R} = 1 - \mathcal{P}$ that it acts like a random

qubit. A random initial state is equally likely to be any pure initial state so, the result probabilities are the same as that of two states on opposite sides of the Bloch sphere equally weighted

$$P(\pm|\mathcal{R}) = \frac{1}{2}P(\pm|\theta,\phi) + \frac{1}{2}P(\pm|\pi-\theta,\phi+\pi) = \frac{1}{2}. \tag{2.46}$$

By equation (2.5) the probability of measurement results can be calculated by weighting the probability for pure and random states by their occurrence probabilities,

$$P(\pm) = P(\pm|\mathcal{P})\mathcal{P} + P(\pm|\mathcal{R})\mathcal{R}. \tag{2.47}$$

Therefore, the measurement probabilities for mixed states are.

$$\begin{aligned} P(+) &= \frac{1}{2}\left(1 + \mathcal{P}\cos(\theta)\cos(\vartheta) + \mathcal{P}\sin(\theta)\sin(\vartheta)\cos(\chi+\phi-\varphi)\right), \\ P(-) &= \frac{1}{2}\left(1 - \mathcal{P}\cos(\theta)\cos(\vartheta) - \mathcal{P}\sin(\theta)\sin(\vartheta)\cos(\chi+\phi-\varphi)\right). \end{aligned} \tag{2.48}$$

Restricting measurements to the equatorial plane of the Bloch sphere, $\vartheta = \pi/2$,

$$\begin{aligned} P(+) &= \frac{1}{2}\left(1 + \mathcal{P}\sin(\theta)\cos(\chi+\phi-\varphi)\right), \\ P(-) &= \frac{1}{2}\left(1 - \mathcal{P}\sin(\theta)\cos(\chi+\phi-\varphi)\right). \end{aligned} \tag{2.49}$$

If both initial pure states and measurements are restricted to the equatorial plane of the Bloch sphere, $\theta = \vartheta = \pi/2$, this becomes

$$\begin{aligned} P(+) &= \frac{1}{2}\left(1 + \mathcal{P}\cos(\chi+\phi-\varphi)\right) \\ P(-) &= \frac{1}{2}\left(1 - \mathcal{P}\cos(\chi+\phi-\varphi)\right) \end{aligned} \tag{2.50}$$

which resembles a Cardioid probability distribution [64] on a sphere. Initial pure states are transformed into mixed states when the probability of a state being affected by some noise source is non-zero. As discussed previously, phase noise can be asymmetric causing a shift in the estimated phase $\phi \to \phi + \delta\phi$ or symmetric, decreasing $\mathcal{P}$.

Other sources of noise that have some non-zero probability of shifting the state out of the equatorial plane of the Bloch sphere would also decrease the value of $\mathcal{P}$ in this equation. Analysing equation (2.49), and decomposing a pure state into its equatorial plane part, $\theta = \pi/2$ with result probabilities given by equation (2.50) and the part at the north or south pole $\theta =\in \{0,\pi\}$ with probabilities $P(\pm) = 1/2$ it is evident that such noise would have a similar effect as symmetric phase noise, reducing $\mathcal{P}$.

For entangled qubits the measurement operators are the same as those used on pure state qubits applied over the entire entangeld Hilbert space. A single measurement operator can be applied to the entire entangled state; the measurement probability in these

cases is the same as the single qubit states. If the total measurement is made up from many separate measurements of the particles of a fully entangled state such as those in equations (2.12) to (2.18), each individual measurement is on a random mixed state and gives $m_j \in \{-1, +1\}$ results with a probability 1/2. Information about the entangled state can only be extracted from knowing the measurements and the results for all of the particles. The net result for the ensemble is $m_{\text{net}} = \prod_m m_j$ and the net measurement would be $M_{\text{net}} = \prod_j M_j$ acting like a single measurement on the entire state.

2.3.2 Classical Fisher information

The classical Fisher information is a way of measuring the amount of information that an observable random variable carries about an unknown parameter of a distribution that models that variable. In multiparameter scenarios the inverse of the classical Fisher information matrix is used is used to calculate the covariance matrices associated with asymptotic maximum likelihood estimates. For a probability distribution $\vec{P}$ with $p(j|\vec{\phi})$ as the conditional probability of the outcome j for the variables $\vec{\phi}$ the most appropriate form of the classical Fisher information matrix terms is the following,

$$\mathcal{I}_{ab}(\vec{\phi}) = \sum_j \frac{(\partial_a P(j|\vec{\phi}))(\partial_b P(j|\vec{\phi}))}{P(j|\vec{\phi})}. \tag{2.51}$$

It is bounded from above by the quantum Fisher information $\mathcal{I}_{ab} \leq \mathcal{F}_{ab}$ with equality indicating that the measurement is optimal for extracting information from the quantum state. It shares the same properties listed for the quantum Fisher information. An important relationship of the Fisher information matrix is the classical Cramér-Rao bound,

$$(\delta a)(\delta b) \geq \frac{[\mathcal{I}^{-1}]_{ab}}{\mu} \geq \frac{1}{\mu \mathcal{I}_{ab}}. \tag{2.52}$$

Another interesting property of the classical Fisher information is that under certain conditions the maximum likelihood estimator is distributed with variance proportional to the inverse of the classical Fisher information [65].

The majority of the work in this thesis takes place in the equatorial plane of the Bloch sphere, where $\theta = \vartheta = \pi/2$ because it gives the maximal Fisher information for phase measurements. In these scenarios, the classical Fisher information of the state $P(\phi)\,|\chi\rangle$ measured in the basis $\{\vartheta = \pi/2, \varphi\}$ is single parameter,

$$\mathcal{I}_\phi = \frac{\mathcal{P}^2 \sin^2(\chi + \phi - \varphi)}{1 - \mathcal{P}^2 \cos^2(\chi + \phi - \varphi)}. \tag{2.53}$$

This shows that under these conditions pure state qubits have $\mathcal{I}_{\phi\phi} = \mathcal{F}_{\phi\phi} = 1$. This is the maximal possible value of the quantum Fisher information showing the standard quantum limit estimation uncertainty $\delta\phi \geq 1/\sqrt{\mu}$ where μ is the amount of parameter-probe

interactions. Therefore, $\theta = \vartheta = \pi/2$ is the optimal choice of state and measurements for information gain about ϕ. The value of φ is not important for the information gain but, as demonstrated in chapter 5, it does have an effect on the estimation range.

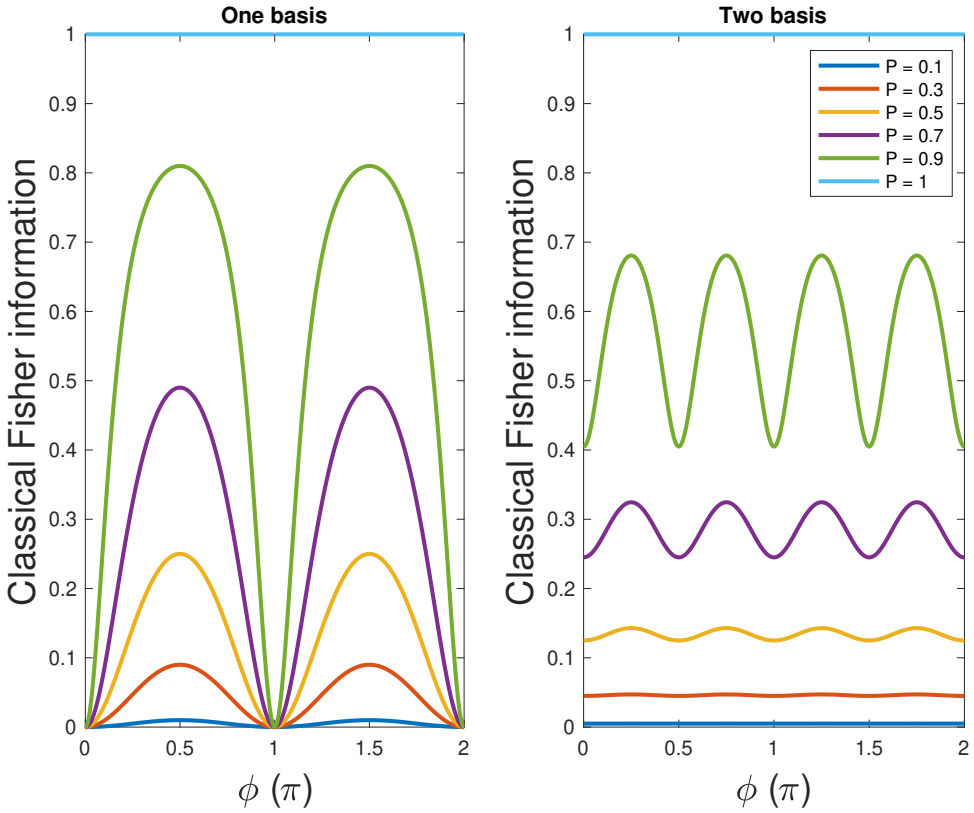

Figure 2.2: The classical Fisher information for mixed state qubits in the equatorial plane of the Bloch sphere with pure state $\{\theta = \pi/2, \chi = 0\}$, acted on by the phase gate $P(\phi)$ and measured in just the $\{\vartheta = \pi/2, \varphi = 0\}$ basis and both the $\{\vartheta = \pi/2, \varphi = 0\}$ and $\{\vartheta = \pi/2, \varphi = \pi/2\}$ bases.

It also shows that noisy qubits have a classical Fisher information that does depend on the value of $\chi + \phi - \varphi$ suggesting that an adaptive protocol could be used to maximise the information gain. ϕ is an unknown, but χ and φ can be changed based on the estimator $\hat{\phi}$ of the parameter ϕ to optimise $\chi + \hat{\phi} - \varphi$. In many of the scenarios discussed in this thesis, two measurement bases, $\chi - \varphi$ and $\chi - \varphi + \pi/2$ are used with equal probability. By the multiple system property of the Fisher information, the classical Fisher information of the system is the sum of the Fisher informations weighted by their occurrence probability,

$$\mathcal{I}_\phi(\text{two bases}) = \frac{1}{2}\mathcal{I}_\phi(\vartheta) + \frac{1}{2}\mathcal{I}_\phi(\vartheta + \pi/2) = \frac{\mathcal{P}^2 - \mathcal{P}^4 + 2\mathcal{P}^4 \sin^2(\phi - \varphi)\cos^2(\phi - \varphi)}{2 - 2\mathcal{P}^2 + 2\mathcal{P}^4 \sin^2(\phi - \varphi)\cos^2(\phi - \varphi)}, \tag{2.54}$$

which becomes 1 for a pure state, $\mathcal{P} = 1$. Figure 2.2 shows the variation in classical Fisher

information for a few values of $\mathcal{P}$ and a range of $\chi + \phi - \varphi$. They show that the use of the two bases constrains the range of Fisher information but does not change the average effect. This indicates that adaptive protocols would still be useful but would gain less advantage. It could be considered an advantage for non-adaptive protocols to use the two bases to ensure a greater minimum information gain.

The Fisher informations are useful in large data data scenarios that are considered to be the asymptotic limit. It is always useful to use the Fisher informations as a measure of information gain, even if the equality of the Cramér-Rao bound cannot be achieved with limited data. Chapter 3 introduces tools and approaches for quantifying limited data information gain.

2.4 Quantum enhanced metrology and sensing networks

Intelligent use of quantum states and parameter interactions can increase the Fisher information, reducing the estimation uncertainty, improving information gain.

2.4.1 Single parameters

When estimating single parameters it is possible to use a single qubit to get a quantum measurement advantage. By interacting the qubit with the parameter B times or increasing the interaction time by a ratio B. Section 2.2 sets out that the net phase gate is,

$$\hat{P}(B\phi) = \hat{P}(\phi)^{\otimes B} = \begin{pmatrix} 1 & 0 \\ 0 & e^{iB\phi} \end{pmatrix}. \tag{2.55}$$

Section 2.3 sets out that the optimal state and measurement for any phase ϕ are $\{\vartheta = \pi/2, \varphi \in [0, 2\pi\}$ and $\{\theta = \pi/2, \chi \in [0, 2\pi\}$, both in the equatorial plane of the Bloch sphere. $B\phi$ is an arbitrary phase so, the same conditions hold for its optimal estimation. Take an arbitrary pure initial state $|\chi\rangle = \frac{1}{\sqrt{2}}(1, e^{i\chi})^T$ and measurement basis $\langle\varphi| = \frac{1}{\sqrt{2}}(1, e^{-i\varphi})$ that satisfy those conditions, the pre-measurement state is

$$|\psi_{\mathcal{P}}\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ e^{i(\chi + B\phi)} \end{pmatrix} \tag{2.56}$$

with quantum Fisher information

$$F_{\phi\phi} = B^2. \tag{2.57}$$

Mixed states have the form $\rho = \mathcal{P} |\psi_{\mathcal{P}}\rangle \langle\psi_{\mathcal{P}}| + \frac{1-\mathcal{P}}{2} I$ where equations (2.5), (2.8) and (2.56) have been combined. By the same logic as equation (2.48), measurement with

the operators $\{M_+, M_-\}$ results in probabilities,

$$P(+|B) = \frac{1}{2}\left(1 + \mathcal{P}\cos(\theta)\cos(\vartheta) + \mathcal{P}\sin(\theta)\sin(\vartheta)\cos(\chi + B\phi - \varphi)\right),$$
$$P(-|B) = \frac{1}{2}\left(1 - \mathcal{P}\cos(\theta)\cos(\vartheta) - \mathcal{P}\sin(\theta)\sin(\vartheta)\cos(\chi + B\phi - \varphi)\right), \tag{2.58}$$

which have a classical Fisher information of

$$\mathcal{I}_\phi = \frac{B^2\mathcal{P}^2\sin^2(\phi - \varphi)}{1 - \mathcal{P}^2\cos^2(\phi - \varphi)}. \tag{2.59}$$

for a mixed state. The measurement probabilities for a pure state are

$$P(+|M) = \frac{1}{2}\left(1 + \cos(\chi + B\phi - \varphi)\right) \tag{2.60}$$
$$P(-|M) = \frac{1}{2}\left(1 - \cos(\chi + B\phi - \varphi)\right) \tag{2.61}$$

which have a classical Fisher information

$$\mathcal{I}_\phi = B^2. \tag{2.62}$$

The B^2 increase is for the Fisher information of the original parameter ϕ. The Fisher information for $B\phi$ is 1. This can be a useful tool for increasing the Fisher information but, it must be used with care in practical scenarios. The B^2 increase in Fisher information comes at the cost of a $1/B$ reduction in estimation range for a parameter ϕ. This effect is demonstrated for $\theta = \pi/2$, $\vartheta = \pi/2$ and $\varphi = 0$ in figure 2.3.

Similarly, the parameter ϕ may be encoded on entangled states. The phase gate $P(\phi)$ is applied to each of the entangled subsystems. This has the same effect as a phase gate $P(B\phi)$ being applied to B entangled qubits. This gives the same Fisher informations, result probabilities and likelihood functions as a single qubit with B-fold interaction. In this sense using an entangled state can be equivalent to multiple passes of a single qubit with the parameter or interacting with the parameter for an integer multiple of time [66].

The classical Cramér-Rao bound, shown in equation (2.52), is defined using μ as the number of independent measurements. In classical estimation strategies the uncertainty in an estimated parameter is limited by the shot-noise limit $\delta\phi \geq 1/\sqrt{\mu}$. This is similar to the standard quantum limit, $\delta\phi \geq 1/\sqrt{N}$ where N is the total number of quantum particles-parameter interactions or the total particle-parameter interaction time, the minimum estimation uncertainty when performing quantum measurements using classical states such as using coherent states to measure phases. These are the same when using repeated measurements with separable qubits to estimate a single parameter where $N = \mu$.

As demonstrated here, B particle-parameter interactions, whether by multiple interactions of a single particle probe or a single interaction by each particle in an entangled

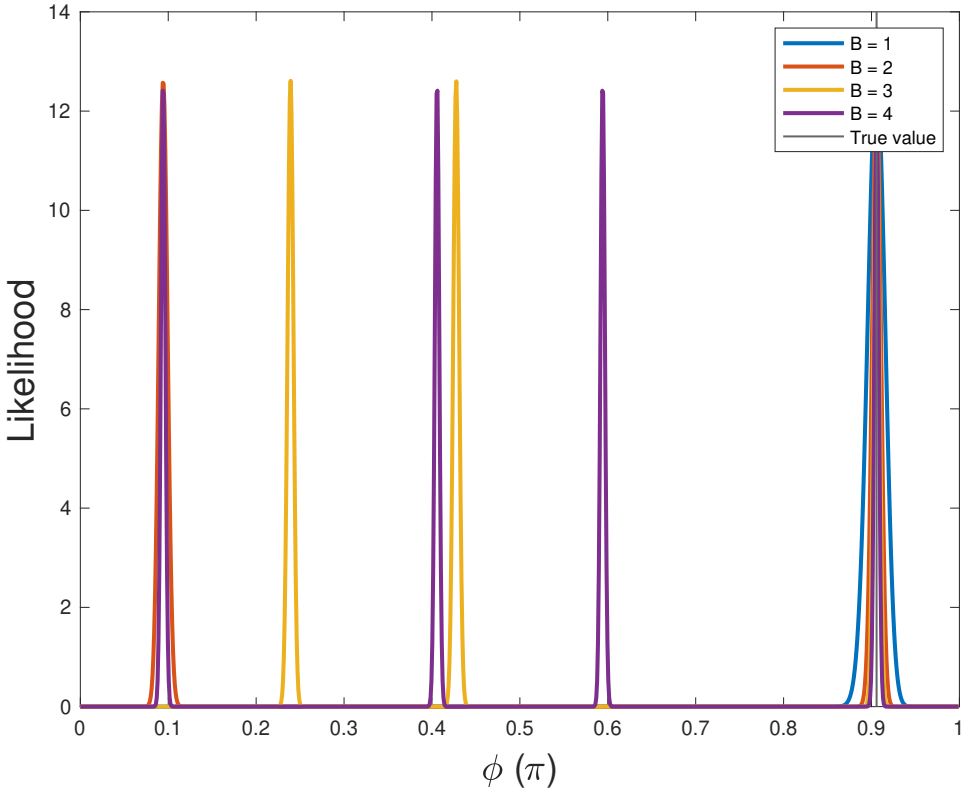

Figure 2.3: An example of the effect of multiple passes causing multiple peaks to likelihood functions. Likelihood functions, properly explained in chapter 3, indicate which values of a variable are likely using the data and no other information. ϕ can be estimated in a π range. $B\phi$ can be estimated in a π/B range. The lines of symmetry are are at $\phi = \frac{k\pi}{B}, k = 1, 2, 3....$

probe the estimation uncertainty is $\delta\phi \geq 1/\sqrt{\mu}B$ which is less than the standard quantum limit. The Heisenberg limit, $\delta\phi \geq 1/N$, drawn from the uncertainty principle is the fundamental limit on the estimation uncertainty of a parameter. A single measurement $\mu = 1$ of the quantum enhanced single parameter estimation, where $N = B$, is Heisenberg limited. However, for practical parameter estimation this is a single shot which is not effective parameter estimation.

By combining parameter estimation using a single parameter-probe interaction per measurement with the estimation from measurements of B parameter-probe interactions the indistinguishability issue can be solved while performing beyond the standard quantum limit. This method is used in chapter 5 for quantum enhanced parameter estimation and to augment information asymmetry with an eavesdropper.

2.4.2 Networked quantum sensors

Quantum networks are systems of physically separated quantum processors that work together to perform some quantum operation(s). Networked quantum sensors use any combination of entangled probes interacting with different parameters and individual probes interacting with multiple parameters to perform quantum enhanced measurement [67]. The principles of encoding a phase multiple times to the same or multiple probes and the effect it has on measurement uncertainty has already been established.

A quantum sensing network is a system where the quantum state evolution of a quantum metrology protocol is performed over multiple nodes. It can provide quantum enhanced estimation by performing joint measurements of parameters encoded into a single quantum state by multiple nodes.

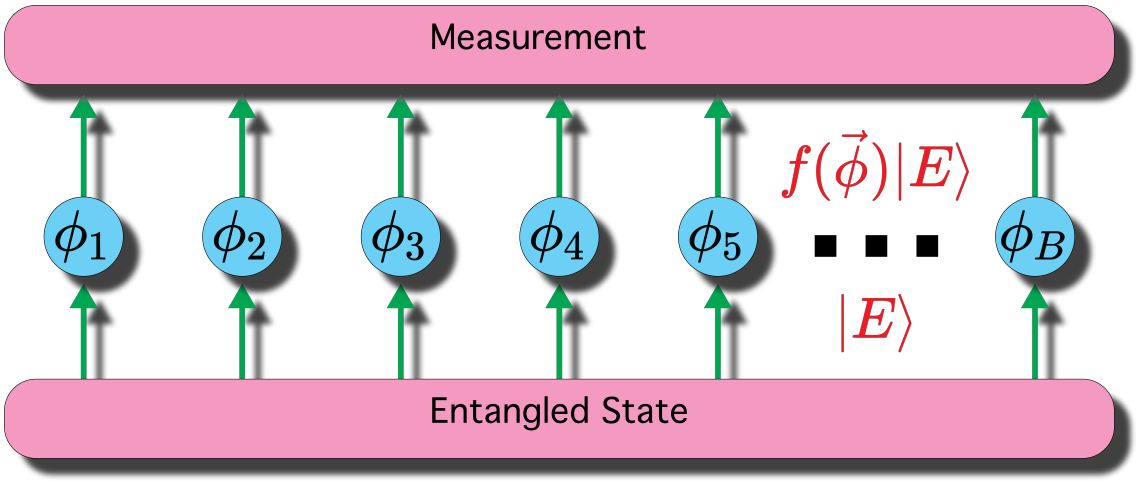

Figure 2.4: A network of quantum sensors that uses entangled states to measure functions of parameters. Each node applies the parameter(s) that they hold to the part of the entangled state that is distributed to them. The total effect is the application of the function of parameters, $f(\vec{\phi})$, to the entire entangled state. This can then be measured and estimated by the individual nodes performing measurements and communicating their results or collecting the entire entangled state at a single node for measurement.

Figure 2.4 demonstrates a sensing network for phase parameters using an entangled state where any one party distributes B probes of an entangled state to B remote sites in a network which each encode a phase ϕ_b. Measurement could be performed at each site or the probe states could be collected for a single measurement operation. As already demonstrated, once a party has the full set of measurement results and knowledge of the initial state, how the measurements were performed does not affect the distribution of results or the information gain. This method is particularly important for scenarios where

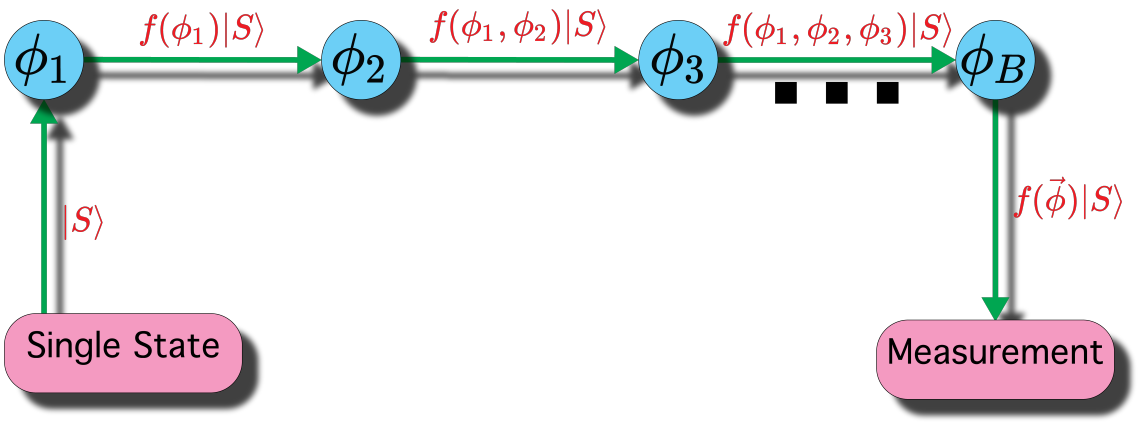

Figure 2.5: A network of quantum sensors that passes a single quantum state between nodes to perform measure functions of parameters. Each node applies the parameter(s) that they hold to the separable state and then send it on to the next node. The total effect is the application of the function of parameters, $f(\vec{\phi})$, to the separable state which can then be measured to perform estimation of the function.

phases must be encoded at the same time, for instance when measuring time or with rapidly changing parameters relative to the quantum communication time between the nodes. It has the disadvantage that large entangled states are more difficult to create and less stable the separable states.

Figure 2.5 demonstrates a sensing network for phase parameters using a single or separable probe state. In this scenario each node encodes a phase to the state that they receive before sending the resultant state to the next node. Once the final remote site has encoded their phase into the state they could perform measurement of the quantum state or send it to another party for measurement. This method is advantageous when phases do not need to be encoded simultaneously due to separable states being more stable and easier to produce than entangled states.

A global measurement strategy such as these is not always advantageous for multi-parameter estimation [39]. For example, in an ideal, noiseless scenario, multiple phases cannot be estimated better using a global estimation strategy than with a local one [53]. Exceptions to this are protocols that use remote nodes to mitigate the effect of local noise sources and defective nodes. For instance, entangling a remote network of quantum clocks [7] all measuring the same time parameter instead of performing the quantum enhanced measurement locally.

2.4.3 Functions of parameters

Global measurement strategies bring improvements to measurement uncertainty over local measurement strategies for functions of parameters. To quantify the increase in information gain the information gain in a local strategy, where each probe interact with only one parameter must be quantified [54] and a measure of resource use consistent between the local and global strategies must be used.

For multiple probe-parameter interactions the resource cost of single probe could be counted linearly $N = \sum_j n_j$ or by root of squares $N = \sqrt{\sum_j (n_j^2)}$ [68–72]. For the purposes of this explanation μ is the number of repetitions of the parameter estimation or rounds of the network protocol and the resource count, N, is the same for the final result regardless of how it is counted.

For some set of measurement phases $\boldsymbol{\phi}$ a d-dimensional vector of continuous differential functions

$$\boldsymbol{\theta} = (f_1(\boldsymbol{\phi}), f_2(\boldsymbol{\phi}), f_3(\boldsymbol{\phi})..., f_d(\boldsymbol{\phi})) \tag{2.63}$$

has Jacobian matrix defined as $J_{jk} = \partial f_j / \partial \phi_k$ the Variance, $\mathcal{V}$, of the functions of parameters transforms as

$$\mathcal{V}(\theta_j) = \sum_{k=1}^{d} \left(\frac{\partial f_j}{\partial \phi_k} \right)^2 \mathcal{V}(\phi_k) \tag{2.64}$$

and Fisher information

$$F(\boldsymbol{\theta}) = J^T F(\boldsymbol{\phi}) J. \tag{2.65}$$

In particular, linear functions are transformed

$$\boldsymbol{\theta} = J^{-1} \boldsymbol{\phi}. \tag{2.66}$$

In general, a local quantum state protocol for the estimation of an arbitrary linear function $\theta = \boldsymbol{\nu}^T \boldsymbol{\phi}$ of B parameters with $\nu_k \geq 0 \forall k \in \{1, 2, 3, ...B\}$ using standard phase gates, $P(\phi_k)$ and the separable ensemble of states,

$$|\psi_{loc}\rangle = 2^{-B/2} \bigotimes_{k=1}^{B} \left(|\lambda_{min,\omega_k}\rangle + |\lambda_{max,\omega_k}\rangle \right), \tag{2.67}$$

where $\boldsymbol{\omega} = B\boldsymbol{x}/\|\boldsymbol{x}\|_1$ is a vector of integers describing the distribution of the number of probe-parameter interactions at each site where for any vector $\boldsymbol{A}$ the p-norm is $\|\boldsymbol{A}\|_p = (\sum_k |\boldsymbol{A}|^p)^{1/p}$ and $\boldsymbol{x}$ is a vector that satisfies these conditions. The local quantum states, $|\lambda_{\omega_k}\rangle$, may contain multiple particles and undergo phase encoding such that they all have the property $\lambda_{max,\omega_k} - \lambda_{min,\omega_k} = \kappa\omega_k$ with the same constant $\kappa > 0 \forall k$. This is achieved using any combination of entanglement and multiple interactions. This is adapted for any

$\nu_k < 0$ by switching the phase encoding of $|\lambda_{min,\omega_k}\rangle$ and $|\lambda_{min,\omega_k}\rangle$ for the relevant k. Thus the estimation variance for a single parameter is

$$\mathcal{V}(\phi_k) \geq \frac{\|\boldsymbol{x}\|_1^2}{\mu\kappa^2 B^2 x_k^2} \tag{2.68}$$

and the estimation variance for the function θ is

$$\mathcal{V}(\theta) \geq \frac{\|\boldsymbol{x}\|_1^2}{\mu\kappa^2 B^2} \sum_{k=1}^{B} \left(\frac{\nu_k}{x_k}\right)^2. \tag{2.69}$$

The vector $\boldsymbol{x}$ that minimises the variance can be found by differentiating $g(x_k) = [x_k + \sum_{k\prime\neq k} x_{k\prime}]^2[\nu_k^2 x_k^{-2} + \sum_{k\prime\neq k}(\nu_k/x_k)^2]$ by all x_k to find the critical point. For arbitrary x_k with $k \in \{1, 2, 3, ...B\}$

$$\frac{\partial g(x_k)}{\partial x_k} = \left[x_k^2 + 2x_k \sum_{k\prime\neq k} x_k'\right] \sum_{k\prime=1}^{B} \left(\frac{\nu_{k\prime}}{x_{k\prime}}\right)^2 + \left(\sum_k x_k\right)^2 \left(\frac{-2\nu_k^2}{x_k^3}\right), \tag{2.70}$$

with solution $\partial g(x_k)/\partial x_k = 0 \forall k$ when $x_k = \nu_k^{2/3} \forall k$ corresponding to a minimum,

$$\mathcal{V}_{loc,minimal}(\theta) \geq \frac{\|\boldsymbol{\nu}\|_{2/3}^2}{\mu\kappa^2 B^2}. \tag{2.71}$$

Spreading the resources equally between the $\tilde{B}$ non-zero elements of ν gives a larger variance

$$\mathcal{V}_{loc,equal}(\theta) \geq \frac{\tilde{B}\|\boldsymbol{\nu}\|_1^2}{\mu\kappa^2 B^2} \geq \mathcal{V}_{loc,minimal}(\theta). \tag{2.72}$$

This is the most efficient strategy for estimating the functions $\boldsymbol{\nu} \propto (\pm 1, \pm 1, ... \pm 1)$ where $\|\boldsymbol{\nu}\|_1^2 = B^2$ corresponds to the sum $\theta = \sum_k \phi_k$ and $\|\boldsymbol{\nu}\|_1^2 = 1$ to the average $\theta = \frac{1}{B}\sum_k \phi_k$. In particular, when there is no local quantum enhancement to the estimation such that $\kappa = 1$, the equally weighted sum of parameters measured using one separable equatorial plane qubit and one interaction for each phase, $B = \tilde{B}$ has estimation variance

$$\mathcal{V}_{loc,minimal}\left(\theta = \sum_k \phi_k\right) \geq \frac{B}{\mu}. \tag{2.73}$$

In this scenario, all of the resource counting methods are the same, $N = \mu B$ making the Fisher information relative to the number of probe-parameter interactions

$$F_{loc}\left(\theta = \sum_k \phi_k\right) = \frac{1}{B^2} \tag{2.74}$$

achieving the minimal measurement uncertainty for a linear network with separable inputs $\delta\theta \geq \sqrt{B/\mu} = B/\sqrt{N}$ [58]. This is the standard quantum limit for measuring a that function of parameter with a B reduction on the standard quantum limit for measuring a single phase.

A global approach can be used to more efficiently estimate the same arbitrary linear function $\theta = \boldsymbol{\nu}^T\boldsymbol{\phi}$ with $\nu_k/\|\boldsymbol{\nu}\|_1 \in \mathbb{Q}$ and B such that $\tilde{\nu}_k \equiv B\nu_k/\|\boldsymbol{\nu}\|_1 \in \mathbb{N}\forall k$ using a GHZ-like state

$$|\psi_{GHZ,\boldsymbol{\nu}}\rangle = \frac{1}{\sqrt{2}}\left(|\lambda_{\max,\tilde{\nu}_k}\rangle^{\otimes B} + |\lambda_{\min,\tilde{\nu}_k}\rangle^{\otimes B}\right) \tag{2.75}$$

where $\lambda_{max,k} - \lambda_{min,k} = \kappa B$ for some $\kappa > 0$ [55]. The corresponding estimation variance is

$$\mathcal{V}_{glo}(\theta) \geq \frac{\|\boldsymbol{\nu}\|_1^2}{\mu\kappa^2 B^2}. \tag{2.76}$$

This can be achieved for the functions $\boldsymbol{\nu} \propto (\pm 1, \pm 1, ... \pm 1)$ where $\|\boldsymbol{\nu}\|_1^2 = B^2$ without locally enhanced quantum measurement, $\kappa = 1$ using the equatorial plane GHZ-like states shown in equation (2.18),

$$\mathcal{V}_{glo,optimal}\left(\theta = \sum_k \phi_k\right) \geq \frac{1}{\mu}. \tag{2.77}$$

Again, in this scenario the resource count is always the same $N = \mu B$ so the Fisher information relative to the number of probe-parameter interactions

$$F_{glo}\left(\theta = \sum_k \phi_k\right) = \frac{1}{B}, \tag{2.78}$$

a B increase relative to the local estimation strategy. This corresponds to a measurement uncertainty $\delta\theta \geq 1/\sqrt{\mu} = \sqrt{B/N}$, a $\sqrt{B}$ reduction compared to the local estimation strategy and a $\sqrt{B}$ reduction on the standard quantum limit for single parameters. It gives a quantum enhanced estimation uncerstainty with estimation beyond the standard quantum limit for the same function of parameters. The optimal global strategy shows a $\|\boldsymbol{\nu}\|_1^2/\|\boldsymbol{\nu}\|_{2/3}^2$ reduction in estimation variance with a maximum reduction of $1/B$ for functions $\boldsymbol{\nu} \propto (\pm 1, \pm 1, ... \pm 1)$.

By re-parameterising a linear function $\nu_k\phi_k \to \phi_k\forall k$ it can be treated as a linear sum of parameters. This is possible to do in scenarios where phase encoding is time dependent (such as magnetic field encoding) by tuning the interaction time or in cases of integer phase multiples by performing multiple interactions of single probes or using entangled probes. Therefore, chapter 6 develops a quantum sensing network using a global approach with the greatest possible information gain relative to the local approach by attempting to estimate the equally weighted sum of the parameters measured at different nodes using the equatorial plane GHZ-like states shown in equation (2.18) to estimate functions of parameters of the form $\theta = \sum_{b=1}^{B} \phi_b$.

The theory of estimating functions has also been developed for single functions when using spin-squeezed states [57] and non-linear functions using an adaptive protocol [59] and

for the estimation of multiple functions simultaneously [56, 61]. Furthermore, practical scenarios have been considered with an experimental demonstration of the estimation of the sum of four phases using entangled squeezed photons [52], theories of optimal estimation of quantum field properties [60] and the theory of estimating general analytic functions of local phase shifts and quadrature displacements in photonic networks [62].

2.5 Chapter summary

This chapter provides the necessary background so that the reader can understand the quantum metrology used throughout this thesis. In addition, it provides numerous analytical results that are used to aid in the decision making for developing the metrology aspects of the SQRS protocols of chapters 5 and 6 and calculating the large data information gain of those protocols.

The chapter covers the first three steps of any quantum metrology protocol, those involving quantum states, initially showing important states, quantum gates, state evolution and measurement operators for phase quantum metrology performed with separable and entangled qubit states. In doing so it introduces the quantum and classical Fisher informations as upper limits on the information gain rate in the asymptotic limit for many identical copies of a quantum state and the measurement results for specific measurements of those quantum states respectively and calculates them for metrology scenarios such as that of chapter 5.

The chapter finishes with a discussion of quantum enhanced metrology and networked sensing. Quantum enhanced metrology for single parameters is relevant to chapter 5. Networked sensing and quantum metrology for functions of parameters are relevant to chapter 6. In particular the advantage in terms of Fisher information and estimation uncertainty for a global measurement strategy over a local measurement strategy is calculated for the best case scenario. This calculation underpins further calculations of information gain in chapter 6 for the network SQRS protocol developed there.

Chapter 3

Statistical methods

This chapter covers the processes for producing and analysing the data that underpins the research discussed in this thesis. Statistics of the information gain underpin both the security and the effectiveness of the metrology in this work.

The protocols developed in chapters 5 and 6 have multinomially distributed sets of results. It follows from the multinomial theorem that n results spread over m bins have m^n combinations. The measurements are independent and identically distributed so, the order of results is not important only the possible combinations of results contribute to information gain. This reduces the possible combinations to

$$\frac{1}{(m-1)!}\prod_{j=1}^{m-1}(n+j). \tag{3.1}$$

In chapter 5 there are four independent probabilities that contribute to the metrology and a fifth probability representing the fidelity checks so, $m = 5$. In chapter 6 the number of possibilities increases with the number of Bobs. For two Bobs $m = 13$ and for three Bobs $m = 29$.

Figure 3.1 shows the number of result combinations for one, two and three Bob secure quantum remote sensing (SQRS) protocols. The number of combinations is so large that it is unfeasible to perform an analysis on every possibility other than for very small numbers of measurements. It is increasingly unfeasible with the number of Bobs. For a single Bob protocol the number of combinations for 10 measurements is 1001 and for 20 measurements is 10626. If the possibility of having to stop due to an eavesdropper being detected is not considered it could be feasible to analyse the data for $\mathcal{O}(10^2)$ possibilities but, in general the number of combinations is far too large. Instead, Monte Carlo methods are used where the analysis of data produced from repeated random sampling provides a good

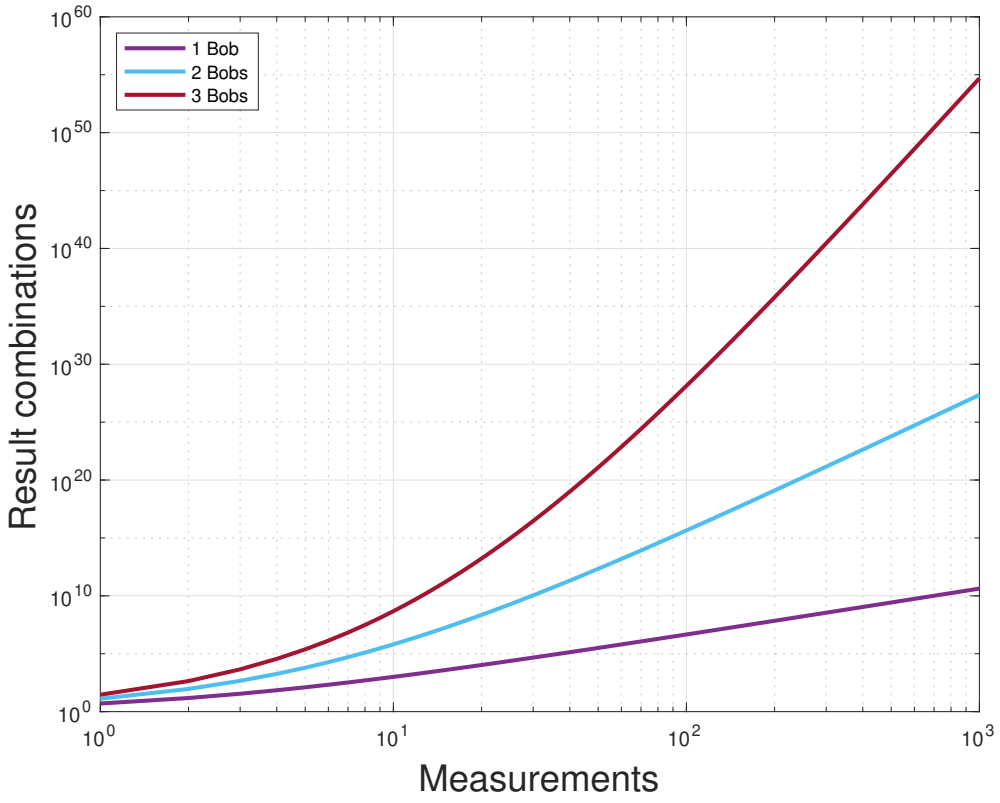

Figure 3.1: The number of result combinations for one, two and three Bob SQRS protocols. Increasing the number of Bobs would further increase the number of combinations.

model of a complex statistical system. One of the disadvantages of Monte Carlo methods is that they still require a large number of samples to get any information gain statistics. This can be mitigated with parallel processing because each simulation is computationally independent.

This chapter discusses the different aspects of Monte Carlo simulations and data analysis used in this research and how they are applied throughout this thesis. The first half of the chapter focuses on the creation of the data. Section 3.1 is an overview of the statistical distributions used to model the behaviour the protocols introduced in later sections. Then, section 3.2 provides an overview of the methods used to simulate the data that underpins the results of chapters 5, 6 and 7.

The second half of the chapter focuses on the data analysis. Initially, section 3.3 shows how to analyse data using Bayesian statistical inference for both large data, in the asymptotic limit, where Fisher information is most useful, and limited data. Furthermore, it introduces some measures of information gain that can be used on the results of many Monte Carlo simulations to indicate the effectiveness of limited data metrology.

Particular to the measurement of phase parameters is the circular nature the parameters being measured. For large data, estimation is precise enough that the circular support for the estimator can be approximated as flat. However, in limited data with minimal prior information, the directional nature of phase must be considered. Therefore, section 3.4 begins with a discussion of limited data phase metrology methods, circular statistics in particular, and ends with a discussion of how the measures of information gain of the previous chapter is adapted to circular statistics.

3.1 Statistical distributions

For a collection of measurement operators $\{M_m\}$, $m = \{1, 2, ..., N\}$, there is a set of measurement result probabilities $\{p_m\}$. For $N = 2$ these are Bernoulli trials, the positive results due to repetitions of this are binomially distributed,

$$Bin(n, p, k) \sim \binom{n}{k} p^k (1-p)^{n-k}, \tag{3.2}$$

where n is the number of Bernoulli trials, p the probability of a positive result and k the number of positive results and

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} \tag{3.3}$$

is the binomial coefficient. This coefficient is the number of unordered possible arrangements of size k from n objects without replacement. It is calculated by combinatorix. Table 3.1 shows the number of ordered and unordered arrangements with and without replacement. These correspond to samples from from populations where once a member of the population has been selected to be part of the sample they are either replaced in the population being sampled allowing them to be chosen again or not.

	Without replacement	With replacement
Ordered	$\frac{n!}{(n-k)!}$	n^k
Unordered	$\binom{n}{k}$	$\binom{n+k-1}{k}$

Table 3.1: Number of possible arrangements of size k from n objects

Conversely, the number of measurements before the first positive result m is geometrically distributed,

$$Geo1(n, p) \sim (1-p)^n p, \tag{3.4}$$

and the number of measurements needed to get the first result m is distributed using the second form of the geometric distribution,

$$Geo2(n,p) \sim (1-p)^{n-1}p \tag{3.5}$$

The number of measurements, n, until k successes occurs is distributed by a negative binomial,

$$NB(n,k,p) \sim \binom{n-1}{k-1}(1-p)^{n-k}p^k. \tag{3.6}$$

This is the the probability of $k-1$ successes from $n-1$ trials multiplied by the probability of success in the final trial.

When $N > 2$, there are more than two possible measurement results and each trial has result given by a categorical distribution. There are generalisations to the binomial and negative binomial distributions for trials with more than two possible results. The multinomial distribution,

$$Mn(n,\vec{x},\vec{p}) \sim \frac{n!}{\prod_m x_m!}\prod_m p_m^{x_m} \tag{3.7}$$

gives the probability distribution of getting a vector $\vec{x}$ of results from a probability distribution $\vec{p}$. Similarly, the number of all measurements until there are x_0 occurrences of measurement M_0 is distributed by a negative multinomial

$$NM(n,\vec{x},\vec{p}) \sim \left(\frac{(n-1)!}{(x_0-1)!\prod_{m=1}^N x_m!}\right)\prod_{m=0}^N p_m^{x_m}. \tag{3.8}$$

The marginal distribution of a subset of a collection of random multinomially or negative multinomially distributed variables, $\vec{q} \subset \vec{p}$, is the multinomial or negative multinomial of the subset of parameters and an additional parameter, the sum of the remaining parameters $\vec{p}_{\text{marginal}} = \left(\vec{q}_{\sum_m p_m \notin q_m}\right)$. The marginal distributions for single variables are the binomial and negative binomial distributions respectively.

The data in this thesis is drawn from multinomial distributions but, the probabilities of each event are determined by quantum mechanics. In particular, $p_m \propto (1 \pm \cos(\varphi + c))$ $\forall m$ and some constant c as described in chapter 2.

3.2 Data creation methods

The SQRS protocols of chapters 5, 6 and 7 can be broken down into rounds corresponding to a single (set of) qubits being created and measured. Each of these rounds are independent and identically distributed until conditions are met which make Alice decide to stop the protocol.

A Markov chain is a stochastic model describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event. In an effective SQRS protocol there is some non-zero probability of any eavesdropper being detected in a round that they attack. Unless the parties running the protocol decide to stop for some other reason, such as having gathered sufficient data, secure protocols follow the Markov chain in figure 3.2. Unlike a standard Markov chain, once the protocol is stopped due to an eavesdropper the probability of it continuing again is zero.

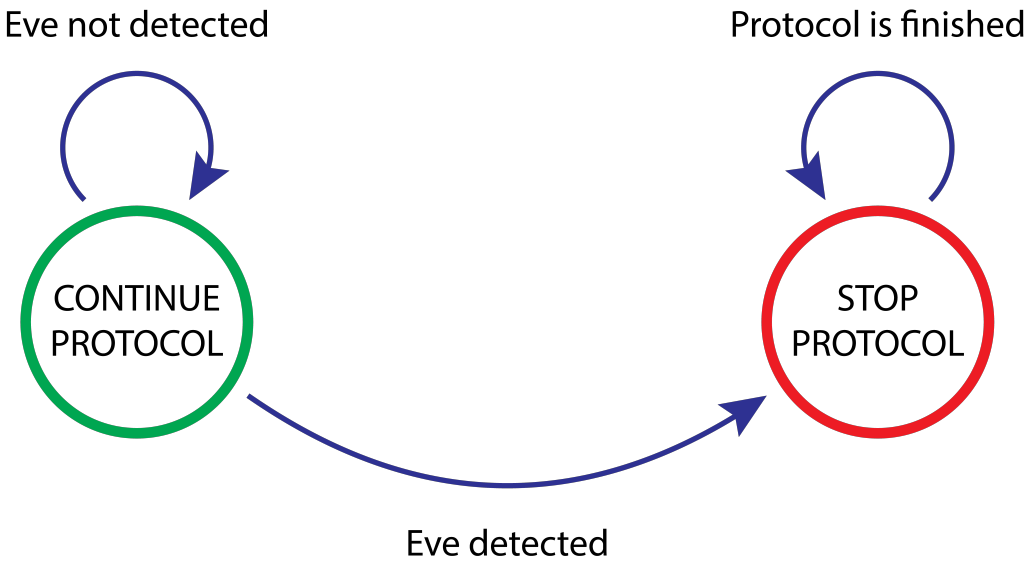

Figure 3.2: A Markov chain for SQRS. Security requires that each round of the protocol must have some chance of detecting an attack by Eve. If that attack is detected, the protocol is stopped. Otherwise, it continues until the parties running it are satisfied with their results.

Each individual round has a set of possible measurement results. These are determined by the quantum mechanics of the protocols and those specific to the metrology aspects of the protocol are set out in chapter 2. When considering only the metrology aspects of the protocols the simulation of results is made significantly easier. In these cases, the Markov chain forcing each round to be considered separately is ignored. This means that, rather than simulating each round separately, the number of each result can be drawn at random from a multinomial distribution with probabilities of individual measurement results governed by the probability distributions given in chapter 2 and the probability of each measurement occurring given in chapters 5 and 6.

For computational efficiency there is a significant advantage to drawing the results directly from the probability distribution. So, when appropriate, this method is used for produce large amounts of data. This is the method used to produce the data in chapter 5

using Matlab. In particular, a custom function named mnrnd2(n,p) produces the data. n is the number of results and p is the probability distribution,

$$\vec{p} = \frac{1}{4}\Big[(1+cos(\phi)),(1+cos(\phi+\pi/2)),(1+cos(\phi+\pi)),(1+cos(\phi+3\pi/2))\Big]. \quad (3.9)$$

Matlab's inbuilt multinomial random number generating function, mnrnd(n,p) is more sensitive to $\sum_j p_j \neq 1$ than the inbuilt cosine function is accurate. The mnrnd2(n,p) function simply re-normalises the probability distribution,

$$\vec{p} \to \frac{\vec{p}}{\sum_j p_j}, \quad (3.10)$$

and calls mnrnd(n,p) to produce data on the protocol metrology.

