Quantum cryptography with structured light

Michael Almeida De Oliveira

Supervisor: Prof. A. Forbes

Faculty of Science
University of the Witwatersrand

A dissertation submitted in fulfilment of the requirements for the degree of
Master of Science

July 28, 2020

Declaration

I declare that I am the author of this work submitted for examination for the Degree of Master of Science at the University of the Witwatersrand, Johannesburg. I also certify that this is solely my own original work, except where due reference is made for work forming part of jointly-authored publications. My contribution and those of the other authors to this work have been explicitly indicated below. I certify that this work has not been submitted in any form for any degree or diploma to any tertiary institution. I confirm that due reference has been provided on all supporting literature and resources.

The work presented in Chapter 4 is under peer review as "Holographically-controlled random numbers from entangled twisted photons" by **M. de Oliveira**, N. Bornman and A. Forbes. M.d.O. was the primary author, developed the theory, performed the experiments and analysed the data; N.B wrote the relevant software. A.F. conceived of the idea and supervised the project. M.d.O. wrote the first draft of the manuscript, with all authors contributing to the subsequent revisions.

The work presented in Chapter 5 was published in Physical Review A as "Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons" by **M. de Oliveira**, I. Nape, J. Pinnell, N. TabeBordbar and A. Forbes. M.d.O. was the primary author, performed the experiments and analysed the data. M.d.O., N.T., J.P., and I.N. developed the theory. A.F. conceived of the idea and supervised the project. M.d.O. wrote the first draft of the manuscript, with all authors contributing to the subsequent revisions.

Michael Almeida De Oliveira
July 28, 2020

Abstract

Contemporary communication techniques generally involve encrypting sensitive data by means of mathematically complex algorithms and then distributing it and the accompanying digital decipher keys along classical channels. However, advances in current computing power pose a threat to the security of these methods, leaving them susceptible to being compromised without being noticed. This has led to an unprecedented surge in the exploration of quantum protocols, where quantum mechanical principles, such as the no-cloning theorem and non-locality, offer unconditional security against an eavesdropper. A current limitation of these protocols is the slower communication rates compared to popular classical implementations. Much focus has been on systems where information is encoded in a single degree of freedom (e.g. polarisation), however we demonstrate that high-dimensional protocols have the potential to overcome the slow rate limitation, offering an increased encoding capacity and a more robust solution.

Spatially structured modes of light carrying orbital angular momentum have become the forerunners for realising high-dimensional quantum protocols. Here, we investigate the high-dimensional generation, manipulation and detection of structured light and in doing so we realise two important applications- the generation and transmission of encryption keys - the key steps of a quantum cryptographic system.

The first application is a quantum random number generator certified by the random outcomes of projective measurements on path superpositions that we engineer using digital holography. We extend our approach to realise a novel random number generator based on the orbital angular momentum entanglement of spontaneous parametric down-converted states. We show that the digital control offered by our setup can be used to compensate for any bias present within system or to generate random numbers with a desired probability distributions. For the second application, we demonstrate the potential of using the high-dimensional encoding space offered by spin-orbit coupled states for quantum secret sharing. We realise the highest number of participants and dimensions thus far and in the process surpass the 1 bit per photon limit of two-dimensional protocols.

To my loving parents

Acknowledgements

I would like to express my deepest gratitude to everyone whose support was a milestone in the completion of this dissertation. In particular, I wish to thank the following people:

First and foremost, to my supervisor, Prof. Andrew Forbes, I am thankful for your consistent guidance and encouragement. You have been an invaluable inspiration in my quest for knowledge and an acquaint mentor to the scientific world. You have taught me how to be a meticulous researcher and an inspiriting communicator of my work. Thank you for all the opportunities to expand my network and scientific footprint.

Throughout this process, I have found a community in the Structured Light Group. Thank you to everyone for never let things get dull or boring. Dr. Valeria Rodriguez-Fajardo and Dr. Najmeh TabeBordbar, I am grateful for our countless coffee runs and authentic discussions. Thank you for being a sounding board when things got tough. Isaac, you were instrumental in showing me the ropes around the lab and for that I am grateful. Jonathan and Bereniece, thank you for your immense contributions and for helping me accelerate my learning. Thank you, Nicholas, for our fruitful discussions and your interesting perspective on life and science.

Lastly, I wish to acknowledge the support and great love of my family. Thank you for your interest in what I am doing. Your every attempt to understand my work will not be forgotten. To my parents, thank you for putting up with me in difficult moments where I felt stumped and for goading me on to follow my dream of getting this degree. This would not have been possible without your unwavering and unselfish love and support.

Table of contents

List of figures

List of tables

List of publications

Journal papers

1. **de Oliveira, M.**, Nape, I., Pinnell, J., TabeBordbar, N., and Forbes, A., "Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons", Physical Review A, 101(4):042303, 2020.

2. Pinnell, J., Nape, I., **de Oliveira, M.**, TabeBordbar, N., and Forbes, A., "Experimental 11-dimensional secret sharing with Perfect Vortex beams", Accepted by Laser & Photonics Reviews.

3. Forbes, A., **de Oliviera, M.**, and Dennis, M.R., "Structured light", Submitted to Nature Photonics.

4. **de Oliveira, M.**, Bornman, N., and Forbes, A., "Holographically-controlled random numbers from entangled twisted photons", Submitted to Physical Review A.

National presentations

1. **de Oliveira, M.**, Nape, I., TabeBordbar, N., and Forbes, A., “Single qubit secret sharing with spatial modes”, Quantum Africa V, Talk, 2019.

2. **de Oliveira, M.**, Nape, I., Pinnell, J., TabeBordbar, N., and Forbes, A., “How to share a secret with twisted light”, African Laser Conference, Talk, 2019.

3. **de Oliveira, M.**, Nape, I., Pinnell, J., TabeBordbar, N., and Forbes, A., “High dimensional quantum secret sharing of images”, African Laser Conference, Poster, 2019.

4. **de Oliveira, M.**, Nape, I., Pinnell, J., TabeBordbar, N., and Forbes, A., “Sharing a secret with patterned light” , Photonics Online Meetup, Poster, 2020.

Chapter 1

Introduction

As cloud computing environments seize our personal and corporate lives, data security is at the forefront of our minds: How is our privacy ensured when browsing the internet? How do corporations securely store and transmit our sensitive information? The answer - cryptography. Cryptography is the science of secure communication, converting meaningful sequences into seemingly arbitrary nonsense using a random encryption key, such that only a key holder can recover the original sequence [1]. Cryptography is a growing research field, with uses in securing online commerce, safeguarding private communications over the internet and many others. Most corporations will use varying levels of cryptography to guarantee the confidentiality of their users' information. They rely on approved cryptographic standards [2] to secure the digital services they offer over both the internet and cloud platforms. But, with the increasing computational capabilities of current technologies, popular classical implementations are becoming inadequate. The focus has since shifted to quantum cryptography, in which the security is no longer subject to mathematical or computational complexity of the classical implementations but rather the probabilistic laws of quantum physics [1].

In order to compete with current technological advances, we need to realise the rapid generation and secure transmission of high-quality encryption keys - the vital principles of any cryptographic protocol.

1.1 Modern cryptography

The ancient art of secret writing dates back to circa 1900 B.C. when an Egyptian scribe etched an inscription with unusual hieroglyphs, whose full meaning was only known to an elite few. Throughout the millennia that followed, the encryption of secret information was of paramount importance to the security and welfare of various civilisations, with specific use in diplomatic missives and war strategies. Many experts have since argued that cryptography, the science of secret writing, emerged in civilisations spontaneously once writing was ascertained. Unsurprisingly, it has evolved into new forms upon the adoption of digital communication. Modern cryptography is the epitome of digital security and communication between billions of people and is used as a tool for commerce, social interaction, and the exchange of an increasing amount of personal information.

Fundamentally, the security of our data relies on the premise of computationally hard problems, particularly number theory problems, such as the prime factorisation or the discrete logarithm problem. These are often problems that are easy to state but have been found difficult to solve. For example, it is computationally easy to combine two large numbers together (i.e., 167 X 199 = 33 233), however, the reverse is computationally more difficult (i.e., to determine what the original two numbers were, given that the answer is 33 233).

Akin algorithms are used for cryptographic key generation which are assimilated and distributed through encryption schemes. The most general encryption schemes are (see Fig. 1.1):

- Asymmetric-key (public-key): Diffie and Hellman introduced the idea of public-key encryption [3]. Here, two different but mathematically related keys are generated, such that the calculation of one key (the private key) is computationally impossible from the other (the public key). The sender uses the public key to encrypt the message and the receiver uses the secret private key to decipher the encoded message.

- Symmetric-key: These encryption algorithms create a key that is used for both encoding and decoding information [4]. The secret key is unique to the sender and receiver, without ever having been transmitted. In this case, the secret key is used by the sender to encode the message and then the same key is used by the receiver to decipher the encoded message.

The looming threat to these cryptographic algorithms is the new paradigm of quantum computation. A common attack on symmetric cryptographic schemes involves brute force, where all possible key combinations, are tested until the message is deciphered. The advent of quantum computing with the likes of the 1996 formulation of Grover's algorithm [5], can provide a quadratic speed up, decreasing the brute force attack time. Co-currently, in 1994 Peter

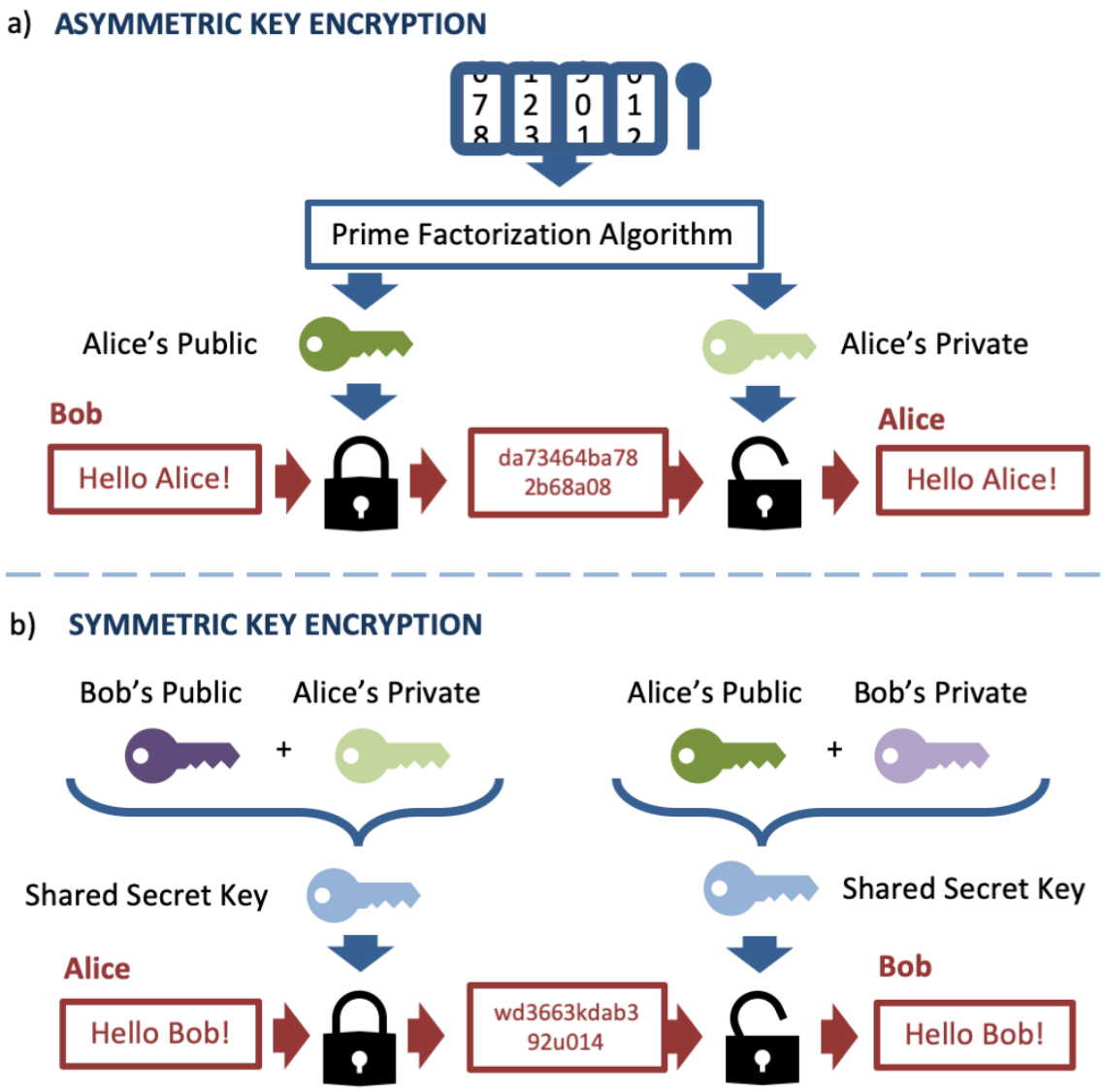

Fig. 1.1 Concept of encryption key schemes. (a) In asymmetric key encryption, Alice generates a public and private key using a random number generator. Anyone can use Alice's public key to encrypt a message and the Alice can use her unique private key to decrypt the message. (b) In symmetric key encryption, Alice and Bob can use each others public key together with their own private key to generate an identical shared secret key. In this way Alice can encrypt her message and Bob can decrypt it, without ever having transmitted the shared secret key.