In addition to considering a network scenario for functions of parameters, chapter 6 considers the amount of information that Eve could gain by attacking the quantum channel before being detected. This is done with Monte Carlo simulations of the entire protocol. This means that each round is considered consecutively with a decision to continue or not between each round as shown by the Markov chain in figure 3.2. Furthermore, the protocol is significantly more complex than the one in chapter 5. It can give one or many measurement results in a single round and the effects of eavesdropping are much more complex.

The disadvantage of simulating the protocol step by step is that it takes more resources. The advantage is that it can be broken down into it's constituent parts making code more flexible. Instead of simulating a single round as a single trial with the result probabilities that could otherwise be put into a multinomial, each step of the process can be treated consecutively.

For example, in a general phase quantum metrology protocol with qubits, the initial state defined by $\{\theta = \pi/2, \chi\}$ could be chosen from a set χ with a probability distribution $\vec{p}(\chi)$ for that choice. Then, the qubit is interacted with a parameter ϕ and measured in a basis $\{\vartheta = \pi/2, \varphi\}$ chosen from the same set $\varphi \in [0, 2\pi)$ with a different probability distribution $\vec{q}(\varphi)$ the data could be produced in three equivalent ways.

First, all of the data could be produced in a single step using the probability distribution

$$P(\pm|\phi, \chi_j, \varphi_k) = p(\chi_j)q(\varphi_k)\frac{1}{2}\big(1 \pm \cos(\chi_j + \phi - \varphi_k)\big). \quad (3.11)$$

Then a multinomial random function can produce a simulated set of results. This is appropriate for fast calculations on systems dependent on simple probability distributions where the number of measurements is defined in advance.

Second, the data is collected one measurement at a time using the same probability distribution. Once all of the data has been collected it is all used at once in a single calculation. This is appropriate for systems dependent on simple probability distributions that may be stopped after a number of rounds that is not determined in advance.

Third, the results can be built up step by step. The j^{th} initial state is chosen from $\vec{p}_\chi$. Then the interaction occurs with the parameter ϕ. Finally, the k^{th} measurement basis is chosen from $\vec{q}_\varphi$ and the measurement is performed. This has the same net probability as the other two methods. This method is appropriate both for complicated protocols and when writing adaptable code where it is easy to make changes to individual steps without recalculating the probabilities and/or re-coding the entire system.

A good example of easy adaptation to small changes to the scenario is phase quantum metrology with some random noise. Chapter 2 sets out the probability distribution for a noisy measurement, requiring significant mathematics to apply the first two methods. With the third method an extra step can be incldued where there some probability of the initial state phase χ being changed to one chosen with a uniform distribution from $[0, 2\pi)$ then treat the final result as if it corresponds to the original initial state.

A big advantage of having these different methods is that they can be used for the same system to verify the overarching statistical models by comparing the result distributions for the different methods. In the specific case of the simulations of chapter 6, the data analysis is often more computationally intensive than the data creation regardless of the method; so, the method of creating the data is less important.

3.3 Bayesian statistical inference

3.3.1 Bayes' rule

This thesis uses Bayesian statistical inference methods. This approach interprets probability distributions as a quantification of the knowledge of parameter(s) being measured. It uses data to update prior knowledge. For this, Bayes theorem,

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}, \tag{3.12}$$

is used. A and B are events and $P(B) \neq 0$. $P(A|B)$ and $P(B|A)$ are the conditional probabilities of event A occurring given B is true and vice-versa. This relationship is derived from the definition of conditional probability

$$P(A|B)P(B) = P(A \cap B) = P(B|A)P(A). \tag{3.13}$$

Bayesian statistical inference uses Bayes theorem and the principle of likelihood functions to update prior knowledge using observed data. A probability density or mass function is the probability of event(s) x, the realisation of a random variable X, occurring given parameter(s) θ, often written

$$x \mapsto f(x|\theta). \tag{3.14}$$

Parameter(s) values are inferred from the probability density/mass function,

$$\theta \mapsto f(x|\theta). \tag{3.15}$$

A likelihood function of for parameter(s) due to some data is made by treating the parameter(s) as a random variable(s) that can be estimated from the data,

$$\mathcal{L}(\theta|x) = P(X = x|\theta), \tag{3.16}$$

with the same value as the probability mass/density function on x, $f(x|\theta)$. It can be used for a variety of tests such as the relative likelihoods of θ_1 and θ_2,

$$R(\theta_1, \theta_2) = \frac{\mathcal{L}(\theta_1|x)}{\mathcal{L}(\theta_2|x)}, \tag{3.17}$$

regions where the likelihood is greater than a certain value, u,

$$\{\theta : \mathcal{L}(\theta|x) > u\}, \tag{3.18}$$

and confidence intervals,

$$\left\{\theta_1, \theta_2 : \sum_{\theta=\theta_1}^{\theta_2} \mathcal{L}(\theta|x)d\theta > v\right\}, \tag{3.19}$$

where $v < 1$. For continuous likelihood functions the confidence interval,

$$\left\{\theta_1, \theta_2 : \int_{\theta_1}^{\theta_2} \mathcal{L}(\theta|x)d\theta > v\right\}, \tag{3.20}$$

has infinitely many solutions, $\{\theta_1, \theta_2\}$. Likelihood functions are also useful in noisy scenarios, a marginal likelihood function is calculated in the same way as a marginal probability distribution,

$$\mathcal{L}(\theta_1) = \int \mathcal{L}(\theta_1, \theta_2)d\theta_2. \tag{3.21}$$

Bayes' theorem written in terms of likelihood functions is Bayes' rule for statistical inference,

$$P(\theta|\vec{x}, \alpha) = \frac{P(\vec{x}|\theta, \alpha)P(\theta|\alpha)}{P(\vec{x}|\alpha)} = \frac{\mathcal{L}(\theta|\vec{x}, \alpha)P(\theta|\alpha)}{P(\vec{x}|\alpha)}, \tag{3.22}$$

where $p(\theta|\alpha)$ is the prior information distribution, $p(\theta|\vec{x}, \alpha)$ is the posterior information distribution, $\vec{x}$ is a sample of observed data points, θ is the parameter of the data point's

distribution and α is the hyperparameter of the prior parameter distribution. The prior distribution is not necessarily the same type of statistical distribution as the likelihood function. For instance, uniform and beta distributions are often used as priors for binomial distributed variables.

As it is a normalisation constant, the denominator is often ignored or applied implicitly when normalising the numerator making it more practical to use the reduced Bayes' theorem,

$$P(\theta|\vec{x},\alpha) \propto \mathcal{L}(\theta|\vec{x},\alpha)P(\theta|\alpha), \tag{3.23}$$

and normalise the result.

The prior and posterior probabilities can be used to predict a new data point,

$$P(x_0|\alpha) = \int \mathcal{L}(\theta|x_0)P(\theta|\alpha)d\theta, \tag{3.24}$$

$$P(x_0|\vec{x},\alpha) = \int \mathcal{L}(\theta|x_0)P(\theta|\vec{x},\alpha)d\theta, \tag{3.25}$$

the prior and posterior predictive distributions respectively. In some inference scenarios the statistical distribution of θ and the best distribution and value of α is not immediately obvious. In such cases these hypothesis are tested using the residuals. This involves removing one (or two or three etc.) data point at a time, called the residual(s), then performing inference and testing how far the data points that have been removed are from the inferred distribution. In general, parameters that reduce the sum of the least squares of the residuals are considered better models.

3.3.2 Prior and posterior distributions

For a binomial distribution, a set of Bernoulli trials, the likelihood function of the probability $\theta = p$ is determined by the results $\vec{x}$ where $x_k \in \{0, 1\}$,

$$\mathcal{L}(p|\vec{x}) = \prod_{k=1}^{K} p_k^x (1-p)^{1-x_k} = p^x (1-p)^{K-x}, \tag{3.26}$$

where $x = \sum_{k=1}^{K} x_k$. The likelihood function depends only on the total number of results. The likelihood function for multinomially distributed variables similarly depends only on the number of results n_k corresponding to each probability p_k where $\sum_{k=1}^{K} p_k = 1$,

$$\mathcal{L}(\vec{p}|\vec{n}) = \prod_{k=1}^{K} p_k^{n_k}. \tag{3.27}$$

The probability distributions used are of the form given in equation (2.50). The protocols introduced in chapters 5 and 6 have a set of possible values $\chi - \varphi = \{0, \pi/2, \pi, 3\pi/2\}$

which give eight possible measurement results for each parameter with four independent probabilities.

$$p_1 = \frac{1}{2}(1+\cos(\phi)) \qquad p_2 = \frac{1}{2}(1-\sin(\phi))$$
$$p_3 = \frac{1}{2}(1-\cos(\phi)) \qquad p_4 = \frac{1}{2}(1+\sin(\phi)) \tag{3.28}$$

where $[\chi-\varphi]_k = (k-1)\pi/2$. These probabilities can be used to determine the result probabilities of the multinomial likelihood function. For instance, noting that $p_1+p_3 = 1 = p_2+p_4$ are the $\pm$ result probabilities for the four cases $[\chi-\varphi]_k$, if all of these possible cases have equal occurrence probability 1/4 then the p_k are 1/2 of those shown above. The likelihood function is of the form

$$\mathcal{L}(\phi|\vec{n}) = \frac{1}{4^n}(1+\cos\phi)^{n_1}(1-\sin\phi)^{n_2}(1-\cos\phi)^{n_3}(1+\sin\phi)^{n_4}, \tag{3.29}$$

where $n = n_1+n_2+n_3+n_4$.

Phase parameters are 2π cyclic. Section 3.4 discusses the statistical implications of phases being directional in nature. However, for the remainder of this section they are treated as if they are unwrapped, $\phi \in [0, 2\pi)$ on a linear scale. The unambiguous prior with the least information is the circular uniform distribution of range 2π,

$$P(\phi|\alpha) = \frac{1}{2\pi} \qquad \phi \in [0, 2\pi). \tag{3.30}$$

As normalisation is often applied implicitly to the calculations of the posterior distribution, the posterior distribution with a uniform prior of width 2π is

$$P(\phi|n_1,n_2,n_3,n_4) \propto (1+\cos\phi)^{n_1}(1-\sin\phi)^{n_2}(1-\cos\phi)^{n_3}(1+\sin\phi)^{n_4}. \tag{3.31}$$

This is the form of the posterior distribution of the data analysis of chapter 5. It is a fairly difficult equation to analyse analytically. Certain statistics such as the maximum likelihood estimator can be found without too much difficulty. The maximum likelihood estimator is found by differentiating the likelihood function (which is equal to the posterior distribution in this case) and finding the value at which the first derivative is zero where the likelihood function is maximised. However, by creating a grid approximation of the posterior distribution the entire distribution can be accounted for and more meaningful statistics inferred. A grid approximation involves defining a grid of possible parameter values such as $\phi_k = (k-1)2\pi/K, k \in \{1,2,3,...,K\}$ which breaks the $[0,2\pi)$ range of possible ϕ values into K evenly spaced data points. Then, the posterior distribution is calculated at every grid point and normalised to create a histogram. This histogram is then used to create plots such as figure 3.3 and measure the information gain. Grid approximation can

be used in multiparameter scenarios but requires memory and calculations of order $\prod_j K_j$ where K_j is the number of grid points for each parameter making it impractical for large numbers of parameters. The posteriors of chapter 6 are significantly more complex so grid approximation is a requirement for calculating all statistics. To avoid exponentially increasing the number of grid points with the number of parameters single parameter grids are made and combined for estimating functions of parameters rather than higher dimensional grids.

An advantage of using the Bayesian model of statistical inference is that any new data can be used to update the current posterior distribution by treating it as a new prior distribution. This means that data can be analysed one result at a time with an identical final analysis to using all of the results at once. This principle is used in chapter 5 by using performing two different parameter estimation protocols and using the posterior of one protocol as the prior for the other. Using two different likelihood functions for each protocol keeps calculations more manageable.

3.3.3 Parameter estimators and posterior distribution analysis

A popular parameter estimator in frequentist statistical inference is the maximum likelihood estimator (MLE)

$$\hat{\phi} = \arg_{\phi\in\Phi} \max \mathcal{L}(\phi|\vec{x}), \tag{3.32}$$

the mode of the likelihood function, where $\Phi = [0, 2\pi)$ is the set of possible values of ϕ. It has two properties that are particularly useful in large data scenarios. If the statistical model is appropriate then the MLE is consitent, meaning it tends towards the true value as the amount of data increases. The MLE is asymptotically efficient,

$$\left(\hat{\phi}_{MLE} - \phi\right) \to \mathcal{N}\left(0, \frac{\mathcal{I}^{-1}}{\sqrt{\mu}}\right), \tag{3.33}$$

where $\mathcal{I}$ is the classical Fisher information matrix and μ is the number of identical independent measurements. This means that the MLE can reach the Cramér-Rao bound with enough data.

In large data scenarios an appropriate prior distribution will have little effect on a well behaved likelihood function. These properties makes the MLE an equally valid estimator in the Bayesian regime for large data. In particular, when the prior distribution is uniform, such as that in equation (3.30), the posterior is proportional to the likelihood function so, the mode of the posterior is the MLE indicating that it has the same properties.

The posterior probability in equation (3.31) is well enough behaved for properties of the MLE to apply so, when a point estimator is useful and there is enough data the MLE

or the mode of the posterior distribution could be used. In particular, in chapter 5 the bias of the MLE helps demonstrate the required amounts of data required to demonstrate some of the behaviour of the likelihood function and indicate the amounts of data required for effective parameter estimation with limited data. Figure 3.3 demonstrates some of the possible shapes of such posterior distributions with 20 data points.

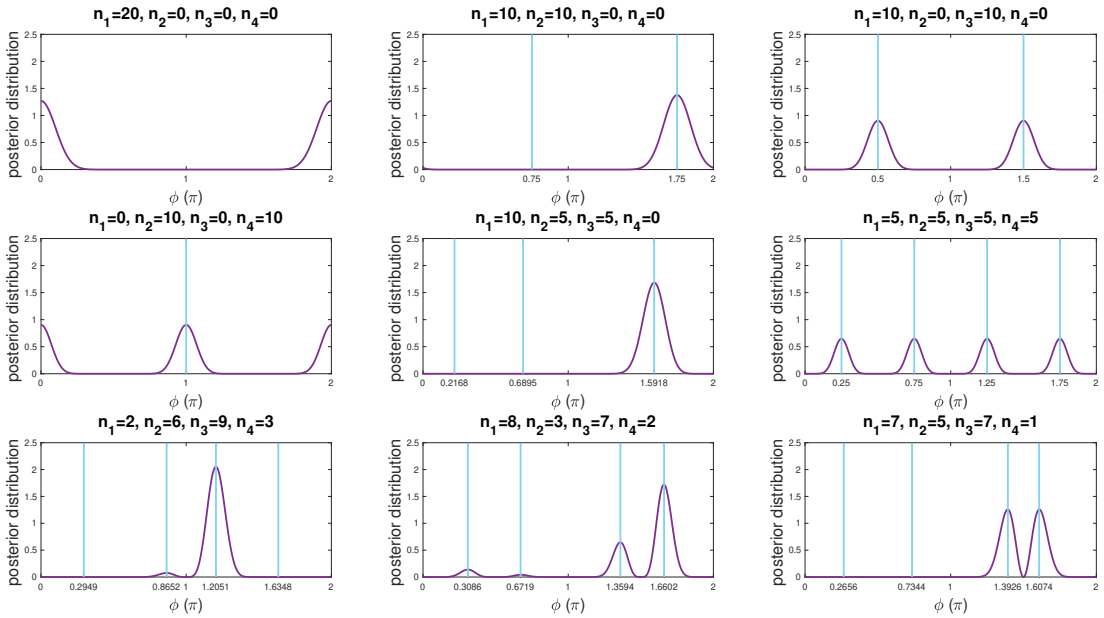

Figure 3.3: A variety of posterior distributions of the form given in equation (3.31) for 20 measurement results. The number of maxima and minima is the same as the number of non-zero measurement result counts. The minima are always at a selection of $\{0, \pi/2, \pi, 3\pi/2\}$. There is up to one maxima in each quadrant.

Bayesian inference in general does not consider a point estimate such as the MLE to contain all of the available information about parameters. Instead, the entire posterior distribution is taken into account. Under the Bayesian model the parameter of interest is considered a random variable with a probability distribution. Therefore any set of values of the posterior distribution can be chosen and used to claim that there is a probability between 0 and 1 that the random variable is a member of that set. These are referred to as credible sets.

This is not possible from a frequentist perspective as the parameter is considered fixed so, the probability that the value of the parameter is in some set of possible values is either 0 or 1. For example, if the likelihood function due to some data has an interval containing 90% of the probability density, it is incorrect to say "the probability is 90%

that the parameter is in that interval". Instead it is said that the interval has a 90% chance of covering the true value. This is referred to as a confidence set.

The difference between a credible and a confidence set is due to the perspective of the statistician. A confidence set is made from a likelihood function when a parameter is considered fixed. A credible set is made from a posterior distribution using both a likelihood function and a prior distribution; the parameter is considered to be a random variable chosen from the prior distribution. This difference in perspective is why Bayesian statistics require the entire posterior distribution to be taken into account.

In the Bayesian regime a credible interval can be made on a case by case basis for the posterior distribution. Figure 3.3 demonstrates some of the posterior distributions using 20 measurement qubits. It provides some examples of posterior distributions which may provide relatively good credible intervals and some that do not. It also illustrates the different shape posterior distributions that occur. When data is drawn from a parameter ϕ the best posteriors are those that group the probability density close to the true value. Of course, in a real experiment the true value would be considered unknown therefore, it is useful to analyse the posterior distributions without knowing the true value.

Credible intervals are a way of analysing this. A posterior distribution that has a credible interval over a short range containing a large posterior parameter probability density is preferred. Considering this, several of the graphs in figure 3.3 have multiple equal peaks that are equally spaced over the 2π range. No matter how narrow these peaks are, such posterior distributions do not provide a good credible interval as the range for any credible interval with greater than 50% probability of containing the true value is larger than π. Some of the graphs have multiple peaks of different heights spaced unevenly over the 2π range. These provide better better credible intervals with some showing at least 90% probability of the parameter being in a range $\pi/2$. The posterior distributions that can provide the best credible intervals are those with either one non-negligible peak or two non-negligible peaks that are close together. There are four examples of this which show a 99% probability of the parameter being in a range of approximately $\pi/2$. Which of them is best is more difficult to quantify without knowing the true value. Arguments could be made for distributions with the narrowest credible interval of any probability being the best choice which would allow statisticians to argue for more than one of the distributions depending on their choice of credible interval probability.

When performing Monte Carlo simulations for metrology it is important not only to be able to analyse the data from a single experiment but to have some measure of the

statistics of the information gain of the data. The standard measures of distributions are the mean square error, variance and bias

$$\text{MSE} = \mathcal{V} + (\text{bias})^2. \tag{3.34}$$

These can be applied to different parameter estimators such as the MLE (mode), median or mean of the posterior distribution. However, as Bayesian inference gives a posterior distribution as a probability distribution for the random parameter, a Bayesian analysis can also take statistics of measures of the effectiveness of the posterior distributions. This means that the mean, variance and distribution of the smallest credible interval of a certain probability could be used as measures of the effectiveness of estimation.

The Cramér-Rao bound shown in equation (2.52) is an important measure of the upper limit of information gain in metrology. For a single parameter it is a measure of the uncertainty $(\delta\phi)^2$ when estimating that parameter. An individual posterior distribution from a single experiment or simulation could exceed the uncertainty limit of the Cramér-Rao bound but the average uncertainty with minimal prior information does not. With enough prior information limited data analysis can exceed the Cramér-Rao bound but in the asymptotic limit the prior information has little effect and the bound is not exceeded. The posterior distribution contains all of the possible information about the parameter(s) so, the error of the posterior distribution can be used as a measure of information gain and it's mean value can be used as a measure of how close the estimation is to the Cramér-Rao bound. The next section introduces a measure of variance specific to circular distributions such as phase estimations and is used in figure 5.4 as a measure of the information estimation uncertainty as a function of the true value and to help demonstrate what parameter values are in the asymptotic limit where uncertainty is close to the Cramér-Rao bound.

Variances provide an effective measure of the estimation uncertainty for unbiased distributions. However, in limited data the posterior distribution is biased. Chapters 6 and 7 require a consistent measure of information gain for very complex posterior distributions that accounts for the bias. Therefore, those chapters use a measure similar to the mean square error that will be introduced in the next section and take the average as a measure of limited data information gain.

3.4 Circular statistics

A difficulty with analysing phase parameters is that they have circular supports. By constraining the range of the estimation so that the posterior distribution is sufficiently narrow, it is defined over an approximately flat space. This allows the use of standard linear statistical models such as the Fisher information. This is usually done in two ways, either the likelihood function is sufficiently narrow, often due to large amounts of data, or the prior information is constrained to be sufficiently narrow [64].

3.4.1 Statistics using vectors

To perform a limited data analysis with as few assumptions as possible neither condition is applied universally in this thesis. Instead, the effectiveness of parameter estimation is quantified in a consistent manner using directional statistics. The principle of directional statistics is to treat each measurement as a vector in a multidimensional space. An example of circular data is the flight direction of birds released from the same point.

In general, directional statistics are defined in hyperspherical coordinate systems. In two dimensions [64], the Cartesian coordinates of the centre of mass of discrete data $(\bar{C}, \bar{S})$ are

$$\bar{C} = \frac{1}{n}\sum_{j=1}^{n}\cos\theta_j = \bar{R}\cos\bar{\theta}, \qquad \bar{S} = \frac{1}{n}\sum_{j=1}^{n}\sin\theta_j = \bar{R}\sin\bar{\theta}, \tag{3.35}$$

where the mean resultant length is

$$\bar{R} = (\bar{C}^2 + \bar{S}^2)^{1/2} \tag{3.36}$$

and when $\bar{R} > 0$ the mean direction is

$$\mu = \begin{cases} \tan^{-1}(\bar{S}/\bar{C}) & \text{if } \bar{C} \geq 0, \\ \tan^{-1}(\bar{S}/\bar{C}) + \pi & \text{if } \bar{C} < 0. \end{cases} \tag{3.37}$$

When $\bar{R} = 0$ the mean direction is undefined. The median and mode (MLE) are equivalent to the linear estimators.

3.4.2 Analysis of distributions

There are two families of dispersion and bias measures in circular statistics. The first family is bounded between $[0, 1]$ or $[0, 2]$ and the second family, like linear measures is unbounded from above, $[0, \infty)$. The bounded measures depend on a measure of the distance between two angles θ and ϕ,

$$d(\theta, \phi) = 1 - \cos(\theta - \phi). \tag{3.38}$$

Using this distance measure, a measure of dispersion of data $\{\theta_j\}$ around an angle ϕ is

$$D(\phi) = \frac{1}{n}\sum_{j=1}^{n}\left(1-\cos(\theta_j-\phi)\right). \tag{3.39}$$

The circular variance, V, is the dispersion around the mean value,

$$V = D(\mu) = 1-\bar{R}, \qquad 0 \le V \le 1. \tag{3.40}$$

These circular dispersion measures have a relationship,

$$D(\phi) = V + Bi^2(\phi), \tag{3.41}$$

where

$$Bi^2(\phi) = 2\bar{R}\left(\sin\left(\frac{\mu-\phi}{2}\right)\right)^2. \tag{3.42}$$

This is analogous to the linear identity

$$\text{Mean square error} = \text{Variance} + \text{Bias}^2 \tag{3.43}$$

$$\frac{1}{n}\sum_{j=1}^{n}(x_j-u)^2 = \frac{1}{n}\sum_{j=1}^{n}(x_j-\bar{x})^2 + (\bar{x}-u)^2, \tag{3.44}$$

where $\theta_j \to x_j$, $\mu \to \bar{x}$ and $\phi \to u$.

To perform statistical inference the continuous form of these measures of distributions are used on posterior distributions using $\phi = \theta_0$ as the true value that the results the posterior distribution is made from are drawn from. In this scenario it is more practical to calculate the mean vector of the posterior distribution, $\vec{r}$ using polar coordinates,

$$\vec{r} = \int_0^{2\pi} P(\theta|\vec{x},\alpha)e^{i\theta}d\theta. \tag{3.45}$$

The mean value and mean resultant length using polar coordinates are

$$\bar{R} = |\vec{r}| \qquad \bar{\theta} = arg(\vec{r}). \tag{3.46}$$

The Maclaurin expansion of the dispersion measure is

$$D(\theta,\xi) = \frac{1}{2}(\theta-\xi)^2 + \mathcal{O}\left((\theta-\xi)^4\right) \tag{3.47}$$

Therefore, a circular analogue to the mean square error of the posterior distribution is the integral of the dispersion around the true value $D(\theta_0)$ weighted by the likelihood function,

$$\xi = D(\theta_0) = \int_0^{2\pi}\left(1-\cos(\theta-\theta_0)\right)p(\theta|\vec{x},\alpha)d\theta \tag{3.48}$$

For narrow likelihood functions this has a relationship $\xi \sim \frac{1}{2}MSE$; in particular for μ measurement results $\lim_{\mu\to\infty}\xi = \frac{1}{2}MSE$. Similarly, the square of the bias is $Bi^2 = Bi^2(\theta_0)$.

These are particularly useful measures due to certain special values. When the likelihood function is a delta function at the true value $\xi, V, Bi^2 = 0$. When it is uniformly distributed $\xi, V = 1$ and $Bi^2 = 0$ and when it is a delta function at $\theta_0 + \pi$, $\xi, Bi^2 = 2$ and $V = 0$. Chapters 6 and 7 use the circular mean square error of the likelihood function as a measure of the information gain that remains consistent for large and limited data and accounts for both the variance and bias.

Some circular measures of dispersion are in the range $[0, \infty)$. For instance, the circular standard deviation,

$$\nu = (-2 \ln \bar{R})^{1/2}, \tag{3.49}$$

is an alternative to the circular variance. For small V, $\nu^2 \simeq 2V$. This measure is particularly useful when used as a comparison to the linear standard deviation. It is defined using the wrapped normal distribution, $\mathcal{WN}(\mu, \nu)$ obtained by wrapping the normal distribution $\mathcal{N}(\mu, \sigma^2)$, onto the circle with probability distribution,

$$P(\phi|\mu, \nu) = \frac{1}{\nu\sqrt{2\pi}} \sum_{k=-\infty}^{+\infty} e^{-\frac{\phi-\mu+2\pi k)^2}{2\nu^2}}. \tag{3.50}$$

For narrow enough distributions it is approximately equal to the linear standard deviation. For the distributions used in this thesis it is closer to the linear standard deviation than the circular variance is to half the linear variance. Therefore, it is used in chapter 5 in place of the linear standard deviation to quantify how much data is needed to reach the asymptotic limit.

As set out in the previous section for linear inference, the final step of Monte Carlo simulations is to make statistics for the quality of the posterior distributions. This section has set out why circular statistical inference is needed for limited data analysis of phase parameters, how to find point estimators such as the mean or mode and dispersion and bias estimators to use in place of the standard linear measures.

Where appropriate, these circular measures are used both for analysing individual posterior distributions and their trends as measures of information gain and quality. It is important that circular inference measures are consistent with the linear measures on which they are modelled. In particular, this means that they must be equal or have a constant proportionality to the linear equivalents in quasi-linear regimes. Quasi-linear regimes are those where the distributions are narrow enough and close enough to the true value to be approximated by a linear support. For example, this is the equivalent to being able to measure the day's walking distance on the surface of the earth using a flat-earth approximation because the distance someone can walk in a day is so much smaller than

the radius of the earth.

In chapter 5 the bias of the MLE is small so the linear bias of the maximum likelihood estimator is used as it is easy to calculate very close to the circular bias for small values and the average circular standard deviation as it is easy to calculate and is more consistent with the linear standard deviation than the circular variance is to the linear variance. Chapters 5, 6 and 7 use the average, Λ of the circular mean square error ξ of the posterior distributions over many simulations of the protocols as a measure of the information gain in limited data because it accounts for all of the data and is consistent with the mean square error, $\xi = \frac{1}{2}MSE$ for small values.

The following is a Matlab function that calculates statistics of phase parameters:

```
%%  First published by Sean William Moore 2024-06,    CC 4.0

%Please cite:
%   Sean William Moore and Jacob Andrew Dunningham. Secure quantum-enhanced measurements on a network of sensors. 2024. arXiv: 2406.19285 [quant-ph]. url: https://arxiv.org/abs/2406.19285


function [mu,nu,mse,var,bias2,rBar] = circStats(position,weight,trueValue)
%circStats finds the circular statistics of the input distributions

%input:
%   position        positions of data points
%   weight          weights of data points
%   trueValue       true value that data is drawn from

%output:
%   mu              circular mean [0,2pi)
%   nu              circular standard deviation [0,infty)
%   mse             circular mean square error [0,2]
%   var             circular variance [0,1]
%   bias2           circular bias squared [0,2]
%   rBar            circular mean resultant length [0,1]

%further information:
%   mse = var + bias2
%   var and nu approximate their linear equivalents for narrow distributions. nu more strictly.

%   K. V. Mardia and P. E. Jupp, Directional Statistics, edited by K. V.
```

```
    Mardia and P. E. Jupp, Wiley Series in Probability and
%   Statistics (John Wiley & Sons, Chichester, England, 1999).

if isempty(weight)
    %no weighting specified, likely that data is unbinned measurement
    %results on circle.
    weight = ones(size(position));
end

if length(position) ~= numel(position)
    error('circStats position has too many dimensions')
end

if isempty(trueValue)
    %value around which to calculate mse and bias2 not defined, set to 0
    trueValue = 0;
end

if size(weight) ~= size(position)
    [sW1,sW2] = size(weight);
    [sP1,sP2] = size(position);
    if sW1 == sP2 && sW2 == sP1
        weight = permute(weight , [2 1]);
    end
end

%weighted sum of cos and sin of angles
r = sum(weight.*exp(1i*position));
%mean direction
mu = mod(angle(r),2*pi);
%mean resultant length
rBar = abs(r)/sum(weight);
%dispersion defined as a function of mean resultant length
nu = sqrt(-2*log(rBar));
mse = sum( (1-cos(position-trueValue)) .*weight ) / sum(weight);
var = 1-rBar;
bias2 = 2*rBar*sin( (mu-trueValue)/2 )^2;

end
```

3.5 Chapter summary

This chapter introduces the statistical methods used to create and analyse the data in this thesis. It begins by setting out the statistical distributions used in the thesis and the methods for creating data. Then, it introduces Bayesian statistical inference methods for data analysis and how to draw statistics of the data analysis. Finally, it gives details of why and how to use circular statistical methods for the data analysis.

Chapter 4

Cryptography for remote quantum metrology

This chapter introduces classical and quantum cryptography and shows how the same principles can be applied to remote quantum metrology to make a variety of SQRS protocols secure against malicious parties.

The beginning of the chapter introduces the standard cryptographic background. Firstly, it introduces the principles of cryptography. Then, it discusses discrete variable quantum key distribution with a particular focus on the BB84 protocol [73]. The SQRS protocols developed in this thesis use similar security proofs to this well regarded cryptography protocol making it important to understand what makes it secure.

The rest of this chapter discusses the literature on cryptographic quantum metrology protocols, SQRS and quantum metrology with tasks delegated to remote, untrustworthy parties. It gives an overview of the different scenarios and the various protocols used to achieve them. In particular, it provides a details of the different methods used to provide security to remote metrology protocols. It proceeds in three sections. The first of these sections introduces the most basic SQRS protocols, anonymous quantum sensing (AQS) protocols that protect the classical information at a remote site used to measure states used for quantum parameter estimation but don't protect against attacks that manipulate the quantum communication channels. The second section introduces a greater variety of scenarios giving a brief overview of the protocols that use quantum key distribution (QKD) to aid in securing the information privacy and ensuring that an eavesdopper does not use a man in the middle (MIM) attack on the quantum communication channels. The final section discusses protocols that use indistinguishable states for security against MIM

attacks.

4.1 Cryptography

Cryptography is the practice of preventing third parties from accessing private messages. Encryption is the process of converting information known as 'plaintext' into a 'ciphertext' that is difficult to return to its original state by a process known as decryption without permission from the owner. This permission is often given through knowledge of some secret key that is used for a publicly known decryption protocol. This does not prevent random manipulation of the messages, it only stops the content from being read by a third party. Changes to the messages can be detected by using encryption to create message authentication codes. Privacy is the security against an eavesdropper learning the plaintext and integrity is the security against the plaintext being changed.

Cryptography has a variety of uses. Historically it has been used to protect information held locally or being sent between remote parties from being accessed by someone who does not have permission and provide security against eavesdropping to communication protocols. The modern age has brought significantly increased computing power and communication speed. This has led to the development and increased use of cryptography both for its historical uses and novel uses such as distributed ledgers used for cryptocurrencies.

A cryptographic system is information-theoretically secure (unconditionally secure) if it is secure against adversaries with unlimited computing resources and time. A one time key of at least equal length as the message is information-theoretically secure. Distributing keys as long as messages for all cryptographic uses is impractical so, instead most classical systems rely on semantic security where only negligible plaintext can be feasibly extracted from any ciphertext.

Semantically secure cryptography relies on a combination of keys and cryptographic algorithms to provide security. A key is information that, when processed through a cryptographic algorithm can encode or decode cryptographic data. The security of classical cryptography protocols relies on sufficiently large keys combined with semantically secure cryptographic algorithms that require enough computation time to be unsolvable by brute force.

One of the methods used in semantically secure classical cryptographic methods is key augmentation. Quantum mechanics has been used to create new cryptographic protocols. In particular, quantum key distribution (QKD) is a popular and well developed group of

protocols that, given that two remote parties can authenticate that they are communicating with each other, allows them to share a key using the rules of quantum mechanics to ensure the privacy of the key. Authentication requires some kind of key [74, 75] so, QKD protocols use quantum mechanics to perform a key augmentation role. The next section discusses discrete variable QKD, the BB84 protocol in particular, because the security principles are similar to those used for the SQRS protocols developed in this thesis.

Cryptographic protocols have also been applied to quantum technologies. For instance, distributed quantum computing [18] allows remote parties to use a quantum computing server to perform calculations while ensuring that only the remote party could interpret the calculation results ensuring information asymmetry. This has inspired the development of a variety of cryptographic quantum metrology protocols that ensure some kind of information asymmetry. The majority of this chapter discusses the literature on cryptographic quantum metrology protocol with a particular focus on those used for measuring phase parameters and functions on phase parameters.

4.2 Discrete variable quantum key distirbution

In QKD, keys are expanded using the principles of quantum mechanics. An initial key is required to provide authentication between two parties [74, 75]. Then, those keys are expanded using quantum states. Assuming prior authentication, this could be used to expand a key into a one time pad for information-theoretically secure cryptography or be used as a key for a semantically secure classical protocol.

Quantum key distribution relies on the no cloning theorem, it is impossible to create an independent and identical copy of an arbitrary unknown quantum state [76, 77]. This means that if an eavesdropper attempts to measure a state chosen at random from a selection of indistinguishable quantum states they cannot do so without risking changing them. This principle has been used to develop numerous quantum key distribution protocols.

The security of quantum channels in SQRS protocols comes from the same principles as discrete variable quantum key distribution. The two most famous discrete quantum key distribution protocols are BB84 [73], a prepare and measure protocol, and E91 [78], an entanglement based protocol. The states used in the novel protocols introduced in chapters 5 and 6 use the same or similar states as BB84 to help ensure security of the quantum channels.

In BB84 Alice sends qubits to Bob with each chosen uniformly at random from the four Pauli-X and Pauli-Y eigenstates. Bob measures these qubits at random in the same

two bases. Then, Alice and Bob publicly declare the basis they used for each qubit, but not the initial states or the measurement results. They discard the information about the qubits in the basis that do not match. Then, Alice chooses a random selection of the initial states for which she and Bob publicly disclose the corresponding initial state and measurement result. In an ideal scenario, any errors indicate an eavesdropper. If there are no errors then bits corresponding to Alice's initial state and Bobs measurement result are used for the secret key.

In a real-world scenario, noise causes some errors so information reconciliation [79], then privacy amplification [80] protocols are used to reduce the rate of erroneous bits and reduce Eve's knowledge of the key respectively. The BB84 protocol has been shown to be information-theoretically secure using single photon sources [81] to create a one time pad under the conditions that the classical communication channel is authenticated with unconditional security, Alice and Bob use trusted and truly random numbers and Eve cannot access Alice and Bob's encoding and decoding devices.

The condition that the classical communication channel must be authenticated with unconditional security indicates that quantum key distribution protocols do not create new keys entirely on their own but are instead a method of augmenting whatever key was already used for the authentication. If proper authentication is not used then the protocol is vulnerable to MIM attacks.

The first condition of information security is that an eavesdropper cannot gain any information from the publicly available information without interfering in the protocol. BB84 achieves this because the density function from Eve's perspective is half the identity matrix,

$$\rho_{Eve} = \frac{1}{4}\left|X+\right\rangle\left\langle X+\right| + \frac{1}{4}\left|X-\right\rangle\left\langle X-\right| + \frac{1}{4}\left|Z+\right\rangle\left\langle Z+\right| + \frac{1}{4}\left|Z-\right\rangle\left\langle Z-\right| = \frac{1}{2}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad (4.1)$$

which gives a quantum Fisher information of 0 for any parameter it interacts with indicating that Eve cannot gain any information about any parameters using this state. This means that Eve cannot gain any information about the key without gaining further knowledge of the individual quantum states.

The second condition is that an eavesdropper cannot interact with the system without risking detection. This can be broadly categorised as man in the middle (MIM) attacks. The first type of MIM attack that needs to be avoided is Eve imitating either Alice or Bob. The assumption of prior authentication deals with this issue.

Two similar and important MIM attacks on quantum cryptographic systems are the

'intercept and resend' (IR) and 'measure and replace' (MR) attacks, where Eve intercepts quantum resources in transit between Alice and Bob and replaces them with her own. In IR attacks she blocks quantum states and replaces them with her own. In MR attacks she measures the states to gain some information about them before replacing them with the most likely state based on her measurement result. This attack demonstrates that secure quantum communication protocols must send states randomly chosen from a selection of indistinguishable states through quantum communication channels. Otherwise, a MR attack would break the security very easily.

First, consider MR attacks. In BB84 MIM attacks are protected against by using two different qubit basis, the Pauli-X and Pauli-Z basis shown in table 2.1, ensuring that Eve measures in the wrong basis with probability 1/2. When Eve measures in the wrong basis she sends a state in her measurement basis which, when Bob measures in the same basis as Alice's initial state, has a detection probability $|\langle X \pm |Z\pm\rangle|^2 = |\langle Z \pm |X\pm\rangle|^2 = 1/2$. When Eve measures in the correct basis she will never be detected. Thus, the probability of Eve being detected when she attacks a single round and Bob measures in the correct basis is

$$\begin{aligned} P(\text{detection single attack}) &= P(d|\text{Eve measure correct basis})P(\text{correct basis}) \\ &+ P(d|\text{Eve measure incorrect basis})P(\text{wrong basis}) = 0 \times \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{1}{4}. \end{aligned} \quad (4.2)$$

The key is only made from the states that Bob uses for measurement so, the probability that Eve is undetected when attacking a key size k is

$$\begin{aligned} P(\text{detected at least once}|k \text{ key bits attacked}) &= 1 - P(\text{undetected}|k \text{ key bits attacked}) \\ &= 1 - \left(1 - \frac{1}{4}\right)^k = 1 - \left(\frac{3}{4}\right)^k. \end{aligned} \quad (4.3)$$

Alternatively, in an IR attack, where Eve does not measure the qubit before replacing it, the probability of Eve choosing the correct state, where she will not be detected, is 1/4, the orthogonal state where she will always be detected is 1/4, and either of the other states, where she is detected 1/2 of the time, is 1/2. So, the probability of detecting a single attack when Alice and Bob use the same basis is

$$P(\text{detection single attack}) = 0 \times \frac{1}{4} + 1 \times \frac{1}{4} + \frac{1}{2} \times \frac{1}{2} + \frac{1}{2} = \frac{1}{2}, \quad (4.4)$$

making her significantly more likely to be detected,

$$P(\text{detected at least once}|\text{k key bits attacked}) = 1 - \left(\frac{1}{2}\right)^k. \quad (4.5)$$

The E91 protocol uses entangled qubits as a resource for quantum key distribution as do many SQRS protocols. If BB84 was adapted so that Alice creates entangled pairs of qubits and sends one of each pair to Bob, then Alice measures them at random in the two measurement bases this would result in Bob receiving qubits of the same kind and with the same distribution as in the BB84 protocol while Alice ensures that the choice of states is truly random. This gives some entanglement based SQRS protocols shown later in this chapter [13] and the entanglement free SQRS protocols introduced in chapter 5 the similar security against MIM attacks as BB84.

A key limitation of quantum key distribution protocols is that they rely on ideal quantum states. A particular issue with the photon implementation is the requirement for single photon states. Laser pulses are coherent states with Poisson distributed photon number. To reduce the probability of more than one photon being present in a pulse very low average photon numbers are used which reduces flux. The reason for this is that, an attacker with a quantum memory could skim off extra photons, storing them until measurement basis are made public and measuring them in the correct basis allowing her to break that part of the key [82].

A popular method for protecting against photon splitting attacks are decoy states [83–85], where multiple randomly chosen intensity levels are used to send photons from Alice to Bob. When announcing her measurement basis, Alice also announces the intensity levels for the transmission of each qubit. Alice and Bob can compare photon number statistics to check the error rate in the number of bits Bob receives to detect a photon splitting attack. These protections are resource intensive and reduce the secret key rate.

The SARG04 protocol [86, 87] is an adaptation to the bit encoding and basis declaration of the BB84 protocol. Instead of announcing the orthogonal basis of the state that she sends, Alice announces that it is one of two non-orthogonal states. For instance the $|X+\rangle$ state is paired with either the $|Z+\rangle$ or $|Z-\rangle$ state. This reduces Eve's ability to break bits from photon splitting attacks but also significantly reduces the secure key rate.

Chapter 7 shows that, as the novel SQRS protocols in this thesis don't need to declare Alice's measurement basis, or even give a possible pair like SARG04, it is significantly better protected against photon splitting attacks than using the same photon source for BB84 quantum key distribution to send equivalent measurement results from Bob to Alice.

4.3 Anonymous quantum sensing

The fundamental principle of SQRS is to perform quantum metrology with at least one of the quantum tasks of a quantum metrology protocol being performed at a remote site. This means that one or two of quantum state preparation, evolution and measurement are delegated to a remote site [88].

Information privacy is qualified by ensuring that an eavesdropper cannot gain information without manipulating the system and is increasingly likely to be detected each time she performs an attack where she manipulates with the communication channels for a round of remote metrology. Similarly, information integrity is qualified by ensuring that the an eavesdropper is increasingly likely to be detected the more that they attempt to spoof the parameter estimation. Security can be quantified by ensuring limits on an eavesdropper's information gain and spoofing ability and ensure information asymmetry between trusted parties and an eavesdropper.

Often called anonymous quantum sensing, AQS, many SQRS protocols, inspired by blind quantum computing [18], focus on ensuring that classical information of measurements on remote parameters is protected but don't protect against attacks on the communication channels, especially the quantum communication channel. This is often achieved by ensuring that the average density function of the parameter estimation states is proportional to the identity matrix ensuring a Fisher information of zero for all but the parties that know what each initial state is.

The earliest SQRS protocols [6, 63] use the arrival time of photon wave-packets to estimate the distance between Alice and some detectors at a remote site Bob. In this scenario, entanglement can be used to give both quantum enhanced parameter estimation and security. It proposes two methods of ensuring the security. The first is an AQS protocol. By entangling the wave-packets and retaining one member of the entangled state and measuring it herself she ensures that only she can interpret the classical information. This is the first example of distributing part of an entangled state to ensure that an eavesdropper cannot interpret the classical information. However, this doesn't protect against manipulations of the communication channels. The second protocol also protects against quantum channel attacks using indistinguishable states so, it will be discussed in the final section of this chapter.

Another protocol uses Dicke states to find which nodes in a quantum network have non-zero magnetic fields [9]. By using a well chosen selection of states with appropriate

probabilities the protocol ensures that the measurement results are independent of the position of the non-zero magnetic field(s). This ensures that only the party that knows the initial states can interpret the results to gain information about the position of the non-zero magnetic fields.

The novel protocols introduced by this thesis are for the metrology of phase parameters and functions of phase parameters at remote sites. Therefore, the rest of this section provides greater detail on the preexisting methods for performing AQS for phase parameters at remote sites.

4.3.1 Quantum remote sensing with asymmetric information gain.

One phase estimation protocol allows a client with the ability to measure quantum states (but not to create them) to delegate the state creation and parameter interaction to a server while ensuring that only the client can interpret the classical information [11]. A pictorial representation of the protocol in comparison to a standard, insecure, sensing protocol is shown in figure 4.1. The protocol allows for the fact that errors in the channel could be time-dependent. Therefore, it uses a destructive random sampling test [89] for the Bell pairs. This requires a very large number of qubits, at least $\mathcal{O}(10^5)$ for greater than 90% fidelity. The protocol can be summarised as follows:

1. The server prepares large set of Bell pairs.
2. the client splits these into four equally sized sets $\{X, Z, M, R\}$, telling the server how they are organised.
3. The server sends one part of every Bell pair to the client
4. The server and client perform the following operations on their members of each set:
   - X set: They both perform Pauli-X measurement.
   - Z set: They both perform Pauli-Z measurement.
   - M set: The client performs Pauli-X measurement and stores the result, $c \in \{0, 1\}$. The server stores the remaining qubit state in a quantum memory.
   - R set: The set is rejected.
5. The client counts number of times X and Z sets give different measurements for client and server. Each disagreement counts as a failure. If the failure rate is acceptable the protocol continues. Otherwise the protocol is aborted.

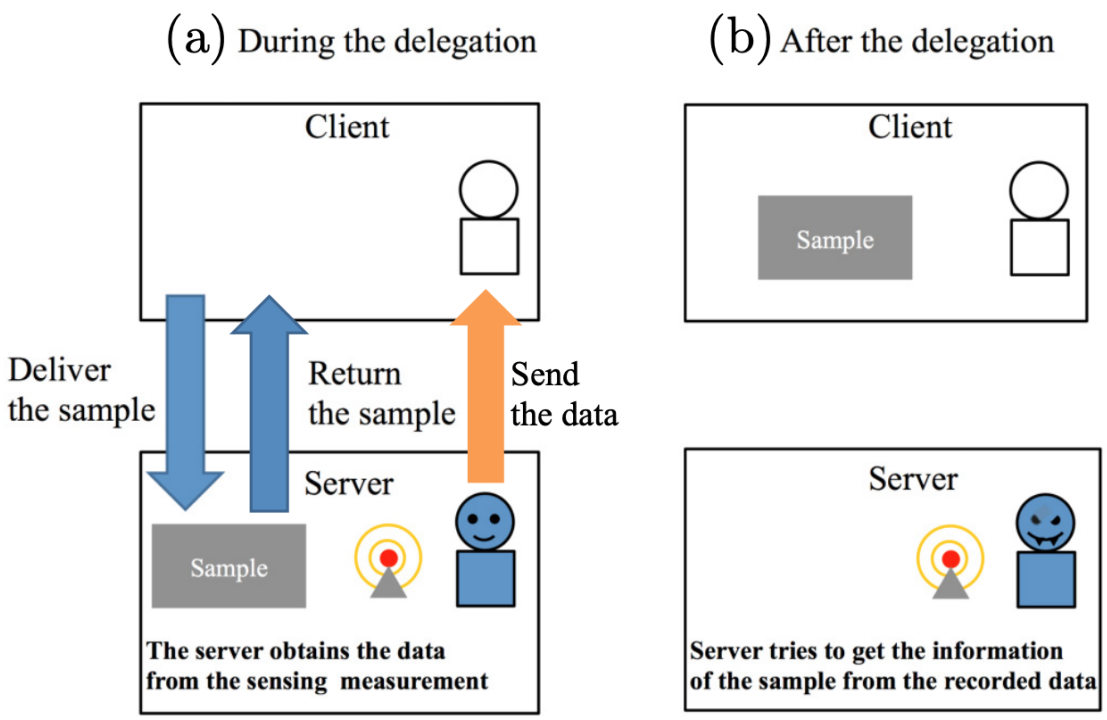

Figure 4.1: The scenario envisaged for quantum remote sensing with asymmetric information gain [11]. In this scenario, no classical information about the parameter remains at the remote site after the end of the protocol

6. The server performs standard quantum metrology with the remaining state and sends the outcome $o \in \{0, 1\}$ to client.