Shor formulated an algorithm that could use quantum principles to efficiently (in polynomial time) reduce the time needed to solve current asymmetric cryptographic algorithms [6] - turning problems that would classically take millennia of computational time into much more feasible computational times like days or weeks (see Fig. 1.2). The technology to effectively do this was non-existent at the time, however, two decades later many advances in quantum processing

hardware have been made. Many believe that quantum computing developments have reached a point where current grade cryptography could be compromised within the next decade, leaving our data vulnerable.

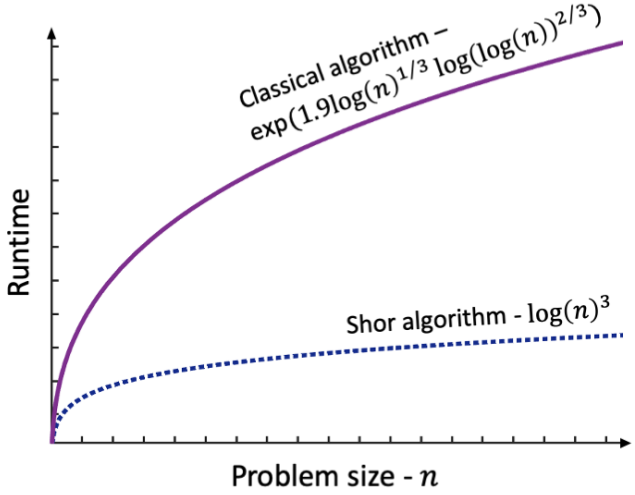

Fig. 1.2 Demonstrating the quantum speed up that the Shor algorithm offers compared to the best classical algorithm, effectively reducing the time needed to perform integer factorisation used in current cryptographic algorithms.

Do not be dismayed. The industry is searching for new quantum-resistant standards and in the process many corporations are implementing mitigation measures to improve the resiliency of their current encryption methods against future quantum computing attacks. One way of doing this is by increasing the required key length, but with the rise of quantum processing, this will only provide temporary protection. Another option involves adapting current asymmetric encryption schemes with underlying algorithms that are resilient to phase estimation transformations and periodic finding (the key techniques used in Shor's Algorithm) [7]. Lattice-based cryptography is the most popular candidate, which uses the shortest vector problem for quantum safe encryption, however, it does not scale well [8]. The point to note is that as quantum computing advances and new quantum algorithms are developed, the current quantum-resistant algorithms could at some point be compromised because they are inherently based on classical principles. Consequently, modern cryptography needs to transition to the quantum realm, leveraging the probabilistic nature of quantum mechanics rather than only number theory and mathematical complexities.

1.2 Quantum mechanics as a cryptographic solution

Current methods of secure communication typically involve encrypting sensitive information and then transmitting it along classical channels together with the digital keys required to decipher the data. They are transmitted as classical bits, 1s and 0s, by a stream of either optical or electrical pulses. They are vulnerable and can be compromised without being noticed. The quantum computing threat posed to the security of the data has forced the exploration of quantum protocols for transmitting and securing information. Quantum mechanical principles, such as the no-cloning theorem [9] and non-locality [10] are at the heart of these protocols. As we will discuss, these principles offer unconditional security against an eavesdropper trying to glean any information about the system [11]. We will further outline common quantum protocols used to generate and distribute the encryption keys necessary for the secure sharing of data. We will consider a major limitation of most current quantum protocols, this being that the secret key generation rate is orders of magnitude lower than current classical communication rates [12], and then we will show how high-dimensional protocols can overcome this limitation, offering a faster and more robust solution.

1.2.1 Principles underpinning quantum cryptography

The beauty of quantum communications is that they are naturally tamper-proof. It follows that in order for an assailant to gain knowledge of the system, they would have to eavesdrop on the system or clone the quantum state and subsequently send an identical copy. However, this is not possible because of the no-cloning theorem of quantum mechanics [9]. In general this means that no quantum state can be measured or observed without disturbing the original state. If a quantum operation existed that was able to copy quantum states, it would be very useful with impressive repercussions, such as faster than light communication [13]. For example, given an unknown quantum state for which there exists no single possible measurement that can distinguish between all possible states without some probability error, then if it were possible to make copies of the unknown state and repeat the optimal measurement many times, then the error probability will converge to the exact state. But such a quantum operation cannot exist.

In order to proceed, we introduce a convenient representation of quantum states using Dirac notation [14]. The convention prescribes the use of state vectors to map a quantum state onto a d-dimensional Hilbert space. Here, the vector states are described by a ket, $|\cdot\rangle$, and consequently their complex conjugate as a bra, $\langle\cdot|$.

Now, suppose we have two quantum systems A and B with identical Hilbert spaces. We wish to copy an arbitrary state of the quantum system A, described by $|\psi\rangle_A = \alpha|0\rangle + \beta|1\rangle$, where the complex coefficients α and β are unknown. To copy this state we combine it with

a 'blank' initial state $|e\rangle_B$ in system B, which is independent of $|\psi\rangle_A$. The initial composite system is then described by the tensor product, $|\psi\rangle_A \otimes |e\rangle_B$ (we will omit the tensor product operator $\otimes$ for simplicity).

We can manipulate this composite system in one of two ways. Either we perform an observation, collapsing the system into some eigenstate of the observable, or we control the Hamiltonian of the system, and thus the time-evolution operator $U(t)$. The former corrupts the information of the quantum state, which is not what we want. Alternatively, the latter evolving up to some fixed time t_0 (independent of $|\psi\rangle_A$), yields a unitary operator U_{copy}. The action of the operator on the basis states is given by,

$$\begin{aligned} |0\rangle_A |e\rangle_B &\xrightarrow{U_{\text{copy}}} |0\rangle_A |0\rangle_B , \\ |1\rangle_A |e\rangle_B &\xrightarrow{U_{\text{copy}}} |1\rangle_A |1\rangle_B . \end{aligned} \tag{1.1}$$

However, no such unitary operator can clone all states perfectly, giving rise to the no-cloning theorem. We prove the no-cloning theorem by contradiction following from the linearity of quantum mechanics. If we apply the unitary operator U_{copy} to the initial composite system, we expect to perfectly copy the unknown state in system A to the blank state in system B, which is then

$$\begin{aligned} |\psi\rangle_A |\psi\rangle_B &= (\alpha |0\rangle_A + \beta |1\rangle_A)(\alpha |0\rangle_B + \beta |1\rangle_B) \\ &= \alpha^2 |0\rangle_A |0\rangle_B + \beta\alpha |1\rangle_A |0\rangle_B + \alpha\beta |0\rangle_A |1\rangle_B + \beta^2 |1\rangle_A |1\rangle_B . \end{aligned} \tag{1.2}$$

However, by the linearity of U_{copy}, when you copy the individual components in the expression of $|\psi\rangle_A$, we arrive at a different state:

$$(\alpha |0\rangle_A + \beta |1\rangle_A) |e\rangle_B \xrightarrow{U_{\text{copy}}} \alpha |0\rangle_A |0\rangle_B + \beta |1\rangle_A |1\rangle_B . \tag{1.3}$$

Here, there are no cross terms and we arrive at a contradiction. Therefore, there exists no perfect unitary operator U_{copy} that can make a perfect copy of an arbitrary quantum state, i.e., U_{copy} cannot act as a general copier [9]. An implication of the no-cloning theorem for quantum communication is that an eavesdropper would introduce errors into the system that would be implicitly detected by the cooperating parties. This is a feature that cannot be found in any classical cryptographic technique. The no-cloning theorem is thus a vital and differentiating ingredient necessary is preserving the security of communication in a post quantum world.

1.2.2 Generating random numbers for encryption

The basis of any cryptographic protocol necessitates the sharing of random encryption keys which are used to securely encrypt and decrypt sensitive information. Notably, random numbers are an indispensable resource for securely sharing and storing important data. In reality, cryptography can be thought of as a distributing key generator, with its very own random process [15]. It follows, that the security of the cryptographic protocol is influenced by the randomness (i.e., unpredictability) of the encryption key, and in effect the process by which it was generated. As a result, sophisticated and more robust protocols require random encryption keys that reflect the quality of the underlying randomness source. Meaning that a random number generator must be implemented in such a way that attackers cannot predict the generated key better than just blindly guessing.

Similarly, as the communication industry searches for mitigation measures to improve the aptitude and security of current cryptographic methods against future attacks, a popular response is to increase the required encryption key length. While this only offers temporary assurance, as more rigorous counter attacks are co-currently developed, it is an expeditious solution. This has also led to a hunt for faster and more convenient random number generators. Appropriately, both fast and high-quality random number generation has the promise to transform the preeminence of cryptography at large [16].

We begin by reviewing the fundamental types of random number generators (RNGs) characterised by their source of randomness. The two types of RNGs are:

- Pseudorandom number generators (PRNG): These generators extrapolate randomness from an initial input and expand it by a deterministic recursive algorithm that outputs a pseudo random sequence following a uniform distribution [17]. In other words, PRNGs generate a sequence that behaves as if it were random. Even if the sequence passes the appropriate randomness standards [18], given enough time the analysis can yield patterns within the sequence.

- True random number generators (TRNG): These generators extract randomness from some physical process that is unpredictable, or at the very least, difficult to predict. The complexity and the copious unknown parameters of these sizeable systems (i.e., the incomplete knowledge of a system), allows for their behaviour to be deemed truly random [19].

We are most interested in quantum random number generators (QRNGs), a distinct type of TRNGs. Here, the uncertainty is a consequence of a quantum event as opposed to insufficient knowledge of the system. The fundamental basis of any QRNG is quantum mechanics, which

enables the existence of inherently unpredictable processes. The current understanding is that the nature of quantum mechanics is the only true source of randomness. Thus, QRNGs are a very attractive choice for the generation of high-quality random keys and seed numbers needed for quantum cryptography. This has led to various QRNG schemes ranging from the early implementations of radioactive decay [20, 21], to more recent methods using emission and detection of photons [22], noise of lasers [23] or quantum vacuum fluctuations [24, 25] as a source of entropy.

As we will see later, quantum optics offers a high speed, versatile and accessible approach to generating high quality quantum random numbers. It has a high application potential due to the high quality and accessibility of the required optical components, as well as the prospect of chip sized integration.

1.2.3 Quantum communication schemes

An equally integral component of quantum communication involves the secure transmission of secret keys for encryption and decryption. This involves sending encrypted data as classical bits over a network, while transmitting the quantum bit (qubit) key used to encrypt the data via a quantum channel. The way in which the quantum key is transmitted is determined by the protocol. The security of the protocols rely on the no-cloning theorem and its inherent ability to protect against eavesdropping [26, 27]. As previously discussed, this means an adversary cannot disrupt or eavesdrop on the quantum key channel without leaving behind trace-fingerprints. If foul play is suspected, the key is discarded and the participants informed of the intrusion.

The most popular and well developed application of quantum communication is quantum key distribution (QKD) between two parties [28]. However, applications requiring the secure communication of information between more than two parties has lead to an interest in multi-party protocols such as quantum secret sharing (QSS) [29] and quantum secure direct communication (QSDC) [30]. Here, we will review the operating principles for both QKD and QSS, followed by a discussion of the potential advantages of implementing these protocols in high-dimensions.

Quantum Key Distribution

Various protocols have been developed for implementing QKD. The most commonly used was proposed by Bennett and Brassard in 1984, and subsequently, is called the BB84 protocol [31]. For simplicity, consider the original description of the protocol using polarisation encoding. The conventional orthogonal polarisation state pairs are: the standard basis of horizontal $|H\rangle$ or

vertical $|V\rangle$ states and the rectilinear basis of diagonal $|D\rangle = 1/\sqrt{2}(|H\rangle + |V\rangle)$ or anti-diagonal $|A\rangle = 1/\sqrt{2}(|H\rangle - |V\rangle)$ states. Note that, a set of orthogonal states is referred to as a basis. Now, since measuring in the standard basis gives a result of $|H\rangle$ or $|V\rangle$, then if the state is prepared as $|H\rangle$ or $|V\rangle$, the measurement will return a distinguishable state. However, if the state is prepared as $|D\rangle$ or $|A\rangle$, then the standard basis measurement will randomly return either $|H\rangle$ or $|V\rangle$. Moreover, after the measurement the state will be polarised to the measurement result, losing all information about its initial polarisation.

The generalised two-dimensional protocol requires the use of two bases, where each basis is conjugate to the other, and the two states within each basis are orthogonal. Extending this to d-dimensions results in the condition described mathematically as [32],

$$|\langle \psi_j | \phi_k \rangle|^2 = \frac{1}{d} \quad (j,k = 1,...,d), \tag{1.4}$$

where $|\psi_j\rangle$ and $|\phi_k\rangle$ are each basis sets forming what is called mutually unbiased bases (MUB). The security of the protocol comes from satisfying Eq. 1.4, as the condition implies that there exists no single measurement that can distinguish between all possible MUB states. The only distinguishable measurement is between any orthogonal states.

The principle of operation behind the BB84 protocol is shown in Fig. 1.3 and consists of two parties (Alice, the sender and Bob, the receiver) who are linked by a quantum channel (for example optical fibre or free-space) and an authenticated classical channel (for example radio or the internet). Alice starts with two random strings of bits, a and b, where the bit value b_i is what decides which basis (0 for the standard basis or 1 for the rectilinear basis) the classical bit, a_i, is encoded in . Alice prepares her photon in the state and basis corresponding the i^{th} bit value of a and b, respectively. Alice then transmits the prepared state to Bob over the quantum channel. Subsequently, Bob randomly selects a measurement basis b'_i (either standard or rectilinear), performs a measurement and records the result of the classical bit as a'_i. After a n number of runs, Alice and Bob use the classical channel to reconcile their prepared and measured states. In other words, Bob communicates over a public channel with Alice to reveal their choice of basis b_i and b'_i. The results that do not correlate are discarded, i.e., both Alice and Bob discard the qubits in a and a' where b_i and b'_i do not match. This occurs approximately half of the time by virtue of the protocol. What remains is a secret key unique to both Alice and Bob. To check the security of their transmission, both Alice and Bob publicly announce a subset of their secret keys and if the error (possibly due to Eve attempting to eavesdropping) is below a set threshold, then the security of the key produced is guaranteed, otherwise the key is compromised and communication terminated.

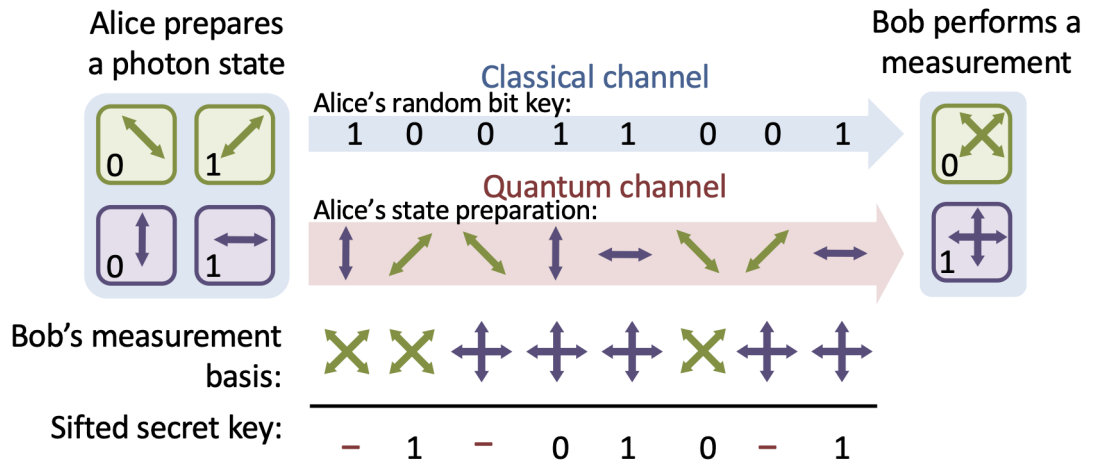

Fig. 1.3 An illustration of the BB84 protocol for QKD. Alice encodes a photon with one of the polarisation states, from either the linear or rectilinear MUBs, associated with her random bit key. Bob randomly selects a measurement basis and performs a measurement. If the choice of basis is correlated the round is accepted, or otherwise discarded. From this, the remaining bits establish the shared secure key between Alice and Bob, with which information is encrypted.

Quantum key distribution schemes, particularly the BB84 protocol, are the most well developed quantum cryptographic protocols, with numerous practical demonstrations ranging from applications in free-space [33–35], fibre [36, 37], underwater [38, 39] and further promising demonstrations with free-space to satellite quantum communication [40, 41].

Quantum secret sharing

While the demand for multiparty communication is significantly less, the secure communication between more than two parties (ruling out QKD protocols) is an important application of cryptography. The simplest solution to sharing a secret between multiple parties is to share copies of the secret with each party. A dilemma arises if no single party should have full access to the secret, for example applications like missile launch codes or passwords for large money transfers which may require multiple parties to agree.

Schemes for generating correlated keys shared among multiple parties have been developed, namely quantum secret sharing (QSS) protocols [29]. In these protocols, a secret is divided into unique shares sent to N-participants and then securely reconstructed by the collaborating parties, making it ideal for securely sharing and storing sensitive information across a network of nodes. Due to the expeditious increase in collaborative tasks, QSS is reaching a similar level of interest as quantum key distribution (QKD).

In 1979, Shamir expanded the idea geometrically by imagining the secret as a point in space and the shares as points along a secret random line [42]. The concept is visualised in Fig. 1.4. Here, we have assumed that Alice wants to share a secret number between Bob and Charlie without either party having any knowledge of the number. The key insight is to think of the number as a secret point on a 2D plane, where the secret is a point on the y-axis (more specifically the y-intercept). Randomness is introduced by selecting a random point on the plane, forming a secret line. At no point does Alice share any information about the line. This method effectively expands the secret and thus the security, by creating lots of redundancy. Now, Bob and Charlie each pick a random point on plane. If both points lie on the line, Alice announces that their points are correlated, otherwise the round is the discarded. Since only two unique points are needed recover the secret line, Bob and Charlie can collaborate and recover the equation of the line and in particular the y-intersect and Alice's secret number. It is trivial that this method is scalable in the number of parties by simply increasing the degree of the polynomial function describing the secret line. This concept forms the basis of many popular secret sharing protocols used today.

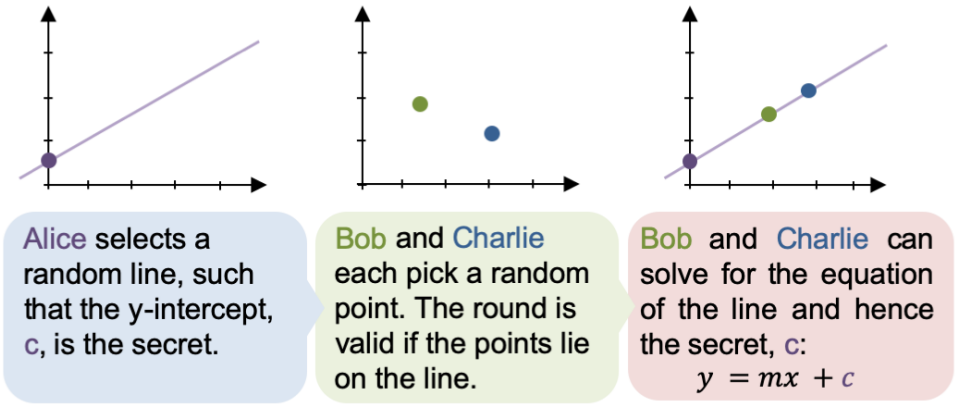

Fig. 1.4 Geometrical conceptualisation of Shamir's secret sharing protocol, showing how a secret can be securely shared between multiple parties.

The first quantum secret sharing (QSS) scheme proposed the use of the Greenburg-Horne-Zeilinger (GHZ) state for three parties [29]. In this protocol, three parties (Alice, Bob and Charlie) randomly pick between a choice of two mutually unbiased measurement bases, and independently measure their own entangled particle, as shown in Fig. 1.5(a). The use of MUBs implies that if either Bob or Charlie use different measurement bases compared to Alice, then their measurement results will be uncorrelated with Alice's result and the round is discarded. If their measurement bases are correlated, Bob and Charlie can collaborate and use their measurement bases and measurement results to infer the otherwise secret result of Alice's

measurement. In this way, Alice can use her key, constructed from her secret measurement results, to encrypt a message, while Bob and Charlie can use Alice's inferred key to decipher the message. In this protocol, at no point does Alice reveal her measurement results.

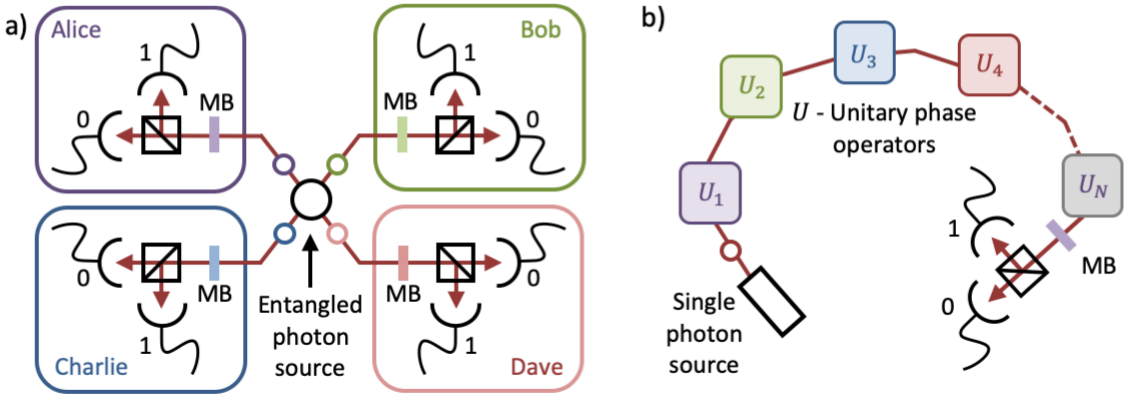

Fig. 1.5 Quantum secret sharing protocols. (a) A schematic of a multi-particle QSS protocol using non-local correlations between multiple entangled photons. Each party independently performs a measurement on their photon, from a choice of two basis. (b) A schematic of a N party single photon QSS protocol where by a photon is prepared in an initial state and sequentially communicated from party to party, each acting on it with a phase operator chosen from a basis set. The last participant then performs a a measurement on the photon. In both cases if the choice of bases are correlated then the collaborating parties can share a secret key.

Soon after, this standard protocol was improved to accommodate an arbitrary number of parties [21], and later, many other schemes emerged including circular [43], dynamic [44], graph state [45] and verifiable [46] QSS. Many of these schemes rely on non-local correlations between multiple particles and as such, experimental realisations [47, 48] have been limited by the notorious inefficiency of multi-photon entanglement.