7. The client performs the bitwise XOR operation $c \oplus o$ to get final the measurement result.

8. The client and the server repeat until the client's metrology requirements are fulfilled.

From a metrology perspective, this protocol provides asymmetric information gain between client and server. However, it requires a very large overhead to ensure state fidelity and is limited to estimating phases in a π range. Nevertheless, it provides a method of asymmetric information gain that adjusts for some quantum state creation and channel noise. This protocol has been extended to consider more noise by dephasing [12].

This protocol is secure in the sense that the server or an eavesdropper cannot gain information solely by reading the server's results. However, it is totally insecure to MIM attacks; the identity of the measurement qubits is publicly declared so any eavesdropper could steal the information without being detected by measuring and replacing that set of qubits in the quantum communication channel. Furthermore, if a malicious party can

manipulate the classical data exchange, there is no information integrity as results could be spoofed undetected by applying the bitwise NOT operation on the parameter measurement results. This kind of attack will be discussed in detail in chapter 7.

A simple modification to give security to the quantum communication channel would be for the server and client to choose their $\{X, Z, M\}$ sets at random. The amount of each can be further optimised for information gain with security and noise requirements. This could be improved further by considering that phases are in the Pauli-X - Pauli-Y plane of the Bloch sphere. Thus, if the client chooses at random between $\{X, Y\}$ and the server between $\{X, Y, M\}$, security would improve and the parameter estimation range would be extended to 2π.

The same verification protocol when used on GHZ states is used to ensure the security of a network SQRS protocol [15] that provides integrity to the estimation of a function of parameters while providing privacy for each of the individual parameters. This protocol runs the verification protocol then each node encodes their parameter, performs their measurement and publicly declares their measurement result. This is repeated many times until sufficient metrology is performed. In this case no party can gain information about the individual parameters from the classical data making it very different from the network protocol in chapter 6 which provides protection to the function of parameters in addition and chapter 7 extends this to the individual parameters.

4.3.2 Experimental demonstration of secure quantum remote sensing

Secure quantum remote sensing has been demonstrated experimentally in a scenario where Bob performs parameter encoding and state measurement, Alice performs state measurement and either of them or a third party performs state preparation [13]. Figure 4.2 demonstrates a medical scenario for which this protocol would be useful.

In this experiment photon Bell pairs were produced and distributed with one member of each pair sent to Alice and the other to Bob. Alice measured her photons in either the Pauli-X or Pauli-Y basis, projecting each Bell pair partner into one of four polarisation states. This ensured that only Alice knew the state arriving at Bob. Therefore, when Bob measures his sample using that member of the Bell pair, only Alice can correctly interpret the measurement result. Their experimental setup is shown in figure 4.3

Firstly, from a metrology perspective, this protocol allows for the estimation of a phase parameter in a 2π range. A previously mentioned protocol already discussed used only used Pauli-X states to perform measurement with gave measurement probabilities of the

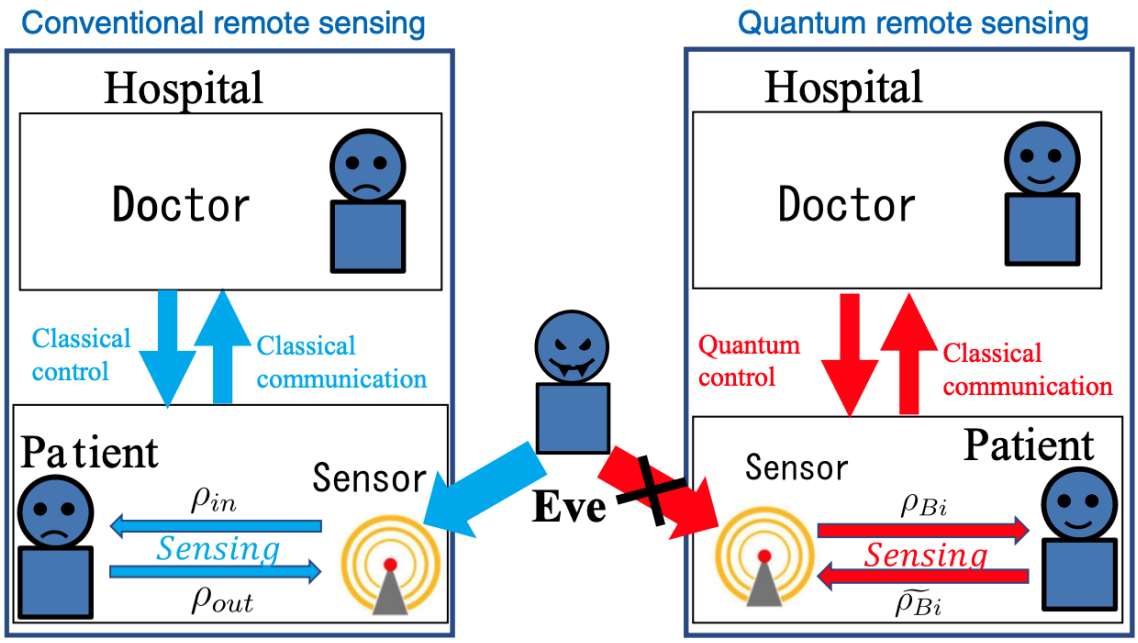

Figure 4.2: A scenario envisaged for secure quantum remote sensing [13] where a doctor securely measures a remote patient. In this scenario, the use of a secure quantum remote sensing protocol stops an eavesdropper from being able to gain information about the parameter by observing the classical measurement results.

form

$$P = \frac{1}{2}(1 \pm \cos\phi), \tag{4.6}$$

which is periodic in π, allowing estimation in a π range. This protocol produces four probabilities,

$$P_X = \frac{1}{2}(1 \pm \sin\phi) \qquad P_Y = \frac{1}{2}(1 \pm \cos\phi). \tag{4.7}$$

Each of P_X and P_Y are periodic in π ranges but those ranges are shifted by $\pi/2$. Therefore, any combination of P_X and P_Y creates a likelihood function that is periodic in 2π.

An advantage of this experimental demonstration is that it considers the imperfections in the experimental apparatus for the creation of states and the nonuniform detection efficiency of single photon detectors. While in an ideal case Alice has classical Fisher information 1 and Eve classical Fisher information 0, these imperfections allow Eve to gain some information about the parameter when interpreting Bob's classical information. The experiment was performed in the large data limit of approximately 60 000 measurements and showed that Alice could get an estimate with precision close to the Cramér-Rao bound while ensuring that Eve's information gain was more than an order of magnitude worse.

The experiment only considered the scenario where Eve attempts to gain information

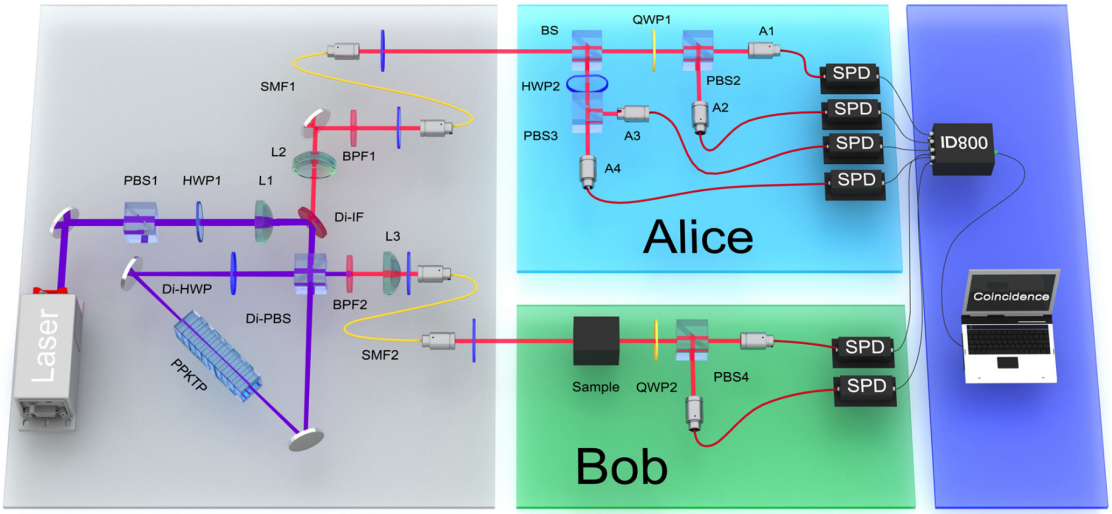

Figure 4.3: The experimental setup for a demonstration of SQRS using distributed entanglement [13]. Here Di denotes dichroic, BS denotes beam splitter, IF denotes interference filter, BPF denotes band-pass filter, SMF denotes single-mode fiber, HWP denotes half-wave plate, QWP denotes quarter-wave plate, PBS denotes polarized beam splitter, L denotes lens, and SPD denotes single photon detector.

from Bobs classical data and it demonstrates that information asymmetry of this type can be achieved experimentally using shared Bell pairs. It does not consider what would happen in a scenario where Eve attacks the quantum channel. State fidelity was only checked in a separate process prior to performing the metrology protocols. Therefore, Eve could attack only the states used for metrology without risking detection. For instance, a MIM attack where Eve replaces quantum states before they arrive at Bob would not be detected. Such attacks are considered more thoroughly in theoretical protocols of the following sections and chapters 5 and 6 where randomly distributed state verification and parameter estimation by Bob(s) is used to ensure that there is no such attack. Furthermore, by using an imperfect entanglement source coincidences of Alice and Bob's measurements must be recorded to ensure that the protocol is properly implemented, highlighting the practical advantage of using separable states like in chapter 5.

The theoretical protocols that protect against man in the middle attacks consider any measurement of state fidelity that does not agree with the initial state to be proof of a potential eavesdropper causing Alice and Bob to stop the protocol. This is incompatible with experimental implementation as demonstrated here. Ensuring information asymmetry when allowing for some experimental noise is a significant direction for future work.

4.4 Quantum remote sensing secured using quantum distributed keys

Generally, SQRS protocols have two security requirements. The first, as set out in the last section is to ensure that classical information can only be interpreted by the parties that are intended to gain information about the unknown parameter(s). The second condition is to limit how much information can be stolen or spoofed by an eavesdropper manipulating the quantum communication channels.

The next two sections discuss a variety of SQRS protocols that delegate different tasks to remote parties. In general, both of the security conditions are required for a secure protocol; the exception is protocols where the party that is intended to gain parameter information is performing all of the quantum state measurement. This section introduces SQRS where QKD is used to ensure security of the quantum channel. The next section will cover SQRS protocols that integrate the quantum channel security into a single protocol.

In one QKD reliant protocol Alice prepares input states that are a combination of quantum states optimised for the metrology and flag qubits in the $|0\rangle$ state [14]. Then she encrypts it using a Clifford operation. The encryption ensures that Eve cannot extract information from the quantum state in transit. Alice and Bob use QKD to share a key which Bob uses to decrypt the state and learn which are the trap qubits. He measures the trap qubits to verify the fidelity of the metrology state.

A similar concept to SQRS is quantum metrology with delegated tasks and untrustworthy nodes. Instead of protecting against attacks by an eavesdropper quantum metrology with delegated tasks where one or two of the three steps of a quantum metrology protocol that involve quantum states is performed by parties other than the parties that are intended to perform the final step, parameter estimation using classical measurement results and attempts by any parties to spoof or steal information they should not have are detected.

A popular quantum metrology protocol with delegated tasks uses entanglement to build a quantum enhanced network of clocks [7] with protection against malicious nodes. This network scenario measures the average time measurement of the clocks measuring the same time parameter spread over the network. It uses uncorrelated qubit states $\left(|0\rangle + e^{i\chi}|1\rangle\right)/\sqrt{2}$ with random χ to verify if there are malicious nodes in the network. Then QKD is used to communicate the classical results. The scope of this protocol could be extended by using the same states used to verify the for malicious nodes could also

be used to verify the fidelity of the distributed quantum states and the integrity of the quantum communication channels to make it into a SQRS protocol.

QKD can be effective in helping ensure the security of SQRS protocols. However, it is against the spirit of SQRS to rely on an entire other protocol to ensure the security. It also reduce the scope of the protocols. Firstly, the classical data held by Bob(s) is not secured against an eavesdropper. Secondly, it requires the Bobs to have the infrastructure for QKD.

By adding a random phase to the distributed entangled states like more recent SQRS protocols do [8, 11, 13, 16] a quantum network of clocks protocol could be made secure without requiring QKD. The protocol set out here provides some inspiration for the network protocol in chapter 6. However, it is a much simpler scenario as it is only verifying for malicious nodes, not communication channel attacks and each node is measuring the same parameter. Therefore, the results of each node can be verified against each other which removes the complications around network fidelity checking for functions of multiple parameters.

4.5 Quantum remote sensing with integrated security

As discussed in section 4.3, the classical information for remote measurement of phase parameters can be protected by distributing an entangled state between the local and remote sites, also called Alice and Bob respectively [11, 13]. Then, by measuring their part of the entangled state and keeping the result secret, only Alice can interpret Bob's results. In general this can be adapted to protect the quantum channel if Alice measures in more than one basis and Bob performs fidelity checking measurements in the same basis as this means that Eve cannot measure and resend in the same basis as Alice and Bob without risking detection.

The metrology and security can be achieved in the same way without using entanglement. The entanglement strategy produces equal amounts of each orthogonal state which makes the average density function of the the measurement states proportional to the identity function which ensures that Eve cannot gain information from the average state. This can be achieved without entanglement by sending one of two orthogonal states independently at random with equal probability in each round. To ensure that an eavesdropper cannot attack the quantum channel without risking detection it is sufficient to use indistinguishable states and perform the proper fidelity checks. This can be achieved by using two or more different orthogonal states.

The first SQRS protocol in section 4.3 was an AQS protocol for estimating the distance between Alice and Bob. The same work introduced the first remote quantum metrology protocol that secures quantum communication channels without using a separate QKD [6, 63] protocol. It uses BB84 QKD as an inspiration. In this protocol Alice and Bob share many copies of a frequency-time of arrival entangled state. Then, each chooses independently at random to measure either the frequency or time of arrival. When they both measure the same variable they should get the same result. If an eavesdropper measures the frequency they remain undetected but gain no information. If they measure the time of arrival they gain useful information but risk detection. This ensures privacy but not integrity. The metrology is not sensitive to the frequency so, the states for which both measure the frequency are used like decoy states whose only purpose is to detect an eavesdropper.

4.5.1 Cryptographic quantum metrology

Decoy states are also used for quantum channel security in a group of protocols for phase measurement where another party, Charlie, who does not prepare or measure states [8], encodes the phases. This is done by having Alice prepare Pauli-X and Pauli-Z $N00N$ eigenstates,

$$|X_N\pm\rangle = \frac{1}{\sqrt{2}}\left(|\lambda_m\rangle^{\otimes N} \pm |\lambda_M\rangle^{\otimes N}\right) \tag{4.8}$$

$$|Z_N+\rangle = |\lambda_M\rangle^{\otimes N} \tag{4.9}$$

$$|Z_N-\rangle = |\lambda_m\rangle^{\otimes N}, \tag{4.10}$$

Charlie applies the unitary operators $U_{m\pi/N}$ and $U_{\phi+m\pi/N}$,

$$U_{m\pi/N}\,|Z_N\pm\rangle = U_{\phi+m\pi/N}\,|Z_N\pm\rangle = |Z_N\pm\rangle \tag{4.11}$$

$$U_{m\pi/N}\,|X_N\pm\rangle = \begin{cases} |X_N\pm\rangle, & \text{if } m \text{ even} \\ |X_N\mp\rangle, & \text{if } m \text{ odd} \end{cases} \tag{4.12}$$

$$U_{\phi+m\pi/N}\,|X_N\pm\rangle = \frac{1}{\sqrt{2}}\left(|\lambda_m\rangle^{\otimes N} \pm e^{i(\phi+m\pi/N)}\,|\lambda_M\rangle^{\otimes N}\right) \tag{4.13}$$

N times, once to each qubit, and Bob performs measurements in the Pauli-X and Pauli-Z basis.

Each Pauli-X eigenstate is sent with equal probability and each Pauli-Z eigenstate is sent with a different but equal probability. This ensures that the density function from

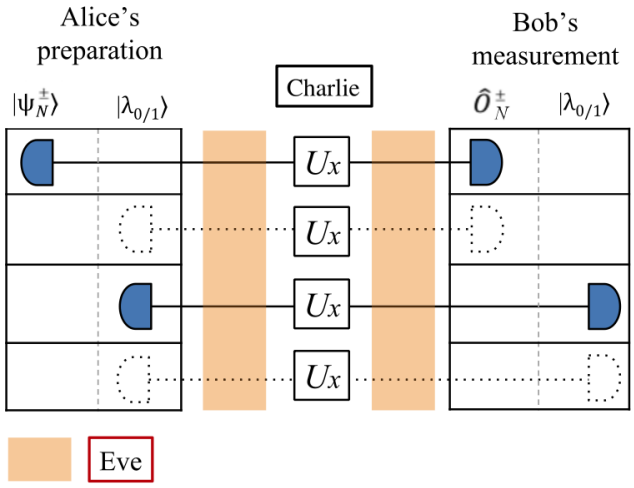

Figure 4.4: A three party SQRS scenario where each of the steps of a remote quantum metrology protocol is done by a different party. Alice sends either phase sensitive states $|\Psi_N^{\pm}\rangle$ or decoy states $|\lambda_{0/1}\rangle$ into the quantum channel which encodes the parameter φ onto the probes. Charlie implements the unitary $U_x, x \in \{\varphi + \frac{\pi m}{N}, m\pi/N\}$. Bob randomly chooses to measure the observable $\hat{O}_N^{\pm}$ or projects onto one of the four basis of the decoy states. They retain only the copies for which their choice of basis agree, denoted by the solid blue markers. The probes are also subjected to possible manipulation by an eavesdropper, Eve, denoted by regions shaded orange.

an eavesdropper's perspective is proportional to the identity matrix ensuring that she has zero quantum Fisher information and therefore can't gain any information about the phases being measured with those states from the measurement results.

The Pauli-X eigenstates are phase sensitive so, they are used for standard phase quantum metrology $N00N$ state enhanced quantum metrology [66, 90, 91]. The Pauli-Z eigenstates are not phase sensitive so they are decoy states used only to verify if an eavesdropper has attacked the quantum channel.

Figure 4.4 shows a three party protocol where Alice creates states, Charlie encodes phases and sets decoy states and Bob measures the states. It proceeds by the following steps:

1. Alice prepares and $|X_N\pm\rangle$ or $|Z_N\pm\rangle$ state chosen at random and sends the first qubit to Charlie.

2. Charlie applies one of two unitary operators $U_{m\pi/N}$ and $U_{\phi+m\pi/N}$, the same operator for each member of the entangled state.

3. Bob independently chooses to measure in the X or Z basis.

4. Alice declares the basis of each state. Bob checks the correlations for the Pauli-Z states to verify for Eve. If they are perfectly correlated, they continue the protocol. When Alice and Bob use a Pauli-Z state and a Pauli-Z measurement there is a 1/4 probability of detecting a measure and resend attack.

5. Charlie reveals on which of the remaining states he applied $U_{m\pi/N}$. Alice reveals whether she applied $|X\pm\rangle$ to each of these states and they check for correlations with Bob's results. They stop if there is not perfect correlation. This step protects against Eve biasing the measurement by adding a phase.

6. Charlie discloses the value of m for the states on which he applied $U_{\phi+m\pi/N}$. For Bob to gain information on the phases, Alice reveals some of the remaining states. For Alice to gain information on the phases, Bob reveals his measurement results for the remaining states.

This can be simplified into a protocol where Alice performs both the state preparation and measurement which can provide more information gain because Alice can always choose to measure in the same basis as the original state. This is a scenario where the classical information does not need to be protected as it is held by the party that is meant to be able to interpret it.

It can also be adapted to a scenario where security is distributed such that additional parties are involved and that all the parties can only interpret the results when they meet and collaborate by distributing extra entangled qubits to the additional parties. However, this requires Bob and all of the third parties to perform the same measurements at the same time using QKD. In all of these protocols Eve can attack the quantum channel between any two parties.

4.5.2 Quantum metrology with delegated tasks

These same principles have been used to make protocols for phase estimation with delegated tasks and untrustworthy parties where one or both of the state preparation and measurements are delegated to an untrustworthy party [88]. Delegated state preparation is achieved using well known state verification protocols [89, 92–97].

Delegated measurement security is achieved by Alice preparing qubits with the parameter encoded and flag qubits then using random Clifford operations to encrypt the states before sending them for measurement, telling the measurer what measurement to use, and

uses classical post-processing to decrypt the measurement results to verify the flag qubits for security and the other qubits to estimate the parameter.

Delegated state preparation and measurement is achieved similarly, Alice requests a specific set of stabiliser states (eg eigenstates of I, X, Y or Z) from a third party then, similar to Charlie in the last protocol, encodes a phase on one of those states, chosen at random, leaving the others to be used as flag qubits performs Clifford operation encryption then proceeds in the same way as the delegated state measurement protocol.

These protocols rely on the party performing the measurements to do so in the proscribed basis and attacks to be performed before that step. A quadratic increase in qubit number is required when the measuring party can use any measurement. As these protocols ensure that when the quantum state measuring party performs the agreed measurement, attacks can only occur between the state encryption and state measurement and (when applicable) the ordering of the initial state and the initial state arrival, they could, in the case of a trusted state measurement party, be analysed from a different perspective where an eavesdropper could attack the quantum communication channels in a MIM attack instead of or in addition to using an untrusted party.

However, like the BB84 QKD protocol the delegated measurement protocol is declared publicly making which makes it more fragile to some attacks by eavesdroppers. Firstly, photon splitting attacks would be undetectable without additional security steps. Chapter 7 show how the protocols developed in this thesis are better protected against photon splitting attacks than protocols that, like BB84 declare their measurement protocol. Secondly, further precautions must be taken so that an eavesdropper cannot not know the decryption protocol while they have access to states in the quantum channel to avoid undetectable MIM attacks. This could be mitigated by using a quantum memory at the measurer site, using another cryptographic protocol such as QKD to share the decryption protocol or if measuring party chose the Clifford decryption at random or not perform any decryption before measuring the state but it would significantly reduce the rate of both fidelity checks and information gain.

When both measurement and state creation are delegated there is little information privacy to the protocol. Both the initial states and the final measurement results are made public. So, even though the identity of the state on which the parameter is encoded is kept secret, when it gives a result that does not correspond to the publicly declared initial state it is revealed. As the initial states are evenly distributed around the Bloch sphere this is sufficient to perform some parameter estimation. As long as Alice chooses the states

on which to encode uniformly at random (or any alternative decision making at this step where the rate of each initial state being encoded is known) Eve can estimate the number of times that each state does not give such a result for each initial state allowing her to gain even more information.

However, when the party that is encoding the parameter is meant to gain the information then privacy can always be assured for the same reason that the it cannot be assured when this step is delegated to an untrustworthy party or performed at a remote site without state fidelity checking for each quantum channel. It is sufficient to add a random, secret phase to ensure that no other party can interpret the phase based on the measurement results and/or initial states. From this perspective cryptographic quantum metrology protocols where the party encoding the parameter is meant to gain the information are are easy to make private. Integrity can be assured by using performing fidelity checks on flag states and ensuring that flag and parameter encoded states are indistinguishable.

4.5.3 Higher dimensional cryptographic quantum metrology

SQRS with integrated security can also be achieved without using decoy states. One protocol uses a set of indistinguishable pairs of orthogonal states with with equal probability of each member of an orthogonal pair to allow Alice to transfer phase information to Bob using states that she produces using higher dimensional states [10]. This protocol follows the following steps:

- Alice prepares uniformly at random the states $|\pm jk\rangle = (|j\rangle \pm |k\rangle)/\sqrt{2}$ with $j \neq k$ and $j, k \in \{1, 2, 3, ..., d\}$, applies the phase operator $|j\rangle\langle j| + e^{i\phi}|k\rangle\langle k|$ and sends it to Bob.

- Once Bob has received the state Alice classically communicates j and k and Bob performs the measurement

$$E_0 = I - E_{1+} - E_{1-} \qquad E_{1\pm} = \frac{1}{2}(|j\rangle \pm |k\rangle)(\langle j| \pm \langle k|) \tag{4.14}$$

- Bob tells Alice the measurement result. If Bob measures E_0 it signifies an eavesdropper and they stop the protocol.

- Repeat the above enough times for metrology purposes.

- Alice tells Bob the measurement basis and Bob estimates the parameter.

By changing $\phi \to N\phi$ or $|j\rangle \to |j\rangle^{\otimes N}$ this can be adapted for quantum enhanced metrology of the phase ϕ. Otherwise, it can be adapted for multiple parameters that

are each sensitive to different dimensions by sending states of the form $(|k_0\rangle + e^{i\phi_1}|k_1\rangle + e^{i\phi_2}|k_2\rangle + ... + e^{i\phi_m}|k_m\rangle)/\sqrt{m+1}$ where $m < d$ and Bob measuring in the basis $E_{j\pm} = \frac{1}{2}(|k_0\rangle \pm |k_j\rangle)(\langle k_0| \pm \langle k_j|)$ and $E_0 - \sum_{j=1}^{d}(E_{j+} + E_{k-})$.

Privacy is ensured firstly because Eve cannot interpret the classical information and secondly because when performing a replace attack on the quantum channel she can conceal the attack with probability $\left(\frac{2}{d}\right)^{\eta}$ for η attacked states by sending states from the set $|\pm jk\rangle$ or $\left(\sum_{j=1}^{d}|j\rangle\right)/\sqrt{2}$ leading to a detection probability approaching 1 as η and d increase.

Integrity is ensured because Eve cannot know which dimensions $\{j,k\}$ a state is in. So, the best she can do is introduce a bias $\Delta\phi_{jk}$ to some j,k. However, if she does not add a bias with the same expectation value $\langle\Delta\phi_{jk}\rangle$ to all $\{j,k\}$ combinations then this could be detected (with large enough data) because of the inconsistencies between the parameter estimations of the different would eventually lead to detection. To avoid this Eve must add phases with the same $\langle\Delta\phi_{jk}\rangle$ for all j,k combinations including $k \leftrightarrow j$. As $\langle\Delta\phi_{jk}\rangle = \pm\langle\Delta\phi_{kj}\rangle$ then $\langle\Delta\phi_{jk}\rangle = 0 \forall j,k$. This means that Eve cannot introduce bias without risking detection.

However, this does not restrict the $\Delta\phi_{jk}$ applied to individual rounds which can be used to increase the estimation uncertainty, reducing the information gain. Thorough data analysis could be used to detect this attack by comparing the estimation uncertainty to the distribution of estimation uncertainties for the data used in the ideal case. This protection does not exist for the multiparameter protocol because Eve could choose to bias any one parameter and there would not be another to check against.

Like the BB84 QKD protocol and the quantum metrology with delegated tasks protocols this protocol requires that the measurement protocol is publicly declared which brings the same security concerns and has the same resolutions with the knock on effect of reducing the information gain of the entire protocol relative to the resources used. This has been discussed already in the context of quantum metrology with delegated tasks. In this case, while the chance of detecting an eavesdropper when using the correct measurement increases with d, the chance of performing the correct measurement is inversely proportional to d for both fidelity checks and parameter estimation.

4.6 Chapter summary

This chapter provides the necessarily background so that the reader can understand the cryptographic principles that are used to secure remote quantum metrology protocols.

It introduces cryptography in general and quantum key distribution with a particular discussion of the well regarded BB84 protocol which shares some of its security principles with the SQRS protocols developed in chapters 5, 6 and 7. Then it provides a thorough review of different SQRS scenarios and protocols with a particular focus on the different methodologies used to make the protocols secure.

The novel protocols introduced in this thesis in chapters 5 and 6 aim to have Alice gain information about an unknown parameter or a function of unknown parameters where each parameter is held by a remote Bob. Alice is responsible for creating the initial states and each Bob is responsible for encoding their phase and measuring the states.

To ensure security these protocols need to fulfil the two conditions set out in this chapter. The first is that Eve cannot gain any information from the classical information, often achieved by ensuring that the average density function of quantum states exposed to Eve is proportional to the identity matrix which can be achieved by sending orthogonal states with equal probability.

The second condition is that Eve cannot manipulate the quantum channel without being detected. This can be achieved by using QKD however, relying on a separate protocol for security is not in the spirit of SQRS and restricts the applicable scenarios to those where Alice and Bob can both perform their part of a QKD protocol. Furthermore, in situations where Bob can maintain local classical information security, it is necessarily advantageous over Bob performing metrology on his own and communicating the results to Alice using QKD. Otherwise, it is ensured by sending indistinguishable states through the quantum channel and performing sufficient fidelity checks on the states.

In chapters 5 and 6 this is achieved by Alice sending the four Pauli-X and Pauli-Y eigenstate qubits or similarly encoded entangled qubit states with equal probabilities and having Bob(s) performing fidelity checking measurements (without encoding the phase) in both the Pauli-X and Pauli-Y basis. These protocols are set up to have integrated security against all of the attacks that previous protocols defend against while optimising the information gain. As Bob encodes the parameter and performs the measurement no decoy states are required so the protocol only uses phase sensitive states which increases information gain relative to the total resource use. As the fidelity checks are chosen at random by Bob, it also only uses two indistinguishable orthogonal pairs of states, the least possible amount, to minimise the rate of fidelity checks performed in the wrong basis. Those chapters go further than the protocols discussed in this chapter by quantifying information privacy using limited data quantum metrology and the amount of information

Eve could steal before being detected.

Chapter 7 focuses on the security of the protocols. It provides more analytical security proofs for the second security condition. It also introduces a third security condition. This chapter states that it is preferable not to use separate cryptography protocols to aid a cryptographic quantum metrology protocol, particularly in reference to QKD, and that it is better for all of the security to be integrated into one protocol. All of the protocols in this chapter and those introduced in chapters 5 and 6 explicitly or implicitly assume authentication of the classical communication channel. Chapter 7 shows how to adapt those protocols using quantum encoded shared secrets and path information delays to protect against manipulations of the classical communication channel so that they don't require any other authentication and have all of the security features integrated into a single quantum protocol.

Chapter 5

Two party secure quantum remote sensing

Two of the most promising quantum technologies are quantum metrology and quantum communications. In the former, quantum correlations are used to measure quantities with a precision beyond what could be achieved by any classical means with the same resources [38]; in the latter, the properties of quantum states are used to create secure communication channels [98]. Cryptographic quantum metrology protocols use the cryptographic principles that underpin secure quantum communication protocols to provide information privacy and integrity to metrology protocols.

Secure quantum remote sensing (SQRS) is a family of protocols where some party gains information about a parameter held at a remote site. Sometimes this is expressed in the same language as delegated quantum computing with a client asking a server to help them measure a parameter in a way that only the client can gain information about the parameter. Otherwise it is expressed in the terminology of quantum key distribution where one party, Alice, produces quantum states and another, Bob, measures them with the parameter being encoded by one of those parties or a further third party, Charlie, and some party(ies) that does not encode the parameter designated to gain information about the parameter. A malicious party aiming to steal (privacy) or spoof (integrity) information has access to the communication channels between the parties, they are considered public.

The first condition for security is that an eavesdropper cannot gain any information from the publicly available classical measurement results. This allows an expansion of the domain of applicable scenarios to those where Alice is intended to gain the parameter information and Bob is not secure from eavesdropping. In situations where Bob is intended

to gain the parameter information this remains a condition. This condition is fulfilled by ensuring that Eve's knowledge of the quantum states travelling between Alice and Bob can reveal no information about the parameter to her. This is achieved by using independent and identically distributed states that average to be proportional to the identity matrix. SQRS protocols do this by sending some of the particles from a larger entangled state [6, 11, 13, 15] or orthogonal quantum states with equal probability [8, 10, 16, 17] and keeping some information about the individual states secret. Even if the states that can be used for parameter estimation and the probability of each being used for each round is public, while they average to a density function proportional to the identity matrix and each individual state is maintained secret this condition is fulfilled.

The second security condition is that an eavesdropper cannot manipulate the quantum states in transit to aid in eavesdropping or spoofing without risking detection. As discussed in chapter 4, this could be achieved with small changes to existing theoretical [11] and experimental [13] protocols that use entanglement. Alternatively, it has been shown theoretically without using entanglement, instead using sets of indistinguishable states [8, 10, 16, 17].

This chapter is about a SQRS protocol that is adapted to perform remote quantum metrology of a single parameter held at a remote site as efficiently as possible while maintaining a predetermined security standard. Alice produces quantum states that she sends to Bob for parameter interaction and measurement. Alice alone is intended to interpret the parameter. The security for the first condition is shown analytically.

Previous protocols [8, 10] that fulfil the second condition do so by demonstrating that, with large enough amounts of data, there is information asymmetry between Alice/Bob and Eve because each quantum state that she manipulates in a man in the middle attack exponentially decreases the probability of going without detection. However, this has limited value because it does not account for how much information could be stolen before Eve is detected. This chapter goes further; first, by setting out the amount of information gain in limited data. Then, it sets a privacy limit as a function of the proportion of the resources used for verifying for the presence of Eve. Furthermore, the ability to perform quantum enhanced measurement and how this may be used to further enhance security is demonstrated and discussed.

The focus of this chapter is to set out the fundamental SQRS protocol for the secure estimation of a single parameter at as single remote site that fulfils the same two security conditions as previous protocols while optimising information gain and providing rigorous

privacy limits. Chapters 6 and 7 extend this work to functions of parameters distributed over remote networks and further security proofs respectively.

The chapter begins by introducing the basic SQRS protocol step by step and with a diagram. Then, it gives an introduction to the metrology aspects. First, it calculates the probabilities of the different measurement outcomes and then uses the resultant classical Fisher information and the range for which the likelihood function is unique to set out why the chosen protocol is optimal for estimating in a 2π range when there is sufficient data. Then, it discusses when the asymptotic limit is reached, when it is appropriate to use the Fisher information and why the parameter estimation methodology used is appropriate for limited data. It sets out a measure of the information gain that is applicable in the limited data regime and a secure method of achieving quantum enhanced parameter estimation using multiple parameter interactions for each probe.

The chapter ends with a discussion of the protocol security. The first security condition is achieved by making the classical information unintelligible to Eve. The second is qualified for information privacy and integrity by demonstrating that any attack by Eve, to steal information or spoof it is exponentially likely to be detected with increasing number of attacks. The information privacy is quantified by using the distribution in the number of attacks before Eve is detected to find a distribution of her average limited data information gain as a function of the ratio of resources used for security checks. Alice's information gain as a function of the number of protocol rounds is demonstrated for various security limits. Finally, there is a discussion quantum enhanced parameter estimation and prior information and how the information asymmetry between Alice and Eve is at least maintained and may be increased when they have different prior informations and Bob uses multiple parameter interactions for each probe.

5.1 Protocol

The basic SQRS protocol is illustrated in figure 5.1. This is a situation where Alice wants to make a measurement remotely at Bob's location without revealing the result to Bob or any eavesdropper, Eve. Alice and Bob share both public quantum and classical communication channels, each of which may be subject to eavesdropping or other external influences. As with similar previous protocols [8–13], Bob can be trusted to follow Alice's instructions. However, he is not required to be a secure node so, his classical information may be stolen without repercussions. Regardless, that information is sent through an un-encrypted classical communication channel making it available to Eve. All details of

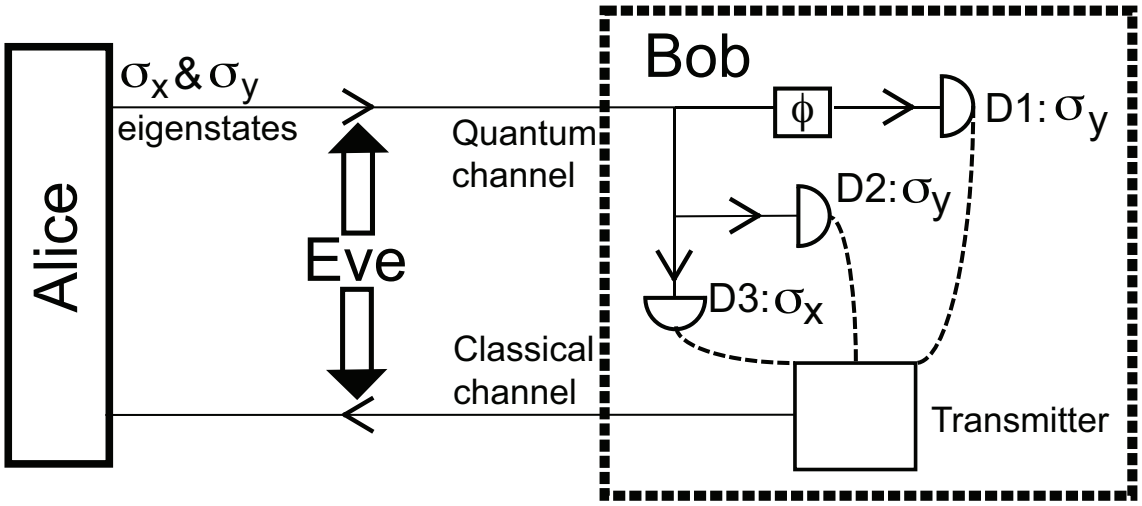

Figure 5.1: Schematic of the secure remote quantum sensing protocol. Alice sends eigenstates of σ_x and σ_y chosen uniformly at random through a quantum channel to Bob. Bob chooses at random either to encodes the parameter of interest, ϕ, on the qubit and measures at D1 in the σ_y basis or measures in the σ_y or σ_x basis D2 and D3 without encoding ϕ. The measurement results and the detectors they correspond to are sent to Alice through a classical channel. Eve can attack the quantum and classical channel to try to gain information about ϕ.

the protocol can be known publicly apart from what state Alice chooses on any given realisation and, of course, the value of the parameter ϕ being measured. The protocol could be applied using any qubits, for instance polarisation encoded photons.

Alice sends appropriately chosen quantum states to Bob through an insecure quantum channel. These are the eigenstates of the Pauli σ_x and σ_y operators, for reasons discussed in the next section. The range of different states and their probabilities can be public but the state of each particular instance is kept hidden by Alice. This assumes that there is sufficient timing and authentication agreement for Alice and Bob to agree on which qubit is which.

At Bob's end the qubits are sent down one of two paths. The first of these paths encodes the parameter of interest, ϕ, on the quantum state and then a measurement is made at detector D1 in the σ_y basis. The second path measures the state directly in the σ_y and σ_x basis at D2 and D3 without encoding ϕ. This serves as a test to verify the fidelity of the qubit states. The outcomes for each measurement and the corresponding detector are sent to Alice publicly through the classical communication channel. Alice performs a Bayesian analysis of the results of each path both to check the fidelity of the states arriving at Bob and to estimate the unknown parameter. In a noiseless scenario

with a possible eavesdropper erroneous fidelity checks signals a man in the middle attack, in a noisy scenario this could be due to the noise.

The detector that each qubit travels to is chosen at random once the qubit arrives at Bob and Eve can no longer interact with it. This ensures that Eve cannot selectively interact with qubits that will be used for parameter estimation. When interacting with qubits in the quantum channel she must take the risk that the qubits that she interacts with are sent to fidelity checking detectors and her presence would be revealed.

5.2 Metrology

This section discusses the metrology aspects of the protocol. Initially, the Fisher information of the protocol is set out and used to help explain the choice of quantum states and measurements. Then, the parameter estimation methodology is set out. This methodology is demonstrated to be appropriate in both the asymptotic limit and limited data. A limited data measure of information gain is introduced and a method for calculating it using Monte Carlo simulations is discussed. Finally, a method of performing quantum enhanced measurements that does not compromise security is given and it's potential effectiveness is demonstrated.

5.2.1 Measurement probabilities and Fisher information

In order to understand how much information Alice gains in the SQRS protocol and why the Pauli-X and Pauli-Y eigenstates and measurements optimise this, consider a general pure state qubit $\cos(\theta/2)\left|0\right\rangle + \sin(\theta/2)e^{i\chi}\left|1\right\rangle$ with $\theta, \chi \in \mathbb{R}$, that she sends to Bob. This is passed through a phase gate at Bob's end with the unknown parameter ϕ, changing the state to $\cos(\theta/2)\left|0\right\rangle + \sin(\theta/2)e^{i(\chi+\phi)}\left|1\right\rangle$. Since Alice knows θ and χ, any publicly transmitted measurement data about $(\chi+\phi)$ would enable Alice to find ϕ, but any party without knowledge of χ would not be able to do so.

Suppose that Bob measures the photon at D1 in the basis $\{+1,-1\} = \{\cos(\vartheta/2)\left|0\right\rangle + \sin(\vartheta/2)e^{i\varphi}\left|1\right\rangle, \sin(\vartheta/2)\left|0\right\rangle - \cos(\vartheta/2)e^{i\varphi}\left|1\right\rangle\}$. The probabilities of these two outcomes are

$$P(\pm 1|\phi) = \frac{1}{2}\left(1 \pm \cos(\theta)\cos(\vartheta) \pm \sin(\theta)\sin(\vartheta)\cos(\zeta)\right), \tag{5.1}$$

where $\zeta = \chi + \phi - \varphi$.

In the asymptotic limit of many measurements, μ, the precision with which Alice can

estimate ϕ is given by the classical Fisher information

$$\mathcal{I}(\phi) = \sum_i \frac{1}{P(i|\phi)} \left(\frac{\partial P(i|\phi)}{\partial \phi} \right)^2, \tag{5.2}$$

and the corresponding Cramér-Rao bound

$$\delta\phi \geq \frac{1}{\sqrt{\mu \mathcal{I}(\phi)}}. \tag{5.3}$$

The classical Fisher information for the measurement Bob makes is

$$\mathcal{I}(\phi) = \frac{\sin^2(\theta)\sin^2(\vartheta)\sin^2(\zeta)}{1 - \cos^2(\theta)\cos^2(\vartheta) - \sin^2(\theta)\sin^2(\vartheta)\cos^2(\zeta) - \cos(\theta)\cos(\vartheta)\sin(\theta)\sin(\vartheta)\cos(\zeta)}. \tag{5.4}$$

This has a maximum value of unity when $\theta = \vartheta = \pi/2$, corresponding to states and measurements in the σ_x-σ_y plane of the Bloch sphere. Chapter 2 demonstrates that quantum Fisher information for the general pure state considered here, $\cos(\theta/2)\,|0\rangle + \sin(\theta/2)e^{i\chi}\,|1\rangle$, is also unity, meaning that this metrology protocol is optimal over all possible measurements because the classical Fisher information saturates the quantum Fisher information. Alice and Bob therefore choose to operate in this plane. The same choice of states and measurements is effective on the other path for verifying that the fidelity of the states is maintained through the quantum channel.

To maintain security, Alice could use any set of symmetric states in this plane and corresponding probabilities so that they average to an identity density matrix. For consistency with previous work and to make it easier to understand, in this basic SQRS protocol Alice uses eigenstates of the σ_x and σ_y operators with equal probabilities, which she sends to Bob who makes measurements in the σ_y basis. The probabilities for Bob to obtain the two different measurement outcomes, given the four possible states that Alice sends, are given in table 5.1.

Suppose that in a given experiment with μ measurements, the number of results for each of the outcomes with probabilities given in table 5.1 is $\{n_j\}$, where $j \in \{1, 2, ...8\}$ and $\mu = \sum_j n_j$, a Bayesian approach gives Alice's likelihood function for ϕ,

$$\mathcal{L}(\phi) \propto (1 + \sin\phi)^{n_1+n_4}(1 - \sin\phi)^{n_2+n_3} \times (1 + \cos\phi)^{n_5+n_8}(1 - \cos\phi)^{n_6+n_7}. \tag{5.5}$$

It can been seen from table 5.1 that the measurement outcome probabilities for the σ_x and σ_y eigenstates depend only on $\sin(\phi)$ and $\cos(\phi)$ respectively. This means that any estimation based solely on one basis such as those used previously [11] for the detection of small phases, can only estimate the parameter in a π range because they give rise to symmetric likelihoods in the 2π range as demonstrated by figure 5.2. For initial states

Eigenstate	**Measurement outcome**	
	$\sigma_y = +1$	$\sigma_y = -1$
$\sigma_x = +1$	$p_1 = \frac{1}{2}(1 + \sin\phi)$	$p_2 = \frac{1}{2}(1 - \sin\phi)$
$\sigma_x = -1$	$p_3 = \frac{1}{2}(1 - \sin\phi)$	$p_4 = \frac{1}{2}(1 + \sin\phi)$
$\sigma_y = +1$	$p_5 = \frac{1}{2}(1 + \cos\phi)$	$p_6 = \frac{1}{2}(1 - \cos\phi)$
$\sigma_y = -1$	$p_7 = \frac{1}{2}(1 - \cos\phi)$	$p_8 = \frac{1}{2}(1 + \cos\phi)$

Table 5.1: The measurement probabilities p_j when Alice sends σ_x and σ_y eigenstates to Bob who encodes ϕ on them and measures in the σ_y basis. The number of times that Bob gets a result corresponding to each p_j is n_j.

$\{\theta = \pi/2, \chi\}$ and measurements $\{\vartheta = \pi/2, \varphi\}$ the measurement outcome probabilities are $P(\pm) = \frac{1}{2}\left(1 + \cos(\chi + \phi - \varphi)\right)$ producing likelihood functions with lines of symmetry at $(\chi - \varphi) + k\pi \ \forall k \in \mathbb{N}$.

This ambiguity can be addressed by using multiple sets of $(\chi - \varphi)$. In particular, using two sets of states that are perpendicular to each other in the Bloch sphere, $(\chi - \varphi)$ and $(\chi - \varphi + \pi/2)$, like this metrology protocol does allows for estimation over the full 2π range. An additional reason for using both σ_x and σ_y states is security. If Alice always sends states from just one of these sets e.g. $\sigma_x = \pm 1$, and that set is publicly known, Eve could measure in this basis without changing the state and so implement a measure and resend attack without being detected.

When considering the entire SQRS protocol including the fidelity checking the phase estimation n_0 may be used with occurrence probability F corresponding to the probability of a fidelity check that doesn't contribute to $\mathcal{L}(\phi)$ The probability of n_j with $j \in \{1, 2, ...8\}$ occurring is reduced by a factor of $1 - F$ with $\mu = \sum_{j=0}^{9} n_j$ as the number of protocol rounds. This reduces the Fisher information relative to the number of protocol rounds by the same amount with a Fisher information $\mathcal{I}(\phi) = 1 - F$.

5.2.2 Limited data

When there are a large number of measurements such as in [13], the Fisher information and Cramér-Rao bound are appropriate for quantifying the precision with which Alice can determine ϕ. However, it is important to explore what happens when there is not enough data to reach that asymptotic limit, not least because sending many copies of the same information represents a security risk; Eve would only need to be able to access a tiny

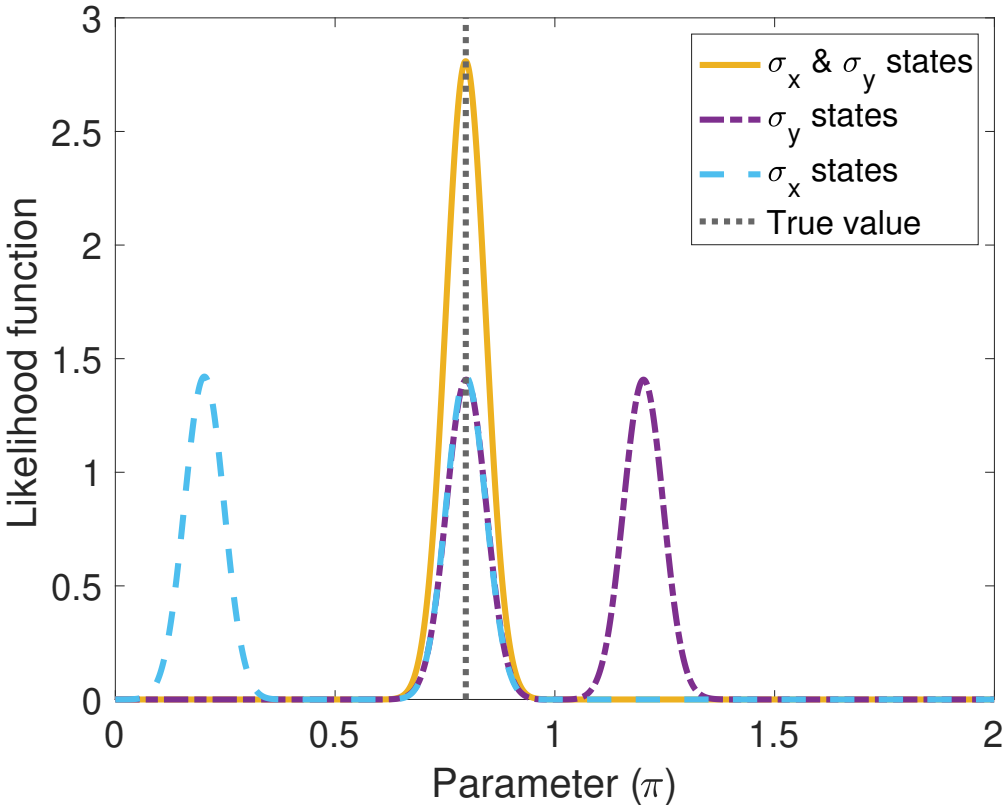

Figure 5.2: Alice's mean likelihood function as given by equation (5.5) with $\mu = 100$ (averaged over 10^3 realisations) and compared with the true value of ϕ. Results are shown when Alice only sends σ_x states or σ_y states. In both these cases there is a periodicity over the 2π range, which creates an identifiability problem. By using both σ_x and σ_y states a single peak corresponding to the true value can be identified.

fraction of the copies to still be able to gain significant information about ϕ. Previous studies have explored how quantum metrology can be applied when there are a limited number of measurements [99–101] and so does this work.