Consequently, quantum secret sharing protocols using single photon states were first proposed [49] and demonstrated using polarisation encoding [50]. Here, as seen in Fig. 1.5(b), each party performs sequential unitary phase operations on the same particle instead of several entangled particles. Based on their choice of imparted phase and measurement basis, the validity of the round is checked. For the valid rounds, a subset of participants can recover Alice's secret key. More recently, a high-dimensional multi-party single photon QSS protocols was theoretically proposed [51–54]. These protocols require d MUBs, making high-dimensional photon encoding and the ability to independently manipulate each dimension essential to realising the protocols. Challenges in high dimensional state preparation, transformation and

detection, the key steps of any QSS protocol, have so far presented barriers to experimental realisation.

Quantum cryptography in high-dimensions

High-dimensional quantum protocols have two considerable advantages over two dimensional protocols. The first and most obvious being the infinite accessible encoding space. This allows for generation rates to exceed the limit set by the saturation and dead time of detectors. The second advantage is the higher resistance to quantum channel noise, meaning that these systems can tolerate a higher quantum bit error rate Q compared to two-dimensional systems [55]. This measure reflects the probability of making detection errors and as a result is 0 for a perfect system.

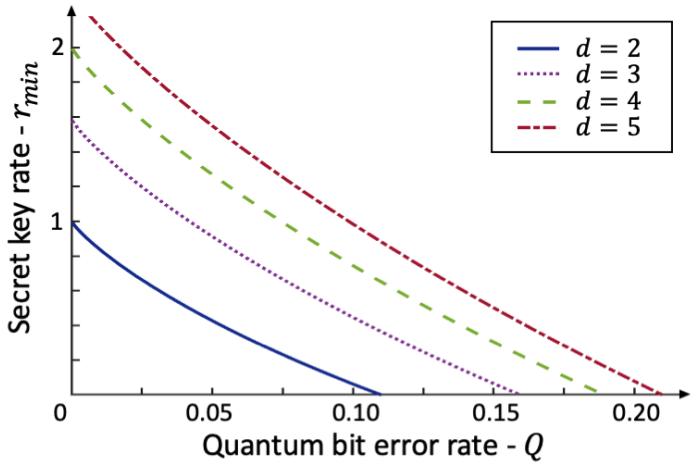

Fig. 1.6 The theoretical secret key rate, $r_{\min}$, versus the quantum bit error rate, Q, for dimensions $d = 2,3,4,5$. This shows that the secret key rate increases with the dimension of the system, with higher dimensions being more robust to errors.

In order to illustrate these benefits, consider another important measure of the implementation called the secret key rate. This measure is indicative of the amount of information that is securely sent between participants. For a d-dimensional system, this is given by [55]

$$r_{\min} = \log_2(d) + 2Q\log_2\left(\frac{Q}{d-1}\right) + 2(1-Q)\log_2(1-Q). \tag{1.5}$$

The maximum secret key rate for a perfect d-dimensional system is $\log_2 d$, increasing with dimension. Figure 1.6 illustrates the theoretical plot of the secret key rate, $r_{\min}$, as a function of the quantum bit error rate Q. From the plot we can deduce that higher dimensional quantum

communication systems can achieve a higher secret key rate at the same error rate. As a consequence, d-level systems are more robust in the presence of an adversary [56]. This has caused interest in the development of protocols that exploit high-dimensional encoding, where ideally, we want to maximise $r_{\min}$ and minimise the error rate Q.

1.3 Structured photons

Quantum states are essential in the transport of information over a provably secure quantum channel. They can be thought of as a quantum measure of information in an analogous way to classical bits in classical information theory. However, a distinction arises in that these states can simultaneously occupy a superposition of states compared to the definite values for classical bits. However, the amount of information encoded into a quantum state is contingent on the basis in which it is measured. For example, a two-dimensional quantum state (qubit) can carry at most only one bit of information, limiting the rate of information transfer. Therefore, a need for faster generation and transmission speeds has resulted in a search for an increased information capacity per photon. A viable solution is structured light [57, 58].

The principles that govern the structuring of light require the assertion of the wave nature of light. In the 1860s, Maxwell showed that light is a manifestation of the oscillating electromagnetic field [59]. Consequently, the newly accepted wave structure of light gained instantaneous acclaim, with many applications in various fields, which focused on structuring light with patterns or modes with distinct properties.

These structured light patterns or modes can be obtained from the solutions to the time-independent wave equation (Helmholtz equation). Solutions to the Helmholtz equation under specific conditions, form a set of modes defined by internal parameters. If these sets of solutions are in fact eigenmodes of the wave equation for a specific system (e.g. free space), then they satisfy the requirements for existence in that system and the structure of the mode is preserved as it propagates. Furthermore, the different modes of a solution set are orthogonal, forming a complete orthogonal basis for the system [60]. As a consequence, an arbitrary field existing within the defined system can be described by a linear combination of the respective basis modes. In the subsequent chapters we will see how these properties are in fact crucial for implementing quantum cryptography with light.

Moreover, with Maxwell's breakthrough, came the consideration that light must also be a carrier of energy and other mechanical effects including linear momentum [61]. Accordingly, light must also carry angular momentum, which in the paraxial approximation of the Helmholtz equation, can be further separated into two components: orbital angular momentum (OAM), associated with the total angular momentum coincident with the transverse spatial profile of the

photon [62, 63] and spin angular momentum (SAM), associated with the circular polarisation of the photon [61]. Progression in understanding and manipulating these properties naturally led to investigations into using OAM as a basis for reaching higher encoding spaces.

1.3.1 Spin angular momentum

Polarisation is a well documented property of light, but has reclaimed much attention owing to its recent angular momentum interpretation. In 1901, Poynting [61] conjectured that polarisation of light can be associated with the spin angular momentum (SAM). This was experimentally confirmed by Beth in 1936 [64], who showed a quarter waveplate rotate due to the torque exerted by circularly polarised light passing through it, which in effect transferred SAM. It follows that SAM corresponds to the rotation of the electric field oscillation as light propagates about the beam axis. This is illustrated in Fig. 1.7.

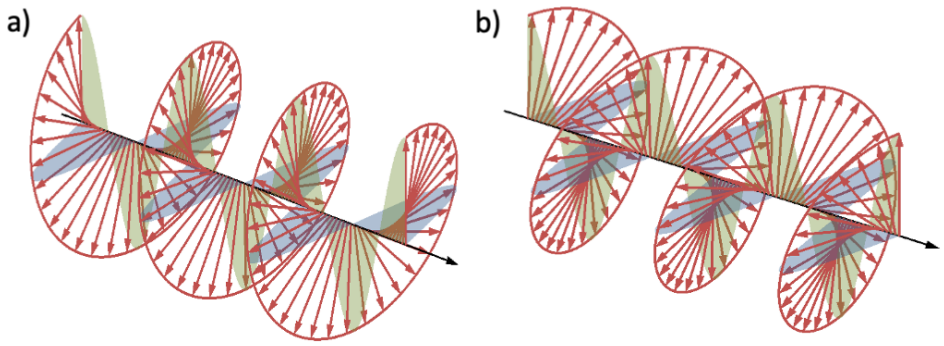

Fig. 1.7 An illustration of the electric field oscillations for circular polarisation states. The superposition of two linear polarised electric fields that are $\pi/2$ and $-\pi/2$ out of phase, produce (a) right and (b) left circularly polarised light respectively.

The rotational direction of the electric field denotes the handedness of the circular polarisation (i.e., right-handed denotes clockwise, left-handed denotes anti-clockwise). Additionally, photons with circular polarisation carry SAM of $\pm\hbar$ per photon, where the sign is determined by the handedness of the polarisation. The quantum states associated with the SAM can be represented using Dirac notation [14]. In particular, right and left circular polarisation states are denoted by $|R\rangle$ and $|L\rangle$, respectively. In the case where the electric field oscillates in a single plane, this is referred to as linear polarisation such as the horizontal $|H\rangle$, vertical $|H\rangle$ and diagonal $|H\rangle$ and anti-diagonal $|H\rangle$ states. In general, one can express any polarisation state as

$$|\psi_{\theta,\alpha}\rangle = \cos\left(\frac{\theta}{2}\right)|R\rangle + e^{i\alpha}\sin\left(\frac{\theta}{2}\right)|L\rangle, \tag{1.6}$$

with $\alpha \in [0, 2\pi]$ describing the relative phase between states and θ describing the weighted contribution of each state.

It is possible to describe any polarisation state on a two dimensional state-space, called the Poincaré sphere [62] (see Fig. 1.8). The probability of locating the photon in any of the eigenstates must be equal to 1 since the qubit must be in some state after all. Thus, by the conservation of probability, the state must be normalised according to,

$$\langle \psi | \psi \rangle = \cos^2\left(\frac{\theta}{2}\right) + \sin^2\left(\frac{\theta}{2}\right) = 1. \tag{1.7}$$

This describes a circle of unit radius, which we will call the amplitude circle. Furthermore, the parameter θ defines the position of the state on the circle, as shown in Fig. 1.8(a). The phase term $e^{i\alpha}$, in Eq. 1.6, is an oscillatory function that maps α to an angular position, which rotates the state about a unit phase circle (see Fig. 1.8(b)). Consequently, the Poincaré sphere combines both the amplitude and phase descriptions of the eigenstates of polarisation into one visual description, as in Fig. 1.8(c).

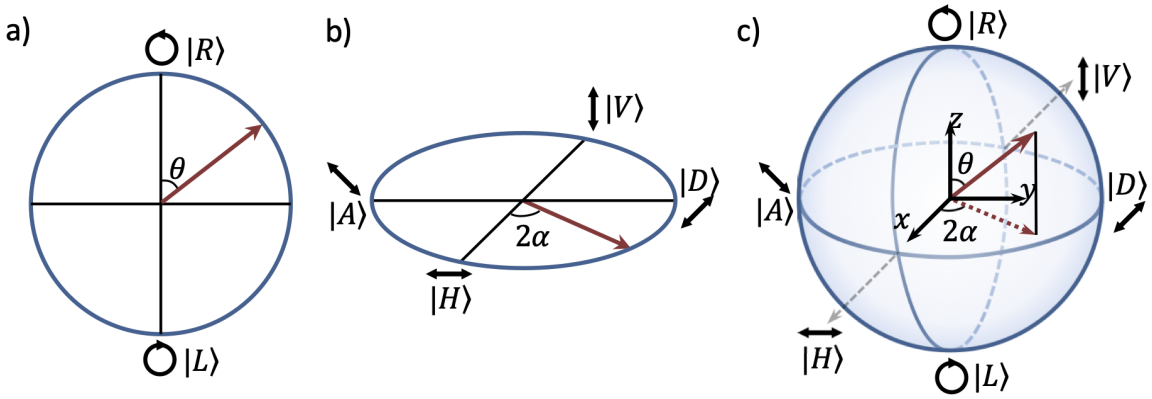

Fig. 1.8 Illustration showing the full control of the Poincare sphere. (a) The parameter θ enables a continuous change in relative amplitudes of left and right circular polarisations, described on a unit circle. (b) The phase parameter α allows for a continuous change in the rotation of the polarisation state, described by a different unit circle. (c) Simultaneous control of both parameters allows for the description of an arbitrary polarisation state on a unit sphere with circular polarisation states at the poles.

For convenience, the poles of the sphere denote the orthogonal circular polarisation states, the equator denotes the linear polarisation states and states which lie between the equator and the poles denote varying elliptical polarisation. Accordingly, each point on the surface of the sphere represents a distinct polarisation state and collectively, all points form all possible polarisation states. Due to orthogonality of the antipodal states, the circularly polarised states

can be expressed as a superposition of the orthogonal linearly polarised states and vice versa. It follows that each state on the Poincaré sphere can then be generally expressed in terms of two other orthogonal states.

1.3.2 Orbital angular momentum

The orbital angular momentum of a photon is another component of the total angular momentum, which is related to the photon's transverse spatial profile. Only in the last few decades has it been exploited experimentally following Allen's demonstration [65] that a photon with an azimuthal phase dependence $e^{i\ell\phi}$, where $\ell \in \mathbb{Z}$ is called the topological or azimuthal charge and ϕ is the angular coordinate, carries an OAM of $\ell\hbar$ per photon. The number of full azimuthal rotations per wavelength (i.e., wavefront spirals resembling a corkscrew, as seen in Fig. 1.9(a)) is related to $|\ell|$. Figure 1.9(b) shows that the handedness of the spiral phase depends on the sign of ℓ, where a positive ℓ denotes a clockwise rotation and a negative ℓ denotes anti-clockwise [66]. A main characteristic of beams that carry OAM are their doughnut like intensity distribution, with a zero intensity at that centre (see Fig. 1.9(c)). It follows that the phase is undefined along the beam propagation axis, called a phase singularity.

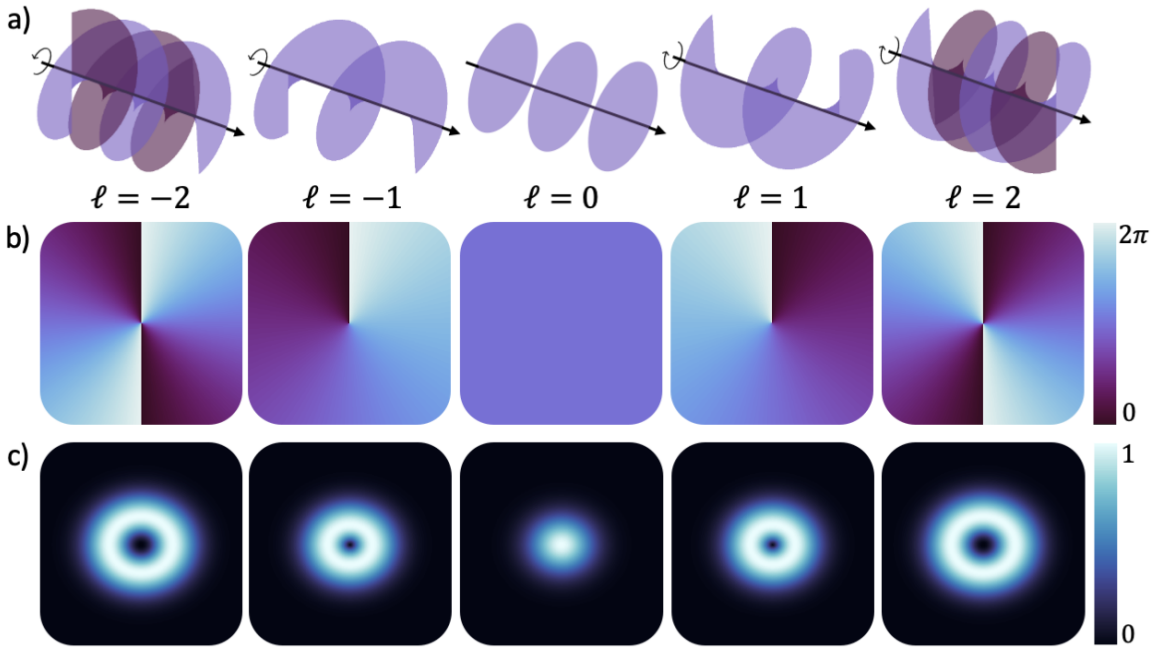

Fig. 1.9 Spatial modes carrying OAM ranging for $\ell = [-2, 2]$. (a) Illustration of the 3D helical wavefronts, where the number and handedness of twist corresponds to the azimuthal index, $|\ell|$. (b) Azimuthal phase-maps for OAM carrying modes, which specified by the azimuthal index ℓ. (c) Characteristic doughnut like intensity distribution for OAM carrying modes.

The functions that describes a set of modes that carry OAM can be obtained from the solutions to the Helmholtz equation in the paraxial approximation [67]. The paraxial approximation results by considering that the propagation of the beam remains close to beam axis (i.e., the wavefront normals propagate approximately parallel). The Helmholtz equation is given by

$$(\nabla^2 + k^2)u(x,y,z) = 0, \tag{1.8}$$

where $\nabla^2 = \frac{\partial^2}{\partial^2 x} + \frac{\partial^2}{\partial^2 y} + \frac{\partial^2}{\partial^2 z}$ is the Laplacian in Cartesian coordinates, k is the wavevector magnitude and $u(x,y,z) = a(x,y,z)e^{ikz}$ is the field function. Note that $a(x,y,z)$ is the complex amplitude that varies with position and e^{ikz} defines a plane wane travelling in the z-direction. We assume the paraxial approximation, whereby $a(x,y,z)$ can be considered a slow diverging function of z. This condition is given by,

$$|\frac{\partial^2}{\partial^2 z}a(x,y,z)| \ll |k\frac{\partial}{\partial z}a(x,y,z)|. \tag{1.9}$$

Under this condition, the paraxial Helmholtz equation is defined as follows [68],

$$\nabla_\perp^2 a(x,y,z) + 2ik\frac{\partial}{\partial z}a(x,y,z) = 0, \tag{1.10}$$

where $\nabla_\perp^2 = \frac{\partial^2}{\partial^2 x} + \frac{\partial^2}{\partial^2 y}$ is the transverse part of the Laplacian. This form of the equation when solved in cylindrical coordinates (r,ϕ,z) using separation of variables, gives solutions that are characteristic of the eigenfunction $e^{i\ell\phi}$ of OAM modes, i.e., they have the following form [65],

$$a(r,\phi,z) = a(r,z)e^{i\ell\phi}, \tag{1.11}$$

where $a(r,z)$ is the radial profile of the beam and ℓ is the azimuthal charge. These beams exhibit circular symmetry due to the coordinate space and reliance on cylindrical variables. There are various sets of modes that can be described by Eq. 1.11, including Bessel-Gaussian (BG) modes [69] and most relevant to this work Laguerre-Gaussian (LG) modes [65].

The complete basis set of orthonormal LG modes is defined by

$$LG_{\ell,p} = \sqrt{\frac{2p!}{\pi(p+|\ell|)!}}\frac{1}{w(z)}\left(\frac{r\sqrt{2}}{w(z)}\right)^{|\ell|} L_p^{|\ell|}\left(\frac{2r^2}{w^2(z)}\right) e^{\frac{-r^2}{w^2(z)}} e^{-i\ell\phi} e^{\frac{-ikr^2}{2R(z)}} e^{-i\varphi_{\ell,p}(z)}, \tag{1.12}$$

where ℓ and p index the azimuthal and radial modes respectively and $L_p^{|\ell|}$ are the generalised Laguerre polynomials. A non zero azimuthal index, $|\ell| > 0$, is responsible for modulating a Gaussian intensity distribution with a null on-axis intensity (optical vortex) and the radial index

p defines the number of radial intensity nulls resulting in $p+1$ concentric rings (see Fig. 1.10 for examples).

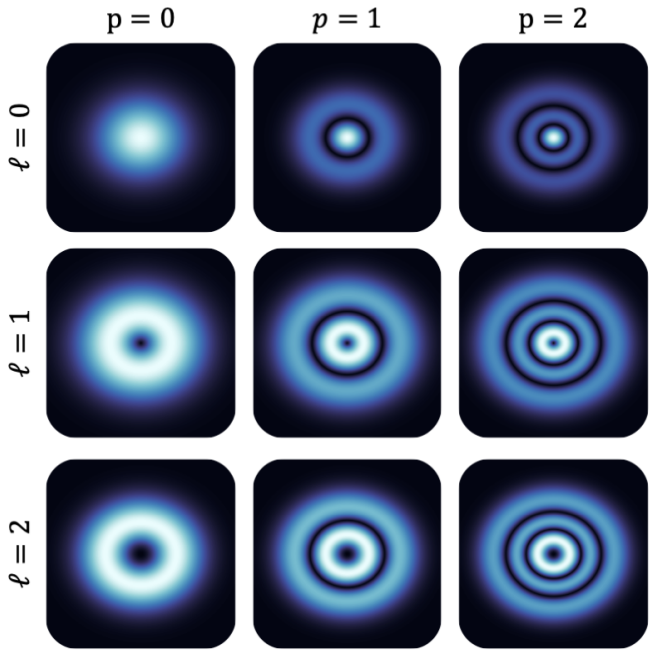

Fig. 1.10 An illustration of the transverse profile of various Laguerre-Gaussian ($LG_{\ell,p}$). The size of the vortex increases with the azimuthal, ℓ, index, and the number of concentric ring increases with the radial, p, index. Particularly, $p+1$ concentric rings are observed.

The beam width along the propagation axis is given by

$$w(z) = w_0\sqrt{1+\frac{z^2}{z_R^2}}, \tag{1.13}$$

where w_0 is the beam waist of a Gaussian beam at $z=0$ and z_R is the Rayleigh range. The Rayleigh range can be defined as the distance at which the beam width is a factor of $\sqrt{2}$ larger than the beam waist and it thus serves as a measure of divergence with respect to the propagation distance [68]. Correspondingly, the curvature associated with the wavefront is characterised by the radius of curvature parameter, R, given by

$$R = z\left(1+\frac{z_R^2}{z^2}\right). \tag{1.14}$$

Furthermore, there is a phase shift that occurs as the beam propagates, called the Gouy phase, which is defined as $\varphi_{\ell,p}(z) = M_{\ell,p}\arctan(z/z_R)$ and is dependent on the indices ℓ and p.

Here, the beam quality, $M^2_{\ell,p} = 2p + |\ell| + 1$, characterises the divergence of the beam from a Gaussian beam with $M^2_{0,0} = 1$.

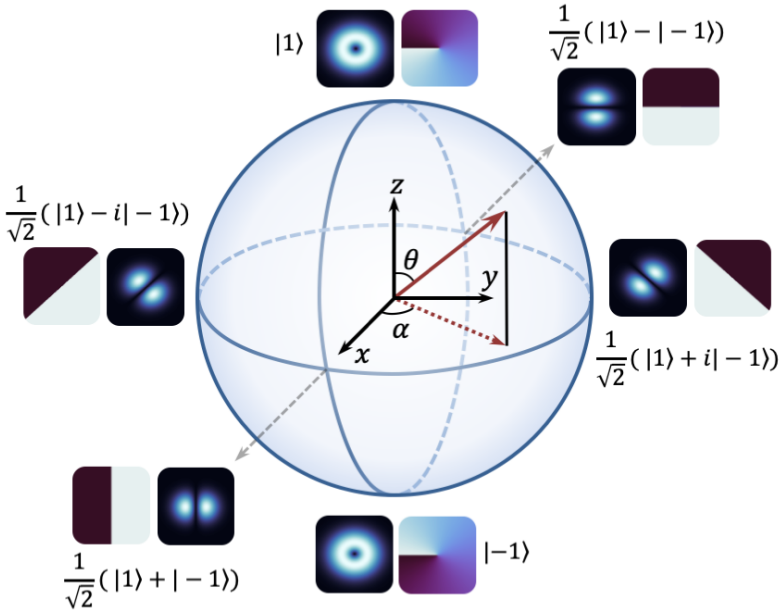

Fig. 1.11 Bloch sphere description for OAM $|\ell| = 1$, showing both the intensity distribution and phase-maps. This is equivalent to the Poincare sphere, however, the poles correspond to pure OAM eigenstates. The Bloch sphere can be used to express any OAM state with a topological charge ℓ.

These LG modes (and in effect any other set of OAM modes defined by Eq. 1.11), can be depicted on a two dimensional state-space, called the Bloch sphere [70] (see Fig. 1.11), analogous to the Poincaré sphere used for polarisation states. Similarly, using Dirac notation, the poles denote the basis states $e^{i\ell\phi} \equiv |\ell\rangle$ and $e^{-i\ell\phi} \equiv |-\ell\rangle$, respectively. The states on the equator denote Hermite-Gaussian modes. In general, any point on the sphere, $|\psi_{\ell,\theta,\phi}\rangle$, can be described in terms of the basis states, given by [70]

$$|\psi_{\ell,\theta,\alpha}\rangle = \cos\left(\frac{\theta}{2}\right)|\ell\rangle + e^{i\alpha}\sin\left(\frac{\theta}{2}\right)|-\ell\rangle\,, \tag{1.15}$$

where θ and α are the angles measured with respect to the z axis and $x-y$ plane, respectively. The parameter θ defines the weighting contribution of each state and $\alpha \in [0, 2\pi]$ is related to the phase difference between them. Note that superpositions of two oppositely charged OAM states result in fringes rotated according to the phase parameter α. From Fig. 1.11 we see a similarity to the rotation of the linearly polarised states in Fig. 1.8(c). More importantly, a

unique sphere can be defined for each ℓ, which corroborates the fact that the OAM modes form an infinite encoding space [58].