For a set of measurement results, $\{n_i\}_{i=1}^{8}$, the likelihood function is given by equation (5.5). In the asymptotic regime this has a shape similar to a normal distribution becoming increasingly narrow with increasing data, a mean corresponding to the true value of ϕ and a variance given by the inverse classical Fisher information. This makes the maximum of the likelihood function a useful estimator. However, limited data estimators drawn from the likelihood function or some posterior distribution may be biased and have a large variance, meaning that the circular support with a period 2π of phase parameters must be accounted for.

When a posterior distribution is non-negligible over the 2π support, the choice of

where to cut the circular support to superimpose it on a flat support and the wrapping of the likelihood function become important and affect the statistics drawn from that distribution [64]. Previous works on SQRS protocols for phase estimation were restricted to large data [8, 10, 13] and parameters close to zero [11] so did not need to take this into account. The circular statistics used here are introduced in chapter 3. In an attempt to be give results applicable to the most general set of prior information scenarios, this Bayesian analysis considers statistics of the entire posterior distribution using minimal prior information, the circular uniform distribution, $P(\phi|\alpha) = \frac{1}{2\pi}\ \forall \pi \in [0, 2\pi)$.

The first statistical degree of freedom for a distribution is the bias. The average bias varies with the true value as shown in figure 5.3. It is sufficiently small that it can be estimated linearly using a 2π range centred on the true value.

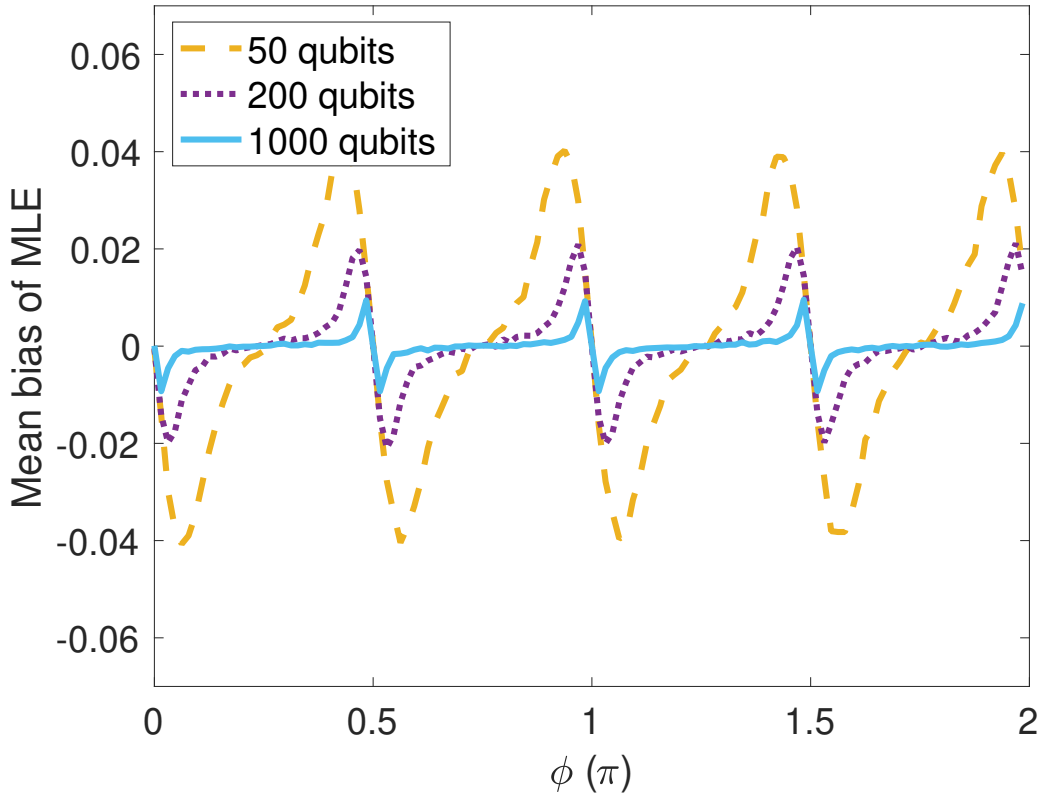

Figure 5.3: The mean bias of Alice's maximum likelihood estimator from the true value of ϕ, shown as a function of ϕ for different total numbers of qubits, μ, used on the measurement path, D1. The bias depends on ϕ but decreases as the number of measurements increases.

The second degree of freedom is the dispersion. The standard deviation is the standard symmetric measure of dispersion; it shows the width of a distribution. In the asymptotic

limit these distributions are narrow enough for the standard deviation to be appropriate but, with low data, the distributions are non-negligible on a full 2π range making it inappropriate. The circular statistic that has a value closest to the linear standard deviation is the circular standard deviation $\nu \in [0, \infty)$ introduced in chapter 3; they are equal in the asymptotic limit. Therefore, this is the most appropriate measure of symmetric dispersion and it's average value as a function of the true value is plotted in figure 5.4. Like the bias, it varies with the true value.

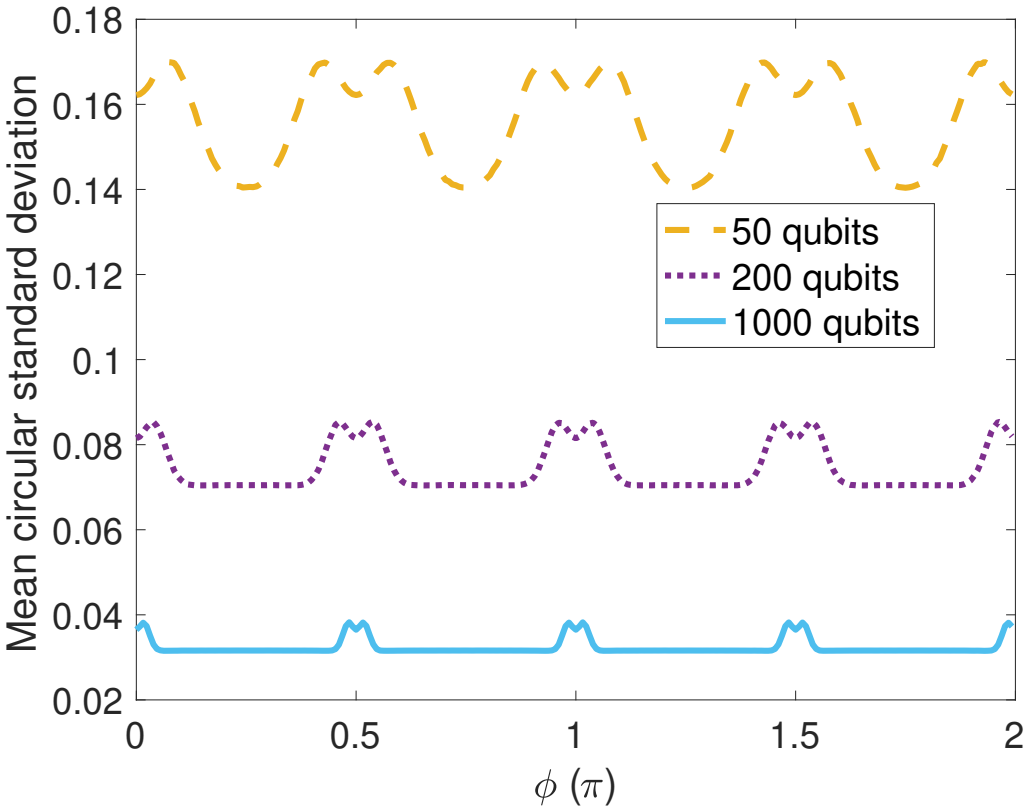

Figure 5.4: The mean circular standard deviation of Alice's likelihood function as a function of the true value of ϕ, shown for different total numbers of qubits, μ, used on the measurement path, D1. This shows that the width of the distribution depends on ϕ, but this dependence reduces as the number of measurements increases.

A comparison of figures 5.3 and 5.4 shows that, for all values of ϕ, the bias is much smaller than the width of the posterior distribution. This means that Alice's Bayesian method of estimating ϕ should also work well in the low data regime. It also shows a pattern in the average bias and average circular standard deviations. Their magnitudes are minimised and maximised for the same values of the true parameter, ϕ.

Alice can optimise her estimation by operating in regions of figures 5.4 and 5.3 that

minimise both the width of the likelihood function and the bias, i.e. avoiding regions where ϕ is close to half-integer multiples of π. She can do this if she has some prior information about ϕ. Alternatively, as the measurement progresses, Alice will build up knowledge of ϕ and can use this to shift to a preferred operating region. In the σ_x-σ_y plane the probabilities of the results can be found by substituting $\theta = \vartheta = \pi/2$ into equation (5.1) to give

$$P(\pm 1) = \frac{1}{2}\left(1 \pm \cos(\chi + \phi - \varphi)\right). \tag{5.6}$$

If Alice wants to shift her peak by χ_0 she can rotate all of her initial states $\chi \in \{0, \pi/2, \pi, 3\pi/2\}$ to $\chi \in \{-\chi_0, \pi/2 - \chi_0, \pi - \chi_0, 3\pi/2 - \chi_0\}$. This would be undetectable to all other parties and would not reveal any information she has about ϕ.

Now that this method of data analysis has been shown to be appropriate in both the large and limited data regimes it can be used to create a measure of the limited data information gain. The Cramér-Rao bound is appropriate in the asymptotic limit under the assumption that there is no bias. When this is not the case a cost function is used. The most popular cost function of linear statistics is the mean square error, $C_{\theta,\hat{\theta}} = (\hat{\theta} - \theta)^2$, which account for both bias and dispersion. It should be applied to the posterior distribution,

$$MSE(\phi, p(\hat{\phi}|\vec{n}, \alpha)) = \oint \left(\hat{\phi} - \phi\right)^2 p(\hat{\phi}|\vec{n}, \alpha) d\hat{\phi}, \tag{5.7}$$

and averaged over the distribution of $\vec{n}$ to be used as a limited data measure of information gain equivalent to the Cramér-Rao bound in asymptotic scenarios with sufficient data and no bias. The cost function

$$C_{\phi,\hat{\phi}} = 4\sin\left(\frac{\hat{\phi} - \phi}{2}\right) = \left(\hat{\phi} - \phi\right)^2 + \mathcal{O}\left(\left(\hat{\phi} - \phi\right)^4\right) \tag{5.8}$$

is often used for limited data phase estimation with minimal prior information due to it being the circular distribution that approximates the MSE with the least number of Fourier components making it the simplest function that approximates the variance for small, unbiased distributions [102]. Applying this cost function is proportional to the circular dispersion centred around the true value introduced as the circular mean square error in chapter 3, $\xi(\hat{\phi}, \phi) \sim 1 - \cos(\hat{\phi} - \phi) \sim \frac{1}{2}MSE$. $\xi \in [0, 2]$ has special values 0 corresponding to infinite unbiased information, a delta function at the true value; 1 corresponding to an equal distribution around the circle such as the minimal circular information represented by the circular uniform distribution; 2 corresponding to infinite maximally biased information, a delta function at the antipodal point from the true value.

$\xi(\hat{\phi}, \phi)$ can be used as an alternative measure of information gain by integrating over the probability distribution of the possible $\vec{n}$ to get a limited data measure of information gain for some true value ϕ (with the same prior information)

$$\Xi(\mu, \phi) = \int d\vec{n} P(\vec{n}|\phi) \oint d\hat{\phi} \left(1 - \cos(\hat{\phi} - \phi)\right) p(\hat{\phi}|\vec{n}, \alpha) \tag{5.9}$$

as a function of $\mu = \sum_j n_j$, the number of measurements, and ϕ, the true parameter value and another measure averaged over all $\phi \in [0, 2\pi)$

$$\Lambda(\mu) = \oint d\phi \int d\vec{n} P(\vec{n}|\phi) \oint d\hat{\phi} \left(1 - \cos(\hat{\phi} - \phi)\right) p(\hat{\phi}|\vec{n}, \alpha). \tag{5.10}$$

This is the average error of the posterior distribution for μ measurements. It can be interpreted in a similar way to the average mean square error of some estimator of some frequentist statistic with a certain number of measurements but applied to a circular Bayesian inference method. In this Bayesian regime it is appropriate to use the posterior distribution in place of a selection of parameter estimators. In this circular statistical regime it is appropriate as a measure of the circular dispersion about the true value that gives a statistic proportional to the mean square error for sufficiently narrow distributions. With large enough data, in the asymptotic limit, it is equivalent to the Cramér-Rao bound. This makes $\Lambda(\mu)$ an appropriate statistic to be used as a measure of information gain for this metrology protocol for all amounts of prior information and data.

The order of measurement results is inconsequential, only the final number of each result is relevant the number of possible result combinations given by equation (3.1) of chapter 3. For the metrology only there are 4 independent probabilities therefore using equation (3.1) with $m = 4$ and $n = \mu$,

$$\text{Combinations metrology only} = \frac{1}{6}(\mu + 1)(\mu + 2)(\mu + 3), \tag{5.11}$$

where μ is the number of rounds of metrology. For the whole protocol there are 5 probabilities that must be accounted for from a metrology perspective with the fifth corresponding to fidelity checks that do not contribute to the information gain,

$$\text{Combinations relevant to metrology full protocols} = \frac{1}{24}(\mu+1)(\mu+2)(\mu+3)(\mu+4), \tag{5.12}$$

where μ is the number of protocol rounds.

Figure 5.5 demonstrates that it is unfeasible to perform such an analysis for large numbers, $\mathcal{O}(10^3)$, of total measurements, even when only accounting for metrology rather than the entire SQRS protocol. To remain consistent throughout, the analysis was performed using Monte Carlo simulations where a vector of sets of measurement results with values

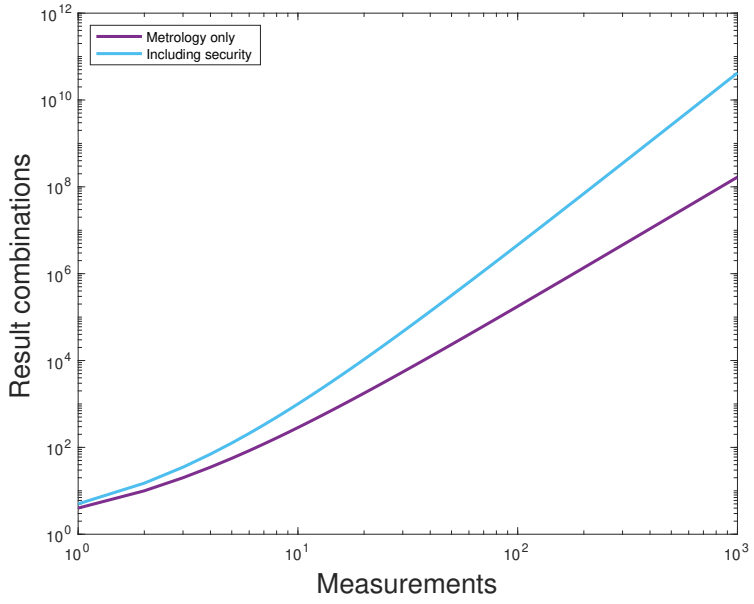

Figure 5.5: Number of result combinations for two party protocol with and without accounting for the fidelity checking. Metrology combinations only is given by equation (5.11). The number of combinations relevant to the metrology while accounting for fidelity checking probes is given by equation (5.12).

$\{\{n_j\}_k\}$ are drawn from the probability distribution and used to create statistics of the information gain. Thus, the statistics may be approximated using a grid approximation for ϕ and $\hat{\phi}$ and repeated statistical sampling for $\vec{n}_k$ to calculate

$$\Lambda_{\text{numerical}}(\mu) = \sum_{l=1}^{L}\sum_{k=1}^{K} P(\vec{n}_k|\phi_l) \sum_{j=1}^{J} \Big(1 - \cos(\hat{\phi}_j - \phi_l)\Big)\, p(\hat{\phi}_j|\vec{n}_k, \alpha), \tag{5.13}$$

where J, K, L are large, $\hat{\phi}_j = \frac{j-1}{2\pi J}$, $\phi_l = \frac{l-1}{2\pi L}$ and $\sum_j \{\{n_j\}_k\} = \mu \ \forall k$. The $\Lambda_E \geq 0$ line of figure 5.11 demonstrates the evolution of Λ, the measure of information gain averaged over the distribution of measurement results for each phase drawn from the uniform prior $p(\alpha) = 1/2\pi,\ \phi \in [0, 2\pi)$, for the metrology of the protocol only.

5.2.3 Quantum enhancement

The quantum features of the protocol can be used to give an enhancement in the measurement precision itself. This is usually achieved by making use of entangled states to improve how the uncertainty in the parameter, $\Delta\phi$, scales with N, the number of particle-parameter interactions used [38]. For unentangled particles, this goes as the standard quantum limit $\Delta\phi \sim 1/\sqrt{N}$, but with entanglement it is possible to achieve a Heisenberg scaling $\Delta\phi \sim 1/N$. A standard approach is to use $N00N$ states that were developed [103],

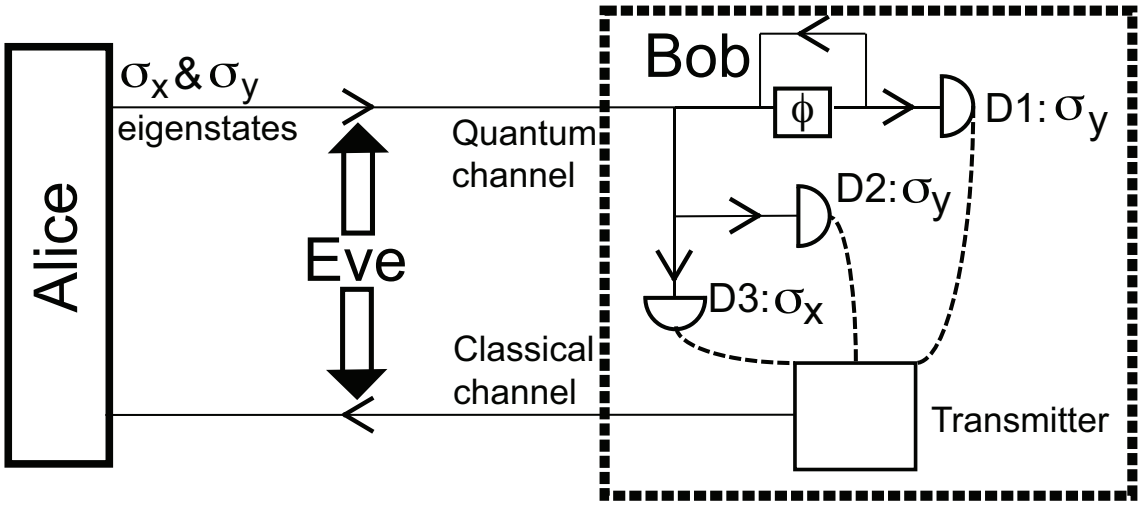

Figure 5.6: Schematic of the secure remote quantum sensing protocol with multiple passes. The protocol proceeds in the same manner as in figure 5.1 with the addition of Bob having the ability to choose to increase the amount of interaction with the parameter. For some implementations, such as measuring magnetic fields, this could be done by controlling the interaction time. Otherwise, it could be done by passing the probe through the phase as shown in this diagram. With photons, for instance, Bob could control this be choosing to place and remove mirrors before on the path either side of the object being probed to create a loop and maintain that loop for the number of passes he chooses.

popularised [104], and named [105] by Jonathan Dowling. These have the form

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|N,0\rangle + |0,N\rangle\right). \tag{5.14}$$

If one mode is subjected to a phase, ϕ, this adds coherently for all N particles, giving

$$|\psi\rangle = \frac{1}{\sqrt{2}}\left(|N,0\rangle + e^{iN\phi}\,|0,N\rangle\right), \tag{5.15}$$

which has a quantum Fisher information with respect to ϕ of N^2, leading to a possible scaling in the measurement precision of $\Delta\phi \sim 1/N$. $N00N$ states have the disadvantage of being fragile to loss and difficult to create. Despite this, experiments have demonstrated them in the laboratory and shown their improved scaling for measurements [106–108].

Practical, noisy applications of the protocol would be limited by the amount of noise both for the information gain and the security which would make $N00N$ states impractical. Instead, here is an entanglement-free protocol for Heisenberg-limited phase estimation that is very much in the spirit of this SQRS protocol and can easily be applied to it [66] without compromising security or many of the issues with $N00N$ states. The idea behind this quantum enhancement is simply that Bob passes the state he receives from Alice

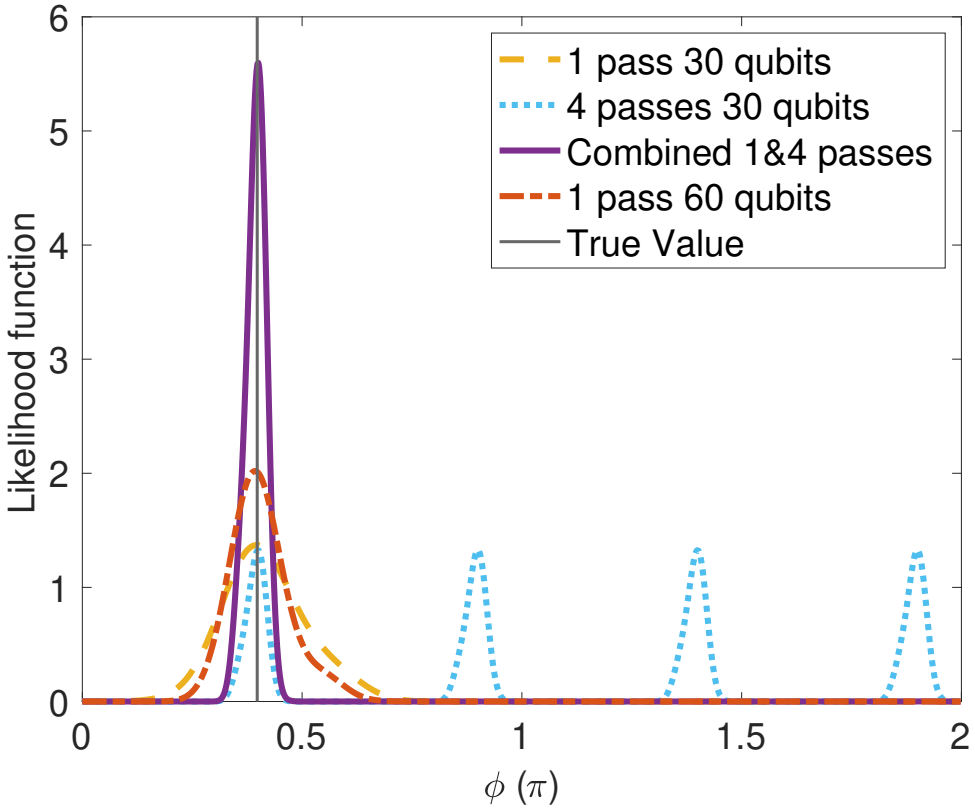

Figure 5.7: The mean likelihood functions averaged averaged 10^4 times for different single-pass and 4-pass measurement strategies. Combining the results from 30 qubits with a single pass and 30 qubits with 4 passes gives a significant advantage over using all 60 qubits for a single pass estimation.

through ϕ multiple times or interacts the qubit with the phase containing Hamiltonian for a longer time before measuring it. For m passes (or an m-fold increase in interaction time) this replaces ϕ with $m\phi$ in the states and corresponding detection probabilities, meaning that the Fisher information is enhanced by a factor of m^2, as can be seen from equation (5.2) or calculated using the eighth property of the quantum Fisher information given in chapter 2. This is a multiplicative factor so it would not allow Eve to gain any knowledge of the parameter ϕ from the classical measurement results under the same conditions that give her a Fisher information of zero for single passes through the sample.

While this is a simple and convenient way of gaining an m-fold enhancement in measurement precision, it has the disadvantage of creating m equally spaced peaks in the likelihood function over a 2π range. The problem with this is that Alice can be left with an identifiability problem where she knows that one of the peaks is correct but not which one. There are different ways of dealing with this [90]. If Alice has prior information

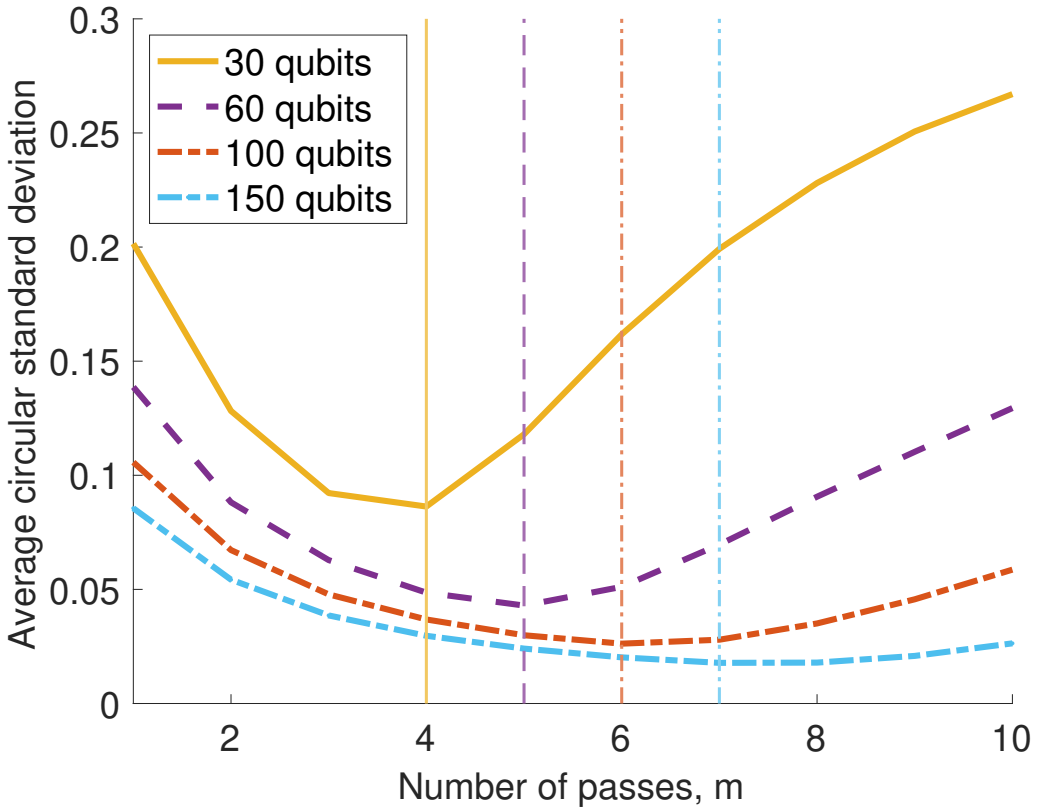

Figure 5.8: The mean circular standard deviation when averaged over many possible true values for the mean likelihood function when combining the results of a single pass and a multipass estimation each with the given number of qubits. The widths initially decrease as the number of passes increases due to the increasing narrowness of the likelihood functions with more passes. However, they then increase again once the number of passes is too great and the single pass estimation begins picking out more than one multipass estimation peak. The vertical lines mark where the minimum circular standard deviation is achieved.

of width $2\pi/m$ she can simply ask Bob to perform m passes giving her a quantum enhancement of m^2, while ensuring there is only a single peak. An approach to scenarios with more limited prior information is to make measurements with different numbers of passes. A single peak can be achieved by combining information from measurements with numbers of passes that have no common factors and sufficient qubits that their peaks do not overlap.

Figure 5.7 illustrates this effect for the combination of single pass and a 4-pass measurement. A single pass measurement with 30 qubits gives a relatively broad likelihood function around the true value of ϕ; a 4-pass measurement with 30 qubits gives narrower peaks, but with a four-fold multiplicity meaning that the true value cannot be identified.

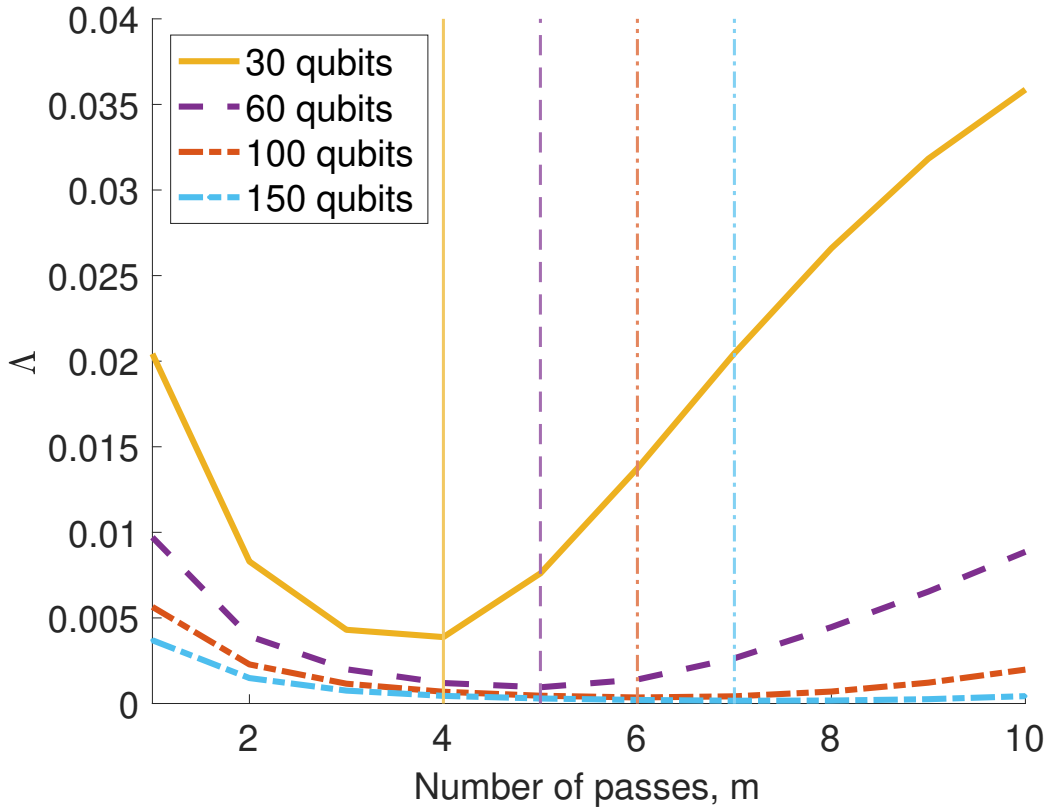

Figure 5.9: Λ when combining the results of a single pass and a multipass estimation each with the given number of qubits. The errors initially decrease as the number of passes increases due to the increasing narrowness of the likelihood functions with more passes and them being well placed. However, they then increase again once the number of passes is too great and the single pass estimation begins picking out the wrong or more than one multipass estimation peak. The vertical lines mark where the minimum Λ is achieved

Combining a single pass and a 4-pass with 30 qubits each (60 in total) gives the best of both worlds with a narrow peak at the right value of ϕ. This is compared with the result using all 60 qubits in single pass measurements, which has a broader peak.

Figures 5.8 and 5.9 illustrate the interplay between the number of qubits used and the minimum circular standard deviation or Λ that can be achieved for single-pass and m-pass strategies that use the same number of qubits for each estimation respectively. Initially, the standard deviation and Λ decrease as the number of passes increases. However, they increase again if there are too many passes for the number of qubits. This is because the single-pass likelihood distribution will not always be narrow and sufficiently well-placed to pick out only the correct single peak from the m-pass distribution, the peaks of which are separated by $2\pi/m$. This leads to a indistinguishability problem providing larger standard

deviation and Λ.

By combining results from different numbers of passes Alice can get an m^2 enhancement to her information with a cost of using enough qubits on a single pass estimation to be sure that she picks out the correct peak. Otherwise, she could use a combination of $m_j \in \mathcal{N}$ that optimise the information gain [66, 90].

5.3 Security

This section discusses security for this protocol. It begins by showing how the first security condition for a SQRS protocol is fulfilled, by ensuring that an eavesdropper can gain no information from the classical measurement results. Then, it shows how man in the middle attacks on the quantum communication channel are detected giving a distribution for the number of rounds until such attacks are detected and a rigorous measure of information privacy to quantify the security for different protocol fidelity checking rate, F. It ends with a discussion of the potential increase in information asymmetry when using a combination of single and multiple pass metrology protocols. The third security condition, protections against manipulations of the classical communications requires a more complex protocol which is discussed in chapter 7.

5.3.1 Protecting classical data

Security of the classical information is maintained because Alice is the only party to know the state of each qubit she sends. If Alice sends each of the σ_x and σ_y eigenstates with equal probability she can ensure that Eve gains no information from the measurement outcomes that Bob sends through the classical channel. This is evident from the probabilities in table 5.1. Since Eve does not know the state, the probability of a $+1$ or -1 measurement outcome is given by taking an equally weighted sum of the probabilities in the corresponding column of table 5.1, i.e

$$P_{Eve}(+1|\phi) = P_{Eve}(-1|\phi) = \frac{1}{2}. \tag{5.16}$$

Since these are independent of ϕ, their derivative with respect to ϕ vanishes and Eve's classical Fisher information, as given by equation (5.2), is zero. Similarly, Eve's density matrix for each photon is $\hat{\rho}_{\text{Eve}} = \frac{1}{2}I$ both before and after interaction with ϕ, giving a quantum Fisher information of zero. This means that Eve can gain no information from the classical channel regardless of the measurements that Bob performs. Comparing this

with 5.2 where Alice obtains the maximum possible information about ϕ, there is a clear information asymmetry between Alice and Eve for this protocol.

5.3.2 Man in the middle attacks

Eve cannot learn anything about the parameter ϕ from the classical information that Bob has and sends through a public channel because she does not know what any of the qubit states are when they arrive at Bob. However, if she were to interact with the qubits in some way as they travel from Alice to Bob, she may be able to determine the state of some of them. For instance, she could perform a MIM attack by manipulating the quantum communication channel. Due to the indistinguishability of the initial states she cannot manipulate the quantum channel without risking changing the state arriving at Bob who has a non-zero probability of performing the correct fidelity check allowing Alice to detect the attack. Eve could perform an 'intercept and resend attack' (IR) by intercepting some qubits and replace them with her own which would allow her to perform her own measurement of the phase. Otherwise, she could measure the intercepted qubits and replace them with her best guess in a 'measure and resend' attack. She could do this until Alice detects a discrepancy in the fidelity checking measurement results and stops the protocol.

Due to the indistinguishability of the quantum states travelling between Alice and Bob, Eve cannot interact with them without risking changing them. If Bob chooses which qubits are used for parameter estimation or state fidelity checking at random once Eve can no longer interact with them he ensures that Eve cannot selectively target only those states that she knows will not be used to test for her presence. As suggested in another SQRS protocol [8], by having a similar set of qubits travel through a quantum channel as the BB84 quantum cryptography protocol [73] similar security is retained.

Single shot detection and expected disagreement

The following is a demonstration that it is statistically unlikely for Eve to attack the quantum channel without being detected by Alice. Therefore, a noiseless implementation this protocol is secure against such attacks.

If Eve were to perform a maximal discrimination measurement on a qubit in flight from Alice to Bob and replace it with her measurement result she would have a probability of $1/2$ of successfully determining what state Alice had sent [109]. This is also a maximal disturbance measurement so Eve has a probability $1/2$ of sending a state in the wrong

eigenbasis to Bob. If this qubit travels to the detector D2 or D3 that corresponds to the original eigenbasis that Alice sent the qubit in, there is a probability of 1/2 of giving a result that does not correspond to that qubit and signals the possibility of such an attack. Thus, each qubit that Eve measures in this way while in transit and is replaced by another that travels to the detector D2 or D3 corresponding to the eigenbasis of the original state has a probability of 1/4 of signalling the attack to Alice. There is a further 1/2 probability of the detector corresponding to the basis of the initial state so the probability of detection in any single round that Eve attacks in this way is $P_{\text{sing,MR}} = 1/8$. Over many attempts the probability of disagreement, P_{dis}, between an original state and Bob's fidelity checking measurement is

$$P_{\text{dis}} = 1 - (1 - P_{\text{sing}})^N \,, \tag{5.17}$$

where P_{sing} is the probability of a disagreement for an attack on a single state and N is the total number of fidelity checking measurements on attacked states. The rate at which Bob sends qubits down the fidelity checking path to D2 or D3 is $0 < F < 1$. With each fidelity checking detector equally likely, the probability of Bob sending a qubit to each detector D2 or D3 is $F/2$ and the parameter estimation detector at D1 is $1 - F$. When Eve attacks μ qubits the expected number that travel to either detector on the fidelity checking path is μF for all the initial states. Thus, the expected disagreement is,

$$P = 1 - (7/8)^{\mu F}. \tag{5.18}$$

In this protocol, the simple approach is that as soon as Alice detects a discrepancy she stops because she cannot be sure that there is no eavesdropper. Equation (5.18) shows that the probability of Eve being detected by this method exponentially approaches unity with the number of states attacked. Any attack that changes the states of the qubits in the quantum channel, such as spoofing Alice's results by adding a phase, would have a similar exponential detection rate.

In an intercept and resend (IR) attack Eve does not measure the states before replacing them and sending new states to Bob. Therefore, from Alice's perspective she is sending a random state which has a 1/2 probability of giving the wrong measurement result when Bob uses the detector, D2 or D3, that corresponds to the initial state which occurs for half the fidelity checking measurements. Thus for such an attack $P_{\text{sing,IR}} = 1/4$ and the expected disagreement is

$$P = 1 - (3/4)^{\mu F}. \tag{5.19}$$

Alice is always more likely to detect an IR attack than a MR attack. Therefore, if Eve is

performing a MIM attack to steal information it is advantageous to perform a MR rather than an IR attack.

Rounds until detected and quantification of information privacy

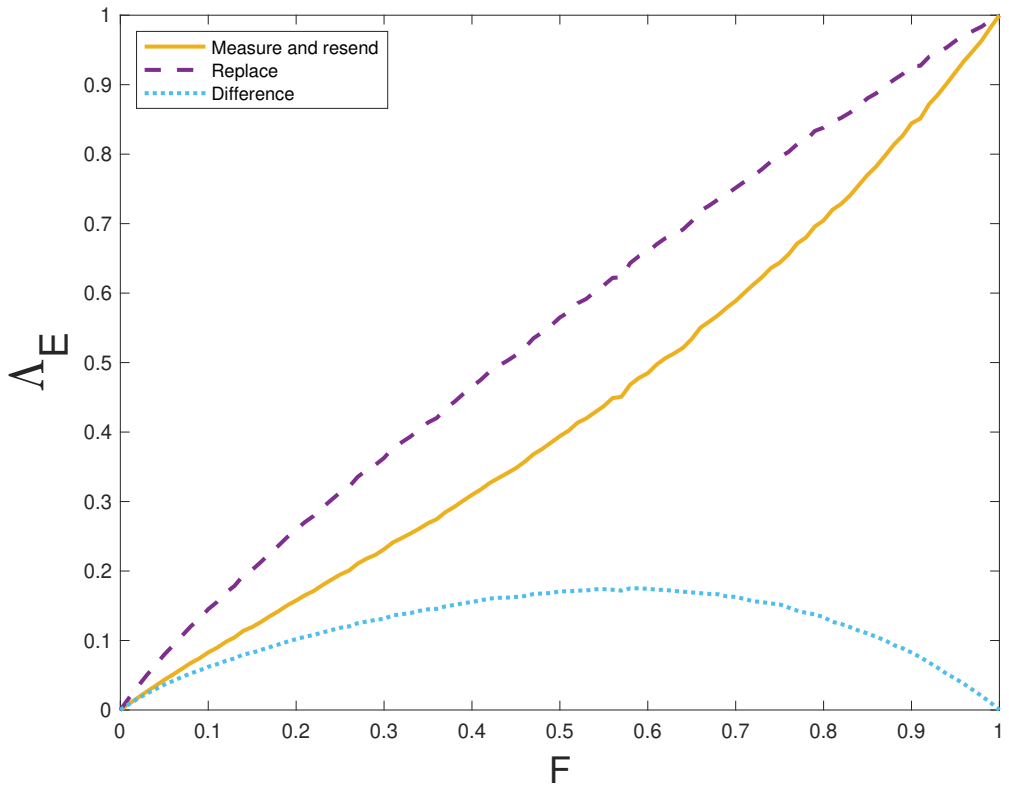

Figure 5.10: Λ_E for a single-Bob protocol with MR and IR attacks. Data was created using simulations of $\Lambda(\eta)$ for $\eta = \{0, 1, 2, ...100\}$ and combining them with the distribution of η given by equation (5.20) with $d = F/8$ and $d = F/4$ respectively. For most values of F the probability of being undetected in more than 100 rounds is negligible meaning the values shown in this plot are the true values of Λ_E. For $F < 0.1$ the probability is not negligible so the values shown in the plot represent a lower bound on Λ_E.

Since this protocol has discrete detection results where Eve is either detected or not, the number of rounds until (but not including) Eve is detected the first time can be modelled using the geometric distribution. The probability that there are η rounds before Eve is detected is given by,

$$P_{Geo1} = (1 - d)^{\eta} d \tag{5.20}$$

where $d = FP_{\text{sing}}$ is the probability that Eve will be detected in any given round. This can be generalised to allowing more than one detection using the negative binomial dis-

tribution.

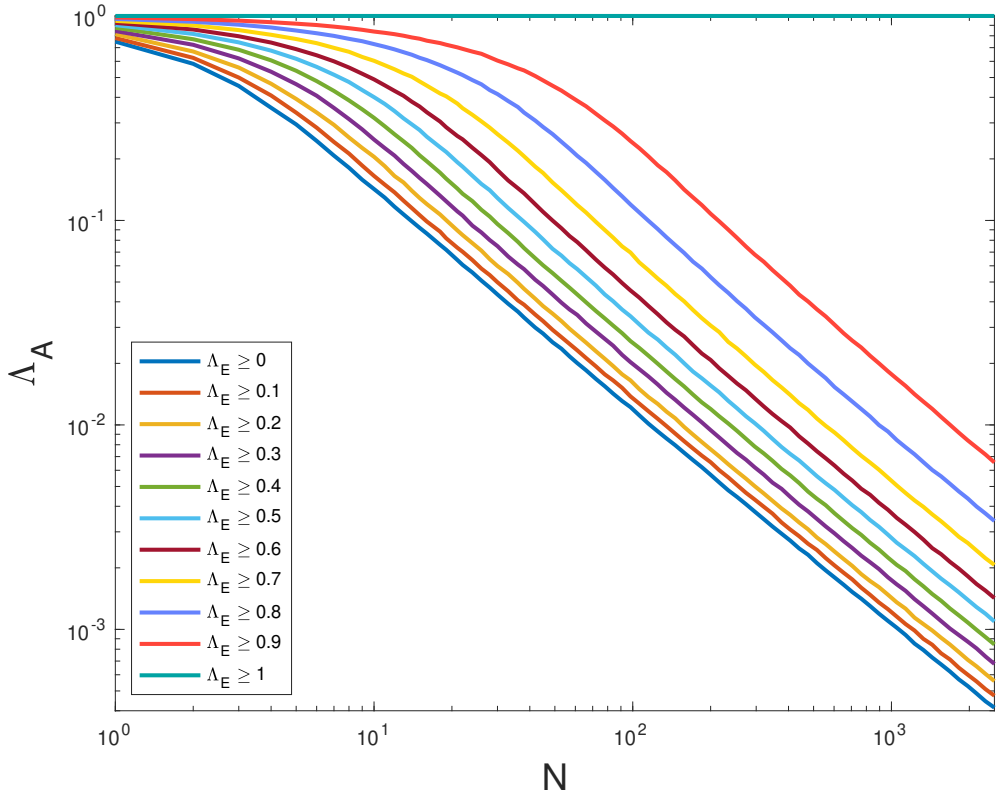

Figure 5.11: Alice's information gain for different privacy limits. The $\Lambda_E \geq 0$ line corresponds to a protocol with metrology only, no security. It shows the standard quantum limit, $\delta\phi \geq 1/\sqrt{\mu}$, where μ is the number of rounds, in the asymptotic limit. Secure protocols show asymptotic metrology with a constant reduction, $\delta\phi \sim (1-F)/\sqrt{\mu}$, relative to the standard quantum limit where F is the rate of fidelity checks.

Figure 5.10 shows a lower limit on the amount of information gain for MR and IR attacks on a single Bob. This is calculated using many Monte Carlo simulation to find Λ for 0 to 100 rounds of the protocol then weighting this using the geometric distribution for the number of rounds before Eve is detected. When F is very small, there is a non-negligible probability that more than 100 rounds can pass before Eve is detected. A further nuance to security is that an eavesdropper should not be able to attack many times without detection so, more than 100 successfully attacked rounds can be considered a failure of security. In these cases the calculations used $\Lambda(\eta > 100) = 0$ making the plot a lower limit of Λ_E for eavesdropping.

Figure 5.11 demonstrates the evolution of Λ_A, the measure of Alice's information gain averaged over the distribution of measurement results for each phase drawn from the

uniform prior $p(\phi|\alpha) = 1/2\pi,\ \phi \in [0, 2\pi)$ for information privacy limits $\{0, 0.1, ..., 1\}$ of the protocol.

Alternatively, instead of limiting Λ_E, a measure of the mean information gain by Eve before the first time that she is detected, the distribution of the circular mean square error ξ_E before the first time she is detected could be calculated and privacy could be defined by limiting the probability that ξ_E on any implementation of the protocol is below a predetermined value.

Multipass security augmentation

Parameter estimation with multiple passes can provide further protection against MIM attacks and the other attacks introduced in chapter 7 where Eve could steal some information while Alice maintains information asymmetry. This additional security is dependent on the state of prior informations of Alice and Eve.

Firstly, if Eve has a broader prior distribution than Alice, say Alice has prior of width $2\pi/m$ and Eve has a prior width $2\pi/\tilde{m}$ where $\tilde{m} \ll m$ then, Alice is assured that any eavesdropping performed by Eve on an m pass estimation protocol will allow her to estimate $m\phi$ but she will end up with an indistinguishability issue when estimating ϕ. For instance, if $\tilde{m} = 1$ then Eve will have m peaks to her posterior distribution in a 2π range. In such scenarios Alice must continue fidelity checking to maintain information integrity.

If Alice and Eve have similar prior distributions then the same effect may be achieved if Alice performs parameter estimation with two different numbers of passes and combines the results to get quantum enhanced estimation. For instance, with minimal priors such as the 2π width uniform distribution, the combination of 1 and m passes such as is demonstrated in figures 5.7, 5.8 and 5.9 can allow Alice to perform quantum enhanced parameter estimation. If Alice maintains significant information asymmetry when performing the m_1 estimation then, if Eve attacks the $m_2 > m_1$ pass metrology protocol using her posterior due to attacks on the single pass metrology protocol as a prior distribution, that prior will be broader than the distance between two of the m_1 pass estimation peaks, $\sim 2\pi/m$, and/or not drawn from enough data to be confident they it is close to the true value causing the same indistinguishability issue no matter how successfully she attacks the m_2 pass protocol.

However, if Eve has a narrower prior distribution than Alice and Alice is using quantum enhancement such as the combination of $m_j \in \mathbb{N}$ pass metrology protocols, she could gain significant information attacking only the metrology protocols with m_j such that $2\pi/m_j$ is

less than her prior. Therefore, it is important that, if Eve's prior is unknown, all parameter estimation is properly protected. The choice of which m_j to be used could be made in a way that is indistinguishable to Eve while she has access to the quantum states. For instance, a key could be used; but, as discussed in chapter 4 using a separate cryptography protocol is against the principles of SQRS protocols with integrated security. Otherwise, Bob could choose at random when he receives each qubit and tell Alice the choice of m_j later which would stop Eve from performing attacks only on specific $m_j\phi$ increasing the effective rate of security checks relative to the rate of useful information Eve could otherwise gather in theses scenarios. This is in the same way that Bob chooses which states to fidelity check at random on arrival from a predetermined distribution.