1.3.3 Spatial modes of light and quantum cryptography

High-dimensional quantum systems have the capability of transforming quantum computation and communication for more pragmatic implementations. Not only do they allow access to d orthogonal encoding states for an increased information capacity per photon, but more importantly, they are more robust and secure in the presence of noise [71]. As such, spatial modes carrying OAM have become a prominent area of research for quantum cryptography, due to their potential for infinite accessible states [72, 66], contrary to the limited two-dimensional states for polarisation.

In 2011, high-dimensional orbital angular momentum encoding was experimentally demonstrated for up to $d = 12$ dimensions [73]. This marked a crucial breakthrough in realising quantum cryptographic protocols, such as quantum teleportation [74, 75], quantum secret sharing [76] and quantum key distribution protocols implemented in $d = 4$ [77] and $d = 7$ [78] dimensions. Accordingly, OAM also gained traction as a quantum resource for many other quantum protocols including entanglement concentration [79] and quantum coin tossing [80].

However, despite its advantages, the realisation of high dimensional protocols with spatial modes, so far, has been hindered by technical difficulties arising in the full manipulation and transmission of this degree of freedom, as well as the efficiency in deterministically detecting single photons in the OAM basis. In this work we hope to circumvent these limitations and exploit the high dimensional encoding space of OAM, to realise the rapid generation and transmission of random keys for high-dimensional quantum cryptography.

1.4 Entangled light

To reiterate, a differentiating characteristic of quantum mechanics is the ability of representing quantum bit information as vectors, in contrast to classical bits which are limited to either 1 or 0. This feature has ethereal repercussions. For example, the possibility of placing the qubit in a state of superposition, in which the value of the qubit (i.e., 1 or 0) becomes probabilistic. Furthermore, spatially separated quantum states can also be intertwined together such that disturbing one qubit affects the other. This phenomenon is called quantum entanglement.

This ominous nature was introduced by Einstein, Podolsky and Rosen (EPR) in 1935, in which they opposed the widely accepted (but incomplete) quantum mechanical description of nature at the time [81]. They advocated that in a system of two spatially separated particles

with correlated positions and momenta, a measurement on an observable of one particle would instantaneously determine the entangled observable of the second particle. This was a controversial discovery as it was a clear violation of local relativistic causality. This lead to the development of local hidden variable theories, where observables were thought to be determined by some unknown variables and thus would account for the instantaneous transfer of information between the two particles.

In 1964, Bell derived inequalities that constrained the statistical correlations of a two particle system [82]. Soon after, a profusion of experiments demonstrated the violation of the inequality and in effect they verified that information is not exchanged instantaneously between the entangled particles, but rather that the knowledge of the state of an entangled particle causes the wavefunction of the other particle to collapse into a definite state [83, 84]. Here, entanglement manifests in the non-local correlations inherent to quantum systems.

However, by examining the mathematical formulation of entanglement, we uncover that the definition is in fact not confined to quantum systems but can be extended into the classical realm. This is a ripe point of contention in the scientific community [85]. Appropriately, we provide a differentiating definition for what we mean by entanglement. Moreover, we explore the formulation of non-local quantum entangled states and extend the description to classically entangled states with coupled degrees of freedom. As we will discuss, the non-seperability of these degrees of freedom has the potential to realise quantum communication in higher dimensions by overcoming the increasing difficulty in independently manipulating each dimension within a single degree of freedom.

1.4.1 Mathematical formulation of entanglement

Following the vector representation of a quantum state, it possible to described the state in terms of a linear combination of the orthogonal basis states, $|j\rangle$, spanning the Hilbert space. In other words if a system can be in one of many possible configurations, then the most general state must be a combination of all these configurations. This is called the superposition principle. Using this notation, we can mathematically describe the superposition of a state as [86]

$$|\psi\rangle = \sum_{j=0}^{\infty} a_j |j\rangle \,, \tag{1.16}$$

where $|a_j|^2$ is the probability amplitude of the system being in the state $|j\rangle$. It follows that the normalisation condition $\langle\psi|\psi\rangle = \sum_{j=0}^{\infty} |a_j|^2 = 1$ must hold. This can be interpreted as the system being in a superposition of states until a measurement is taken, at which it then

determines the unique state the system is in. This is analogous to Schrödinger's cat thought experiment, where the cat is s both alive and dead at the same time while the box is closed.

Now, consider two spatially separated non-interacting subsystems A and B, with Hilbert spaces spanned by bases $|j\rangle_A$ and $|k\rangle_B$, the most general state is given by

$$|\psi\rangle_{AB} = \sum_{j,k=0}^{\infty} a_{jk} |j\rangle_A |k\rangle_B . \tag{1.17}$$

Again, $|a_{jk}|^2$ is the probability of the system being in a product state $|j\rangle_A |k\rangle_B$, where we have omitted the tensor product operator for clarity. If the state in Eq. 1.17 can be separated and written as a product of the two systems, it is said to be separable, i.e.,

$$|\psi\rangle = \left(\sum_{j=0}^{\infty} b_j |j\rangle_A \right) \left(\sum_{k=0}^{\infty} c_k |k\rangle_B \right) = |\phi\rangle_A |\varphi\rangle_B . \tag{1.18}$$

If the system cannot be factorised as in Eq. 1.18 due to $a_{jk} \neq b_j c_k$, then the state is non-separable and entangled [87]. This provides a mathematical condition for entanglement that depends on the non-separability of the states of a compound system, given that the systems are correlated.

It is worth noting that we have not detailed the nature of either system (i.e., whether they are quantum or classical systems). Nevertheless, we rationally reached a definition for entanglement that is not confined to quantum systems, but is rather linked to the mathematical definition of separability that makes no mention of non-locality. Hence, entanglement can be said to extend into the classical realm where the internal degrees of freedom of a single classical system can be shown mathematically to be classically entangled [88, 89]. This term has sparked some controversy in the scientific community, with many suggesting that the word entanglement to be associated with quantum systems only [85]. It is then necessary make a clear distinction between classical and quantum entanglement. More specifically, in this thesis, quantum entanglement refers to non-local correlations inherent to quantum particles and classical entanglement refers to local correlations within a classical system.

Entanglement has become a valuable resource for quantum computing and communication, and as a result requires verification. While there are various ways to characterise the degree of entanglement of a system, a standard and widely used approach is through a statistical operator called the density matrix, ρ. The statistical state of a system can be described by using density matrices. For pure states, the density matrix is described as

$$\rho = |\psi\rangle \langle\psi| , \tag{1.19}$$

whereas for mixed states, with a probability p_n of the system being in the state $|\psi_n\rangle$, is given more generally by,

$$\rho = \sum_n p_n |\psi_n\rangle \langle\psi_n| . \tag{1.20}$$

Here, the density matrix has a trace equal to unity and is positively definite with positive eigenvalues. The matrix allows for the calculation of various measures that describe the nature the quantum states [87], including the degree of separability and an indication of their purity. Later, we will explore density matrices as a method of reconstructing the quantum state of entangled photons.

1.4.2 Maximally entangled Bell states

Two qubit quantum states which exhibit maximal correlations and maximally violate Bell's inequality, known as Bell states, are the simplest examples of quantum entanglement [90]. We can construct these Bell states from the qubit logic basis $\{|0\rangle, |1\rangle\}$ as follows

$$|\phi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |0\rangle_B \pm |1\rangle_A |1\rangle_B) \tag{1.21}$$

$$|\psi^{\pm}\rangle = \frac{1}{\sqrt{2}}(|0\rangle_A |1\rangle_B \pm |1\rangle_A |0\rangle_B). \tag{1.22}$$

As before, the two spatially separated systems are denoted by A and B. It is clear that both Eq. 1.21 and Eq. 1.22 are non-separable. This means that they cannot be decomposed into single particle states and hence we can not determine the state of each qubit separately. The implication is that a measurement of the qubit in system A determines the outcome of the qubit in system B. Consider the state $|\phi^+\rangle$ such that if system A is projected onto the state $|0\rangle$, then the entangled system B will immediately collapse to state $|0\rangle$. Furthermore, all four maximally entangled two qubit states form a 4-dimensional biphoton Hilbert space, called as the Bell basis, which has lead to various proposals and implementations of quantum protocols using Bell states.

Additionally, it has been shown that Bell states can be experimentally prepared using a photon's single degree of freedom such that each of its eigenstates is associated with a state from the logic basis. This has been demonstrated using polarisation [83, 84], time [91, 92] and OAM [93] degrees of freedom of a single photon. It then follows that we can define a classically entangled state of a single photon using different degrees of freedom, where the correlation is in the respective degrees of freedom. Here, a measurement of in one degree of freedom determines the outcome of the measurement in the other degree of freedom. We wish

to explore the hybrid coupling between spin (SAM) and orbital (OAM) angular momentum of a single photon as a quantum cryptographic solution.

1.4.3 Spin-orbit coupled states

The coupling of polarisation to the spatial profile of a beam forms a state space that is a tensor product of the polarisation ($|R\rangle$ and $|L\rangle$) and the OAM ($|\ell\rangle$ and $|-\ell\rangle$) spaces. The resulting Hilbert space is spanned by the scalar basis modes, $\{|R\rangle|\ell\rangle, |L\rangle|-\ell\rangle\}$ and $\{|R\rangle|-\ell\rangle, |L\rangle|\ell\rangle\}$. These scalar modes have uniform circular polarisation distributions, making them separable. This follows from Fig. 1.12(a) depicting a scalar mode, where the arrows represent the uniform direction of the electric field oscillations across the beam profile (i.e., polarisation). By placing a polariser in the beams path, projecting it into the horizontal and vertical bases, the spatial distribution (i.e., pattern) remains unchanged, albeit a variation in intensity according to the angle of the polariser. This shows the separability of the polarisation and spatial profile of the scalar beam as one does not affect the other.

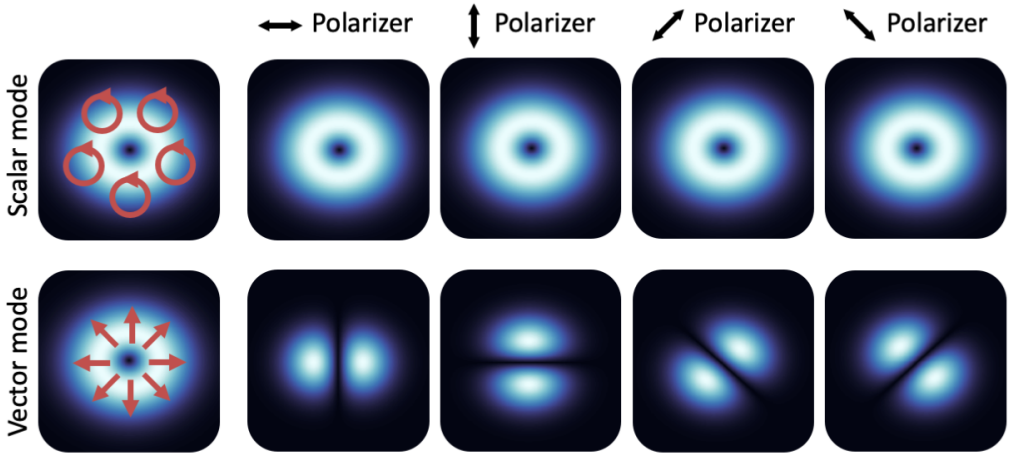

Fig. 1.12 Intensity and polarisation mapping of a scalar (top row) and a vector beam (bottom row), with uniform and non-uniform polarisation respectively. The polarisers project the beams into the respective polarisation bases. The corresponding intensity distribution patterns reiberlect the non-separability of the polarisation and spatial degrees of freedom for vector beams.

A superposition of one of the scalar basis pairs results in non-separable states, called vector modes [94]. The vector nature of these modes arises from the spatially changing (i.e., non-uniform) polarisation distribution. Consider an example of a vector mode depicted in Fig. 1.12(b). Here, the arrows indicate a clear in-homogeneous distribution of polarisation. If passed through a polariser, the spatial distribution changes as a particular polarisation state is

filtering out. In other words, a measurement on the polarisation degree of freedom, affects the outcome of the measurement on the spatial degree of freedom.

Mathematically, spin-orbit coupled modes are described by:

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|\ell\rangle\,|R\rangle + e^{i\alpha}\sin\left(\frac{\theta}{2}\right)|-\ell\rangle\,|L\rangle\,, \tag{1.23}$$

where θ indicates the relative weighting of each mode, while α is related to the relative phase between them. Here, it is clear that the state cannot be factored and thus is non-separable in both the spatial and polarisation components. We emphasise that entanglement is mathematically defined by the existence of strong correlations between states and resolve that vector beams also exhibit some form of entanglement, albeit local. Hence, we can say that vector beams are classically entangled in spin and orbital momentum.

Note again that the polarisation space has only two orthogonal basis states and as a result, a similar representation to the Poincaré sphere may be used to illustrate all the possible vector modes for a particular combination of OAM to polarisation coupling. The extension to the Poincaré sphere representation was termed a Higher-Order Poincaré sphere (HOPS) [95]. Figure 1.13(a) illustrates an example of a HOPS for a general $|\ell|$ spin-orbit coupling. Since the OAM basis states are of the same magnitude $|\ell|$, then the total spatial distribution remains unchanged for all the modes on the sphere (i.e., constant doughnut shape).

The poles contain modes described by a single basis pair (i.e., uniform circular polarisation distributions) and thus are the contributing scalar modes that form the maximally entangled vector modes at the equator. Every other state on the sphere is also non-separable and as a result are also vector beams. Modes defined on the equator contain equal weightings of opposite circular polarisation such that the effective polarisation is linear. From Fig. 1.13(b) we see that the parameter α describes the angle of the orientation of polarisation with respect to the normal of a concentric circle. Also, the parameter θ, describes the respective weighting of circular polarisation, resulting in elliptically polarised modes.

The non-separability of spin-orbit coupled modes has been exploited for demonstrating Bell-like inequalities with classical light [96] and at the single photon level [97, 98]. Additionally, their efficacy has been experimentally demonstrated for quantum communication techniques, including QKD [99], rotational invariance for alignment free quantum channels [41] and more recently multi-dimensional communication through fibre [100]. Herein, we employ classically entangled spin-orbit coupling to take advantage of their increased encoding capacity and accessible manipulation of each degree of freedom, with the hope of realising quantum cryptographic protocols in high-dimensions.

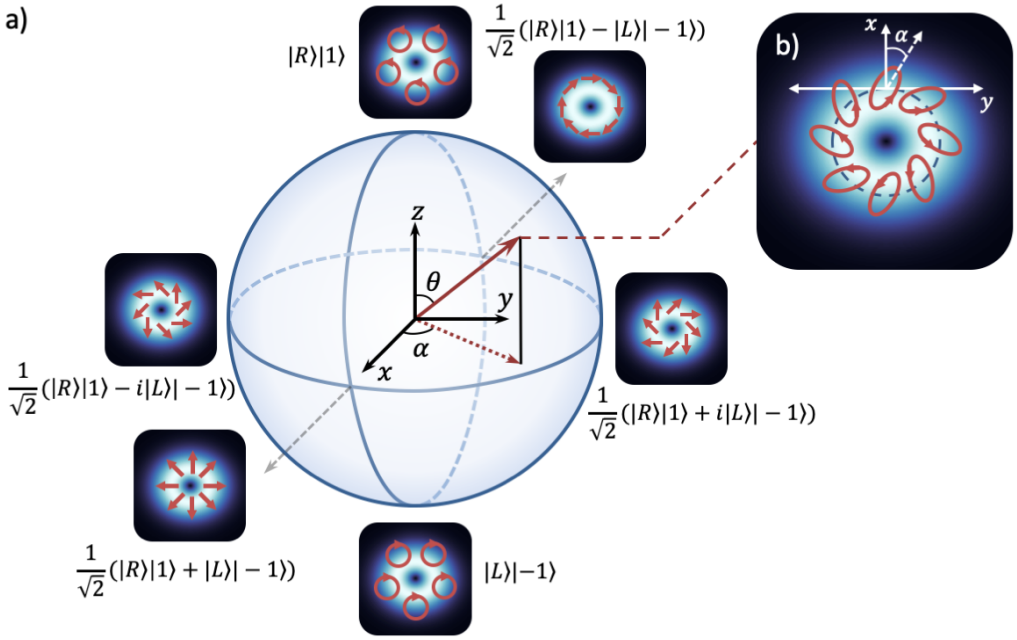

Fig. 1.13 Illustration of spin-orbit coupled states on the Higher-order Poincare sphere (HOPS). (a) The poles denote non-entangled states, $\{|R\rangle|1\rangle, |L\rangle|-1\rangle\}$, forming the subspace spanning all other states described by the surface of the sphere. The equator denotes maximally entangled states. (b) Arbitrary spin-orbit coupled state showing the polarisation orientation of the state, which is dependent on the parameter α.

1.5 Outline

The realisation of quantum cryptography relies on the generation, manipulation and detection of the degree of freedom in which the information is encoded. The work presented here, centres on experimentally achieving these quantum protocols in high-dimensions, pushing the bound on the amount of information encoded and extracted from the photons.

The dissertation is structured in the following manner: Chapter 2 explores the methods used to generate and detect spatial modes that carry orbital angular momentum (OAM). In particular, we investigate various optical elements that offer control over the geometric and dynamic phase of light. We demonstrate two techniques to generate OAM carrying modes, including spatial light modulators (SLMs) for spatial mode generation and q-plates with spatially varying optical axes for spin-orbit coupled mode generation. We also characterise waveplates and dove prisms to offer complete control in manipulating the polarisation and OAM degrees of freedom. Moreover, we demonstrate deterministic and projective detection methods for OAM and vector modes.

In Chapter 3, we implement spontaneous parametric down-conversion (SPDC) as a method of generating two photon entanglement. Here, we implement the projective measurement technique, as investigated in Chapter 2, to detect the entangled photons in the OAM degree of freedom. We describe the setup and alignment procedure and perform various quantum measurements to verify and characterise the entanglement of our system. A spiral bandwidth measurement is used to show that our system conserves orbital angular momentum. We also test our system against local hidden variable theories by demonstrating a Bell inequality violation with OAM. Lastly, we investigate the high-dimensional entanglement of our system and reconstruct the generated state by performing a full quantum state tomography. As a whole, Chapters 2 and 3, present a complete toolbox for the realisation of high-dimensional quantum cryptographic protocols.

Chapters 4 and 5 present our new experimental realisations of two quantum cryptographic protocols [101, 102], focusing on the generation and distribution of the encryption keys necessary for the secure sharing of data. In Chapter 4, we generate random numbers certified by the intrinsic randomness of the quantum SPDC system. Here, the randomness is inherent in the outcomes of the projective measurements we perform on the path superpositions that we engineer using digital holography. The digital control allows us to compensate for any bias present within our transmission and detection system. We further extend our approach to realise a novel quantum random number generator based on the generated states entangled in OAM. We show that by performing projective measurements onto various OAM combinations, we can generate random numbers with discreet probability distributions.

In Chapter 5, we demonstrate the potential of using the high-dimensional encoding space of spin-orbit coupled states for quantum secret sharing. We show the scalability of our approach by implementing the protocol in two-dimensions with ten participants, and then in three-dimensions with three participants. Our scheme exploits the optics characterised herein, to demonstrate the highest realisation of dimensions and participants thus far, allowing us to exceed the 1 bit per photon limit of two-dimensional protocols.

Lastly, in Chapter 6, we conclude the work presented within this dissertation and summarise the contributions we have made to the field of quantum cryptography. Our work provides a practical approach to realising these protocols in high-dimensions, for a faster and more robust solution.

Chapter 2

Experimental techniques

The complete realisation of quantum communication with photons relies on the full generation, manipulation and detection of the degree of freedom in which the information is encoded. In particular, there must exist a mechanism that offers complete control to move between the required quantum states. Implementing these key principles in d-dimensions of a single degree of freedom, for example OAM, becomes increasingly complex. An interesting solution involves coupling different degrees of freedom to reach higher dimensions. Specifically, the coupled degrees of freedom must exhibit non-separable correlations upon manipulation. This condition for entanglement is a quintessential property that guarantees the security of quantum communication. In fact, the benefit of coupling multiple degrees of freedom has been shown in quantum key distribution [103], superdense coding [104], teleportation [105], game strategies [106] and quantum walks [107].

Here, we will focus on techniques that exploit the dynamic and geometric phase of light for the generation, manipulation and detection of spin-orbit coupled modes of light. We characterise the operation of various optical elements, including waveplates for polarisation control and dove prisms for OAM rotation control. We then extend the toolbox to include holographic generation of spatial modes and geometric phase generation of spin-orbit coupled modes. We also explore deterministic and projective detection methods for OAM and vector modes. This toolbox covers the essential techniques for the realisation of a high-dimensional quantum communication protocol, encoded in the polarisation and spatial degrees of freedom.

2.1 Dynamic phase control

Optical elements can be designed in such a way that light transversing through the medium is retarded and accumulates a phase. Changes to the thickness or the refractive index of the medium will affect the path or propagation time of the light through the medium. More intuitively, since the speed at which the electric field travels is related to the refractive index by $v = c/n$, it follows that a change in refractive index alters the speed of the wave, causing the light to effectually gain a phase. The phase that accumulates due to these dynamic processes is called a dynamic phase and is described by [108],

$$\phi = \frac{2\pi nL}{\lambda}. \tag{2.1}$$

where n is the refractive index of the medium, L is its thickness and λ is the wavelength of the light.

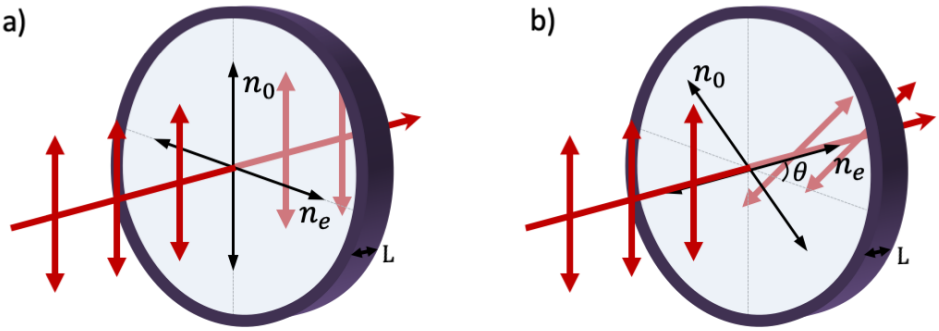

Fig. 2.1 Illustration of a uniform birefringence waveplate of thickness L. The fast axis is aligned with (a) the x-axis and (b) rotated by an angle θ. A rotation of the polarisation dependent refractive indices (n_o and n_e) impart a dynamic phase on the incident electric field. The phase shift can be controlled by varying the thickness or refraction indices.

Certain materials are birefringent in that they have different refractive indices for orthogonal components of an electric field (see Fig. 2.1(a)). These materials are extremely useful in designing optical elements that allow for the full control of the SAM of light. Moreover, similar optical devices that rely on the varied thickness or non-uniform refractive index to impart a dynamic phase, such as spiral phase plates and spatial light modulators, are also important in the generation of OAM beams. As we will see, careful selection of these two parameters allows for control over the dynamic phase imparted to a light beam.

2.1.1 Controlling spin angular momentum with waveplates

As previously discussed, the spin angular momentum of a photon is related to its polarisation state determined by the orientation of electric field oscillations. It follows that, by introducing a phase shift between the orthogonal components of the photon's electric fields, it is possible to manipulate its polarisation state [109]. This phase manipulation can be achieved by varying the thickness and refractive index of the medium that the orthogonal orientations of the electric field experience. An efficient way of doing this is to use waveplates.

Waveplates are commonly made from birefringent crystals, such as quartz or mica. The orthogonal components of an electric field transversing these materials will incur different phase shifts according to the refractive index of the axis traversed. According to Eq. 2.1, the relative phase difference φ imparted on the electric field components is given by,

$$\varphi = \phi_e - \phi_o = \frac{2\pi(n_e - n_o)L}{\lambda}, \tag{2.2}$$

where n_e and n_o are the extraordinary and ordinary refractive indices along the slow and fast axis of the material, respectively. Figure 2.1 illustrates the principle of operation. The vertical electric field component, E_y, experiences the ordinary refractive index along the slow axis of the material while the orthogonal horizontal electric field component, E_x, experiences the extraordinary refractive index along the fast axis of the material, imparting a relative phase difference φ between components.