5.4 Summary and outlook

Summary

This chapter shows a method of performing metrology at a remote site secure from eavesdropping by using the indistinguishability of non-orthogonal quantum states to prevent Eve making measurements undetected on the quantum communication channel and states chosen such that the average state is proportional to the identity matrix to protect classical information.

This protocol has improved measurement capabilities and practicality compared to previous SQRS protocols for the estimation of phase parameters. Firstly, by not requiring entanglement [11, 13] and only requiring qubit states [10] it is a more practical protocol than most. Furthermore, by using only phase sensitive quantum states it avoids wasted resources [8]. Its efficiency is further highlighted by showing that by passing qubits through the sample multiple times Alice can get Heisenberg scaling of the measurement precision without using entanglement or compromising the security. The correct likelihood peak in a 2π range can be correctly identified by combining the results of measurement protocols with different numbers of passes and sufficient data. This quantum enhancement could also be used to further enhance information asymmetry when Eve is able to perform some attacks on quantum states.

This protocol is analysed in limited data to highlight its practicality for real world applications where data may be limited by time, resource cost or security. Such analysis is particularly important for quantifying information privacy. Like previous protocols, this is shown to have an exponentially increasing probability with the amount of quantum

resources attacked in a MIM attack [8, 10]. However, this work goes further by determining the distribution of the number of rounds that can be attacked in such a manner before an eavesdropper is detected and providing a rigorous measure of information privacy, Λ_E, the average circular mean square error of the posterior distribution of ϕ that an eavesdropper may acquire using minimal prior information before they are detected.

There are various extensions to this protocol and the results in this chapter. One extension is to functions of parameters held at several remote locations, the subject of chapter 6. Another is to provide further security proofs and enhancements. This is provided by chapter 7 where extensions to the protocol to protect against MIM attacks that manipulate the classical information sent from Bob to Alice are considered.

Noise

A significant direction for further research not covered in detail by this thesis is noise. Some SQRS protocols allow and adjust for some noise to the metrology aspects of their protocols. Three [11, 12, 15] use a destructive random sampling test [89] while another uses quantum state tomography [13]. The protocol suggested here can also adjust for noise. If, instead of considering noise to be caused by an eavesdropper and stopping when it is detected then, it can be estimated and adjusted for. Chapter 2 sets out some of the effects of noise on quantum metrology. In scenarios with a known phase bias this can be adjusted for during data analysis without affecting the information gain. Symmetric noise (symmetric phase noise or out of equatorial plane noise) causes reductions in Fisher information for phase estimation. This noise can be estimated from the error rate of the fidelity checks. Figure 5.12 demonstrates the average effect on a likelihood function when not adjusting for noise or adjusting for noise using the true value of the noise rate. In a practical application the posterior distribution for the noise rate, equivalent to the rate of random qubits replacing the initial pure states, $\mathcal{R} = 1 - \mathcal{P}$, could be drawn from the fidelity check results and used with equation (2.50) for parameter estimation.

It is evident that such noise is not an issue for the metrology aspects of the SQRS protocol. The issue is for noisy scenarios where there is an eavesdropper. Previous protocols that allow for noise do not account for the potential loss of privacy due to the amount of information that an eavesdropper can steal in a MIM attack under the guise of noise [11–13, 15]. In these scenarios there could be some distribution of the expected noise rate and an eavesdropper could attempt to hide MIM attacks on the quantum channel due to the variance of this distribution. This make security more difficult to quantify than the work

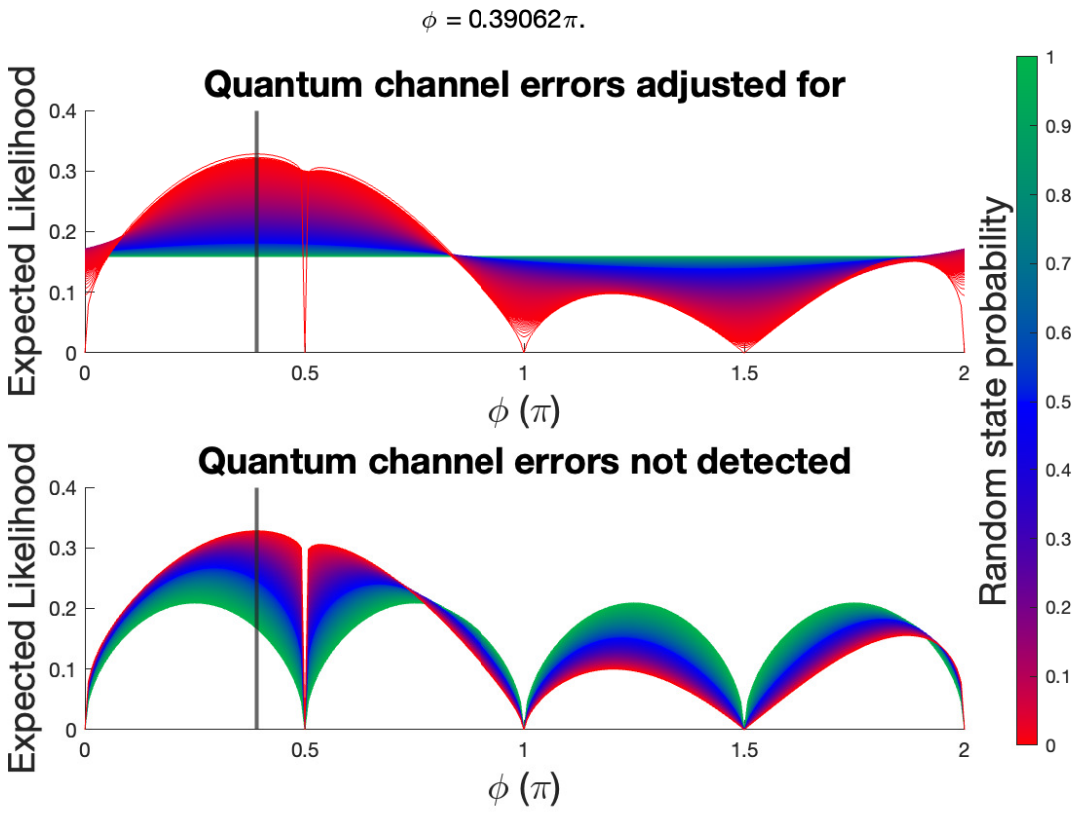

Figure 5.12: An example of quantum phase metrology with and without symmetric noise adjustment. The two figures show the expected contribution of a single measurement to the likelihood function for large numbers of measurements when there are varying amounts of symmetric noise that may be represented by a probability of a random state being measured for $\mathcal{R} \in [0, 1]$. A large data likelihood function would have result numbers close to the expected value and closely resemble the likelihoods plotted to the power of μ. In both cases the amount of information gain reduces with the increase in noise, as shown by the reduction in likelihood at the true value. When the quantum channel errors are adjusted for the MLE remains unbiased. However, when they are not adjusted for the likelihood function becomes biased and the MLE shifts toward the closest value $\pi/4+j\pi/2$, $j \in \{0, 1, 2, 3\}$.

presented here.

Here, the privacy is dependent on the number of rounds attacked by Eve regardless of how many rounds Alice and Bob attempt. In the secure noisy scenario Eve could potentially steal more information the longer the protocol runs. Privacy would be ensured by ensuring the error rate of the fidelity checks is within the acceptable limits and it would be quantified by the amount of information that Eve can steal before this limit is reached due to the variation in the noise rate. This would be a worthwhile direction for future work.

Chapter 6

Secure networks for estimating sums of parameters

SQRS protocols combine quantum metrology with quantum communications to enable high-precision measurements of parameters at remote locations with guaranteed security. They are an interesting demonstration of how two quantum technologies can be integrated into one protocol and have applications in cases where the remote party's security is compromised or it is not practical for them to have the infrastructure for quantum key distribution (QKD).

The standard setup [6–17] is that one party, Alice, wants to measure a parameter at one or more distant Bobs. These remote parties are trusted to work together and follow each other's instructions but their communication channels and any information held by the Bobs is vulnerable to attacks from an eavesdropper, Eve. Alice achieves her goal by sending the Bobs carefully chosen quantum states (known only to her) that fulfil the dual roles of enabling quantum-enhanced measurement precision and detecting external attacks. The Bobs then use these states to either measure their parameter or check the fidelity of the state and send the results back to Alice via a classical channel. This means that the information in both the quantum and classical channels needs to be secure. To protect the classical information, the average of the probe states sent from Alice to Bob is chosen to be the identity matrix to ensure that no information can be gained from the publicly declared results. To protect the quantum channel, Alice sends states that Eve cannot unambiguously distinguish on a single shot meaning that she cannot determine what they are without risking detection.

Most SQRS protocols [6, 7, 9, 11–15] use entanglement (such as Bell states) shared by

Alice and Bob, with Alice measuring her part of the entangled state in one or more non-orthogonal bases to project Bob's part into a state that only she knows. This motivates Eve to attack the quantum channel to try to determine this state. If Alice measures in two or more non-orthogonal bases and Bob verifies a randomly chosen selection of the states, there is a non-zero probability that Eve is detected each time she attacks the quantum channel. To gain meaningful information, Eve needs to make multiple attacks and the probability of her not being detected on at least one of them decreases exponentially with the number of attempts. A similar outcome can also be achieved without entangled states by using multidimensional probes [10], qubits in the Pauli-X and Pauli-Z eigenstates [8] or qubits in the Pauli-X and Pauli-Y eigenstates [16, 17].

A natural extension of SQRS is to consider networks of sensors [7, 9, 15, 17]. Joint measurements such as those performed with entangled probes are known to give a quantum advantage when measuring a function of parameters at the different sensors [53–62]. As demonstrated at the end of chapter 2, the greatest advantage is for a sum of the parameters ϕ_b held by each Bob, i.e. the $\theta = \sum_{b=1}^{B} \phi_b$. In this case entanglement can increase the precision, relative to combining the results of separate measurements, by a factor of $\sqrt{B}$, where B is the number of Bobs [55]. The problem, however, is that entangled states can also make it exponentially more difficult to detect an eavesdropper [8]. The reason for this is that all the Bobs must independently and randomly choose to either measure their parameter or do a fidelity check – this ensures that Eve cannot attack only the quantum states that will not be used for fidelity checking. However, Alice will only detect Eve if all the Bobs simultaneously choose to perform a fidelity check [8]. Such an occurrence becomes exponentially unlikely as the number of Bobs increases.

A possible way around this is to allow for secure communication between the Bobs so they can decide in advance when they should all do a fidelity check. However, as set out in chapter 4, this is not in the spirit of SQRS where quantum metrology and quantum communications are seamlessly integrated into one protocol, nor does it help when it is not practical or possible for the Bobs to have the infrastructure for QKD. Furthermore, the security for such scenarios is the same as the two party scenario of chapter 5 where a single Bob measures a function of parameters rather than a single parameter.

This chapter shows how to overcome the exponential inefficiency of entangled states in detecting an eavesdropper without requiring a separate QKD protocol. This is achieved with a hybrid protocol that uses a combination of both entangled and separable states. The scenario considered is shown in figure 6.1 and consists of one Alice, multiple Bobs and

no separate secure communication protocol between the parties. It uses the same qubit states as used in chapter 5 [16] for separable states and a similar security encoding on GHZ-like states for the entangled states.

In section 6.1 the network SQRS protocol for functions of parameters is set out and the reason it is secure is explained. The protocol applies to various numbers of Bobs, a variable denoted by the letter B. It must assure some level of security and provide effective metrology. These are both influenced by the two independent protocol parameters: the probability that each round of qubits are separable, $S \in [0, 1]$, or entangled, $E = 1 - S$, and the probability that each Bob interacts the parameter before measuring the state, $M \in [0, 1]$, or directly measures the state as a fidelity check $F = 1 - M$. The two independent protocol parameters, $\{S, F\}$, are adjusted depending on B to optimise the metrology for a given security limit.

Section 6.2 discusses the quantum metrology aspects of the protocol. Due to the non-zero probability of each Bob performing a fidelity checking measurement, F, in some rounds the initial entangled states measure sums of subsets of the parameters. The section begins by calculating the Fisher informations of the protocol for arbitrary protocol parameters with the round count N as the resource count. However, as B increases the number of different parameter combinations increases exponentially making the asymptotic, large data, limit where there is an equality for the Cramér-Rao bound, difficult to reach in secure network scenarios. This also makes the data analysis complex because data from different subsets of parameters has a large effect on the quality of the parameter estimation and is computationally intense. This section sets out a method for optimising the information gain from the data and perform the parameter estimation computationally efficiently.

Section 6.3 shows how Alice's information gain can be maximised for a given privacy limit. Two scenarios are considered: 1. Alice performing a predetermined number of rounds and 2. Eve attacking every round by measuring and replacing the states in the quantum channel with her own entangled states until Alice detects her for the first time and stops the protocol. A privacy limit of $\Lambda_E \geq 0.5$ is set as a limit on the average information Eve can gain over many simulations using circular Bayesian methods. The section introduces an optimisation algorithm for Alice's information gain with this privacy limit by searching through an array of possible $\{S, F\}$ combinations and then repeating the search in the vicinity of the optimal values.

This was applied to protocols where the initial quantum states for each round are separable, $\{S = 1, F \in (0, 1)\}$, entangled, $\{S = 0, F \in (0, 1)\}$, or from a hybrid protocol

with either, $\{S \in (0,1), F \in (0,1)\}$. The results of the optimisation show that entangled initial states are not effective for security as the number of Bobs increases, whereas separable initial states remain secure but have reduced measurement precision. Using a hybrid protocol with some separable and some entangled initial states allows for both enhanced measurement precision and security. Finally, the hybrid protocol results are used to show that Alice can perform quantum enhanced measurement, with lower parameter estimation uncertainty than an local metrology strategy without security where each parameter is measured separately while ensuring information privacy.

6.1 Protocol

The network SQRS protocol for linear functions of parameters proceeds as follows:

1. Alice prepares either an entangled state or a set of separable states with probabilities E and S respectively. These are chosen from a set that cannot be distinguished on a single shot and have occurrence probabilities such that the average state is proportional to the identity matrix. She keeps the state secret. The encoding for each member of the separable set is independent so, she does not send a set of identical separable states. When using qubits and GHZ states, the separable states sent to each Bob, b, of the B Bobs is of the form

$$|S_b\rangle = \left(|0\rangle + e^{i\chi_b}|1\rangle\right)/\sqrt{2} \tag{6.1}$$

and the entangled states with an element sent to each Bob are

$$|E\rangle = \left(|0\rangle^{\otimes B} + e^{i\chi}|1\rangle^{\otimes B}\right)/\sqrt{2} \tag{6.2}$$

for B Bobs. For both types of initial state $\chi_b, \chi \in \{\chi_0, \chi_0+\pi/2, \chi_0+\pi, \chi_0+3\pi/2\}$ at random with equal probability for each state sent. For the purposes of this chapter the choice of χ_0 is arbitrary, it could be $\chi_0 = 0$ such that Pauli-X and Pauli-Y like states are used.

2. Alice sends the quantum states through a quantum communication channel to the Bobs with each receiving the state required for their individual parameter estimation. An eavesdropper could perform the first step of a man in the middle attack here by measuring and replacing (or simply replacing) the probes in some or all of the rounds or attempt to bias the results by adding some phase to all of the qubits.

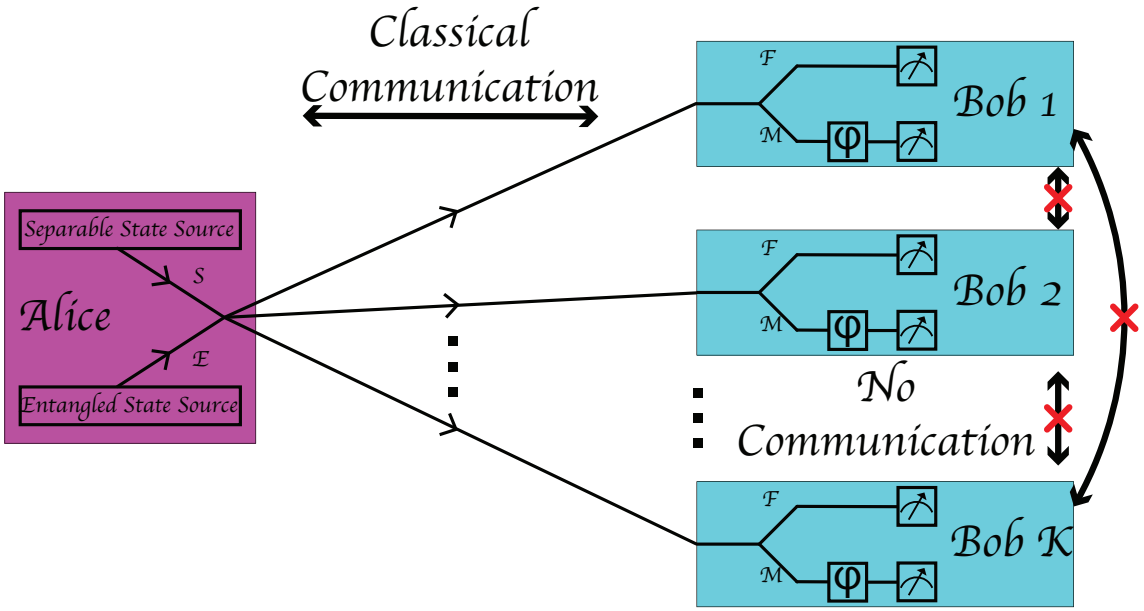

Figure 6.1: A protocol for estimating functions of quantum parameters held at multiple remote sites while maintaining security from eavesdropping and spoofing. In this scenario each Bob holds a parameter and Alice is attempting to estimate some linear function of these parameters. Each Bob can be trusted to follow Alice's instructions but they are not guaranteed to be secure from observation. The Bobs do not need to be able to communicate with one other. Alice sends states that are entangled over all of the Bobs or an equal sized set of separable states to all of the Bobs in each round with probabilities E and $S = 1 - E$ respectively. Each Bob chooses at random to interact the state they receive with their parameter or not with probabilities M and $F = 1 - M$ respectively. Then, they measure them and send the discrete measurement results to Alice through a public classical communication channel. Alice uses these results to verify for an eavesdropper and estimate the function of parameters.

3. Each Bob independently, at random but with predetermined probabilities M and F either interacts their probe with their parameter or not respectively and then measures it. These measurements are performed in the χ_0 and $\chi_0 + \pi/2\}$ basis with equal probability (Pauli-X and Pauli-Y when $\chi_0 = 0$). Here, Eve could perform the second step of a man in the middle attack by observing the measurement results of the Bobs. The measurement probabilities are of the form $\frac{1}{2}(1+\cos(\varphi+k\pi/2))$ where $k \in \{0, 1, 2, 3\}$ depends on the initial state and measurement basis and φ is the sum of the parameters that measurement state has interacted with [16].

4. All the Bobs communicate their measurement outcomes (along with whether they

interacted the state with their parameter) to Alice through the public classical communication channel. Similar to stage 3 above, Eve could perform the second step of a man in the middle attack by observing the publicly announced results.

5. Alice is able to use the measurements from the Bobs along with her knowledge of the states she sent to perform an estimation of $\theta = \sum_{b=1}^{B} \phi_b$. She is also able to continuously check for eavesdropping by looking for anomalies in the fidelity checking results where the Bobs did not interact the state with their parameter. She can then decide whether it is safe to continue the protocol, returning to step 1.

All SQRS protocols must find a way to balance both security and estimation efficiency. Without an eavesdropper any protocol would be most efficient for measurements by having fidelity checking rate, $F = 0$ and parameter measurement probability$M = 1 - F = 1$. Alternatively, the most secure protocol has $F = 1$ and $M = 0$. It is best that F be equal for all Bobs and likewise for M, as this optimises the measurement efficiency and the security. This can be illustrated by considering the optimal measurement states for each Bob, M_b, occurring with probabilityproportional to $\prod_{j=1}^{B} M_b \leq M_{\text{mean}}^{B}$ with equality when all $M_b = M_{\text{mean}}$. Similarly, the optimal probability of fidelity checks for each Bob, F_b, can be found from $E\prod_{j=1}^{B} F_b + S\sum_{j=1}^{B} F_b \leq EF_{\text{mean}}^{B} + SBF_{\text{mean}}$ with equality when all $F_b = F_{\text{mean}}$ and thus all $M_b = M_{\text{mean}}$. Therefore, F and M are used as the same fidelity checking and parameter measurement probabilities for all Bobs.

The security principles are the same as in chapter 5. The quantum states used in each round are either the same as those used in that chapter or entangled states with the same encryption. They are chosen from the same set of possibilities with the same probability of each.

The first security condition is that Eve cannot interpret the classical measurement results to gain insight into the measured parameters or their sum without interacting with the system. From her point of view the density function of each round of qubits is proportional to the identity matrix giving her no Fisher information fulfilling this condition.

The second security condition, that Eve is exponentially more likely to be detected with each round where she manipulates the quantum channel and that her information gain is limited, follows due to the same logic as chapter 5. When Alice sends a separable state to a Bob that performs a fidelity check, due to the indistinguishability of the set of possible states and the non-zero probability of the Bob performing the appropriate fidelity checking measurement, she may attempt verify whether Eve has performed an attack that round. Similarly, when Alice sends an entangled state to the Bobs who all perform a

fidelity check, she can also attempt to verify if Eve has performed an attack that round. Therefore, for fixed $\{S, F\}$, by the same logic used in chapter 5, Eve is exponentially more likely to be detected with each round she attacks by manipulating the quantum channel regardless of the attack.

However, in network scenarios the choice of $\{S, F\}$ is significantly more complex than in two party scenarios. There are two variables affecting both the security and information gain different amount for different B to optimise over. The security increases (information gain decreases) with increasing S and increasing F. For every S there is a value of F that sets the privacy limit to Λ_E. In this chapter this is optimised numerically. Chapter 7 provides further insight with some analytical results for the distribution of the rounds until Eve is detected and considers greater variety of attacks and limiting distributions of Λ_E as a function of $\{S, F\}$.

6.2 Metrology

This section discusses the information gain when using a secure network to estimate functions of parameters. The information Alice and Eve gain can be calculated in the same way and depends on the number of rounds N and the protocol parameters B, S ($E = 1 - S$) and F ($M = 1 - E$). The results in this section will be given in terms of these four independent parameters: N, B, S and F. If Eve performs an attack where she replaces states with her own entangled or separable states then the results correspond to $S = 0$ or $S = 1$ respectively.

In a protocol with B Bobs each measuring a parameter ϕ_b, the set of combinations of Bobs that perform parameter measurement or not in each round is of size 2^B; there are $\binom{B}{m}$ combinations for m parameters being measured. The set of possible combinations is written $\vec{\varphi} = \{0, \phi_1, \phi_2, ..., \phi_1 + \phi_2, \phi_1 + \phi_3, ..., \theta\}$ with each $\varphi_k(m)$ the k^{th} element of $\vec{\varphi}$ with m parameters measured. Section 6.2.1 demonstrates how the Fisher information of the protocol can be calculated by combining the information due to the sets of $\varphi_k(m)$ for each m. Section 6.2.2 shows that the number of possible parameter combinations makes the asymptotic limit difficult to reach, parameter estimation computationally intensive and the quality of parameter estimation in limited data dependent on the approach used. It provides a method of optimising the information gain while remaining computationally efficient.

6.2.1 Fisher information

This section provides a calculation of the Fisher information for the protocol using the number of protocol rounds as the resource count. The results apply to both the classical and quantum Fisher informations. This protocol combines both local (separable initial states) and global (entangled initial states) measurement strategies. It will use $\mathcal{I}_m$ for the Fisher information, both classical and quantum when m parameters are measured together. This allows the results to be applied to similar protocols with different Fisher informations for different numbers of parameters being interacted such as those with phase noise during parameter interaction.

First, consider the (quantum) Fisher information in a protocol using only separable initial states. Each Bob has a probability M of performing a parameter estimation. Therefore, measurements of each of the ϕ_b will occur with a probability of M per round. Measuring each parameter separately and summing them to get an estimation for $\theta = \sum_{b=1}^{B} \phi_b$ gives a (quantum) Fisher information

$$\mathcal{I}(\theta|\text{separable only protocol}) = \frac{M\mathcal{I}_1}{B}. \tag{6.3}$$

The Fisher information using the number of probe-parameter interactions in an noiseless implementation using pure qubits (where $\mathcal{I}_1 = 1$) is M/B^2 showing an M reduction compared to the local estimation without security in chapter 5. If the protocol has a mix of states, the information gain due to separable states would be weighted by the probability of a separable initial state occurring

$$\mathcal{I}(\theta, S) = \frac{SM\mathcal{I}_1}{B}. \tag{6.4}$$

For entangled initial states, the probability of each sum of m parameters $\varphi_k(m), k \in \{1, 2, ..., \binom{B}{m}\}$ being measured is equal. Therefore, it is practical to combine them to find the (quantum) Fisher information due to all of those parameters. They each have an equal probability

$$P(m, k|B, F, E) = EM^m F^{B-m} \tag{6.5}$$

of occurring. Their sum is

$$\sum_{k=1}^{\binom{B}{m}} \varphi_k(m) = \binom{B-1}{m-1}\theta. \tag{6.6}$$

This is evident by considering choosing only and all those combinations that contain an arbitrarily specific parameter there remain m-1 parameters to pick out of a remaining set of $B-1$. Therefore, $\binom{B-1}{m-1}$ combinations contain each parameter and so the sum of all

of them contains the same multiple of that parameter. The (quantum) Fisher information for a single measurement follows the relationship

$$\mathcal{I}(aX) = a^2\mathcal{I}(X), \tag{6.7}$$

and (quantum) Fisher information due to an equally probable set of A states that sum to aX is

$$\mathcal{I}(aX) = a^2\mathcal{I}(X)/A. \tag{6.8}$$

Therefore, the (quantum) Fisher information from the $\binom{B}{m}$ sums of m of the B parameters have a Fisher information

$$\mathcal{I}(\theta|\text{entangled, } m \text{ parameters in a round}) = \frac{\binom{B-1}{m-1}^2}{\binom{B}{m}}\mathcal{I}_m = \frac{m}{B}\binom{B-1}{m-1}\mathcal{I}_m. \tag{6.9}$$

Combined with the occurrence probability of each individual state, this contributes

$$\mathcal{I}(\theta, E, m) = EM^mF^{B-m}\frac{m}{B}\binom{B-1}{m-1}\mathcal{I}_m. \tag{6.10}$$

In an entangled protocol the Fisher information when all B Bobs perform Fidelity checks is $\mathcal{I}_B$. In a noiseless scenario using pure GHZ states $\mathcal{I}_B = 1$ so, the Fisher information using the number of parameter-probe interactions is M^m/B showing an M^m reduction relative to the global estimation without security in chapter 5. When $m < B$ the estimation is a hybrid of the global and local estimation strategies.

The (quantum) Fisher information combines additively so, for independent data X and Y

$$\mathcal{I}_{X,Y}(\theta) = \mathcal{I}_X(\theta) + \mathcal{I}_Y(\theta). \tag{6.11}$$

Therefore, the (quantum) Fisher information for the entire system relative to the number of rounds is found by adding the information from equations (6.4) and (6.10) for $m = 1, 2, ...B$,

$$\mathcal{I}_{\text{total}} = \frac{SM\mathcal{I}_1}{B} + \sum_{m=1}^{B} EM^mF^{B-m}\frac{m}{B}\binom{B-1}{m-1}\mathcal{I}_m. \tag{6.12}$$

6.2.2 Limited data estimation optimisation

The probability of each $\varphi_k(m)$ being measured is dependent only on the number of parameters measured m,

$$P_k(m) = SM\Big|_{m=1} + EM^mF^{B-m}. \tag{6.13}$$

The (quantum) Cramér-Rao bound is valid only in the asymptotic limit of a large number of independent measurements [99–101, 110]. One condition of the asymptotic

limit is that the maximum likelihood estimator becomes unbiased. It is important for this analysis to quantify when this limit is reached. For single qubit measurements, chapter 5 shows there is an estimation bias of the maximum likelihood estimator for some values of the phase being estimated in limited data; as the amount of data increases that bias reduces and the range of values with non-negligible bias also reduces [16]. Similarly, the mean standard deviation of likelihood functions is at the Cramér-Rao bound for the same values of the phase where the bias is negligible [16]. Approximately 1000 measurements is sufficient for both of these effects to affect only a small range of possible phases and by a reduced amount. Therefore, 1000 measurements is a useful approximation of the asymptotic limit for any single φ_k in this protocol [16].

To be able to combine estimators of φ_k in the same way as the Fisher information of the system is calculated each φ_k must be measured in the asymptotic limit. The number of φ_k increases exponentially with the number of Bobs 2^B. Apart from the case of $E = 0$ or $F = 0$, these will all have a non-zero probability of occurring. If $E = 1$ and $F = 0.5$ they are all equally likely to occur, doing so with probability2^{-B}; for any other protocol parameters some will be even less likely. For all of them to be measured in the asymptotic limit at least 1000×2^B rounds are needed. Therefore, as the size of the network increases, more rounds are required for the Cramér-Rao bound to be valid.

The asymptotic limit can almost be reached by considering that for some choices of protocol parameters the $\varphi_k(m)$ for some values of m are extremely unlikely to occur. However, it is not advantageous to consider only the system parameters that reduce the number of φ_k that need to be considered. For instance, taking $F = 0.1$ or $F = 0.9$ many of the m are quite unlikely but they have low Fisher information and security respectively; while $0.1 < F < 0.9$ increases the number of φ_k that need to be considered, if there are enough rounds it provides better information gain than $F = 0.1$ and it always provides better security than $F = 0.9$, so as demonstrated in figure 6.4(c), less extreme values of F provide good balance between the two effects.

The number of results for all of the φ_k is distributed as a multinomial and the marginal of each φ_k is a binomial. When there are a lot of $\varphi_k(m)$ compared to the number of rounds the mean number of results for each is small and the standard deviation is large. This makes it inefficient to combine all $\binom{B}{m}$ to estimate $\binom{B-1}{m-1}\theta$ for limited data. Instead, more information is gained by combining those that have the most results and sum to some multiple of θ.

This effect is particularly noticeable for $F \sim 0.5$ where the most probable m are $\lceil B/2 \rceil$

and $\lfloor B/2 \rfloor$. Say B is even, the most probable m is $B/2$ with $\binom{B}{m}$ different combinations occurring with probabilities $\sim 0.5^B$. This effect can most easily be demonstrated for $B = 4$ and $m = 2$, the lowest number of Bobs for which it occurs. The relevant combinations of parameters are

$$\begin{aligned}
\varphi_1(2) &= \phi_1 + \phi_2 \\
\varphi_2(2) &= \phi_1 + \phi_3 \\
\varphi_3(2) &= \phi_1 + \phi_4 \\
\varphi_4(2) &= \phi_2 + \phi_3 \\
\varphi_5(2) &= \phi_2 + \phi_4 \\
\varphi_6(2) &= \phi_3 + \phi_4.
\end{aligned} \tag{6.14}$$

With a large enough amount of data it would be effective to estimate $\sum_{k=1}^{6} \varphi_k(2) = 3\theta$ and use it to estimate θ. When $S = 0$ and $M = 1$ all of the $\varphi_k(m)$ have the same 2^{-B} probability of occurring and the number of times each occurs n_j multinomially distributed,

$$Mn\left(\vec{n}, \frac{\vec{1}}{2^B}\right) \sim \frac{n!}{\prod n_j!} 2^{-B} \tag{6.15}$$

where $j \in \{1, 2, ..., 2^B\}$. As set out in chapter 3, the marginal for any subset of the $\varphi_k(m)$ is a multinomial distribution with probabilities given by the subset and the sum of the remaining probabilities,

$$Mn\big((n_0, n_1, n_2, ...n_J), \big((1 - J2^{-B}), 2^{-B}, 2^{-B}, ...2^{-B}\big)\big) \sim \frac{n!}{\prod_{j=0}^{J} n_j!} 2^{-B(n-n_0)} (1 - J2^{-B})^{n_0}, \tag{6.16}$$

where $n = \sum_{j=0}^{J} n_j$ and n_0 is the number of results not corresponding to the set of interest. Therefore, the probability of $n_j = 0$ for any set of J parameter combinations is $P(\bigcap_{j=1}^{J} x_j = 0) = (1 - 2^{-B}J)$. The addition rule of probabilities generalised to J events is

$$\begin{aligned}
P(\bigcap_{j=1}^{J} X_j) = \sum_{j=1}^{J} P(X_j) - \sum_{i,j=1, i\neq j}^{J} P(X_i \cup X_j) + \sum_{i,j,k=1, i\neq j\neq k}^{J} P(X_i \cup X_j \cup X_k) - \\
... + (-1)^{J-1} P(X_1 \cup X_2 \cup ... \cup X_J)
\end{aligned} \tag{6.17}$$

and De Morgan's law of probability generalised to J events is

$$P(\bigcap_{j=1}^{J} \overline{X_j}) = P(\overline{\bigcup_{j=1}^{J} X_j}), \tag{6.18}$$

where $P(\overline{X}) = 1 - P(X)$. Combining these laws,

$$P(\bigcap_{j=1}^{J} \overline{X_j}) = \sum_{j=1}^{J} P(\overline{X_j}) - \sum_{i,j=1,i\neq j}^{J} P(\overline{X_i \cap X_j}) + \sum_{i,j,k=1,i\neq j\neq}^{J} P(\overline{X_i \cap X_j \cap X_k}) - \\ ... + (-1)^{J-1} P(\overline{X_1 \cap X_2 \cap ... \cap X_J}). \quad (6.19)$$

Using the event X_j to represent $x_j = 0$ the probabilities $P(x_j \neq 0) = 1 - (1 - 2^{-B})^n$ and $P(\overline{\bigcap_{k=1}^{K} x_k = 0}) = 1 - (1 - k \times 2^{-B})^n$ with multiplicity $\binom{J}{k}$ the probability of there being at least one result for J of the $\varphi_k(m)$ is

$$P(n_j > 0, j \in \{1, 2, ...J\}|B, n) = \sum_{k=0}^{J} (-1)^k \binom{J}{k} \left(1 - k \times 2^{-B}\right)^n. \quad (6.20)$$

Figure 6.2 shows his distribution for $B = \{1, 2, 3, 4, 5, 6, 7\}$. Clearly, the amount of data required to draw any information for $m = \lceil B/2 \rceil$ increases rapidly with B. Furthermore, this only shows the probability of there being at least one result for all of the parameter combinations. If this is not the case and there is minimal prior information, no information at all can be gained from all of those measurement results. However, even if there is at least one result and/or more than minimal prior information for some or all of the sums of m parameters this remains a poor method of extracting optimal information gain.

Even when using sufficient amounts of rounds to be assured of having at least one result for each $\varphi_k(m)$ the variation in the number of measurement results for each has a notable effect on the final estimation uncertainty. The marginal distributions of the number of results corresponding to each $\varphi_k(m)$ are binomial distributed with mean $\mu = np$ and standard deviation $\sigma = \sqrt{np(1-p)}$. When n is small $\sigma \sim \mu$ so the number of results for each $\varphi_k(m)$ varies drastically. Bienaymé's identity for the variance of the combination of J independent variables, X_j shows that,

$$Var\left(\sum_{j=1}^{J} X_j\right) = \sum_{j=1}^{J} Var\left(X_j\right) = \sum_{j=1}^{J} \frac{1}{n_j}, \quad (6.21)$$

As each $n_j \sim Bin(n, p)$, the variance of the sum will be disproportionately affected by the smallest n_j, reducing it's value compared to the mean n_j. $J = \binom{B}{m}$ increases with B so this has an increased affect with the size of the network. This principle produces a figure of merit,

$$n_{\text{effective}}\left(\sum_{j=1}^{J} X_j\right) = \left(\sum_{j=1}^{J} \frac{1}{n_j}\right)^{-1} \quad (6.22)$$

for limited data analysis where $n_{\text{effective}}(\sum_{j=1}^{J} X_j)$ is the number of measurements with a single parameter estimation of $\sum_{j=1}^{J} X_j$ gives an equivalent variance. When the n_j are

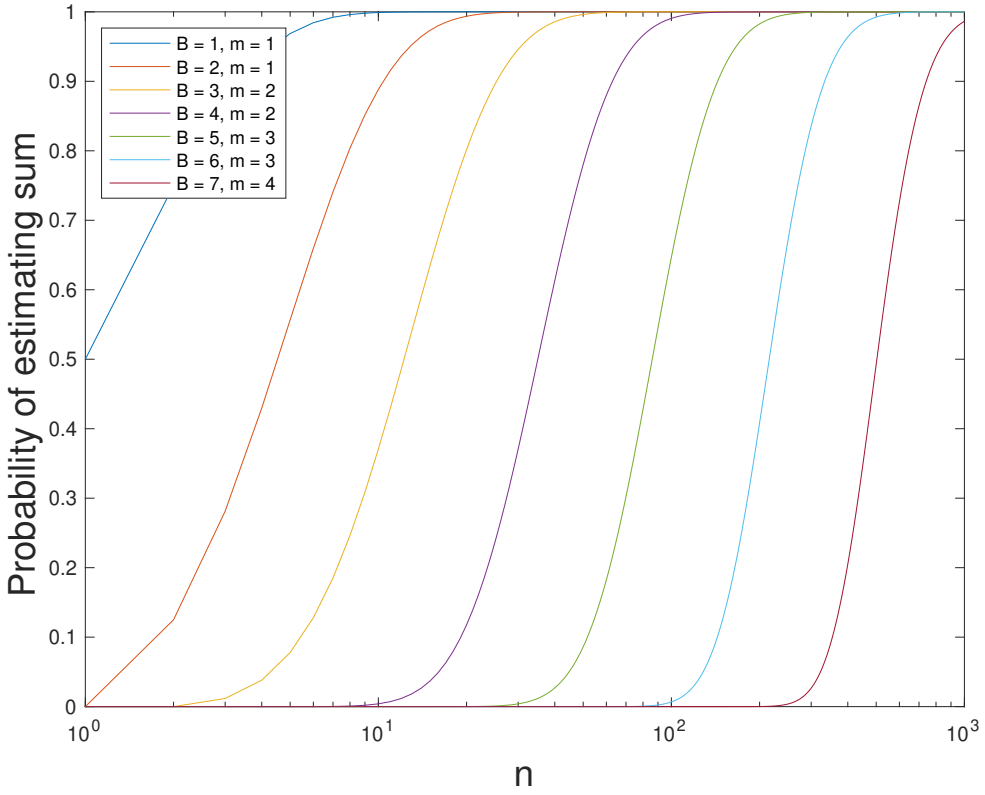

Figure 6.2: The probability of at least one result for each parameter combination using equation (6.20) with $J = \binom{B}{m}$. This is the probability of being able to draw any information about the sum of all of the parameters θ from the the set of sums of m parameters for B Bobs.

drawn from some non-constant distribution, such as the binomial distribution in this case, $n_{\text{effective}}(\theta)$ is always bigger when performing the estimation over the smallest possible combinations of $\varphi_k(m)$ that sum to any multiple of θ. Recalling that $Var(a\theta) = a^2 Var(\theta)$ for some constant a such that $n_{\text{effective}}(\theta) = a^2 n_{\text{effective}}(a\theta)$, the effective number of measurements when performing a single estimation from the $\varphi_k(m)$ with any specific m is

$$n_{\text{effective, one estimation}}(\theta) = \binom{B-1}{m-1}^2 \sum_{j=1}^{J} \frac{1}{n_j}, \tag{6.23}$$

where $J = \binom{B}{m}$. Writing J' as the smallest number of $\varphi_k(m)$ to sum to a multiple $\tilde{J} = \frac{J'}{J}\binom{B-1}{m-1}$ of θ forming a set of J/J' combinations the effective number of measurements for the multiple estimation method is

$$n_{\text{effective, multiple estimations}}(\theta) = \sum_{l=1}^{J/J'} \tilde{J}^2 \sum_{j=1}^{J'} \frac{1}{n_j}. \tag{6.24}$$

These effective number of measurements for the two methods have the inequality,

$$n_{\text{effective, multiple estimations}}(\theta) \geq n_{\text{effective, one estimation}}(\theta), \tag{6.25}$$

with equality when there are the same number of results for each $\varphi_k(m)$, $n_j = \frac{1}{J}\sum_{j=1}^{J} n_j \forall j \in \{1, 2, ..., J\}$. Furthermore, when there are multiple combination sizes possible the largest group of smallest combinations is always more effective. Returning to the $\{B = 4, m = 2\}$ example,

$$n_{\text{effective, one estimation}}(\theta) = 9\left(\frac{1}{n_1} + \frac{1}{n_2} + \frac{1}{n_3} + \frac{1}{n_4} + \frac{1}{n_5} + \frac{1}{n_6}\right)^{-1} \tag{6.26}$$

$$n_{\text{effective, multiple estimations}}(\theta) = \left(\frac{1}{n_1} + \frac{1}{n_6}\right)^{-1} + \left(\frac{1}{n_2} + \frac{1}{n_5}\right)^{-1} + \left(\frac{1}{n_3} + \frac{1}{n_4}\right)^{-1}, \tag{6.27}$$

where $J = 6$, $J' = 2$, $J/J' = 3$ and $\tilde{J} = 1$. If $n_j = 10 \forall j \{1, 2, 3, 4, 5, 6\}$ then $n_{\text{effective}}(\theta) = 15$ for both methods. However, if instead $n_1 = 11$ and $n_2 = 9$ then

$$n_{\text{effective, one estimation}}(\theta) = 14.9497 < 14.9749 = n_{\text{effective, multiple estimations}}(\theta) < 15. \tag{6.28}$$

There is a further complication to the data analysis. For larger B there are values of m for which there might be multiple ways of combining the $\varphi_j(m)$ to get the smallest possible multiple of θ. For example, when $\{B = 6, m = 2\}$ the measured parameter $\varphi_1(2) = \phi_1 + \phi_2$ could be made a part of the following three combinations,

$$\theta = \varphi_1(2) + \varphi_{10}(2) + \varphi_{15}(2), \tag{6.29}$$

$$\theta = \varphi_1(2) + \varphi_{11}(2) + \varphi_{14}(2), \tag{6.30}$$

$$\theta = \varphi_1(2) + \varphi_{12}(2) + \varphi_{13}(2), \tag{6.31}$$

where

$$\varphi_{10}(2) = \phi_3 + \phi_4, \tag{6.32}$$

$$\varphi_{11}(2) = \phi_3 + \phi_5, \tag{6.33}$$

$$\varphi_{12}(2) = \phi_3 + \phi_6, \tag{6.34}$$

$$\varphi_{13}(2) = \phi_4 + \phi_5, \tag{6.35}$$

$$\varphi_{14}(2) = \phi_4 + \phi_6, \tag{6.36}$$

$$\varphi_{15}(2) = \phi_5 + \phi_6. \tag{6.37}$$

The different combinations could give different $n_{\text{effective}}$. Therefore, the algorithm to optimise the information gain from data relating to arbitrary $\{B, m\}$ by maximising

$n_{\text{effective}}$ proceeds as follows. First, make a list of all of the possible sets of combinations of the $\varphi_k(m)$ with the same m that sum to the smallest possible integer multiple of θ. Then, search for the way of combining them that maximises the sum of the $n_{\text{effective}}$ and use those sets of combinations to estimate the posterior distribution. The number of possible combinations increases rapidly with the number of Bobs, in particular when $m \not\approx 1, B$. Therefore, to improve computation speed for larger numbers of Bobs (eg 16) when the number of combinations is very large, perform the optimisation for the $\varphi_k(m)$ with the largest n_j, record the best combinations, add the next largest to the remaining set and repeat until no non-zero data combinations are available. This method only accounts for the amount of measurement results, a direction for future work could be to calculate $n_{\text{effective}}$ with different prior information for different parameters using a figure of merit that accounts for the resulting posterior distributions.

Once the method of combining the data is chosen the data is analysed using the following method. First, perform a grid approximation to likelihood functions, $\mathcal{L}(\varphi_k)$, numerically by splitting the 2π support into $K = 1024$ equally-sized bins such that $\theta_k = \theta_0 + k/K,\ k \in \{0, 1, 2, ..., K-1\}$ and calculating the value of the likelihood function for each bin.

Then, combine two or more likelihood functions to find the likelihood function of the sum of some of the $\varphi_k(m)$ (with the same m) parameters by convolving them using fast Fourier transforms. This reduces the order of operations for the convolution from $\mathcal{O}(K^2)$ to $\mathcal{O}(K \log K)$ operations and can convolute as many likelihoods as needed in a single calculation providing further efficiency improvements. This produces likelihoods $\mathcal{L}(\tilde{J}\theta|\vec{n})$ which, by transforming the support, provides $\mathcal{L}(\theta|\vec{n})$.

Do this for all of the $\varphi_k(m)$ for which there is sufficient data then take the product of all the $\mathcal{L}(\theta|\vec{n})$ and normalise to get a final normalised likelihood function for the protocol. The results in the next section and in chapter 7 use a uniform prior distribution $p(\theta|\alpha) = \frac{1}{2\pi}$ over an arbitrary 2π range. The prior distribution of the other $\varphi_k(m)$ are not important for the estimation of θ unless they combine to provide an improved prior distribution for θ.

Thus, the posterior distribution, $p(\theta|\vec{n}, \alpha)$ is equal to the normalised likelihood function. This broad prior with limited data creates broad posterior distributions which requires the use circular statistical inference methods including circular analogue to the mean square error introduced in chapter 3 and already used in chapter 5 as a measure of information gain. Similarly to chapter 5 this is applied to the posterior distribution of θ

as a measure of information gain in the next section and chapter 7.

6.3 Optimising information gain with a privacy limit

This section introduces an optimisation algorithm used to search for the optimal protocol parameters, the separable state rate, S, and fidelity checking rate, F, for a privacy limit of $\Lambda_E \geq 0.5$ as a function of the number of Bobs B and protocol rounds N. First, the objective of the optimisation is introduced and an algorithm to do so is discussed. Then, the optimisation results for the hybrid protocol introduced in section 6.1, a similar protocol using only entangled states and another similar protocol using only separable states are used to show the effectiveness and superiority of the hybrid protocol. Finally, it shows that the hybrid protocol can ensure both security and parameter estimation beyond the standard quantum limit.

6.3.1 Parameter optimisation algorithm

The optimal independent parameters $\{S, F\}$ for any number of Bobs B and protocol rounds N can be found using Monte Carlo simulations to calculate measures of information gain for Alice and Eve for specific protocol parameters and an optimisation algorithm to find the optimal parameters. Information gain from two different scenarios are compared to demonstrate the effectiveness of the protocol in the low-data minimal prior information regime for estimating θ while maintaining security against an eavesdropper in man in the middle attacks where Eve intercepts the states that Alice sends, measures them and replaces them with corresponding entangled states. In the first scenario there is no eavesdropping, a set of results $\vec{n}$ where $\sum_j n_j = N$ is simulated and grid approximation of Alice's posterior distribution for θ, $p(\theta|\vec{n}, \alpha)$ is used to calculate the circular mean square error. As introduced in chapter 3 and applied using equation (5.13) of chapter 5, this is averaged to find Λ_A as a measure of Alice's limited data information gain.

In the second scenario Eve attacks every round measuring and replacing the states with her own states that are entangled over all Bobs and correspond to her measurement results. She continues to do this until Alice detects her the first time at which point the protocol is stopped. The security requirements are dependent on the specific scenario. Here, the privacy limit is set such that Eve's average circular mean square error is bounded $\Lambda_E \geq 0.5$, approximately equivalent to a linear mean squared error of at least 1. This gives Alice a guarantee on how little information Eve can gain. The limit put on Λ_E can,

of course, be varied depending on the scenario and application.

The following algorithm optimises $\{S, F\}$ such that Λ_A, Alice's average posterior distribution circular mean square error, is minimised for the security limit $\Lambda_E \geq 0.5$, for various numbers of Bobs and round counts by searching through the possible protocol parameters. First, for $B = \{1, 2, 3, 4, 5, 6\}$ Bobs, $N = \{100, 500, 2500\}$ rounds and an evenly spaced 11×11 grid of possible S and F in the range $[0, 1]$, simulate Alice's information gain for N rounds and Eve's information gain until the first time she is detected 16 times for 64 sets of B randomly chosen parameters, ϕ_b, $b \in \{1, 2, ..., B\}$ (the same set for all simulations for $\{B, N\}$). Then, using the method described in section 6.2.2, calculate the posterior distribution $p(\theta|\vec{n}, \alpha)$ with a circular uniform prior for θ, $p(\theta|\alpha) = 1/2\pi$ for each set of results. Using equation (5.13) of chapter 5 with this posterior distribution grid approximation to calculate the circular mean square error of the posterior distribution and average to calculate Λ_A and Λ_E numerically at that point in that grid.

In chapter 7 figures 7.1 and 7.2 demonstrate the security is monotonic in both F and S for each B. The Fisher information is also monotonic in the opposite direction. However, as demonstrated in section 6.2.2, the limited data information gain is not necessarily monotonic if $\{S, F\}$. Therefore, to find the optimal values of $\{S, F\}$ the algorithm searches near the optimal value of F for each value of S in the grid. So, to search for better parameters, build a new, evenly spaced, grid with half the spacing of the previous grid out of those points and all of the points between them and repeated the previous step. The figures in section 6.3.2 are from repeating the optimisation step 3 times and using the results of the simulations for the single grid point that minimised Λ_A while $\Lambda_E \geq 0.5$ for each $\{B, N\}$.

6.3.2 Parameter optimisation results

These two scenarios were chosen because the detection of Eve depends on the number of rounds that she attacks, not the number of rounds that Alice attempts. Also, to be sure that Eve could not get as much or more information than Alice, Alice would want to ensure that Eve is detected a long time before reaching the total number of rounds. If Alice reaches the total number of rounds intended and Eve attacks without being detected it should because she has only attacked a relatively small proportion of the rounds and thus cause only a small perturbation to Alice's results. Therefore the algorithm minimises Λ_A while ensuring $\Lambda_E \geq 0.5$ but, it is also important to ensure that Eve is detected long before the end of the predetermined rounds.

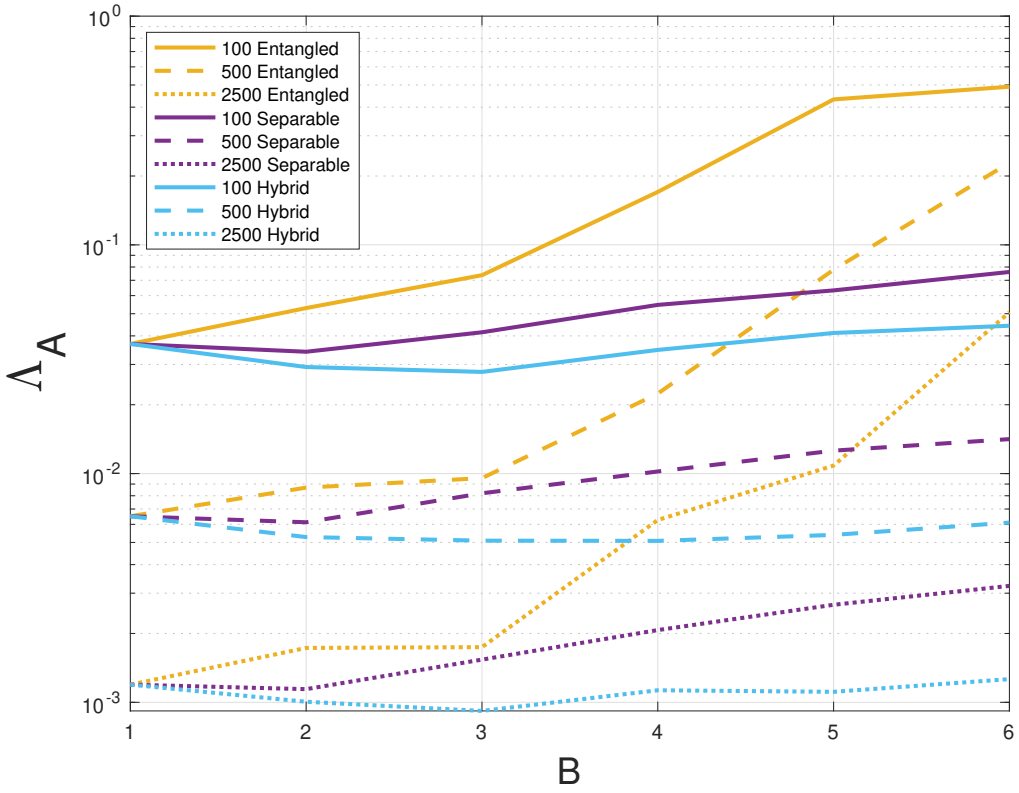

Figure 6.3: The mean, Λ_A of Alice's likelihood function circular mean square error, $\xi(\vec{n}, \vec{\phi})$ averaged over the sets of possible results $\vec{n}$ for many different values of Bobs' phases $\vec{\phi}$ in situations where Eve's mean circular mean square error has a lower bound $\Lambda_E \geq 1/2$ and minimised with respect to the protocol parameters S and F for a measure and replace with entangled states attack. This is plotted for three approaches: initial states entangled over all Bobs; initial states separable between the Bobs; hybrid of separable and entangled initial states used with probability of separable initial state S for each round. Solid lines represent a maximum of 100 rounds, dashed lines for 500 rounds and dotted lines for 2500 rounds.

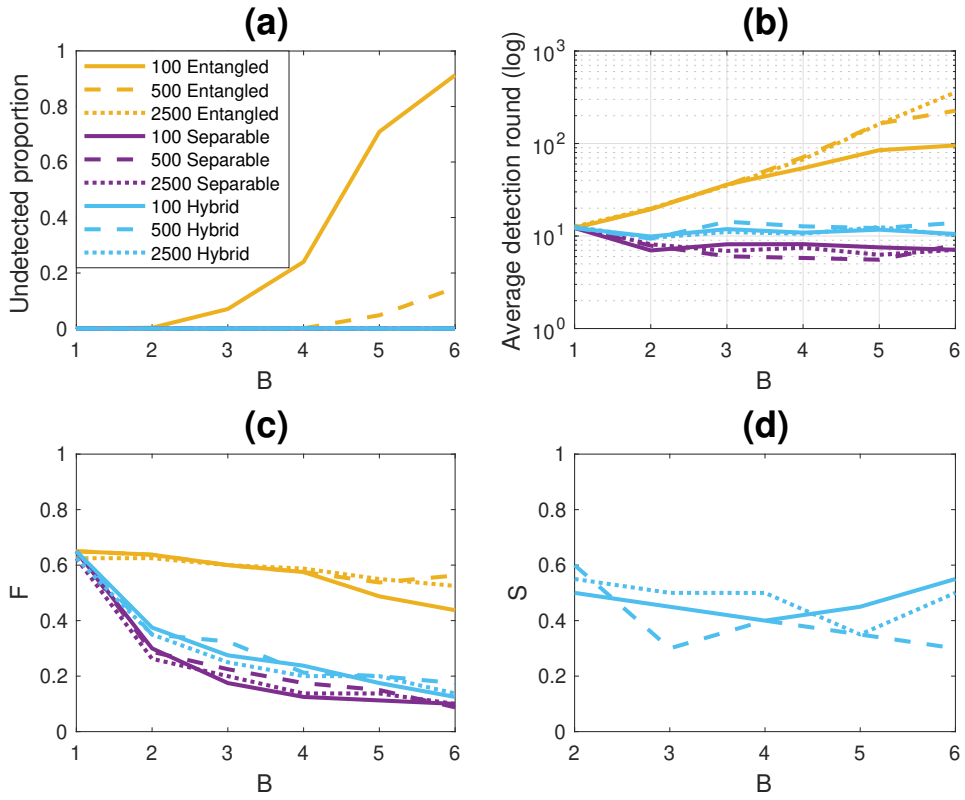

Figure 6.4: Optimisation results for $\Lambda_E \geq 0.5$ when Eve perform a measure and resend entangled state attack. (a)The proportion of times that Alice does not detect Eve before the end of the protocol. Other than 100 and 500 rounds entangled initial states, all of the lines are at or very close to zero and cannot be distinguished on this plot. (b) The number of rounds until Alice detects Eve for the first time. (c) Fidelity checking probabilities F. (d) Separable state probabilities S for the hybrid protocol.

The results of these simulations for 100, 500 and 2500 rounds are shown in figure 6.3. They demonstrates that a hybrid of separable and entangled initial states outperforms the use of only one of the two, showing little variation in information gain with the number of Bobs. The remainder of this section will discuss these results in more detail while comparing them to figure 6.4 which shows (a) the probabilityof Eve going undetected, (b) the rounds until detection and (c,d) the protocol probabilities chosen by the optimisation algorithm.

Entangled initial states are plotted in yellow on the figures. Figure 6.3 demonstrates that this choice of Alice's initial state performs increasingly worse than separable-only initial states and a hybrid protocol as the number of Bobs increases to the point that with low data and larger numbers of Bobs, Alice does little better than the security limits

placed on Eve (i.e. $\Lambda \geq 0.5$). There are two issues with entangled initial states. The first is that, with limited data, it is difficult to gain much information for certain protocol parameters, as suggested in section 6.2.2. The second is that security reduces with the size of the network, as suggested in section 6.1.

For low data a protocol with entangled only initial states performs even worse than figure 6.3 would suggest because the proportion of the large number of rounds where Eve goes undetected before the end of the protocols. The results shown in figure 6.3 do not account for Eve going undetected. Figure 6.4(a) shows that 5 or more Bobs with 500 rounds and 3 or more Bobs with 100 rounds there is a non-negligible probability of Eve going undetected for the entire protocol. Firstly, this is unacceptable from a security point of view. Secondly, figure 6.4(b) demonstrates that this corresponds to an average number of rounds before detection being of the same order of magnitude as the total rounds. This means that the effect of an undetected eavesdropper (who may attack only some rounds) on Alice's estimation would be more than a small amount of noise making her perform even worse than in figure 6.3 or forcing her to perform significantly more fidelity checks than figure 6.4(c) suggests which would also make her estimation even worse.

Separable initial states are plotted in dark purple on the figures. These show excellent security features regardless of the number of rounds. It can be seen in figure 6.4(b) that Alice's optimised information gain is achieved while ensuring that Eve can attack fewer than 10 rounds on average before she is detected, independent of the number of rounds or number of Bobs. For separable states, the number of fidelity checks for a constant F increases linearly with the number of Bobs so, as demonstrated in figure 6.4(c), F can be reduced as the number of Bobs increases. However, the disadvantage of using separable initial states is that there is no quantum enhanced measurement precision from entangled states limiting the estimation uncertainty to be greater than the standard quantum limit. Figure shows 6.3 that this causes the measurement efficiency to reduce with the number of Bobs. The reduction is close to the linear reduction in a metrology protocol without security.

Hybrid initial states are plotted in light blue on the figures. As the number of Bobs increases, the security is increasingly reliant on the separable initial states, figure 6.4(d). This is because the average number of security checks per round for entangled initial states is given by F^B and so reduces rapidly with network size. By contrast, the average number of security checks per round for separable initial states increases with network size as BF since there is the possibility of more than one check per round. The fidelity

checking probability for hybrid initial states when optimised to fulfil security conditions and minimise Alice's estimation dispersion is shown in figure 6.4(c) and follows a similar shape to the separable initial states. Similar to the separable only states, the average number of rounds before Eve is detected remains fairly low for any number of Bobs. It is not quite as low as the case of separable only states because, as shown in figure 6.4(d), many rounds make use of entangled states which have reduced security as discussed above. However, it remains sufficiently small that, in cases where Eve does not make enough attacks to be detected, Alice's information is approximately that given by a protocol with no eavesdropper.

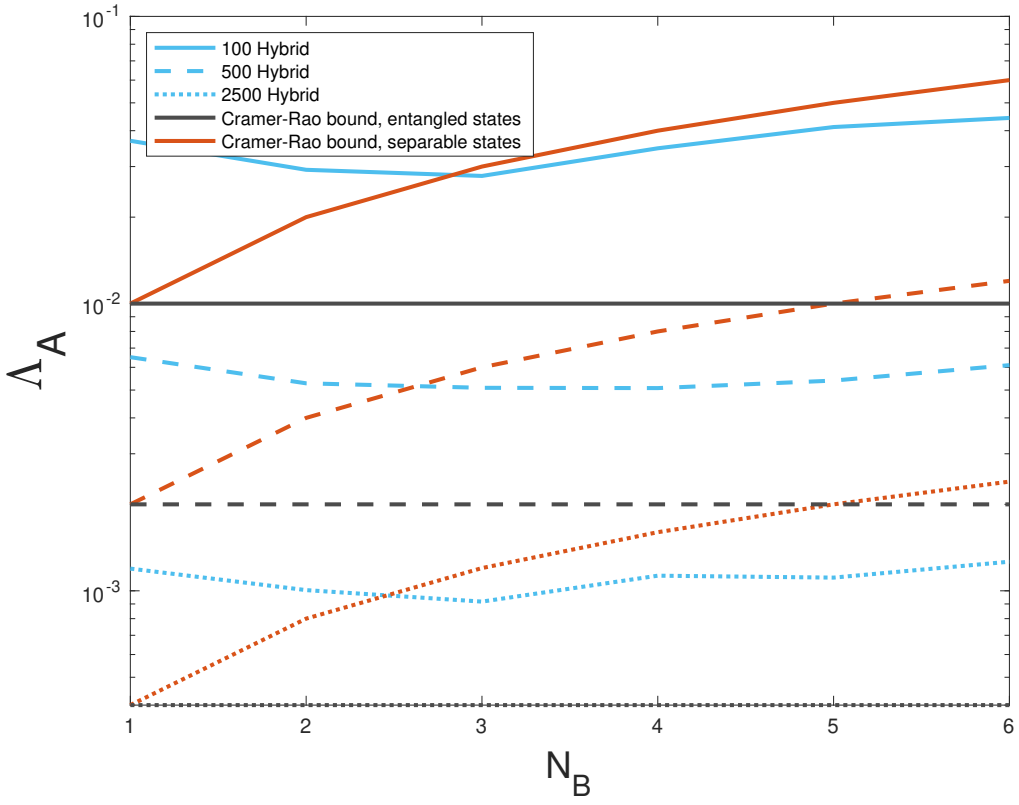

Figure 6.5: Comparison of Alice's maximum Λ_A while limiting Eve's $\Lambda_E \geq 1/2$ with the Cramér-Rao bound for non-secured metrology protocols using separable and entangled probes. When the blue line is below the equivalent red line it shows estimation beyond the standard quantum limit achieved by combining the results of separable estimations.

Using optimisation of the parameter estimation set out in section 6.2.2 is very important for producing these results. It's effect is increased for larger numbers of Bobs and more limited data. In particular, it allows Alice and Eve to extract significantly more information in these scenarios. The information gain limit of $\Lambda_E \geq 0.5$ is very small so

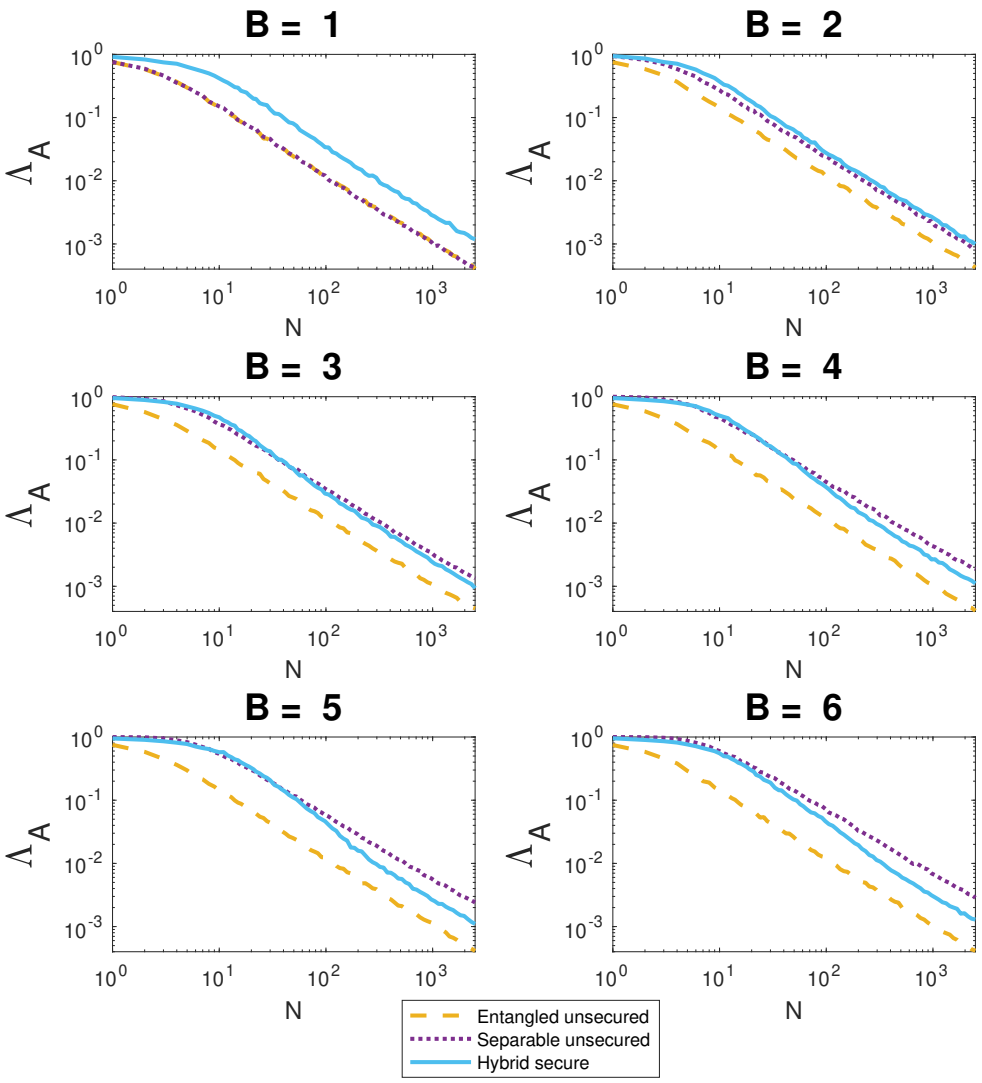

Figure 6.6: Λ_A as a function of the number of rounds, N, for different protocols and different numbers of Bobs. The purple dotted line is the result for an non-secured ideal system using separable states. This represents the standard quantum limit which scales as B/N. The yellow dashed line shows the result for an unsecured ideal system using entangled states. This shows estimation beyond the standard quantum limit at $1/N$. The solid blue line is the result for a system that uses a combination of separable and entangled initial states and is secure up to $N = 2500$. The protocol parameters have been taken from figure 6.4 for $N = 2500$. The information gain has not been optimised for fewer rounds but security is guaranteed. In some cases the secure hybrid protocol performs worse estimation than the separable unsecure protocol for low data and better for more data. This is because, as set out in section 6.2.2, the secure hybrid protocol produces information for θ beyond the standard quantum limit through the $\varphi_k(m)$ but can only do so when there are measurement results available for an appropriate selection of them requiring more data to become effective.

it is even more important when calculating Eve's information gain. If the more basic, single estimation technique is used instead neither party can gain much information from entangled states with low data and $F \not\approx 0, 1$. This forces the results of figure 6.4 (c) for the entangled only protocol to large F as B increases which in turn gives $\Lambda_A \approx \Lambda_E$ so that no party gains any information making the entangled only protocol appear to be even less effective. Critically, using the more complex data analysis methodology improves the results for the hybrid protocol. Using the basic methodology figure 6.3 would show Λ_A increasing with B instead of the almost flat line shown here.

The Cramér-Rao bounds for similar metrology protocols without security for separable and entangled initial states have variances given by B/N and $1/N$ respectively, where N is the number of rounds. Corresponding to single qubits being used to measure single parameters, B/N is the standard quantum limit. When using hybrid initial states there is a trade-off between the enhanced security of separable states and enhanced measurement precision of entangled states. Figure 6.5 shows that for three or more Bobs, the hybrid protocol (with $\Lambda_E \geq 0.5$) has an average dispersion less than the Cramér-Rao bound for separable probes and 3 or more Bobs. This shows quantum enhanced measurements and security combined into a single protocol.

Figure 6.6 shows plots of Λ_A for 1 to 6 Bobs between 1 and 2500 rounds for protocols with no fidelity checking and either separable or entangled initial states only compared to the hybrid protocol as optimised for 2500 rounds. It clearly demonstrates that the hybrid protocol, while being secure, is also capable of performing quantum enhanced measurements for functions of parameters spread across a network of sensors with increasing effectiveness with network size. Using the values for F and S for the hybrid protocol optimised for 2500 rounds ensures that the protocols conform to the security limit up to 2500 rounds. However, it is not optimised for information gain with fewer rounds. This would be further enhanced by combinations of single and multiple pass estimations of θ set out for two-party SQRS [16] in chapter 5.

6.4 Summary and outlook

Summary

This chapter demonstrates a method of performing quantum-enhanced metrology for sums of phase parameters at a collection of remote sites with information privacy and integrity. The security persists even when the eavesdropper has access to the measurement results,

the information in all classical communication channels and the ability to measure and manipulate states in quantum communication channels. It is qualified by demonstrating that Eve cannot interpret the classical information without interfering with the quantum communication channel and that she is exponentially more likely to be detected with each round where she manipulates that channel.

Privacy is quantified by defining a measure of limited data information gain as the average circular mean square error of Eve's posterior distribution from the data that she can get from measure and replace attacks before being detected and choosing protocol parameters to ensure it. Furthermore, it optimises the protocol parameters for Alice's information gain while ensuring a privacy limit of $\Lambda_E \geq 0.5$ and demonstrates that the protocol can have this level of security while achieving parameter estimation beyond the standard quantum limit for three or more Bobs.

These results show a way of implementing quantum enhanced sensing for functions of parameters over remote networks with information privacy. The performance would be further enhanced by using multipass protocols of chapter 5. Chapter 7 provides further security proofs including the number of spoofing attacks on the quantum channel before detection, the distribution of the information stealing rounds before detection and a lower limiting distribution on Λ_E as a function of the protocol parameters [17]. It also extends the scope of the security introducing quantum encoded shared secrets and security against attacks manipulating the classical communication channels [16].

Outlook

The protocol can be generalised to all linear functions of parameters by finding the optimal distribution of resources using the methodology at the end of chapter 2 and following the same steps used here for sums of parameters. In general, each of Bob's parameters could be considered to be a linear function of parameters to be encoded rather than a single parameter. In cases where there are integer parameter multiples of parameters, multiple probe parameter interactions could be used by each Bob and in cases where the phase encoding is time dependent the probe parameter interaction time could be controlled. Furthermore, if the situation is such that each parameter at a Bob can only be interacted with by a single probe then Alice could send entangled probes to the relevant Bobs for the parameter interaction. These methods would maintain the same security in terms of the number of attacks before detection but the information gain for the function would be different. The protocol Fisher information would be more difficult to calculate in such

scenarios but, the Matlab code in the relevant github repositories owned by the S-W-Moore profile, could be easily applied to such scenarios which gives a limited data measure of information gain from which the information gain in the asymptotic limit, such as the Fisher information, can be approximated.

The protocol could also be adapted to further metrology scenarios such as different prior distributions [99–101, 110], noisy scenarios [12, 13] and non-linear functions of parameters [59, 111]. Chapter 7 quantifies the security of the protocol introduced in this chapter for a single parameter ϕ_b. Another interesting direction for future work is to consider scenarios where Alice and Eve are interested in estimating different functions of parameters and have different prior informations. Using entanglement over subsets of Bobs could be useful for this.

A significant difficulty with practical implementation of this protocol is the decoherence of GHZ states. This would not be an issue for the security as separable states are sufficient to provide that. It would only reduce the information gain. Chapter 7 does not account for this. Therefore, in addition to the noise discussed in the outlook for chapter 5 the decoherence of the GHZ states would be an additional source of noise to consider for the network protocol. Furthermore, for practical application of secure network protocols it would be valuable to analyse the applicability of more noise resistant entangled states which can still bring a measurement advantage such as W states.

Chapter 7

Man in the middle attacks

To perform SQRS cryptographic principles are used to ensure privacy and integrity. Privacy is a measure of how much information an adversary such as the eavesdropper, Eve, may gain. In the case of SQRS, when Eve has some knowledge of both the initial quantum state and the measurement result she improves her ability to estimate the unknown parameter that was being measured. Therefore, privacy may be qualified by demonstrating that the more Eve attacks to steal information the more likely she is to be detected by Alice and/or Bob allowing them to stop the protocol. It is quantified by limiting the possible information that Eve can gain from those attacks.

Information integrity is a measure of the fidelity of the information compared to the ideal case. For metrology this means that Alice gets an unbiased parameter estimate from the protocol regardless of the actions of Eve (or noise). Similarly to privacy, it is qualified by demonstrating that the more Eve attempts to bias Alice's parameter estimation the more likely her presence is detected. It can be quantified by creating a measure of the amount of bias that Eve can impart on Alice's estimation without being detected. There is a key difference when qualifying privacy and integrity; to successfully spoof Alice's results the attack on the integrity must remain undetected.

In chapter 4 three security conditions were set out for SQRS. All of the protocols discussed by that chapter fulfilled the first condition, Some were shown to to fulfil the second and minor changes for others were suggested so that they, too, could fulfil the second. The novel protocols introduced in chapters 5 and 6 were shown to fulfil the first condition and how effectively they could fulfil the second condition was demonstrated. The subject of this chapter is man in the middle attacks. It gives greater detail and more analytical results for the security of the novel protocols in this thesis with regards to the

second security condition and shows how the third security condition can achieved.

The first security condition is that Eve cannot gain any information about the parameter of interest from the classical data alone. This ensures that observation of the system is not sufficient to attack privacy so, a successful attack must involve her interacting the system enacting the protocol. For example, man in the middle (MIM) [112] or side channel attacks. Chapters 5 and 6 explain that their protocols fulfil this security condition by ensuring that the density function from Eve's perspective is proportional to the identity ensuring that she can extract no meaningful information from the available data.

The second security condition is that any attack that manipulates the quantum communication channel is exponentially more likely to be detected with the number of rounds attacked and their effect is limited. Chapters 5 and 6 show that any such attack would be detected and demonstrate show optimisations of their protocols for the information gain while maintaining a specific privacy limit on Eve's information gain. Section 7.1 goes further. It begins by setting out the probability of different attacks being detected on a single round. Then, it uses those results to find a limiting distribution for the number of attacks before detection. Finally, it shows a limiting distribution of the security limits for network SQRS.

The third security condition is that any attack that manipulates the classical channel is exponentially more likely to be detected with the number of rounds attacked and their effect is limited. In general SQRS protocols assume that there is some classical information authentication that is used to ensure that Alice knows that she is communicating with Bob but Eve can still interpret the information shared. Fulfilling this condition without using classical authentication expands the domain of applicable scenarios to those where there is no encryption on the classical communications so that all of the security is integrated into as single protocol. Section 7.2 introduces a more advanced protocol between Alice and each Bob that ensures protection against attacks on the classical communication channels. First, methods of quantum encoding shared secrets are given. Then, it shows that a path information delay protects against spoofing with manipulations of the classical communication channel. Finally, limits on the amount of information that can be stolen by manipulating the classical information to hide MIM attacks on the quantum communication channel are demonstrated.

This chapter also considers an important issue with a practical method of implementation, photonics. The issue is photon splitting attacks on qubits travelling through the quantum communication channel. Section 7.3 demonstrates how, due to the fact that

the novel protocols introduced in chapters 5 and 6 never publicly declare the basis of the initial states, they are significantly better protected against such attacks than SQRS and quantum key distribution protocols that do declare the state basis. This would permit a practical implementation of these protocols to maintain good levels of privacy with significantly higher flux.

7.1 Quantum channel protection

This section gives greater details on the quantum communication channel protections for the two SQRS protocols set out in chapters 5 and 6. It begins with the probability of different attacks being detected on a single protocol round. Then, it uses these probabilities to build distributions for the number of rounds that Eve can attack before she is detected as functions of the independent parameters $\{B, S, F\}$, the number of Bobs, separable state and fidelity checking probabilities respectively. Finally, it uses those distributions to set lower limits on Λ_E the privacy bound on Eve's average information gain before being detected.

Chapter 5 sets out the single state detection probabilities for a single round on a separable state being verified by a single Bob. For an intercept and replace attack (IR) the state on arrival is random giving a probability $d_{IR} = 1/2$ of being detected when Bob sends the state to a fidelity check corresponding to the initial state. There are two equally probable fidelity checks states so the probability of detection is $P_{\text{sing,IR}} = 1/4$ if a Fidelity check is performed. Alternatively, a measure and resend attack (MR) has a probability $d_{MR} = 1/4$ of being detected when the correct fidelity check is used [8, 16] and $P_{\text{sing,MR}} = 1/8$ when any fidelity check is used. If instead Eve attempts to spoof the result by applying some phase gate $P(\delta\phi)$ in the quantum communication channel the probability of detection when using the correct fidelity check is $d_{SP}(\delta\phi) = \frac{1}{2}(1 - \cos(\delta\phi))$ and the probability from any fidelity check is $P_{\text{sing,SP}} = \frac{1}{4}(1 - \cos(\delta\phi))$.

For the single Bob protocol of chapter 5 equation (5.20) gives the distribution of the number of rounds before Eve is detected and figure 5.10 gives the corresponding privacy limit as a function of the fidelity checking rate, F. If, instead, Eve attacked a single parameter of a multiple Bob protocol from chapter 6 then the detection probability would be similar. For separable initial state $d(\text{separable}) = FP_{\text{sing}}$ would be unchanged. For entangled initial states d would be unchanged but a fidelity check would occur only when all of the Bobs simultaneously decide to perform a fidelity check with probability F^B.

Thus, $d(\text{entangled}) = F^B P_{\text{sing}}$ and the probability of detection in a single round is

$$d(\text{single parameter attack}) = \left(SF + EF^B\right) P_{\text{sing}}, \tag{7.1}$$

where P_{sing} could be $P_{\text{sing,IR}}$, $P_{\text{sing,MR}}$ or $P_{\text{sing,SP}}$. Therefore, transforming $F \to SF + EF^B$ figure 5.10 gives the security for a single parameter being attacked and equation (5.20) can be used to calculate the distribution of rounds until an attack is detected.

For multiple Bobs the number of rounds where Eve gains information could include the one where Eve is detected. The probability including this round is given by another form of the geometric distribution,

$$P_{Geo2} = (1-d)^{\eta-1} d. \tag{7.2}$$

If Alice only uses GHZ states, then the number of rounds that Eve gains information from, η, is distributed by equation (5.20). If Alice uses a separable state, the number of rounds that she gains information on can be described by either equation (5.20) or equation (7.2) depending on whether she gained any information from the final round. A separable state will have several independent tests and measurements making it possible for Eve to gain some information as well as being detected one or more times in a single round. The maximum information gained for separable states is therefore bounded by what she would get from the number of rounds distributed by equations (5.20) and (7.2) from below and above respectively.

In a protocol using both separable and entangled initial states, an upper limit on the number of rounds from which Eve gains information before she is detected K times can be set by combining the two geometric distributions into a special negative trinomial as a distribution limiting the number information gaining measurements before detection from above,

$$P_{SNT}(K) \leq \sum_{k=0}^{\min(\eta-1,K)} \binom{K}{k} u^{\eta-k} \, d_S^k \, d_E^{K-k}, \tag{7.3}$$

where $u = 1 - d_S - d_E$ is the probability of being undetected in each round, d_S and d_E are respectively the probabilities of being detected from a separable or an entangled state in each round and η is the number of measurements that Eve could have got results for before being detected. Similar to the single Bob case, combined with values of $\Lambda(\eta)$ this puts a lower bound on Λ_E, an upper bound on Eve's average information gain given the protocol parameters.

The detection probability depends both on the type of attack that Eve performs and the initial state. The probability that Eve is detected on a single measurement, when her

strategy is to intercept and replace (IR) Alice's state with a random one, is d_{IR}. With initial entangled states, Alice requires a coincidence of all the Bobs performing a fidelity check, $p = F^B$ and the net measurement to be in the same basis as the original state $p = 1/2$ in order to detect Eve. The probability of an IR attack being detected when the initial state is entangled, $d(IR|E)$, is given by

$$d(IR|E) = d_{IR}F^B/2. \tag{7.4}$$

It is possible to detect Eve more than once in a single round when separable initial states are used. The relevant probability is that of there being at least one detection. For an IR attack the probability a detection by a single Bob is dependent on d_{IR}, F and the probability that the Bob performs the fidelity check in the same basis as the initials state $p = 1/2$. So the probability of a replace attack being detected at least once in a round when the initial state is separable, $d(IR|S)$, is given by

$$d(IR|S) = \left(1 - (1 - d_{IR}F/2)^B\right). \tag{7.5}$$

If Eve measures the quantum states and replaces (MR) them with her best guess at the same kind of state, the probability of her being detected, d_{MR}, in a fidelity check is less than it would have been if the replacement state was not informed by the measurement outcome, i.e. $d_{MR} \leq d_{IR}$. So, the probabilities of being detected on a single round for measure and replace attacks using separable states to replace separable states, $d(MR, S|S)$ and an entangled state to replace and entangled state, $d(MR, E|E)$, are given by

$$d(MR, S|S) = \left(1 - (1 - d_{MR}F/2)^B\right) \tag{7.6}$$

and

$$d(MR, E|E) = d_{MR}F^B/2 \tag{7.7}$$

respectively. If Eve measures an entangled state and replaces it with a separable state, when all of the Bobs perform a fidelity check Alice will interpret the state as if it was an entangled state. The net phase of the set of separable states sent by Eve would be the same as the phase if she had measured and replaced with an entangled state so the detection probability on a single round where Eve measures an entangled state and replaces it with a separable state, $d(MR, S|E)$, is the same as if she replaced it with an entangled state,

$$d(MR, S|E) = d_{MR}F^B/2. \tag{7.8}$$

If Eve measures a separable state and replaces it with an entangled state each Bob has an equal probability of getting a measurement result that corresponds to each of the

Detection probability in each round		
Eve attack type	separable initial state	entangled initial state
IR random separable	$S\left(1-(1-d_{IR}F/2)^B\right)$	$Ed_{IR}F^B/2$
IR random entangled	$S\left(1-(1-d_{IR}F/2)^B\right)$	$Ed_{IR}F^B/2$
MR separable	$S\left(1-(1-d_{MR}F/2)^B\right)$	$Ed_{MR}F^B/2$
MR entangled	$S\left(1-(1-d_{IR}F/2)^B\right)$	$Ed_{MR}F^B/2$
spoof $\delta\phi/b$ applied to b Bobs	$S\left(1-(1-d_{SP}(\delta\phi/b)F/2)^b\right)$	$Ed_{SP}(\delta\phi)F^B/2$

Table 7.1: The probability of Eve being detected at least once in a round. Decoherence of GHZ states would have a similar affect to IR attacks so.

initial states. The results are dependent on each other and the state that Eve sent but their distribution is the same for each Bob no matter the state Eve sent and no matter the initial state that Alice sent. Therefore, the detection probability when measuring a separable state and replacing it with an entangled state, $d(MR, E|S)$, is the same as a replace attack on a separable state,

$$d(MR, E|S) = \left(1-(1-d_{MR}F/2)^B\right). \tag{7.9}$$

The most practical way for Eve to attempt spoofing Alice's estimate for the function of parameters is to add a phase $\delta\phi$ to any single parameter as it requires only attacking a single quantum communication channel. In general, Eve could perform a spoofing attack by adding any set of phases to any set of initial parameters. Say, instead she added phases, $\vec{\delta\phi}$ to b Bobs such that $\sum_{j=1}^{B}\delta\phi_j = \delta\phi$ then the probability of be detected by entangled initial states would be unchanged,

$$d(SP|E, \vec{\delta\phi}) = d_{SP}(\delta\phi)F^B/2. \tag{7.10}$$

The probability of being detected by separable initial states would depend on the individual phases,

$$d(SP|S, \vec{\delta\phi}) = \left(1-\prod_{j=1}^{b}\left(1-d_{SP}\left((\delta\phi)_j\right)F/2\right)\right). \tag{7.11}$$

These probabilities are summarised in Table 7.1. As $d_{MR} \leq d_{IR}$, it is clear that when attacking the privacy it is always advantageous for Eve to use a measure and resend attack rather than a replace attack. The detection probability is lower when replacing with a separable state than an entangled state but, the information gain is less. Therefore, it is not immediately obvious which attack is better for Eve. However, as the number of Bobs

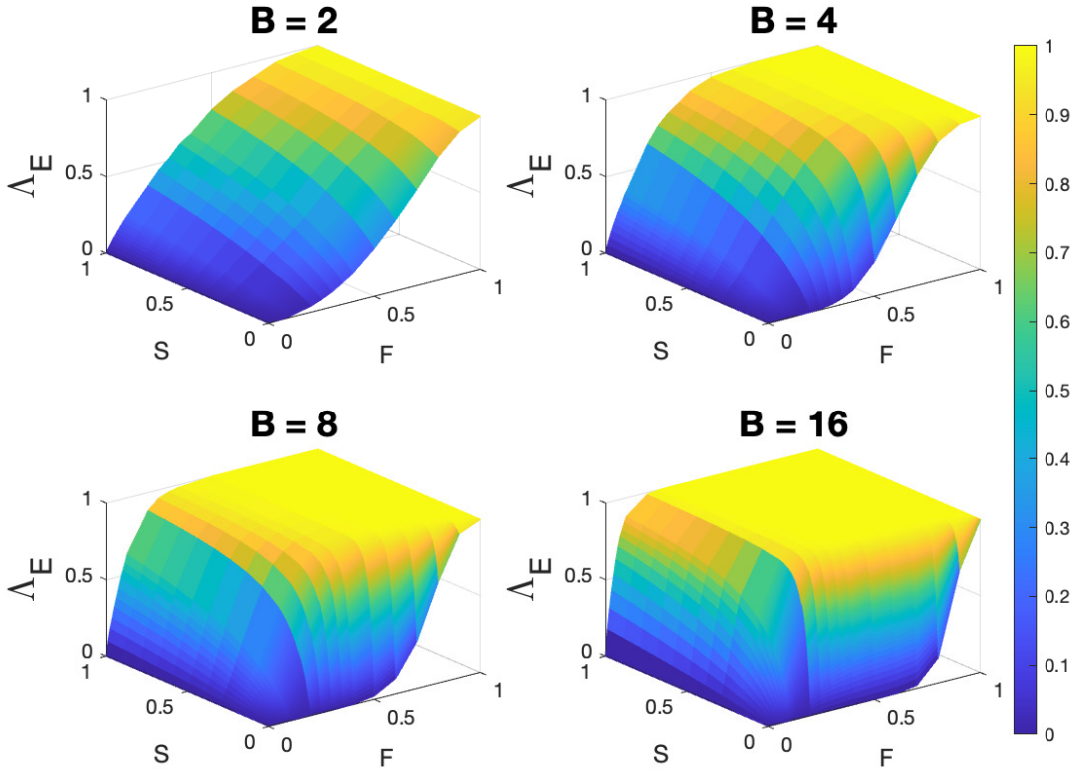

Figure 7.1: A lower limit on Λ_E for 2, 4, 8 and 16 Bobs when performing a MR attack with entangled states. The greater the value, the more secure the protocol.

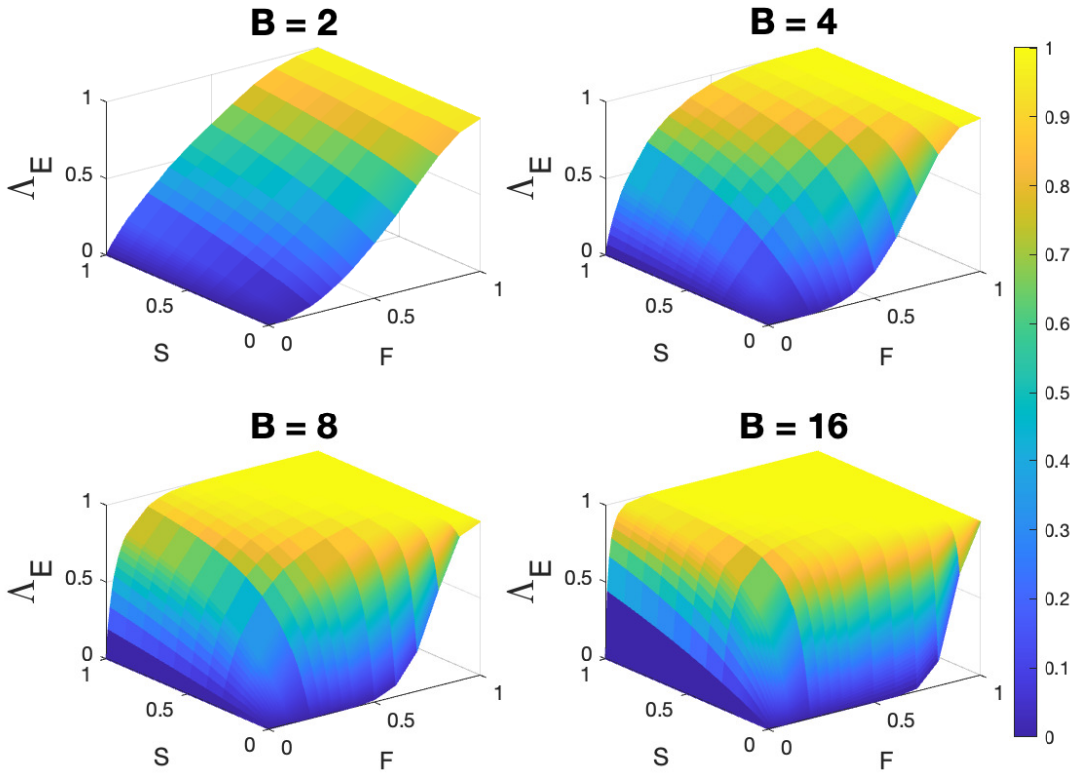

Figure 7.2: A lower limit on Λ_E for 2, 4, 8 and 16 Bobs when performing a MR attack with separable states. The greater the value, the more secure the protocol.

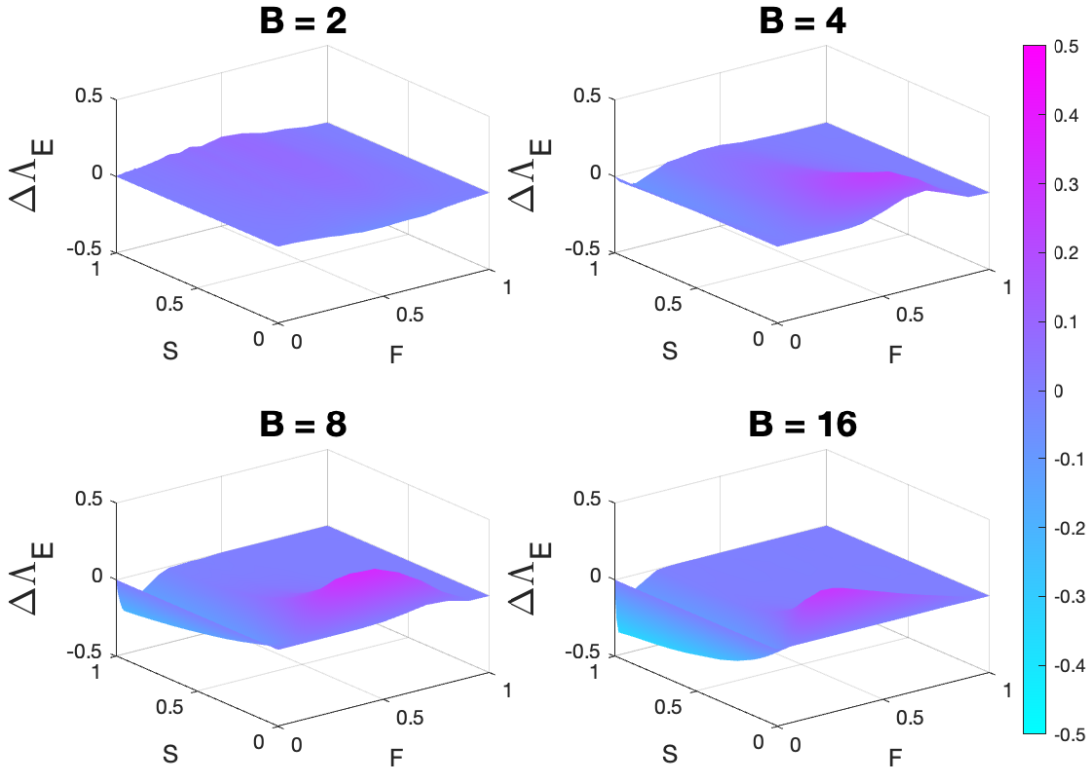

Figure 7.3: The difference in security between the two attacks in figures 7.1 and 7.2, Λ_E(entangled)$-\Lambda_E$(separable). The difference is negligible for the high security choices of S and F, i.e. both close to 1, indicating that the choice of attack type makes little difference. With lower security S and F entangled attacks show an advantage for low fidelity while separable states show an advantage for low separable state probability. These differences increase with the number of Bobs.

increases, a secure protocol increasingly relies on separable states for security. So, the advantage of using measure and replace entangled over replace entangled reduce rapidly with the size of a secure network.

In these protocols Alice stops the first time she detects Eve. Substituting $K = 1$ into equation (7.3),

$$P_{SNT}(1) \leq u^{\eta-1}\Big|_{\eta\geq 1} d_S + u^{\eta}\, d_E, \tag{7.12}$$

as a distribution that limits the number of rounds where Eve gains information before she is detected from above. Like the $B = 1$ case, $d_{IR} = 1/2$ and $d_{MR} = 1/4$. These, combined with the equations in Table 7.1 determine this distribution in terms of the protocol parameters. Similar to the single Bob scenario in figure 5.10 of chapter 5, Monte Carlo simulation was used to find $\Lambda(\eta)$ for $\eta \in \{0, 1, 2, ...50\}$ and by using a limiting value

$\Lambda(\eta > 50) \geq 0$ and weighting by the probability distribution of equation (7.1) puts a lower limit on Λ_E for Eve's attacks.

Figures 7.1 and 7.2 show this lower limit for 2, 4, 8 and 16 Bobs when measuring and replacing with entangled and separable states respectively. When deciding the parameters S and F for an implementation of the protocol Alice may choose a security limit Λ_E then use any values on these plots that is greater than Λ_E to get that level of security. If the intended number of rounds is very large the (inverse) Fisher information can be used to choose the optimal value. However, as discussed in section 6.2.2 of chapter 6, the intricacies of limited data information gain in these scenarios mean that the Fisher information may not be appropriate and it may be better to use some other method to choose optimal values. Either results of optimisation algorithms such as those in section 6.1 of chapter 6 can be used or, as the secure region is already determined, it suffices to perform a Monte Carlo simulation for the number of rounds Alice wants to use to determine a good choice of S and F selected from those values near the security limit calculated here.

7.2 Classical channel protection

This section shows how some straightforward adaptations to protocols of chapters 5 and 6, shown in figures 5.1 and 6.1, brings further security features to those protocols. The protocol between Alice and any Bob with these additional security features is shown in figure 7.4. Section 7.2.1 discusses how shared secrets can be applied to the protocol to enhance its security. Section 7.2.2 shows how delayed path information communication stops Eve from spoofing Alice's parameter estimation. Section 7.2.3 demonstrates that the amount of information that Eve could gain from MIM attacks and hide by changing data in the classical communication channel is very limited.

7.2.1 Shared secrets

In order for Alice and Bob to be sure they are communicating with the party they think they are, quantum cryptographic protocols such as key distribution and SQRS require channel authentication [74] which requires some shared secret key. So far, it has been assumed that Alice and Bob are able to authenticate their communication channels by the same process. However, to integrate all of the security features into a single protocol, quantum encoded shared secrets should be used instead to alert Alice to the deception and stop Eve from gaining any useful information about ϕ from Bob. Two different methods of adding secrets can be used as quantum encoded authentication and an additional privacy

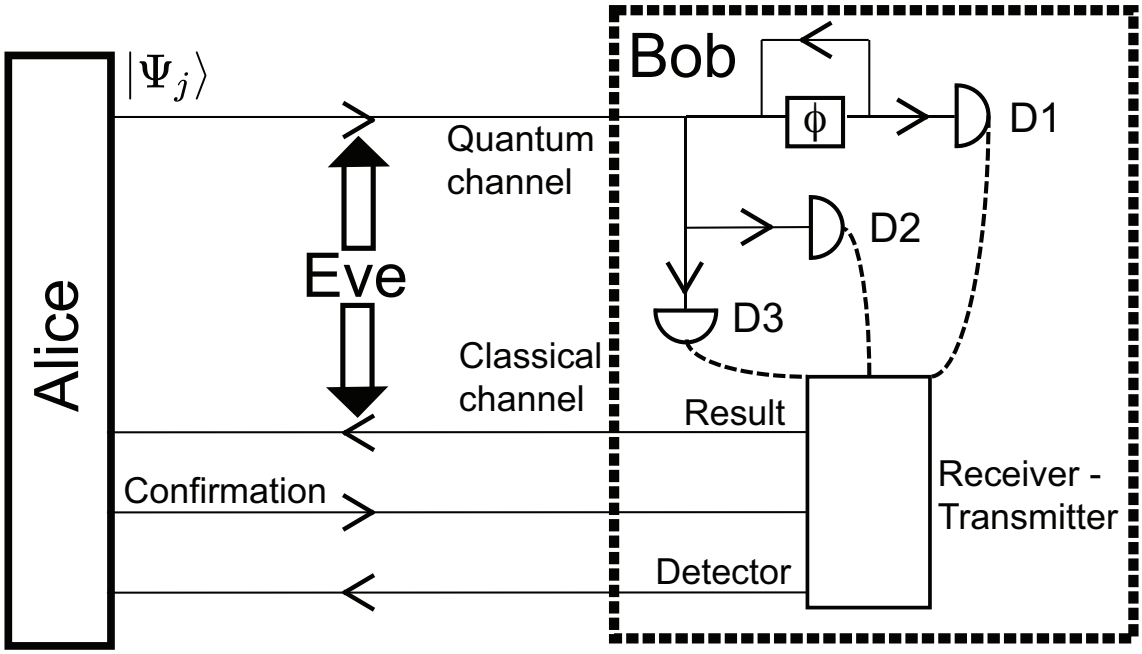

Figure 7.4: The SRS protocol between Alice and each Bob with additional security features. Alice sends states $|\Psi_j\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle + e^{i\chi_j}|1\rangle\right)$, $\chi_j \in \{\chi_0, \chi_0+\pi/2, \chi_0+\pi, \chi_0+3\pi/2\}$ to Bob through the quantum channel, where χ_0 is a secret shared between Alice and Bob. On the fidelity checking path, F, Bob performs projective measurements onto $\frac{1}{\sqrt{2}}\left(|0\rangle \pm ie^{i\chi_0}|1\rangle\right)$ at detector D2 and $\frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{i\chi_0}|1\rangle\right)$ at detector D3. On the parameter measurement path, M, Bob controls the number of times that the states pass through ϕ and then performs a projective measurement onto $\frac{1}{\sqrt{2}}\left(|0\rangle \pm e^{i\tilde{\epsilon}}|1\rangle\right)$ at detector D1, for some secret $\tilde{\epsilon}$. Bob initially sends the measurement result to Alice through the classical channel keeping which detector that performed the measurement secret. On receipt of the measurement result Alice sends a confirmation message to Bob who then sends the information on which detector performed the measurement.

measure.

Suppose Alice and Bob share a secret value for an angle, χ_0, that Alice shifts her states by, i.e $\chi \in \{\chi_0, \chi_0+\frac{\pi}{2}, \chi_0+\pi, \chi_0+\frac{3\pi}{2}\}$. If Bob then uses the angles χ_0 and $\chi_0+\pi/2$ for his measurements on the test paths D2 and D3, the state checking relationships remain the same as if neither party had rotated by χ_0. This can be seen from equation (5.6) where $\phi = 0$ on the test paths and $(\chi - \chi_0) \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$. This means that Alice can tell if Eve tries to impersonate Bob because the test outcomes she sends Alice will not match what Alice expects. Eve will not be able to tell whether Alice has shifted her basis without measuring some of the states Alice sends and she would be quickly detected if she tried to do this. Similarly, if Alice is sending an entangled state to multiple Bobs with each

performing measurements in the $(\chi_0)_j$ basis then Alice can add a phase $\sum_{j=1}^{B}(\chi_0)_j$ to her entangled state to get the same effect when they all perform their measurements.

Alice and Bob could share another secret $\tilde{\epsilon}$ for the orientation of the detector D1 on the parameter measuring path. By equation (5.6) of chapter 5 Alice would perform measurements with probabilities $P(\pm 1) = \frac{1}{2}\left(1 \pm \cos(\chi + \phi - \tilde{\epsilon})\right)$ with four values of χ that only she knows. If Eve tries to impersonate Alice to Bob she gains no meaningful information about ϕ. Eve would control χ in this scenario so that she gains information about $\phi - \tilde{\epsilon}$. However, without knowledge of the secret value of $\tilde{\epsilon}$ this tells her nothing about ϕ. Similarly, with initial states entangled over multiple Bobs when a selection of Bobs, $\mathbb{M}$ perform parameter estimation and the selection $\mathbb{F}$ perform fidelity checking Alice would estimate with measurement probability $P(\pm 1) = \frac{1}{2}\left(1 \pm \cos(\chi + \phi - \sum_{\mathbb{M}} \chi_j - \sum_{\mathbb{F}} \tilde{\epsilon}_j)\right)$ and Eve would remain unable to interpret the results.

7.2.2 Spoofing

As shown in section 7.1, any attempt to spoof Alice's results by adding a phase in the quantum channel would be detected by Alice. However, Eve could attempt to spoof the results and give Alice a false estimation of ϕ without her realising it by manipulating the $\{-1, +1\}$ data in the classical channel that correspond only to measurements of ϕ, i.e. not fidelity checking outcomes. For example, as demonstrated in figure 7.5, if Eve swaps *every* such datum, Alice will be led to believe that the correct value of the parameter is $\phi + \pi$. This can be seen from equation (5.5), where swapping $\phi \to \phi + \pi$, $n_1 \leftrightarrow n_2$, $n_3 \leftrightarrow n_4$, $n_5 \leftrightarrow n_6$, $n_7 \leftrightarrow n_8$, the probability distribution is unchanged.

By ensuring that Eve cannot know the path that was used or interact with Bob sending that information to Alice until after Alice has received the result, Bob guarantees that Eve cannot change the results for the measurement path without also changing the results of the test path which would reveal such an attack to Alice.

This is shown by the three classical information exchanges between Alice and Bob in figure 7.4. When a measurement is made Bob keeps which detector made the measurement a secret and sends only the measurement result $\{-1, +1\}$ to Alice. Once Alice has received the result she sends a message to Bob to confirm this. On receipt of this message, Bob sends the information of which detector and therefore, which path, the qubit was sent through. They proceed similarly for each qubit.

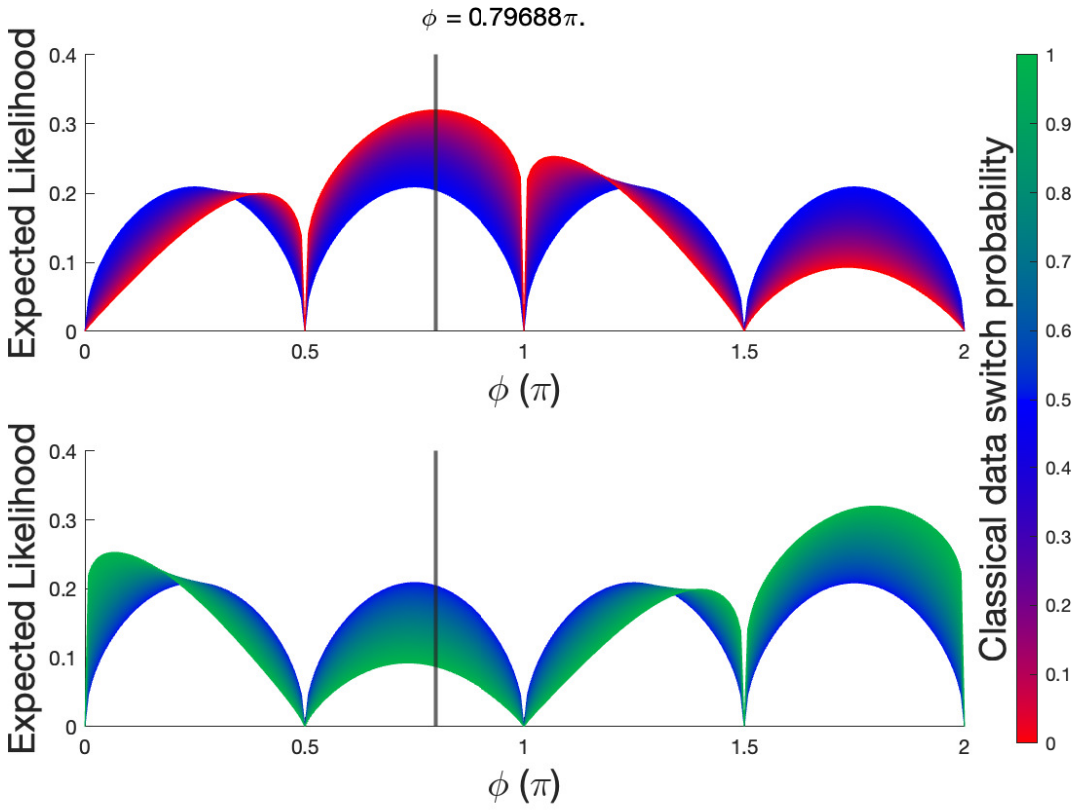

Figure 7.5: An example of quantum phase metrology when the classical data is spoofed. The two figures show the expected contribution of a single measurement to the likelihood function for large numbers of measurements when there are varying amounts of spoofing where the $\{+1, -1\}$ results for each parameter measurement have a probability in the range $[0, 1]$ of being spoofed. One figure shows the range $[0, 0.5]$ and the other shows $[0.5, 1]$. They are separated to avoid an overlap.

7.2.3 Disguising man in the middle attacks

To find out anything about ϕ, Eve needs to know the states that are used in Bob's measurements. Eve could attempt this by performing IR or MR MIM attacks. But, it has been shown throughout chapters 5, 6 and section 7.1 of this chapter that, by appropriately choosing protocol parameters $\{S, F\}$, this would be detected rapidly by Alice's checks on the states that the Bobs use for fidelity checking. What if, instead, Eve jointly attacked both the quantum and classical channels so that when she measured a quantum state, she hid this by amending the classical data that Bob sends.

In figure 7.4 it is clear that it is never to Eve's advantage to swap the detector value 1 for 2 or 3 in the classical data as this will only aid Alice in detecting her. Suppose instead that Eve attempts to hide the states that she has measured by changing the classical data

that Bob sends so that these are not identified as fidelity checks, i.e. switching appropriate values of 2 and 3 for 1. In this way, Alice would not check any of the states that Eve had measured and she could, in principle, go undetected while gaining information about ϕ.

One way of mitigating this is possible because Alice and Bob have to agree that a certain fraction of the states will be used for fidelity checks, F. This fraction can be publicly declared. Alice can then perform a statistical analysis of the number of test and measurement states declared in Bob's message. If it deviates from what is expected, this will give evidence that Eve is intervening.

This means that, while Eve can cover up the quantum states she measures by swapping the classical data to ensure these are not checked as test states, the number of times she can do this is limited by her not wanting to reveal herself through the biased distribution of $\{1, 2, 3\}$ in the classical data. Eve will only want to swap 2 and 3 for 1 so the distribution will become skewed. Doing the opposite would be equivalent to performing an IR attack on the quantum channel. The question is whether Eve will be detected before she gains meaningful information about ϕ.

The $\{1, 2, 3\}$ data sent to Alice has a binomial distribution with variance $\sigma^2 = \mu p(1-p)$, where μ is the number of states and p is the probability that a given state is used as a test, $\{2, 3\}$. Eve's measurements will be detected if she swaps more than $\sim \sigma = \sqrt{\mu p(1-p)}$ elements of the data set, meaning she can measure $\sqrt{\mu(1-p)/p}$ states because only the fraction p are fidelity test states and so need swapping. Overall, Eve will successfully gain information from $(1-p)\sqrt{\mu(1-p)/p}$ states because, of the states she detects, only the fraction $(1-p)$ will be used by Bob for measurements of ϕ. Alice can limit the information Eve receives by setting the total number of information-gaining states she manages to measure and hide to 1, which then gives $\mu = p/(1-p)^3$. By comparison, Alice will have $n(1-p)$ information-gaining measurements. The ratio of Eve's to Alice's information-gaining measurements is $(1-p)^2/p$. This is a monotonically decreasing function of p, so is minimised for $p = 1$. However, this $p = 1$ means that all the states are used for tests and Alice would get no information. Instead, for practical purposes it effective to use p close to 1 to both minimise the ratio and ensure that Alice can get information about ϕ. As an example, take $p = 0.9$, which means that Alice gets 90 information-gaining states, while Eve gets only 1 for one standard deviation (as fixed above). Alice's and Eve's Bayesian predictions of ϕ are shown in figure 7.6 for $\phi = 0.4\pi$ and different values of p. Alice correctly predicts this value with a clear peak, whereas Eve gains very little information.

Eve could get around this problem by employing a MR strategy and only altering the

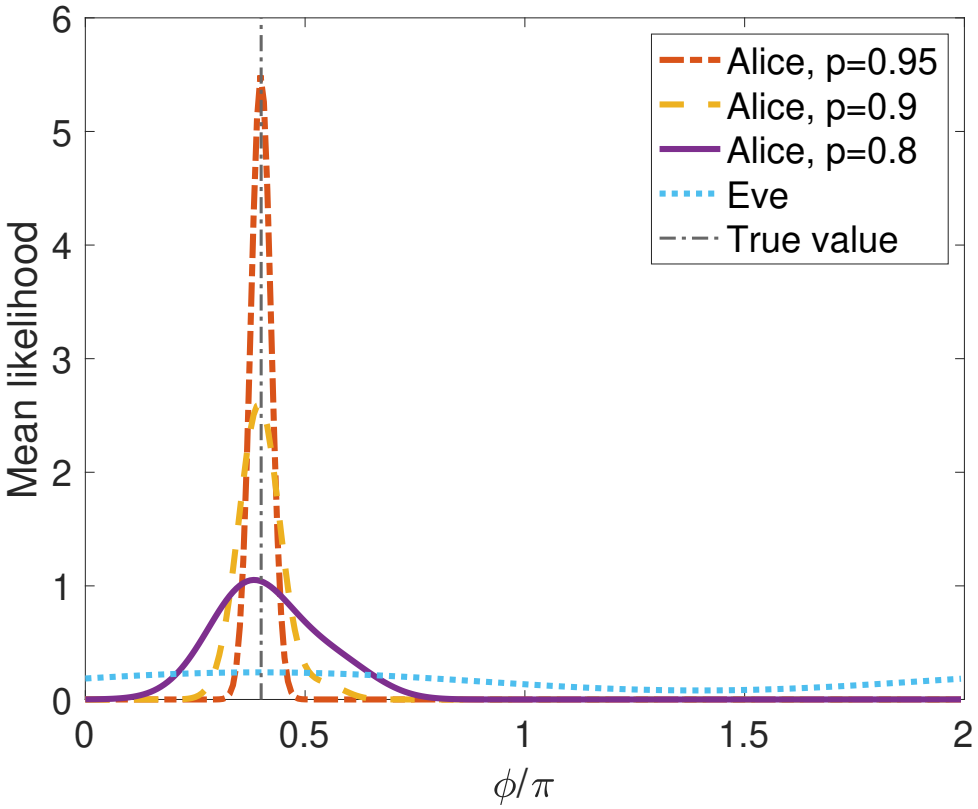

Figure 7.6: Bayesian prediction of ϕ for Alice and Eve with a MIM attack on a single Bob for a true value of ϕ of 0.4π and results have been averaged 10^6 times. Eve has 1 information gaining measurement while Alice uses $p \in \{0.8, 0.9, 0.95\}$ which allows her to use 20, 90 and 280 information-gaining measurements respectively. If Eve uses a measure and resend attack on the quantum channel half of the time she measures in the wrong basis giving Alice the wrong result for the affected measurement.

values 2 and 3, i.e. the fidelity checking measurement outcomes, in the classical data that is sent to Alice. If Eve measures and resends quantum states that subsequently go down the fidelity checking path and are measured in a different basis to the one that Eve measured in, she could switch the values 2 and 3. She will not have to change the measurement outcome because the fidelity checking measurement basis, $\{2, 3\}$, will only correspond to Alice's initial state when Eve has measured and replaced that state in the same basis. If she uses each basis with equal probability for her own measurements then the rate of neither will change regardless of Alice's initial state so, Alice could not verify for such an attack by investigating the fluctuations in the rates of detectors 2 and 3 compared to the initial states. This would hide what she had done because she can be sure that the subset of states Alice checks will not have been altered. This attack can be prevented by Alice

and Bob using a secret basis, χ_0 as introduced in section 7.2.1 making the protocol robust to man in the middle attacks of this sort.

7.3 Practical photonic implementation

Chapters 5 and 6 both demonstrated that for their respective protocols Eve gains no information about ϕ from the information communicated in the classical channel alone and if she tries to measure states in the quantum channel, she will be detected exponentially quickly. This section shows the viability of photons for the practical implementation of these protocols by considering photon-number splitting attacks [113, 114] by an eavesdropper.

The security of the quantum channel so far has been based on the assumption that Alice sends ideal qubits such as perfect single-photon states. If a state sometimes contains more than one photon, there is the possibility of Eve skimming off a photon, without Alice or Bob knowing, and using it to gain information about ϕ. There has, therefore, been a lot of interest in creating single-photon sources and current systems for realising this include colour centres, trapped atoms, quantum dots and heralded spontaneous parametric down conversion sources [115]. While good progress is being made, none of these systems are ideal; they can be difficult to implement and suffer from some degree of multi-photon emissions and low flux rates. The SQRS protocols discussed here are significantly more secure to photon-splitting attacks than many other quantum cryptographic protocols, including some SQRS and quantum key distribution protocols, making them less reliant on single-photon sources.

Instead of single photon sources, consider highly attenuated weak coherent state sources. For practical implementations, it is important to consider the rate at which Alice gains information. Having a higher average photon number per state increases the flux rate of photons arriving at Bob and therefore the bandwidth and information gain rate of Alice. However, this also increases the rate of there being two or more photons in a wave-packet and therefore the probability of Eve succeeding in a photon-number splitting attack. Current photon-based quantum key distribution protocols typically use decoy states to overcome this problem [83–85]. However, the novel SQRS protocols introduced in this thesis ensure significant information asymmetry between Alice and Eve even in the presence of photon-number splitting attacks, especially when combined with singlepass-multipass combined estimation.

The number distribution for photons in a coherent state is

$$P_{coh}(k) = \frac{e^{-\bar{k}}\bar{k}^k}{k!}, \tag{7.13}$$

where $\bar{k}$ is the mean photon number. The rate at which Alice gains information is proportional rate at which there is at least one photon per state, i.e. $1 - e^{-\bar{k}}$. Whenever there is more than one photon, there is the possibility of Eve gaining information. However, these protocols differ to many other quantum cryptographic protocols such as BB84. As stated in chapter 4, in those other protocols, Alice and Bob publicly reveal to each other what bases they used. If Eve manages to steal some photons, she is able to wait until this information is revealed and then measure her photons in the same basis to find some of the bits of the key. In the novel SQRS protcols introduced in this thesis, Alice and Bob never need to communicate any such information. So, even if Eve gains some photons without being detected, she does not know what basis to measure them in.

This difference is illustrated by comparing the asymptotic information gained by photon splitting in these protocols to those that declare their measurement basis. In protocols where the measurement basis is revealed Eve can gain all the information about the split photons. The rate of Eve's information gain relative to Alice's in protocols such as BB84 is therefore

$$\left(\frac{E}{A}\right)_{BB84} \leq \frac{\sum_{j=2}^{\infty} P_{coh}(j)}{\sum_{j=1}^{\infty} P_{coh}(j)} = \frac{e^{\bar{k}} - 1 - \bar{k}}{e^{\bar{k}} - 1}. \tag{7.14}$$

For the novel SQRS protocols introduced in this thesis, consider that Eve has access to Bob's classical information as it is sent through a public communication channel. Therefore, if she has some information about the state of a photon that Alice sends to Bob she may use this and Bob's measurement result to gain some information about ϕ.

Splitting photons enables Eve to gain a copy of the qubit being sent to Bob. By measuring this copy, Eve gains some information about Bob's state before its interaction with ϕ. From this and Bob's publicly available measurement outcomes, Eve's Fisher information for ϕ can be non-zero.

To put limits on the relative information rate of Eve compared to Alice in SQRS consider the quantum Fisher information when Eve is able to perfectly obtain any extra photons. If she splits off one photon she can perform any set of measurements on it. If she splits off more than one photon the simplifying assumption that she gains full information about the photon is made. This gives an upper bound to the relative information of Eve to Alice in the asymptotic limit

$$\left(\frac{E}{A}\right)_{SQRS} \leq \frac{\mathcal{F}_E(\phi)P_{coh}(2) + \sum_{j=3}^{\infty} P_{coh}(j)}{\sum_{j=1}^{\infty} P(j)} = \frac{e^{\bar{k}} - 1 - \bar{k} - \frac{1-\mathcal{F}_E}{2}\bar{k}^2}{e^{\bar{k}} - 1}, \tag{7.15}$$

where $\mathcal{F}_E(\phi)$ is Eve's quantum Fisher information for ϕ when she has a single copy of the initial state she has split off. For the four photon states that Alice can send $\{|\sigma_x = \pm 1\rangle, |\sigma_y = \pm 1\rangle\}$ the probabilities for Eve to get the result, +1, corresponding to a projection onto $\cos(\Gamma/2)|0\rangle + \sin(\Gamma/2)e^{i\gamma}|1\rangle$, are

$$P(E_{+1}|\sigma_x = \pm 1) = \frac{1}{2}\left(1 \pm \sin(\Gamma)\cos(\gamma)\right) \tag{7.16}$$

$$P(E_{+1}|\sigma_y = \pm 1) = \frac{1}{2}\left(1 \pm \sin(\Gamma)\sin(\gamma)\right). \tag{7.17}$$

Using Bayes' rule for Eve's posterior probability gives the probability she has a state $|\Psi_j\rangle$ given the measurement outcome E_{+1}

$$P(\Psi_j|E_{+1}) = \frac{P(E_{+1}|\Psi_j)P(\Psi_j)}{\sum_j P(E_{+1}|\Psi_j)P(\Psi_j)}, \tag{7.18}$$

where $P(E_{+1}) = \sum_j P(E_{+1}|\Psi_j)P(\Psi_j) = \frac{1}{2}$ and $P(\Psi_j) = \frac{1}{4}$ for all j, since the probability of all of the initial states to be equal. For the specific case of the σ_x and σ_y eigenstates,

$$P(\sigma_x = \pm 1|E_{+1}) = \frac{1}{4}\left(1 \pm \sin(\Gamma)\cos(\gamma)\right) \tag{7.19}$$

$$P(\sigma_y = \pm 1|E_{+1}) = \frac{1}{4}\left(1 \pm \sin(\Gamma)\sin(\gamma)\right). \tag{7.20}$$

Since each photon that Eve splits off is a copy of a photon that Bob measures, Eve can use her knowledge of the state from photon splitting to gain information about ϕ. When Eve is able to measure a single copy of a photon's initial state her corresponding density matrix for that state is

$$\hat{\rho}_E = \frac{1}{2}\Big(I + \frac{1}{2}\sin(\Gamma)\cos(\phi+\gamma)\sigma_x + \frac{1}{2}\sin(\Gamma)\sin(\phi+\gamma)\sigma_y\Big). \tag{7.21}$$

From this Eve has a quantum Fisher information, $\mathcal{F}_E$, for ϕ of

$$\mathcal{F}_E = \frac{1}{4}\sin^2(\Gamma) \leq \frac{1}{4}. \tag{7.22}$$

This has its maximum value when Eve measures in the same σ_x-σ_y plane as Alice's states and is independent of the orientation, γ, of the projective measurement in that plane. Substituting $\mathcal{F}_E = 1/4$ into equation (7.15) gives an upper bound to the information Eve gains from photon splitting attacks relative to Alice. These results are shown as a function of mean photon number per state in figure 7.7 and compared with BB84. SQRS

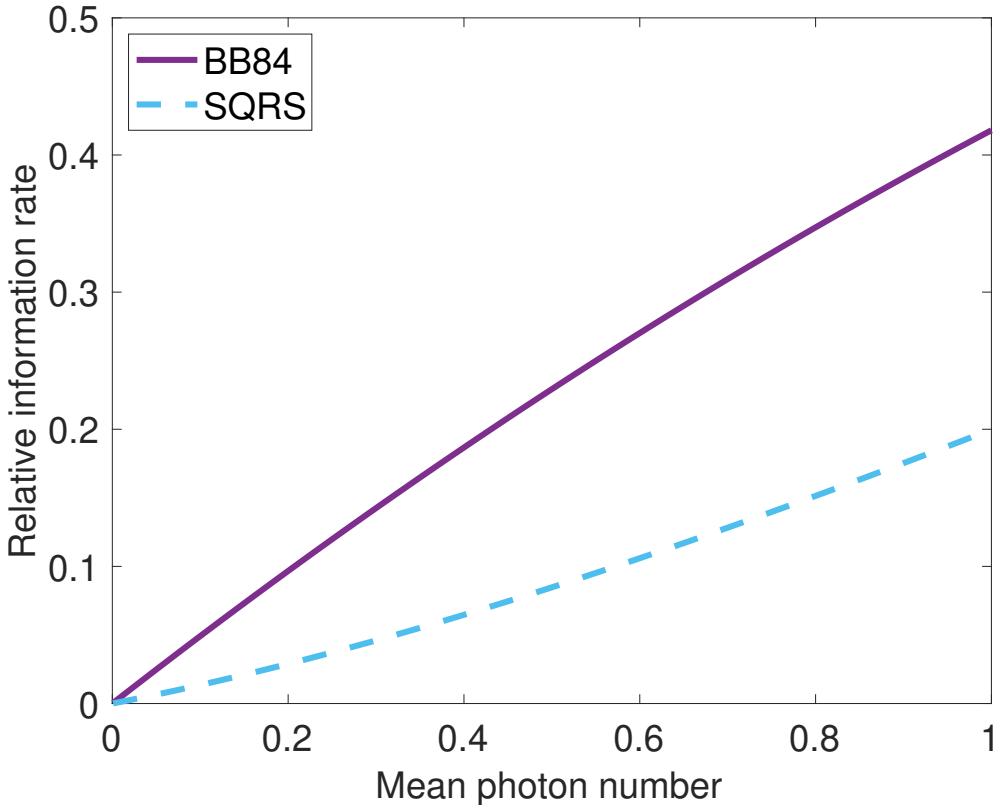

Figure 7.7: Upper bound to the information that Eve gains relative to Alice when making photon-number splitting attacks, as a function of the mean number of photons in each state. Results are compared for BB84 (solid line) and SQRS (dashed line). SQRS can be seen to be significantly more secure to these attacks than BB84.

is significantly less vulnerable to photon splitting attacks than BB84. The same results apply so long as Alice sends states with equal probability of having $\chi \in \{\chi_0, \chi_0+\pi/2, \chi_0+\pi, \chi_0+3\pi/2\}$, for any χ_0, which she controls.

If Alice uses a well-chosen multipass-singlepass combination such as those shown in figure 5.8 of chapter 5 the information asymmetry between Alice and Eve when performing photon splitting attacks will be further enhanced. Eve, with less information for the singlepass test than Alice will be unable to pick out only one peak or guarantee that she picks out the correct peak from the multipass test. Therefore, unless she has sufficient prior information to pick out the correct peak before starting, she will not be able to take advantage of the Heisenberg scaling that Alice gets using the multipass method.

When using limited data and a well-chosen multipass-singlepass combination Alice and Bob may decide to continue with the protocol regardless of the possibility of a man in the middle attack knowing that Eve would be able to extract a much smaller amount of

information than Alice.

In a network scenario with multiple Bobs Eve would struggle to gain non-negligible information from split photons. This is primarily because, without knowing if the initial state is separable or entangled Eve cannot easily interpret individual measurement results. Furthermore, information gain due to entangled states would be increasingly difficult to get as network size increases because she would have to split photons from every qubit to be able to gain any information and the more there are, the less likely she is to guess the correct initial state from measuring them. Still, Eve could still gain a little information by acting as if her estimates are made in a noisy regime where the noise rate is the probability of Alice's initial state not being the separable or entangled state that Eve thinks that she may be using to perform estimation in that specific round. Clearly, the information gain due to photon splitting attacks is even less for networks which would allow Alice to use coherent states with a higher flux rate.

7.4 Summary and outlook

Summary

This chapter extends the security proofs given in chapters 5 and 6 for the SQRS protocols that they introduce and provides adaptations to those protocols against a greater variety of MIM attacks. It gives stricter privacy bounds on these SQRS protocols than has been provided for any previous SQRS protocol and considers a greater variety of possible attacks than any previous SQRS protocol including some attacks involving manipulations of the classical communication channel and photon splitting attacks.

It begins with attacks on Alice's information privacy and integrity using the quantum channel. First, the probability of an attack on a single state round is given for many types of attacks are detected. These include spoofing attacks on the privacy and both MR and IR attacks using both entangled and separble states. Then a limiting distribution for the number of rounds until each attack is detected is calculated for the cases where Eve attacks a single parameter (in a one or multiple Bob scenario) and the function of parameters for a multiple Bob scenario.

It considers attacks on both the classical and quantum communication channels. A more secure set up for Alice and each Bob is given. This includes quantum encoded shared secrets and a path information communication delay which protects against spoofing by manipulating the classical communication channel. Furthermore, it introduces the concept

of hiding a quantum channel attack by manipulating the classical data demonstrating that the protocols maintain good privacy against such attacks with the aid of quantum encoded shared secrets.

Finally, it discusses a practical implementation using photons. It demonstrates the effect on privacy of photon splitting attacks on these SQRS protocols compared to quantum cryptographic protocols that declare the basis of their communicated quantum states in the asymptotic limit when coherent state photon sources are used. It shows a significant advantage to these SQRS protocols which could allow them to be used with a higher flux of photons than other protocols while maintaining information asymmetry.

Outlook

The security proofs for these protocols could be extended in a number of ways. Firstly, other measures of privacy could be used such as ensuring there is a very high probability that Eve's circular mean square error, ξ, is greater than a specific value instead of the mean Λ_E. More variety of quantum channel attacks could be considered, such as those where Eve may send either entangled or separable states in different rounds, states that are entangled over less Bobs and situations where Alice and Eve are attempting to estimate different functions of parameters and have different prior informations. Furthermore, privacy limits could be set when more than one attack is used simultaneously. In this chapter quantum channel attacks, quantum channel attacks that can be hidden in the distribution of the fidelity checking rate and photon splitting attacks are considered separately when they could all be used together. Finally, spoofing attacks could be investigated to the same level of detail as MR attacks have been by providing a measure of how much Eve could bias Alice's estimation relative to her detection.

As suggested throughout chapter 4 and in the outlook of chapter 5 these protocols use idealised models. Section 7.3 is a first look at the security issues caused by implementation with photons. It compares the amount of information that an eavesdropper could steal from photon splitting quantum cryptographic protocols that declare their measurement basis such as the BB84 protocol to those the novel SQRS protocols developed in the thesis. This depends on Eve's ability to discriminate the quantum state from split photons; this has probability 1 for the BB84 protocol and 1/4 for the novel SQRS protocols. A worthwhile direction for future work would be to extend the comparison for photon splitting attacks with other protocols that do not declare their measurement basis such as the BBM92 [116] QKD protocol. For that protocol in particular Alice sends $|X+\rangle$ and $|Z+\rangle$

states and key transmission occurs when Bob measures $|X-\rangle$ or $|Z-\rangle$ which would occur 1/4 of the time. As the states are not spread equally around a plane of the Bloch sphere Eve could discriminate better than she can for the SQRS protocols. This would provide more protection than BB84 but less than the SQRS protocols presented here and would be represented in figure 7.7 by a line in-between the two already there.

Photon splitting is not the only issue with practical implementations of quantum cryptographic protocols. Side-channel attacks, where the Eve performs attacks that take advantage of imperfect detectors has been solved for QKD with the invention of measurement device independent QKD [117]. An important direction of future work for other quantum cryptographic protocols is to develop similar protections. Another point of fragility for practical implementations is source imperfections such as the assumption of perfect phase randomisation or Trojan horse attacks [118]. These attacks issues would also have to be considered when building real devices.

Chapter 8

Conclusion

Secure quantum remote sensing is a new and rapidly evolving subject that brings cryptographic methods to quantum metrology of parameters at remote locations. Theoretical protocols have three building blocks: quantum metrology, statistical methods and cryptography.

Quantum metrology is well defined for systems where many measurements can be made on a set of quantum states that are either identical or intended to be identical but affected by some noise. The qubit, a two level quantum system, is the most fundamental building block of quantum metrology. The many states of a qubit, their interaction with parameters and the measurement of those parameters is well defined. Furthermore, the amount of information about parameters that could be extracted from quantum states such as qubits from many measurements of copies of those states, the quantum Fisher information, is well defined. Its classical analogue, the classical Fisher information, bounded from above by the quantum Fisher information, measures the information gain due to some set of probabilities. These probabilities can be calculated from the quantum mechanics of qubits. Fisher information is used to define the Cramér-Rao bound as a limit on the disperison of parameter estimates in the asymptotic limit of large data making it a useful measure of information gain in such regimes.

The effectiveness of quantum metrology is less well defined in scenarios with limited data where measures like the Fisher informations are not applicable. Bayesian statistical inference methods are appropriate for estimating parameters in limited data quantum metrology. In particular, they allow a scientist to make use of any prior knowledge about the estimated parameters and combine it with the the knowledge of the parameters that can be drawn from some data to get a probability density function for the true value of the

parameter known as the posterior distribution. Qubits are often represented using a Bloch sphere, where the quantum state can be any position on a sphere. A fundamental class of parameters measured in quantum metrology are phase parameters, how far around the equator a qubit state is. They are circular parameters with period 2π, meaning that any estimator should also be on a circular support. A shift around a circle of $X + 2\pi$ gives the same final state as a shift of X. When prior information and data are limited, the posterior distribution from a Bayesian inference accounting for both can be non-negligible around a 2π range making linear statistical methods inappropriate. Instead, circular statistical methods should be used. These methods give statistics such as estimators and measures of dispersion equivalent to linear statistics for distributions narrow enough to be on an approximately flat support.

To quantify the quality of information gain in limited data many iterations of a quantum phase metrology protocol must be performed and statistics of the quality of their circular statistics must be made. The probability distributions of the measurement results of such protocols are well defined. Therefore, a theoretical physicist can implement Monte Carlo methods simulating many iterations of the protocol numerically to get such statistics. These in turn are used as measures of the information gain for limited data.

Cryptography is the process of using encryption to ensure the privacy and integrity of some information. In quantum cryptographic methods encryption can be performed by ensuring that only designated parties have knowledge of quantum states and/or measurement results. These principles are applied to quantum metrology to encrypt measurement data to ensure that only designated parties can interpret them. Limited data quantum metrology is particularly important for cryptographically secure protocols. An eavesdropper may not need to steal or spoof much information to have a profound effect. Therefore, the Monte Carlo simulations described here are important for very secure protocols, quantifying the privacy in particular.

The basic principle of secure quantum remote sensing protocols with two parties can be summarised as follows: Alice creates quantum states and sends them to Bob for measurement. One of the two parties encodes a phase on some or all of the states. They communicate classically some of the initial states and/or measurement results. Those states that did not get encoded with a parameter are used to check the fidelity while the others are used so that the party not in possession of the phase can estimate it. There are three security conditions for such protocols.

The first is that an eavesdropper cannot estimate the parameter without having prior

knowledge of the initial state on an individual run; knowledge of the probability distribution of the states that can be used is insufficient. This can be achieved by ensuring that density function of states average to the identity. Protocols fulfilling only this condition are used to perform anonymous quantum sensing, similar in principle to anonymous quantum computing.

The second condition is that an eavesdropper cannot attack the quantum communication channel, interacting with it, without risking detection. Some protocols assure this using a separate quantum key distribution protocol however, it is not in the spirit of secure quantum remote sensing to use an entirely separate protocol to ensure its security. Other protocols, such as the novel protocols in this thesis, assure this security by using some states for fidelity checks without encoding any parameters. The works developed in this thesis go further by quantifying the information privacy in limited data using a statistic of an eavesdropper's information gain before her attacks are detected.

A third security condition, considered for the first time in the works developed in this thesis is to protect against manipulations of classical communications without implementing a separate cryptography protocol. Previously, classical authentication was assumed for SQRS protocols. However, once again, it would be better for all of the security features to be integrated into a single protocol. This is achieved for the first time in the material that this thesis is drawn from by using quantum encoded shared secrets and a path information delay.

One of the principle aims of quantum metrology is to perform parameter estimation beyond the standard quantum limit. That is the amount of information that can be gained using classical states and interactions such as coherent state polarised photons interacting with a single phase parameter before being measured. The novel protocols developed here show parameter estimation beyond the standard quantum limit while ensuring a rigorous limit on an eavesdropper's information gain, ensuring information privacy. The single parameter protocol does this by combining the results from different numbers of parameter probes interactions for each qubit used in parameter estimation.

The protocol for functions of parameters performs estimation beyond the standard quantum limit by distributing entangled states across many Bobs so that each can encode their parameter and measure their part of the state. However, as each Bob must choose at random and independently to encode their phase or perform a fidelity check the effective rate of security checks on entangled states reduces with network size. It ensures security by using states separable between the Bobs and maintaining the choice of entangled or

separable on an individual round secret which provides increased security checks with increasing network size.

Practical implementation of such protocols depends on many factors. To aid in this, these protocols are optimised for information gain while maintaining security and do not use entanglement when it can be avoided. Furthermore, unlike many cryptographic quantum protocols they do not declare the basis of the initial state making them significantly more resistant to photon splitting attacks, especially on larger networks. This makes polarised photons a realistic implementation method.

Beyond the scope of the material here, the most important direction of future theoretical work is to aid practical implementation. The most important issue for practical implementation is the effect of noise on the information gain and ability to detect an eavesdropper. Any noise would reduce the information gain for SQRS. GHZ states are particularly prone to decoherence so, one direction for future work would be to adapt the network SQRS protocol to using more stable states such as W states to provide a global measurement advantage. Any noise would cause failed fidelity checks therefore, to provide protection in noisy scenarios, protocols would have to compare the actual amount of noise to the expected amount of noise without an eavesdropper to check for the eavesdropper performing MIM attacks such as MR then use methods such as those suggested in the conclusion of chapter 5 to perform unbiased noisy estimation. Practical implementations would also have to deal with attacks on the hardware such as side-channel attacks and Trojan horse attacks. A future direction of research would be to adapt protocols to defend against these types of attacks by, for instance, following the principles of measurement device independent QKD.

Further theoretical extensions include but are not limited to different functions of parameters, multiple functions of parameters simultaneously, attacks with asymmetric prior information, attacks for different functions of parameter, different measures of privacy and quantifying the information integrity to the same level of detail as the privacy.

To conclude, this thesis demonstrates novel methods for secure quantum-enhanced networks of remote sensors to efficiently estimate remote parameters and functions of remote parameters while ensuring information integrity and quantifying information privacy.

Bibliography

[1] W. H. Zurek. "Decoherence, einselection, and the quantum origins of the classical". In: *Rev. Mod. Phys.* 75 (3 May 2003), pp. 715–775. DOI: 10.1103/RevModPhys.75.715. URL: https://link.aps.org/doi/10.1103/RevModPhys.75.715.

[2] A. V. Rau, J. A. Dunningham, and K. Burnett. "Measurement-Induced Relative-Position Localization Through Entanglement". In: *Science* 301.5636 (2003), pp. 1081–1084. DOI: 10.1126/science.1084867. eprint: https://www.science.org/doi/pdf/10.1126/science.1084867. URL: https://www.science.org/doi/abs/10.1126/science.1084867.

[3] A. Barenco et al. "Elementary gates for quantum computation". In: *Phys. Rev. A* 52 (5 Nov. 1995), pp. 3457–3467. DOI: 10.1103/PhysRevA.52.3457. URL: https://link.aps.org/doi/10.1103/PhysRevA.52.3457.

[4] C. L. Degen, F. Reinhard, and P. Cappellaro. "Quantum sensing". In: *Rev. Mod. Phys.* 89 (3 July 2017), p. 035002. DOI: 10.1103/RevModPhys.89.035002. URL: https://link.aps.org/doi/10.1103/RevModPhys.89.035002.

[5] N. Gisin et al. "Quantum cryptography". In: *Rev. Mod. Phys.* 74 (1 Mar. 2002), pp. 145–195. DOI: 10.1103/RevModPhys.74.145. URL: https://link.aps.org/doi/10.1103/RevModPhys.74.145.

[6] V. Giovannetti, S. Lloyd, and L. Maccone. "Positioning and clock synchronization through entanglement". In: *Phys. Rev. A* 65 (2 Jan. 2002), p. 022309. DOI: 10.1103/PhysRevA.65.022309. URL: https://link.aps.org/doi/10.1103/PhysRevA.65.022309.

[7] P. Kómár et al. "A quantum network of clocks". In: *Nature Physics* 10.8 (Aug. 2014), pp. 582–587. ISSN: 1745-2481. DOI: 10.1038/nphys3000. URL: https://doi.org/10.1038/nphys3000.

[8] Z. Huang, C. Macchiavello, and L. Maccone. "Cryptographic quantum metrology". In: *Phys. Rev. A* 99 (2 Feb. 2019), p. 022314. DOI: 10.1103/PhysRevA.99.022314. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.022314.

[9] H. Kasai et al. "Anonymous Quantum Sensing". In: *Journal of the Physical Society of Japan* 91.7 (2022), p. 074005. DOI: 10.7566/JPSJ.91.074005. URL: https://doi.org/10.7566/JPSJ.91.074005.

[10] D. Xie et al. "High-dimensional cryptographic quantum parameter estimation". In: *Quantum Information Processing* 17.5 (Apr. 2018), p. 116. ISSN: 1573-1332. DOI: 10.1007/s11128-018-1884-z. URL: https://doi.org/10.1007/s11128-018-1884-z.

[11] Y. Takeuchi et al. "Quantum remote sensing with asymmetric information gain". In: *Phys. Rev. A* 99 (2 Feb. 2019), p. 022325. DOI: 10.1103/PhysRevA.99.022325. URL: https://link.aps.org/doi/10.1103/PhysRevA.99.022325.

[12] H. Okane et al. "Quantum remote sensing under the effect of dephasing". In: *Phys. Rev. A* 104 (6 Dec. 2021), p. 062610. DOI: 10.1103/PhysRevA.104.062610. URL: https://link.aps.org/doi/10.1103/PhysRevA.104.062610.

[13] P. Yin et al. "Experimental Demonstration of Secure Quantum Remote Sensing". In: *Phys. Rev. Applied* 14 (1 July 2020), p. 014065. DOI: 10.1103/PhysRevApplied.14.014065. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.14.014065.

[14] N. Shettell, E. Kashefi, and D. Markham. "Cryptographic approach to quantum metrology". In: *Phys. Rev. A* 105 (1 Jan. 2022), p. L010401. DOI: 10.1103/PhysRevA.105.L010401. URL: https://link.aps.org/doi/10.1103/PhysRevA.105.L010401.

[15] N. Shettell, M. Hassani, and D. Markham. "Private network parameter estimation with quantum sensors". In: (July 2022). DOI: 10.48550/arXiv.2207.14450.

[16] S. W. Moore and J. A. Dunningham. "Secure quantum remote sensing without entanglement". In: *AVS Quantum Science* 5.1 (Feb. 2023), p. 014406. ISSN: 2639-0213. DOI: 10.1116/5.0137260. eprint: https://pubs.aip.org/avs/aqs/article-pdf/doi/10.1116/5.0137260/16774756/014406_1_online.pdf. URL: https://doi.org/10.1116/5.0137260.

[17] S. W. Moore and J. A. Dunningham. *Secure quantum-enhanced measurements on a network of sensors*. 2024. arXiv: 2406.19285 [quant-ph]. URL: https://arxiv.org/abs/2406.19285.

[18] J. F. Fitzsimons. "Private quantum computation: an introduction to blind quantum computing and related protocols". In: *npj Quantum Information* 3.1 (June 2017), p. 23. ISSN: 2056-6387. DOI: 10.1038/s41534-017-0025-3. URL: https://doi.org/10.1038/s41534-017-0025-3.

[19] M. A. Nielsen and I. L. Chuang. *Quantum Computation and Quantum Information: 10th Anniversary Edition*. Cambridge University Press, 2010.

[20] L. K. Grover. "A fast quantum mechanical algorithm for database search". In: *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*. STOC '96. Philadelphia, Pennsylvania, USA: Association for Computing Machinery, 1996, 212–219. ISBN: 0897917855. DOI: 10.1145/237814.237866. URL: https://doi.org/10.1145/237814.237866.

[21] D. Deutsch and R. Jozsa. "Rapid Solution of Problems by Quantum Computation". In: *Proceedings of the Royal Society of London Series A* 439.1907 (Dec. 1992), pp. 553–558. DOI: 10.1098/rspa.1992.0167.

[22] R. Cleve et al. "Quantum algorithms revisited". In: *Proceedings of the Royal Society of London Series A* 454.1969 (Jan. 1998), p. 339. DOI: 10.1098/rspa.1998.0164. arXiv: quant-ph/9708016 [quant-ph].

[23] P. Shor. "Algorithms for quantum computation: discrete logarithms and factoring". In: *Proceedings 35th Annual Symposium on Foundations of Computer Science*. 1994, pp. 124–134. DOI: 10.1109/SFCS.1994.365700.

[24] P. W. Shor. "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer". In: *SIAM Journal on Computing* 26.5 (1997), pp. 1484–1509. DOI: 10.1137/S0097539795293172. eprint: https://doi.org/10.1137/S0097539795293172. URL: https://doi.org/10.1137/S0097539795293172.

[25] D. Boneh and R. J. Lipton. "Quantum Cryptanalysis of Hidden Linear Functions". In: *Advances in Cryptology — CRYPT0' 95*. Ed. by D. Coppersmith. Berlin, Heidelberg: Springer Berlin Heidelberg, 1995, pp. 424–437. ISBN: 978-3-540-44750-4.

[26] W. van Dam and G. Seroussi. "Efficient Quantum Algorithms for Estimating Gauss Sums". In: *arXiv: Quantum Physics* (2002). URL: https://api.semanticscholar.org/CorpusID:13515010.

[27] S. Aaronson. "BQP and the polynomial hierarchy". In: *Proceedings of the Forty-Second ACM Symposium on Theory of Computing*. STOC '10. Cambridge, Massachusetts, USA: Association for Computing Machinery, 2010, 141–150. DOI: 10.1145/1806689.1806711. URL: https://doi.org/10.1145/1806689.1806711.

[28] G. Brassard et al. "Quantum Amplitude Amplification and Estimation". In: *arXiv e-prints*, quant-ph/0005055 (May 2000), quant–ph/0005055. DOI: 10.48550/arXiv.quant-ph/0005055. arXiv: quant-ph/0005055 [quant-ph].

[29] A. Ambainis. "Quantum Walk Algorithm for Element Distinctness". In: *SIAM Journal on Computing* 37.1 (2007), pp. 210–239. DOI: 10.1137/S0097539705447311. eprint: https://doi.org/10.1137/S0097539705447311. URL: https://doi.org/10.1137/S0097539705447311.

[30] R. P. Feynman. "Simulating Physics with Computers". In: *International Journal of Theoretical Physics* 21.6-7 (June 1982), pp. 467–488. DOI: 10.1007/BF02650179.

[31] D. S. Abrams and S. Lloyd. "Simulation of many-body Fermi systems on a universal quantum computer". In: *Physical Review Letters* (Sept. 1997). URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.79.2586.

[32] I. Kassal et al. "Polynomial-time quantum algorithm for the simulation of chemical dynamics". en. In: *Proc Natl Acad Sci U S A* 105.48 (Nov. 2008), pp. 18681–18686.

[33] M. H. Freedman, A. Kitaev, and Z. Wang. "Simulation of Topological Field Theories by Quantum Computers". In: *Communications in Mathematical Physics* 227.3 (June 2002), pp. 587–603. ISSN: 1432-0916. DOI: 10.1007/s002200200635. URL: https://doi.org/10.1007/s002200200635.

[34] D. Aharonov, V. Jones, and Z. Landau. "A Polynomial Quantum Algorithm for Approximating the Jones Polynomial". In: *Algorithmica* 55.3 (Nov. 2009), pp. 395–421. ISSN: 1432-0541. DOI: 10.1007/s00453-008-9168-0. URL: https://doi.org/10.1007/s00453-008-9168-0.

[35] A. J. Daley et al. "Practical quantum advantage in quantum simulation". In: *Nature* 607.7920 (July 2022), pp. 667–676. ISSN: 1476-4687. DOI: 10.1038/s41586-022-04940-6. URL: https://doi.org/10.1038/s41586-022-04940-6.

[36] J. Liu et al. “Quantum Fisher information matrix and multiparameter estimation”. In: *Journal of Physics A: Mathematical and Theoretical* 53.2 (Dec. 2019), p. 023001. DOI: 10.1088/1751-8121/ab5d4d. URL: https://doi.org/10.1088\%2F1751-8121\%2Fab5d4d.

[37] R. A. Fisher. “The mathematical foundations of theoretical statistics”. In: *Phil. Trans. Roy. Soc. A* 222 (1922), pp. 309–368.

[38] V. Giovannetti, S. Lloyd, and L. Maccone. “Advances in quantum metrology”. In: *Nature Photonics* 5.4 (Apr. 2011), pp. 222–229. ISSN: 1749-4893. DOI: 10.1038/nphoton.2011.35. URL: https://doi.org/10.1038/nphoton.2011.35.

[39] L. Pezzè. “Entanglement-enhanced sensor networks”. In: *Nature Photonics* 15.2 (Feb. 2021), pp. 74–76. ISSN: 1749-4893. DOI: 10.1038/s41566-020-00755-x. URL: https://doi.org/10.1038/s41566-020-00755-x.

[40] D. F. Walls. “Squeezed states of light”. In: *Nature* 306.5939 (Nov. 1983), pp. 141–146. ISSN: 1476-4687. DOI: 10.1038/306141a0.

[41] Ángel Rivas and A. Luis. “Sub-Heisenberg estimation of non-random phase shifts”. In: *New Journal of Physics* 14.9 (Sept. 2012), p. 093052. DOI: 10.1088/1367-2630/14/9/093052. URL: https://dx.doi.org/10.1088/1367-2630/14/9/093052.

[42] R. Demkowicz-Dobrzański, W. Górecki, and M. Guţă. “Multi-parameter estimation beyond quantum Fisher information”. In: *Journal of Physics A: Mathematical and Theoretical* 53.36 (Aug. 2020), p. 363001. DOI: 10.1088/1751-8121/ab8ef3. URL: https://dx.doi.org/10.1088/1751-8121/ab8ef3.

[43] M. Bailes et al. “Gravitational-wave physics and astronomy in the 2020s and 2030s”. In: *Nature Reviews Physics* 3.5 (May 2021), pp. 344–366. ISSN: 2522-5820. DOI: 10.1038/s42254-021-00303-8. URL: https://doi.org/10.1038/s42254-021-00303-8.

[44] S. W. Moore. *Secure quantum remote sensing without entanglement.* Version 1.0. Feb. 2023. DOI: 10.1116/5.0137260. URL: https://github.com/S-W-Moore/Secure-quantum-remote-sensing-without-entanglement.

[45] S. W. Moore. *Secure quantum enhanced measurements on a network of sensors.* Version 1.0. June 2024. URL: https://github.com/S-W-Moore/SecureQuantumEnhancedMeasurementsOnANetworkOfSensors.

[46] A. Mohammed and N. Varol. “A Review Paper on Cryptography”. In: June 2019, pp. 1–6. DOI: 10.1109/ISDFS.2019.8757514.

[47] K. Bhattacharjee and S. Das. "A search for good pseudo-random number generators: Survey and empirical studies". In: *Computer Science Review* 45 (2022), p. 100471. ISSN: 1574-0137. DOI: https://doi.org/10.1016/j.cosrev.2022.100471. URL: https://www.sciencedirect.com/science/article/pii/S1574013722000144.

[48] D. Feng. "Review of Quantum navigation". In: *IOP Conference Series: Earth and Environmental Science* 237.3 (Feb. 2019), p. 032027. DOI: 10.1088/1755-1315/237/3/032027. URL: https://dx.doi.org/10.1088/1755-1315/237/3/032027.

[49] X. Wang et al. "Probabilistic Map Matching for Robust Inertial Navigation Aiding". In: *NAVIGATION: Journal of the Institute of Navigation* 70.2 (2023). ISSN: 0028-1522. DOI: 10.33012/navi.583. eprint: https://navi.ion.org/content/70/2/navi.583.full.pdf. URL: https://navi.ion.org/content/70/2/navi.583.

[50] N. Aslam et al. "Quantum sensors for biomedical applications". In: *Nature Reviews Physics* 5.3 (Mar. 2023), pp. 157–169. ISSN: 2522-5820. DOI: 10.1038/s42254-023-00558-3. URL: https://doi.org/10.1038/s42254-023-00558-3.

[51] L. Pezzé et al. "Optimal Measurements for Simultaneous Quantum Estimation of Multiple Phases". In: *Physical Review Letters* 119 (May 2017). DOI: 10.1103/PhysRevLett.119.130504.

[52] X. Guo et al. "Distributed quantum sensing in a continuous-variable entangled network". In: *Nature Physics* 16.3 (Mar. 2020), pp. 281–284. ISSN: 1745-2481. DOI: 10.1038/s41567-019-0743-x. URL: https://doi.org/10.1038/s41567-019-0743-x.

[53] P. A. Knott et al. "Local versus global strategies in multiparameter estimation". In: *Physical Review A* (Dec. 2016). URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.94.062312.

[54] T. J. Proctor, P. A. Knott, and J. A. Dunningham. *Networked quantum sensing.* 2017. arXiv: 1702.04271 [quant-ph].

[55] T. J. Proctor, P. A. Knott, and J. A. Dunningham. "Multiparameter estimation in networked quantum sensors". In: *Physical Review Letters* (Feb. 2018). URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.120.080501.

[56] J. Rubio et al. "Quantum sensing networks for the estimation of linear functions". In: *Journal of Physics A: Mathematical and Theoretical* 53.34 (Aug. 2020),

p. 344001. DOI: 10.1088/1751-8121/ab9d46. URL: https://dx.doi.org/10.1088/1751-8121/ab9d46.

[57] Z. Eldredge et al. "Optimal and secure measurement protocols for Quantum Sensor Networks". In: *Physical Review A* (Apr. 2018). URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.97.042337.

[58] W. Ge et al. "Distributed quantum metrology with linear networks and separable inputs". In: *Physical Review Letters* (July 2018). URL: https://journals.aps.org/prl/abstract/10.1103/PhysRevLett.121.043604.

[59] K. Qian et al. "Heisenberg-scaling measurement protocol for analytic functions with Quantum Sensor Networks". In: *Physical Review A* (Oct. 2019). URL: https://journals.aps.org/pra/abstract/10.1103/PhysRevA.100.042304.

[60] T. Qian et al. "Optimal measurement of field properties with quantum sensor networks". In: *Phys. Rev. A* 103 (3 Mar. 2021), p. L030601. DOI: 10.1103/PhysRevA.103.L030601. URL: https://link.aps.org/doi/10.1103/PhysRevA.103.L030601.

[61] J. Bringewatt et al. "Protocols for estimating multiple functions with quantum sensor networks: Geometry and performance". In: *Phys. Rev. Res.* 3 (3 July 2021), p. 033011. DOI: 10.1103/PhysRevResearch.3.033011. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.3.033011.

[62] J. Bringewatt et al. "Optimal function estimation with photonic quantum sensor networks". In: *Phys. Rev. Res.* 6 (1 Mar. 2024), p. 013246. DOI: 10.1103/PhysRevResearch.6.013246. URL: https://link.aps.org/doi/10.1103/PhysRevResearch.6.013246.

[63] V. Giovannetti, S. Lloyd, and L. Maccone. "Quantum-enhanced positioning and clock synchronization". In: *Nature* 412.6845 (2001), pp. 417–419. ISSN: 1476-4687. DOI: 10.1038/35086525. URL: https://doi.org/10.1038/35086525.

[64] K. V. Mardia and P. E. Jupp. *Directional Statistics*. Ed. by K. V. Mardia and P. E. Jupp. Wiley Series in Probability and Statistics. Chichester, England: John Wiley & Sons, Nov. 1999.

[65] W. K. Newey and D. McFadden. "Chapter 36 Large sample estimation and hypothesis testing". In: vol. 4. Handbook of Econometrics. Elsevier, 1994, pp. 2111–2245. DOI: https://doi.org/10.1016/S1573-4412(05)80005-4. URL: https://www.sciencedirect.com/science/article/pii/S1573441205800054.

[66] B. L. Higgins et al. “Entanglement-free Heisenberg-limited phase estimation”. In: *Nature* 450.7168 (Nov. 2007), pp. 393–396. ISSN: 1476-4687. DOI: 10.1038/nature06257. URL: https://doi.org/10.1038/nature06257.

[67] V. Giovannetti, S. Lloyd, and L. Maccone. “Quantum Metrology”. In: *Phys. Rev. Lett.* 96 (1 Jan. 2006), p. 010401. DOI: 10.1103/PhysRevLett.96.010401. URL: https://link.aps.org/doi/10.1103/PhysRevLett.96.010401.

[68] H. F. Hofmann. “All path-symmetric pure states achieve their maximal phase sensitivity in conventional two-path interferometry”. In: *Phys. Rev. A* 79 (3 Mar. 2009), p. 033822. DOI: 10.1103/PhysRevA.79.033822. URL: https://link.aps.org/doi/10.1103/PhysRevA.79.033822.

[69] P. Hyllus, L. Pezzé, and A. Smerzi. “Entanglement and Sensitivity in Precision Measurements with States of a Fluctuating Number of Particles”. In: *Phys. Rev. Lett.* 105 (12 Sept. 2010), p. 120501. DOI: 10.1103/PhysRevLett.105.120501. URL: https://link.aps.org/doi/10.1103/PhysRevLett.105.120501.

[70] L. Pezzè, P. Hyllus, and A. Smerzi. “Phase-sensitivity bounds for two-mode interferometers”. In: *Phys. Rev. A* 91 (3 Mar. 2015), p. 032103. DOI: 10.1103/PhysRevA.91.032103. URL: https://link.aps.org/doi/10.1103/PhysRevA.91.032103.

[71] M. Gessner, L. Pezzè, and A. Smerzi. “Sensitivity Bounds for Multiparameter Quantum Metrology”. In: *Phys. Rev. Lett.* 121 (13 Sept. 2018), p. 130503. DOI: 10.1103/PhysRevLett.121.130503. URL: https://link.aps.org/doi/10.1103/PhysRevLett.121.130503.

[72] D. Branford and J. Rubio. “Average number is an insufficient metric for interferometry”. In: *New Journal of Physics* 23.12 (Dec. 2021), p. 123041. DOI: 10.1088/1367-2630/ac3571. URL: https://dx.doi.org/10.1088/1367-2630/ac3571.

[73] C. H. Bennett and G. Brassard. “Quantum cryptography: Public key distribution and coin tossing”. In: *Theor. Comput. Sci.* 560 (2014), pp. 7–11.

[74] L.-J. Wang et al. “Experimental authentication of quantum key distribution with post-quantum cryptography”. In: *npj Quantum Information* 7.1 (May 2021), p. 67. ISSN: 2056-6387. DOI: 10.1038/s41534-021-00400-7. URL: https://doi.org/10.1038/s41534-021-00400-7.

[75] A. Dutta and A. Pathak. “A short review on quantum identity authentication protocols: how would Bob know that he is talking with Alice?” In: *Quantum In-*

formation Processing 21.11 (Nov. 2022), p. 369. ISSN: 1573-1332. DOI: 10.1007/s11128-022-03717-0. URL: https://doi.org/10.1007/s11128-022-03717-0.

[76] W. K. Wootters and W. H. Zurek. "A single quantum cannot be cloned". In: 299.5886 (Oct. 1982), pp. 802–803. DOI: 10.1038/299802a0.

[77] D. Dieks. "Communication by EPR devices". In: *Physics Letters A* 92.6 (1982), pp. 271–272. ISSN: 0375-9601. DOI: https://doi.org/10.1016/0375-9601(82)90084-6. URL: https://www.sciencedirect.com/science/article/pii/0375960182900846.

[78] A. Ekert. "Quantum cryptography based on Bell's theorem." In: *Physical review letters* 67 6 (1991), pp. 661–663. URL: https://api.semanticscholar.org/CorpusID:27683254.

[79] G. Brassard and L. Salvail. "Secret-Key Reconciliation by Public Discussion". In: *Advances in Cryptology — EUROCRYPT '93*. Ed. by T. Helleseth. Berlin, Heidelberg: Springer Berlin Heidelberg, 1994, pp. 410–423. ISBN: 978-3-540-48285-7.

[80] C. H. Bennett, G. Brassard, and J.-M. Robert. "Privacy Amplification by Public Discussion". In: *SIAM Journal on Computing* 17.2 (1988), pp. 210–229. DOI: 10.1137/0217014. eprint: https://doi.org/10.1137/0217014. URL: https://doi.org/10.1137/0217014.

[81] P. W. Shor and J. Preskill. "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol". In: 85.2 (July 2000), pp. 441–444. DOI: 10.1103/PhysRevLett.85.441. arXiv: quant-ph/0003004 [quant-ph].

[82] G. Brassard et al. "Limitations on Practical Quantum Cryptography". In: 85.6 (Aug. 2000), pp. 1330–1333. DOI: 10.1103/PhysRevLett.85.1330. arXiv: quant-ph/9911054 [quant-ph].

[83] W.-Y. Hwang. "Quantum Key Distribution with High Loss: Toward Global Secure Communication". In: *Phys. Rev. Lett.* 91 (5 Aug. 2003), p. 057901. DOI: 10.1103/PhysRevLett.91.057901. URL: https://link.aps.org/doi/10.1103/PhysRevLett.91.057901.

[84] Y. Zhao et al. "Experimental Quantum Key Distribution with Decoy States". In: *Phys. Rev. Lett.* 96 (7 Feb. 2006), p. 070502. DOI: 10.1103/PhysRevLett.96.070502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.96.070502.

[85] X. Ma et al. "Practical decoy state for quantum key distribution". In: *Phys. Rev. A* 72 (1 July 2005), p. 012326. DOI: 10.1103/PhysRevA.72.012326. URL: https://link.aps.org/doi/10.1103/PhysRevA.72.012326.

[86] V. Scarani et al. "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations". In: *Phys. Rev. Lett.* 92 (5 Feb. 2004), p. 057901. DOI: 10.1103/PhysRevLett.92.057901. URL: https://link.aps.org/doi/10.1103/PhysRevLett.92.057901.

[87] C. Branciard et al. "Security of two quantum cryptography protocols using the same four qubit states". In: *Phys. Rev. A* 72 (3 Sept. 2005), p. 032301. DOI: 10.1103/PhysRevA.72.032301. URL: https://link.aps.org/doi/10.1103/PhysRevA.72.032301.

[88] N. Shettell and D. Markham. "Quantum metrology with delegated tasks". In: *Phys. Rev. A* 106 (5 Nov. 2022), p. 052427. DOI: 10.1103/PhysRevA.106.052427. URL: https://link.aps.org/doi/10.1103/PhysRevA.106.052427.

[89] Y. Takeuchi et al. "Resource-efficient verification of quantum computing using Serfling's bound". In: *npj Quantum Information* 5.1 (Apr. 2019), p. 27. ISSN: 2056-6387. DOI: 10.1038/s41534-019-0142-2. URL: https://doi.org/10.1038/s41534-019-0142-2.

[90] D. W. Berry et al. "How to perform the most accurate possible phase measurements". In: *Phys. Rev. A* 80 (5 Nov. 2009), p. 052114. DOI: 10.1103/PhysRevA.80.052114. URL: https://link.aps.org/doi/10.1103/PhysRevA.80.052114.

[91] B. L. Higgins et al. "Demonstrating Heisenberg-limited unambiguous phase estimation without adaptive measurements". In: *New Journal of Physics* 11.7 (July 2009), p. 073023. DOI: 10.1088/1367-2630/11/7/073023. URL: https://dx.doi.org/10.1088/1367-2630/11/7/073023.

[92] S. Pallister, N. Linden, and A. Montanaro. "Optimal Verification of Entangled States with Local Measurements". In: *Phys. Rev. Lett.* 120 (17 Apr. 2018), p. 170502. DOI: 10.1103/PhysRevLett.120.170502. URL: https://link.aps.org/doi/10.1103/PhysRevLett.120.170502.

[93] Y. Takeuchi and T. Morimae. "Verification of Many-Qubit States". In: *Phys. Rev. X* 8 (2 June 2018), p. 021060. DOI: 10.1103/PhysRevX.8.021060. URL: https://link.aps.org/doi/10.1103/PhysRevX.8.021060.

[94] Y.-C. Liu et al. "Efficient Verification of Dicke States". In: *Phys. Rev. Appl.* 12 (4 Oct. 2019), p. 044020. DOI: 10.1103/PhysRevApplied.12.044020. URL: https://link.aps.org/doi/10.1103/PhysRevApplied.12.044020.

[95] H. Zhu and M. Hayashi. "Efficient Verification of Pure Quantum States in the Adversarial Scenario". In: *Phys. Rev. Lett.* 123 (26 Dec. 2019), p. 260504. DOI: 10.1103/PhysRevLett.123.260504. URL: https://link.aps.org/doi/10.1103/PhysRevLett.123.260504.

[96] H. Zhu and M. Hayashi. "General framework for verifying pure quantum states in the adversarial scenario". In: *Phys. Rev. A* 100 (6 Dec. 2019), p. 062335. DOI: 10.1103/PhysRevA.100.062335. URL: https://link.aps.org/doi/10.1103/PhysRevA.100.062335.

[97] D. Markham and A. Krause. "A Simple Protocol for Certifying Graph States and Applications in Quantum Networks". In: *Cryptography* 4.1 (2020). ISSN: 2410-387X. DOI: 10.3390/cryptography4010003. URL: https://www.mdpi.com/2410-387X/4/1/3.

[98] S. Pirandola et al. "Advances in quantum cryptography". In: *Adv. Opt. Photon.* 12.4 (Dec. 2020), pp. 1012–1236. DOI: 10.1364/AOP.361502. URL: https://opg.optica.org/aop/abstract.cfm?URI=aop-12-4-1012.

[99] J. Rubio, P. Knott, and J. Dunningham. "Non-asymptotic analysis of quantum metrology protocols beyond the Cramér–Rao bound". In: *Journal of Physics Communications* 2.1 (Jan. 2018), p. 015027. DOI: 10.1088/2399-6528/aaa234. URL: https://dx.doi.org/10.1088/2399-6528/aaa234.

[100] J. Rubio and J. Dunningham. "Quantum metrology in the presence of limited data". In: *New Journal of Physics* 21.4 (Apr. 2019), p. 043037. DOI: 10.1088/1367-2630/ab098b. URL: https://dx.doi.org/10.1088/1367-2630/ab098b.

[101] J. Rubio and J. Dunningham. "Bayesian multiparameter quantum metrology with limited data". In: *Phys. Rev. A* 101 (3 Mar. 2020), p. 032114. DOI: 10.1103/PhysRevA.101.032114. URL: https://link.aps.org/doi/10.1103/PhysRevA.101.032114.

[102] R. Demkowicz-Dobrzański. "Optimal phase estimation with arbitrary a priori knowledge". In: *Phys. Rev. A* 83 (June 2011). DOI: 10.1103/PhysRevA.83.061802.

[103] A. N. Boto et al. “Quantum Interferometric Optical Lithography: Exploiting Entanglement to Beat the Diffraction Limit”. In: *Phys. Rev. Lett.* 85 (13 Sept. 2000), pp. 2733–2736. DOI: 10.1103/PhysRevLett.85.2733. URL: https://link.aps.org/doi/10.1103/PhysRevLett.85.2733.

[104] J. P. Dowling. “Quantum optical metrology – the lowdown on high-N00N states”. In: *Contemporary Physics* 49.2 (2008), pp. 125–143. DOI: 10.1080/00107510802091298. URL: https://doi.org/10.1080/00107510802091298.

[105] H. Lee, P. Kok, and J. P. Dowling. “A quantum Rosetta stone for interferometry”. In: *Journal of Modern Optics* 49.14-15 (2002), pp. 2325–2338. DOI: 10.1080/09500340210000011536. URL: https://doi.org/10.1080/0950034021000011536.

[106] M. W. Mitchell, J. S. Lundeen, and A. M. Steinberg. “Super-resolving phase measurements with a multiphoton entangled state”. In: *Nature* 429.6988 (May 2004), pp. 161–164. ISSN: 1476-4687. DOI: 10.1038/nature02493. URL: https://doi.org/10.1038/nature02493.

[107] J. C. F. Matthews et al. “Heralding Two-Photon and Four-Photon Path Entanglement on a Chip”. In: *Phys. Rev. Lett.* 107 (16 Oct. 2011), p. 163602. DOI: 10.1103/PhysRevLett.107.163602. URL: https://link.aps.org/doi/10.1103/PhysRevLett.107.163602.

[108] D. Leibfried et al. “Creation of a six-atom ‘Schrödinger cat’ state”. In: *Nature* 438.7068 (Dec. 2005), pp. 639–642. ISSN: 1476-4687. DOI: 10.1038/nature04251. URL: https://doi.org/10.1038/nature04251.

[109] S. Zhang et al. “Minimal disturbance discrimination of symmetric pure states on the Bloch sphere’s equator”. In: *Phys. Rev. A* 77 (4 Apr. 2008), p. 044302. DOI: 10.1103/PhysRevA.77.044302. URL: https://link.aps.org/doi/10.1103/PhysRevA.77.044302.

[110] J. Sidhu and P. Kok. “Geometric perspective on quantum parameter estimation”. In: *AVS Quantum Science* 2 (Feb. 2020), p. 014701. DOI: 10.1116/1.5119961.

[111] M. Valeri et al. “Experimental adaptive Bayesian estimation of multiple phases with limited data”. In: *npj Quantum Information* 6.1 (Dec. 2020), p. 92. ISSN: 2056-6387. DOI: 10.1038/s41534-020-00326-6. URL: https://doi.org/10.1038/s41534-020-00326-6.

[112] Y.-Y. Fei et al. “Practical decoy state quantum key distribution with detector efficiency mismatch”. In: *The European Physical Journal D* 72.6 (June 2018), p. 107. ISSN: 1434-6079. DOI: 10.1140/epjd/e2018-90110-3. URL: https://doi.org/10.1140/epjd/e2018-90110-3.

[113] B. Huttner et al. “Quantum cryptography with coherent states”. In: *Phys. Rev. A* 51 (3 Mar. 1995), pp. 1863–1869. DOI: 10.1103/PhysRevA.51.1863. URL: https://link.aps.org/doi/10.1103/PhysRevA.51.1863.

[114] W.-T. Liu et al. “Proof-of-principle experiment of a modified photon-number-splitting attack against quantum key distribution”. In: *Phys. Rev. A* 83 (4 Apr. 2011), p. 042326. DOI: 10.1103/PhysRevA.83.042326. URL: https://link.aps.org/doi/10.1103/PhysRevA.83.042326.

[115] I. Aharonovich, D. Englund, and M. Toth. “Solid-state single-photon emitters”. In: *Nature Photonics* 10.10 (Oct. 2016), pp. 631–641. ISSN: 1749-4893. DOI: 10.1038/nphoton.2016.186. URL: https://doi.org/10.1038/nphoton.2016.186.

[116] C. H. Bennett, G. Brassard, and N. D. Mermin. “Quantum cryptography without Bell’s theorem”. In: *Phys. Rev. Lett.* 68 (5 1992), pp. 557–559. DOI: 10.1103/PhysRevLett.68.557. URL: https://link.aps.org/doi/10.1103/PhysRevLett.68.557.

[117] H.-K. Lo, M. Curty, and B. Qi. “Measurement-Device-Independent Quantum Key Distribution”. In: 108.13, 130503 (Mar. 2012), p. 130503. DOI: 10.1103/PhysRevLett.108.130503. arXiv: 1109.1473 [quant-ph].

[118] N. Gisin et al. “Trojan-horse attacks on quantum-key-distribution systems”. In: 73.2, 022320 (Feb. 2006), p. 022320. DOI: 10.1103/PhysRevA.73.022320. arXiv: quant-ph/0507063 [quant-ph].

Appendix A

Numerical methods

Many of the results in this thesis rely on numerical calculations that I performed in Matlab. Throughout the thesis I introduce numerical methods when appropriate and discuss the methodology specific to the results. The computational methods used to get these results are significant in complexity, computational intensity and code length. Therefore, this appendix provides a guide for any reader who would like to replicate these results without copying the code directly. The Matlab code used to produce the main results of the thesis is much too long to be included in the thesis; it is available on github [44, 45] instead. However, there are two basic examples at the end of this chapter.

This chapter will proceed by three parts. First, the parameter estimation for the protocol introduced in chapter 5 without man in the middle attacks is demonstrated in two different ways: by simulating individual rounds and performing Bayesian updating, by simulating a set of results from the known distribution and creating a single likelihood function. Then, it sets out the methodology for performing a simulation for an entire protocol. Finally, it sets out the more complex methodology required for the data analysis with multiple Bobs used in chapters 6 and 7.

As set out in chapter 3 there are multiple ways of performing a single simulation of an SQRS protocol. The following Matlab codes were developed to teach new PhD students about the different methods of performing simulation and data analysis for single parameter phase estimation.

A.1 Introductory parameter estimation

The first Matlab code demonstrates data production by simulating step by step. Then it performs two different methods of data analysis: the production of likelihood functions

for each additional data point by Bayesian updating using the 8 different types of results, estimation of all of the data at once after it has all been recorded accounting using the 8 different types of results.

To perform the Bayesian updating data analysis:

1. Set pseudorandom number stream
2. Declare number of rounds and arrays for parameter support, probabilities, results, likelihood functions
3. within for loop
   (a) Choose true state and Eve's guess of true state at random from list of four possibilities
   (b) Declare result probability based on true value and initial state
   (c) Use pseudorandom number to simulate result and record
   (d) Go through list of possibilities, when arriving on initial state and result for this round update the likelihood function by taking the product of the previous likelihood function with the probability of the corresponding initial state-result combination.

As each round is independent and identically distributed only the number of each initial state result combination influence the final likelihood function. Therefore, to produce a likelihood function from all of the data in one step, it is sufficient to count the total number of each initial state result combination and use equation (5.5) to produce a likelihood function.

The second Matlab code functions similarly to the first when performing the data analysis in one step. However, instead of using a for loop to go through the individual rounds it is produced in a single step using a function for producing multinomial random numbers.

A.2 Methodology for simulating entire network protocol and performing data analysis

The SQRS protocols can be simulated using using the methodology set out in figure A.1. The data analysis can be performed using a similar methodology as the previous section for a single Bob. For multiple Bobs figure A.2 outline the method to optimise the information

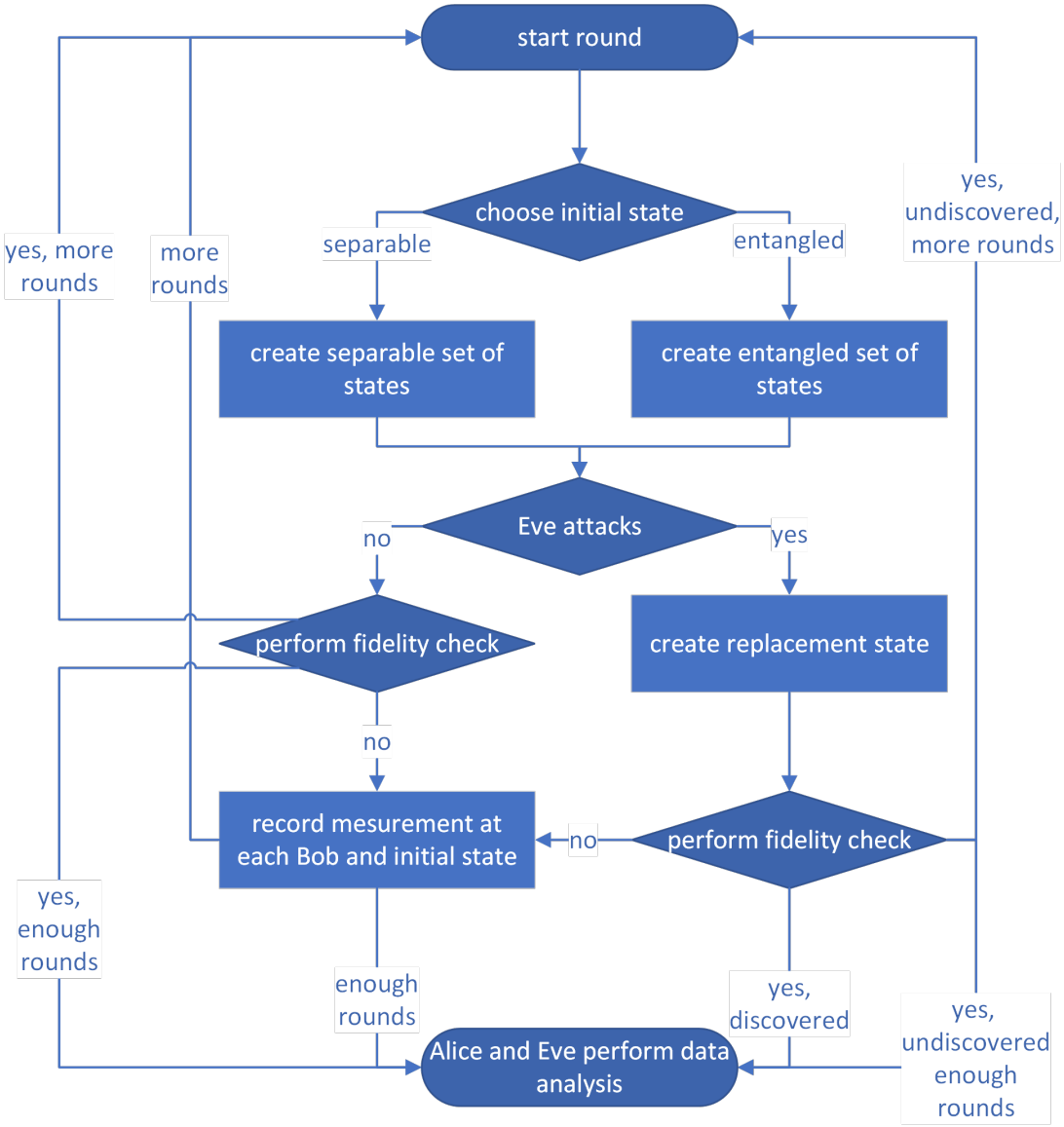

Figure A.1: Flow chart outlining the SQRS protocol with multiple Bobs with MIM attacks. Additional complications include accounting for Alice recording the initial state that she set not what Eve replaced it with when there is an attack and fidelity check success rate depending on both the attack type used by Eve and the initial state that Alice produced.

gain and figure A.2 demonstrates how to perform the parameter estimation. The steps for a Monte Carlo simulation are as follows:

1. Array and variable preallocation
2. loop through true values
   (a) loop through repetitions
      i. simulate protocol
      ii. analyse data and record statistics
   (b) gather statistics for true value
3. gather statistics over multiple true values

The parameter optimisation protocol is explained in detail in section 6.3.1.

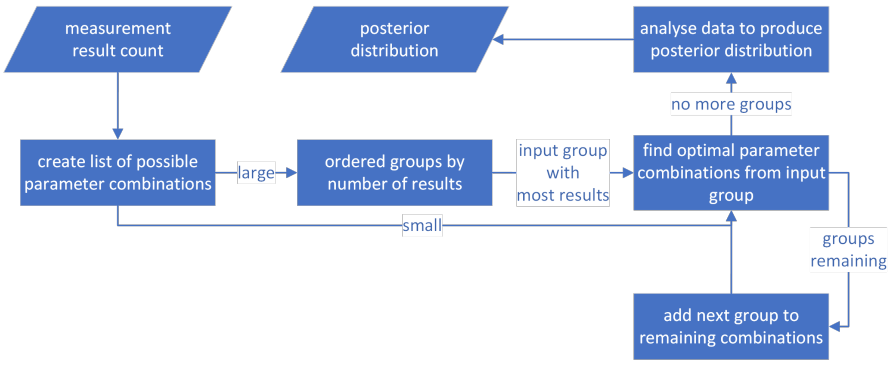

Figure A.2: Flow chart for producing the optimal information gain with multiple Bobs. The data analysis step is represented in figure A.3

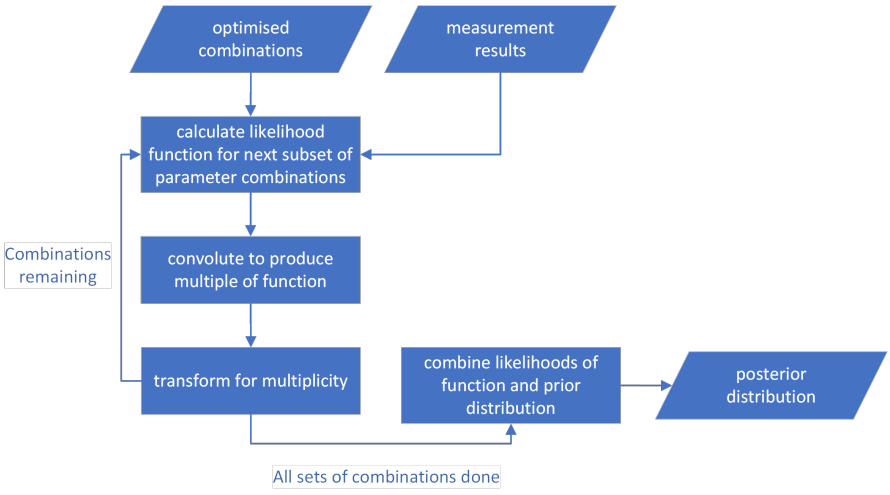

Figure A.3: Flow chart for data analysis with multiple Bobs.

A.3 Introductory example codes

Step by step

```
%% Written by Sean William Moore 2024-01-15, based on code from 2021-03-17
    to 2021-03-22 & 2022-06-22,    CC 4.0

%% Introduction

%The aim of this code is to give a first introduction to secure quantum
%remote sensing without entanglement as set out in
%https://doi.org/10.1116/5.0137260 . Input probabilities are similar to
%table 1 but here the measurement is a Pauli-X+ test with Xp,Xm,Yp,Ym
%representing the intial states |X/Y +- > .

%This code uses a Monte Carlo simulation choosing what happens to each
%parameter estimation qubit in turn in a noiseless scenario. The simulation
%is also used as an example of Bayesian updating. Finally, the results are
%analysed in a single step.

%There is no prior information in this code. With the data being circular,
%we use a flat prior over the 2pi range. This code is not intended for
%limited data analysis or very large data due to its simplicity. The
%maximum number of qubits that can be consistently estimated for with
%single step calculation is 1021 because 2^{-1022} is the minimum value for
%a double. The code can become unstable, particularily for Eve due to her
%results being noisy, more than approximately 500 qubits may give her NaN
%results. Bayesian updating is slower but more stable numerically.

%Press command-f search for pause( & change value for running speed
%changes.

%% Code admin

clear
close all
fig = 1;


%Reset random number generator
reset(RandStream.getGlobalStream,sum(100*clock));

```

```
%%  Histogram creation

%Parameter to be estimated is phi
nPhiStep = 1000; %number of phi bins in the histogram and related arrays
%Base of the histogram
phi=linspace(0,2*pi,nPhiStep+1);
phi(end) = []; %Remove the end because 0 and 2pi are the same points
dPhi=phi(2)-phi(1);

likelihoodBayesianUpdatingAlice = ones(1,nPhiStep)*dPhi;
likelihoodBayesianUpdatingEve = ones(1,nPhiStep)*dPhi;


%%   Choosing the number of states

prompt= 'How many photons do you want to use (<=1000)? ';
nPhotons= input(prompt); %n  is the number of states. Need better than a
    double to use higher than 1000



%%  Setting up the true value
phi0root = ceil(nPhiStep*rand); %Chooses random values between 1 and
    nPhiStep, therefore positions in the phi array
phi0 = phi(phi0root);
%phi0 = 2*pi*rand; as an alternative

%%  Preallocating/initiallising arrays

TrueState = zeros(1,nPhotons);
EveState = zeros(1,nPhotons);
BobResult = zeros(1,nPhotons);
probabilityVector = zeros(1,nPhotons);

%%  Setting the probability arrays here to reduce repetative computations
Xp = (1 + cos(phi))/2; %
Xm = (1 - cos(phi))/2;
Yp = (1 - sin(phi))/2;
Ym = (1 + sin(phi))/2;

%% Monte Carlo Simulation

```

```
78 %note: for is used during analysis & debugging. If Bayesian updating
79 %removed, parfor may be used here to increase speed. Other optimisations
80 %not included for simplicity
81
82 figure(fig)
83 fig=fig+1;
84 for a= 1:nPhotons
85     %Choosing the true state at random. Alice knows this.
86     TrueState(a) = randi([0,3]);
87     %However, Eve must guess what the state is
88     EveState(a) = randi([0,3]);
89
90     %Bob's measurement depends on the true state
91
92     if TrueState(a) == 0
93         probabilityVector(a) = (1+cos(phi0))/2;
94     elseif TrueState(a) == 1
95         probabilityVector(a) = (1-cos(phi0))/2;
96     elseif TrueState(a) == 2
97         probabilityVector(a) = (1-sin(phi0))/2;
98     elseif TrueState(a) == 3
99         probabilityVector(a) = (1+sin(phi0))/2;
100    end
101
102    %A Bernoulli test is performed to see what the results would be. This
103    %depends on the probabilities defined by quantum mechanics. We use a
104    %random number to simulate the Bernoulli test.
105
106    BobResult(a) = rand <= probabilityVector(a) ;
107    %1 is for a positive result. 0 for a negative result.
108
109 %%   Bayesian updating
110 % use { to comment out Bayesian updating from here
111    if BobResult(a) == 1
112        if TrueState(a) == 0
113            likelihoodBayesianUpdatingAlice =
    likelihoodBayesianUpdatingAlice .* Xp;
114        elseif TrueState(a) == 1
115            likelihoodBayesianUpdatingAlice =
    likelihoodBayesianUpdatingAlice .* Xm;
116        elseif TrueState(a) == 2
117            likelihoodBayesianUpdatingAlice =
```

```
likelihoodBayesianUpdatingAlice .* Yp;
118         elseif TrueState(a) == 3
119             likelihoodBayesianUpdatingAlice =
likelihoodBayesianUpdatingAlice .* Ym;
120         else
121             error('BayesianUpdating Alice')
122         end
123
124         if EveState(a) == 0
125             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
.* Xp;
126             %These align with interpretation given in next section. View
127             %that first as it is easier to understand.
128         elseif EveState(a) == 1
129             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
.* Xm;
130         elseif EveState(a) == 2
131             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
.* Yp;
132         elseif EveState(a) == 3
133             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
.* Ym;
134         else
135             error('BayesianUpdating Eve')
136         end
137     elseif BobResult(a) == 0
138         if TrueState(a) == 0
139             likelihoodBayesianUpdatingAlice =
likelihoodBayesianUpdatingAlice .* (1-Xp);
140         elseif TrueState(a) == 1
141             likelihoodBayesianUpdatingAlice =
likelihoodBayesianUpdatingAlice .* (1-Xm);
142         elseif TrueState(a) == 2
143             likelihoodBayesianUpdatingAlice =
likelihoodBayesianUpdatingAlice .* (1-Yp);
144         elseif TrueState(a) == 3
145             likelihoodBayesianUpdatingAlice =
likelihoodBayesianUpdatingAlice .* (1-Ym);
146         else
147             error('BayesianUpdating Alice')
148         end
149
```

```
150         if EveState(a) == 0
151             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
    .* (1-Xp);
152         elseif EveState(a) == 1
153             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
    .* (1-Xm);
154         elseif EveState(a) == 2
155             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
    .* (1-Yp);
156         elseif EveState(a) == 3
157             likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve
    .* (1-Ym);
158         else
159             error('BayesianUpdating Eve')
160         end
161
162     else
163         error('BayesianUpdating BobResult')
164     end
165 %Normalisation
166     likelihoodBayesianUpdatingAlice = likelihoodBayesianUpdatingAlice./(sum
    (sort(likelihoodBayesianUpdatingAlice))*dPhi);
167     likelihoodBayesianUpdatingEve = likelihoodBayesianUpdatingEve./(sum(
    sort(likelihoodBayesianUpdatingEve))*dPhi);
168 %Plotting
169     subplot(4,4,mod(a-1,16)+1)
170     plot(phi/pi,likelihoodBayesianUpdatingAlice,'DisplayName','Alice')
171     hold on
172     plot(phi/pi,likelihoodBayesianUpdatingEve,'DisplayName','Eve')
173     hold off
174     xline(phi0/pi)
175     title([num2str(a), ' qubits'])
176     xticks(0.25:.5:1.75)
177     ylabel('L(\phi)')
178     xlabel('\phi (\pi)')
179     pause(1)
180 %}
181 end
182
183 %%  Alice & Eve's interpretations of the results
184
185 %Alice's interpretation of the results. She counts the number of times that
```

```
%she got each result.

A1 = sum(TrueState ==0 & BobResult ==1); %|X+> initial state, 1 as result
A2 = sum(TrueState ==0 & BobResult ==0); %|X+> initial state, 0 as result
A3 = sum(TrueState ==1 & BobResult ==1); %|X-> etc.
A4 = sum(TrueState ==1 & BobResult ==0);
A5 = sum(TrueState ==2 & BobResult ==1); %|Y+>
A6 = sum(TrueState ==2 & BobResult ==0);
A7 = sum(TrueState ==3 & BobResult ==1); %|Y->
A8 = sum(TrueState ==3 & BobResult ==0);

%Eve's interpretation of the results
E1 = sum(EveState ==0 & BobResult ==1);
E2 = sum(EveState ==0 & BobResult ==0);
E3 = sum(EveState ==1 & BobResult ==1);
E4 = sum(EveState ==1 & BobResult ==0);
E5 = sum(EveState ==2 & BobResult ==1);
E6 = sum(EveState ==2 & BobResult ==0);
E7 = sum(EveState ==3 & BobResult ==1);
E8 = sum(EveState ==3 & BobResult ==0);


%%  Alice & Eve estimating their likelihoods resepctively

%   Likelihood = P1^N1*P2^N2*P3^N3 ....etc.
%Alice:
AliceLikelihood = Xp.^A1.*(1-Xp).^A2 .* Xm.^A3.*(1-Xm).^A4 .* Yp.^A5.*(1-Yp
    ).^A6 .* Ym.^A7.*(1-Ym).^A8;
%Normalising
AliceLikelihood = AliceLikelihood./(sum(sort(AliceLikelihood))*dPhi);
%Eve:
EveLikelihood = Xp.^E1.*(1-Xp).^E2 .* Xm.^E3.*(1-Xm).^E4 .* Yp.^E5.*(1-Yp)
    .^E6 .* Ym.^E7.*(1-Ym).^E8;
%Normalising
EveLikelihood = EveLikelihood./(sum(sort(EveLikelihood))*dPhi);



%%  Finding the maximum likelihood estimators

%Find the point in the histogram
```

```
[~,AliceMLE] = max(AliceLikelihood);
%Find the value of that point
AliceMLE = phi(AliceMLE);
%Same for Eve
[~,EveMLE] = max(EveLikelihood);
EveMLE = phi(EveMLE);

%%  Plots
figure(fig)
fig=fig+1;
plot(phi/pi,AliceLikelihood,'DisplayName','Alice')
hold on
plot(phi/pi,EveLikelihood,'DisplayName','Eve')
xline(phi0/pi,'--r','DisplayName','True value','LineWidth',2)
xline(AliceMLE/pi,'-.g','DisplayName','Alice maximum likelihood estimator',
    'LineWidth',.2)
xline(EveMLE/pi,'-.b','DisplayName','Eve maximum likelihood estimator','
    LineWidth',.2)
ylabel('L(\phi)')
xlabel('\phi (\pi)')
xticks(0:.25:2)
legend
title(['The likelihood functions for Alice and Eve after a Bayesian test
    with ' num2str(nPhotons) ' photons'])
```

Using distribution of result counts

```
%% Written by Sean William Moore 2024-01-15, based on code from 2021-03-17
    to 2021-03-22 & 2022-06-22,    CC 4.0

%% Introduction

%The aim of this code is to give a second introduction to secure quantum
%remote sensing without entanglement as set out in
%https://doi.org/10.1116/5.0137260 . Input probabilities are similar to
%table 1 but here the measurement is a Pauli-X+ test with Xp,Xm,Yp,Ym
%representing the intial states |X/Y +- > .

%This code calculates the resutls for Alice and Eve in a single step based
%on the statistical distribution of the results. Each inital state has a
%probability of giving a +1 or -1 result summing to 1. There is a 1 in 4
%probability that each state is occurs in each round. Therefore, we may use
%a multinomial with probability array 1/4 times the array of probabilities
```

```
%for each state to model the result distribution.

%Eve cannot know the initial state, knowing only that there is a
%probability of 1/4 of each occurring. Therefore, she must mix the
%probability distribution with 1/4 probability of each qubit being in each
%state

%There is no prior information in this code. With the data being circular,
%we use a flat prior over the 2pi range. 2pi inclusive. This code is not
    intended for
%limited data analysis or very large data due to its simplicity. The
%maximum number of qubits that can be consistently estimated for with
%single step calculation is 1021 because 2^{-1022} is the minimum value for
%a double. The code can become unstable, particularily for Eve due to her
%results being noisy, more than approximately 500 qubits may give her NaN
%results. Bayesian updating is slower but more stable numerically.

%Press command-f search for pause( & change value for running speed
%changes.

%% Code admin

clear
close all

color_order = get(gca,'colororder');
%Reset random number generator
rng('shuffle','twister');

%%  Grid creation

%Parameter to be estimated is phi
precisionRoot = 10;
precision = 2^precisionRoot; %number of phi bins in the histogram and
    related arrays
dPhi = 2*pi/precision; %bin width
%Base of the histogram
phi=linspace(dPhi,2*pi,precision);


%%   Choosing the number of states

```

```
prompt= 'How many photons do you want to use (<=1000)? ';
nQubits= input(prompt); %n  is the number of states. Need better than a
    double to use higher than 1000



%%  Setting up the true value
phi0 = 2*pi*rand;
%phi0root = ceil(precision*rand); %Chooses random values between 1 and
    precision, therefore positions in the phi array
%phi0 = phi(phi0root); as an alternative


%%  Setting the probability arrays here to reduce repetative computations
Xp = (1 + cos(phi))/2; %
Xm = (1 - cos(phi))/2;
Yp = (1 - sin(phi))/2;
Ym = (1 + sin(phi))/2;

%%  Single step results

probabilityArrayAlice = [(1+cos(phi0))/2,(1 - (1+cos(phi0))/2 ),(1-cos(phi0
    ))/2,(1- (1-cos(phi0))/2 ),(1-sin(phi0))/2,(1 - (1-sin(phi0))/2 ),(1+
    sin(phi0))/2,(1 - (1+sin(phi0))/2 )];

AliceResults = mnrnd(nQubits, probabilityArrayAlice/4 );

probabilityArrayEve = 1/4*probabilityArrayAlice + 1/4*circshift(
    probabilityArrayAlice,2) + 1/4*circshift(probabilityArrayAlice,4) +
    1/4*circshift(probabilityArrayAlice,6);

EveResults = mnrnd(nQubits, probabilityArrayEve/4 );


%%  Alice & Eve estimating their likelihoods resepctively

%   Likelihood = P1^N1*P2^N2*P3^N3 ....etc.
%Alice:
AliceLikelihood = Xp.^AliceResults(1).*(1-Xp).^AliceResults(2) .* Xm.^
    AliceResults(3).*(1-Xm).^AliceResults(4) .* Yp.^AliceResults(5).*(1-Yp)
    .^AliceResults(6) .* Ym.^AliceResults(7) .*(1-Ym).^AliceResults(8);
%Normalising
```

```
AliceLikelihood = AliceLikelihood./(sum(sort(AliceLikelihood))*dPhi);
%Eve:
EveLikelihood = Xp.^EveResults(1).*(1-Xp).^EveResults(2) .* Xm.^EveResults
    (3).*(1-Xm).^EveResults(4) .* Yp.^EveResults(5).*(1-Yp).^EveResults(6)
    .* Ym.^EveResults(7).*(1-Ym).^EveResults(8);
%Normalising
EveLikelihood = EveLikelihood./(sum(sort(EveLikelihood))*dPhi);



%%  Finding the maximum likelihood estimators

%Find the point in the histogram
[~,AliceMLE] = max(AliceLikelihood);
%Find the value of that point
AliceMLE = phi(AliceMLE);
%Same for Eve
[~,EveMLE] = max(EveLikelihood);
EveMLE = phi(EveMLE);

%%  Plots
figure
plot(phi/pi,AliceLikelihood,'color',color_order(4,:),'DisplayName','Alice')
hold on
plot(phi/pi,EveLikelihood,'color',color_order(3,:),'DisplayName','Eve')
xline(phi0/pi,'--','color',color_order(6,:),'DisplayName','True value','
    LineWidth',2)
xline(AliceMLE/pi,'-.','color',color_order(4,:),'DisplayName','Alice
    maximum likelihood estimator','LineWidth',.2)
xline(EveMLE/pi,'-.','color',color_order(3,:),'DisplayName','Eve maximum
    likelihood estimator','LineWidth',.2)
ylabel('L(\phi)')
xlabel('\phi (\pi)')
xticks(0:.25:2)
legend
title(['The likelihood functions for Alice and Eve from a statistical
    simulation with ' num2str(nQubits) ' photons'])
```