Next, we introduce the Jones matrix formalism to describe the operation of a waveplate. In this formalism, the operation of an optical element can be described by a 2x2 matrix, whereby its product with the incident input state E_{in} results in the correct output state E_{out}, given by [109],

$$\begin{pmatrix} E_{out,x} \\ E_{out,y} \end{pmatrix} = \begin{pmatrix} U_{11} & U_{12} \\ U_{21} & U_{22} \end{pmatrix} \begin{pmatrix} E_{in,x} \\ E_{in,y} \end{pmatrix}, \tag{2.3}$$

where the U is the optical element matrix acting on the input state.

We will begin by considering the simple case in which the orthogonal electric field components, E_x and E_y, are aligned with the waveplate's fast and slow axes. Here, the horizontal component, E_x experiences a phase retardance $e^{-i\phi_e}$ by the fast axis and the vertical component experiences a phase retardance $e^{-i\phi_o}$ by the slow axis. The Jones matrix formalism describes

the operation of the waveplate by,

$$U_{WP}(0) = \begin{pmatrix} e^{-i\phi_e} & 0 \\ 0 & e^{-i\phi_o} \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\varphi} \end{pmatrix}, \tag{2.4}$$

where we have extracted the global phase $e^{-i\phi_e}$. This is possible as we are only interested in the relative phase between the electric field components.

We can generalise this description to include the rotation of the waveplate by an angle θ with respect to the fast axis [68]. The rotation of the waveplate's optical axis may be described by

$$U_{WP}(\theta) = R(-\theta)U_{WP}(0)R(\theta) \tag{2.5}$$

$$= \begin{pmatrix} \cos^2\theta + e^{-i\varphi}\sin^2\theta & (1-e^{-i\varphi})\sin\theta\cos\theta \\ (1-e^{-i\varphi})\sin\theta\cos\theta & \sin^2\theta + e^{-i\varphi}\cos^2\theta \end{pmatrix}, \tag{2.6}$$

where $R(\theta)$ is the rotation matrix given by

$$R(\theta) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}. \tag{2.7}$$

The behaviour of a waveplate is characterised by the relative phase imparted between the electric field components. It follows that a suitable relation between the thickness and birefringence of the material results in a controlled phase shift between the orthogonal electric field components, thereby altering its polarisation [108]. The half-waveplate (HWP) and the quarter-waveplate (QWP) are essential to achieve full polarisation control. Following Eq. 2.6, the Jones matrix description for a HWP is [110],

$$U_{HWP}(\theta) = \begin{pmatrix} \cos(2\theta) & \sin(2\theta) \\ \sin(2\theta) & -\cos(2\theta) \end{pmatrix}, \tag{2.8}$$

where the phase is retarded for a half wavelength, $\varphi = \pi$, converting rectilinear polarisation to superpositions of linear polarisation. Similarly, the Jones matrix description for a QWP

is [110],

$$U_{QWP}(\theta) = \begin{pmatrix} \cos^2\theta + i\sin^2\theta & (1-i)\sin\theta\cos\theta \\ (1-i)\sin\theta\cos\theta & \sin^2\theta + i\cos^2\theta \end{pmatrix}, \tag{2.9}$$

where the phase is retarded for a quarter wavelength, $\varphi = \pi/2$, converting linear polarisation to circular polarisation. Using a combination of waveplates, one can generate any state on the Poincare sphere from a horizontally polarised state (see Table 2.1 for appropriate examples).

Output state	$\|R\rangle$	$\|L\rangle$	$\|H\rangle$	$\|V\rangle$	$\|D\rangle$	$\|A\rangle$
HWP(θ_1)	0	0	0	$\pi/4$	$\pi/8$	$-\pi/8$
QWP(θ_2)	$\pi/4$	$-\pi/4$	0	0	0	0

Table 2.1 Polarisation control of an input horizontally polarised state using waveplates. The waveplate angles are specified relative to the fast axis.

The HWP and QWP were experimentally exercised with the setup and the results are shown in Fig. 2.2. Here, horizontally polarised light was directed through a HWP to a polarising beam splitter (PBS). This projects the beam into the horizontal or vertical polarisation basis. The output ports of the PBS were observed using a CCD camera (see Fig. 2.2(b)). The PBS was then replaced by a polarisation grating (PG) which spatially separated circular polarisation components, allowing the characterisation of a QWP in Fig. 2.2(c). The effect of a HWP on circular polarised light was also characterised, in Fig. 2.2(d), using a combination of a QWP and HWP. The results showed good correlation with the theory derived using the Jones matrix representation.

2.1.2 Generating and detecting OAM modes

Modes of light carrying OAM can also be generated using optical elements which are designed with careful control of the thickness or refractive index of the medium. This can be done using spiral phase plates, which rely on the varied thickness and uniform refractive index to impart OAM. Similarly, the same phase change can be imparted by varying the refractive index and fixing the thickness of the medium. Computer controlled liquid crystal displays called spatial light modulators (SLMs) allow each pixel's refractive index to be tailored by an appropriately

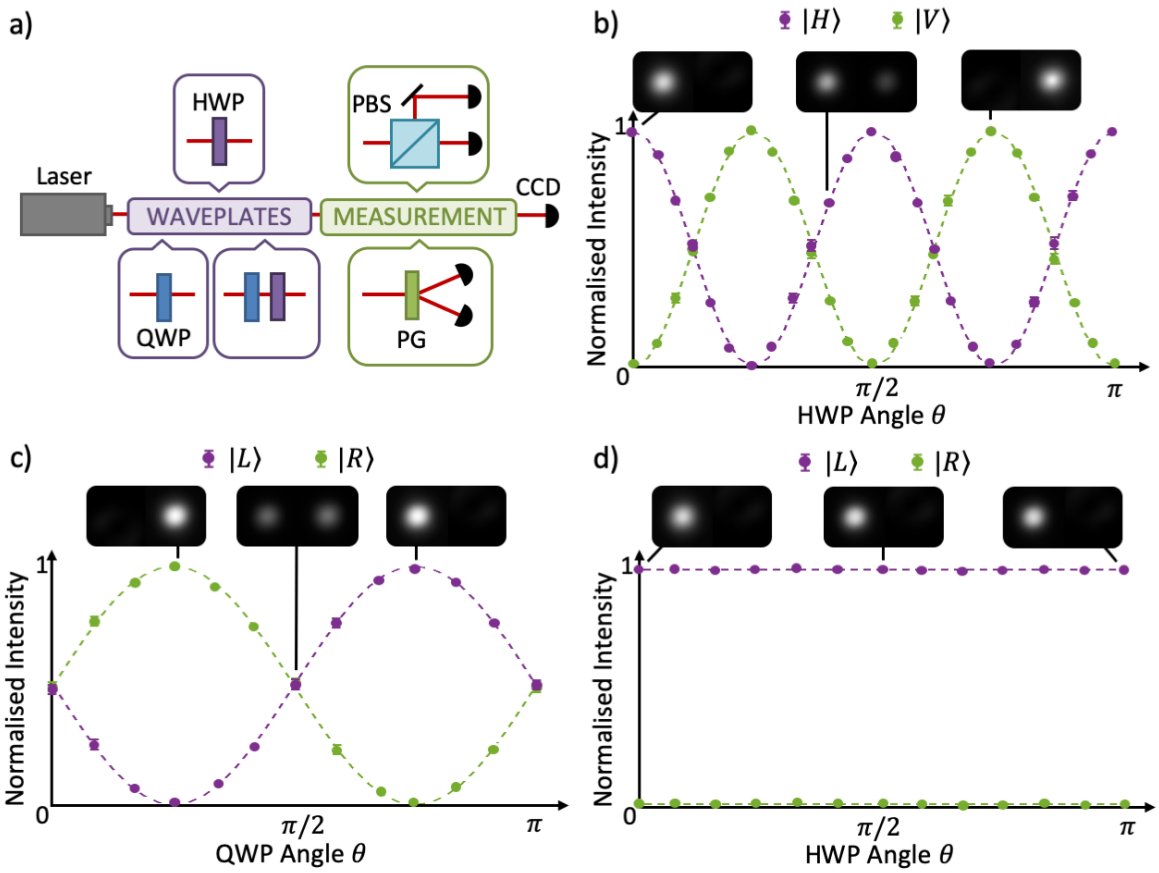

Fig. 2.2 Experimental waveplate characterisation. (a) Setup used to test waveplate operations in the linear (top row) and circular (bottom row) polarisation bases. Experimental results for horizontally polarised light incident on (b) a HWP and (c) a QWP. (d) Experimental results for circularly polarised light incident on a HWP. Insets above the graphs show the intensity profile detected by the CCD for various waveplate angles.

applied voltage. SLMs offer the advantage of digital control over the dynamic phase to add OAM to a light beam. As we will discuss, this also works in reverse, in that it can also remove OAM, perfect for OAM detection.

Spiral phase plates

A spiral phase plate (SPP) is an optical element, often made of fused silica, with a gradually increasing helical path length and uniform refractive index (see Fig. 2.3). The working principle of a SPP depends on the gradual thickness variation of the plate, which increases proportionally to the azimuthal angle ϕ around the center of the plate. This imparts a helical transverse profile that carries OAM [111].

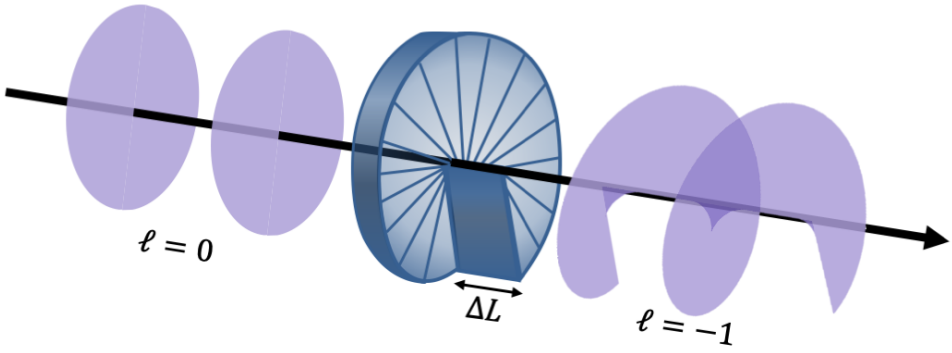

Fig. 2.3 Generation of OAM modes using a spiral phase plate. The gradual spiral thickness of the plate imparts a helical phase with OAM ℓ proportional to the refractive index and step height ΔL.

The step height, ΔL, of a SPP with a refractive index, n, is determined and constructed for a particular wavelength λ and desired OAM charge ℓ. The relation is given by [111],

$$\ell = \frac{n\Delta L}{\lambda}. \tag{2.10}$$

where the step height is given in units of 2π. Since the step height is sufficiently small, the paraxial regime still holds such that a SPP can be considered to only operate on the phase of the light transversing through it. This imparts an azimuthally dependent dynamic phase given by $e^{-i\ell\phi}$. This phase is characterised by the topological charge ℓ and defines a phase singularity at the center, demonstrating the formation of the helical nature of OAM beams (see Fig. 2.3).

A clear disadvantage, however, is that SPP are wavelength and charge specific. Moreover, increasing the number of spirals (i.e., topological charge), decreases the diffraction efficiency of the plates as the resolution of the spiral surface decreases.

Spatial light modulators

An azimuthally dependent dynamic phase can also be achieved using digital holograms encoded onto a SLM, where by the refractive index of the medium is varied in contrast to its thickness. SLMs comprise of liquid crystals interfaced between two arrays of electrodes (see Fig. 2.4). Liquid crystals have properties between conventional liquids and solid crystals, such that they can be oriented in a crystal-like manner. The crystals orientations are structured to be aligned parallel to the electrodes and can be further orientated in the direction of an applied voltage between the electrodes [112]. Because of the birefringence of the crystals, the tilt control of the crystals enables the tailoring of the refractive index of each crystal [68]. Following a

similar argument to the working of a waveplate, this process can be used for dynamic phase control. Further, clever manipulation of phase-only SLMs also allows for complex amplitude modulation [113].

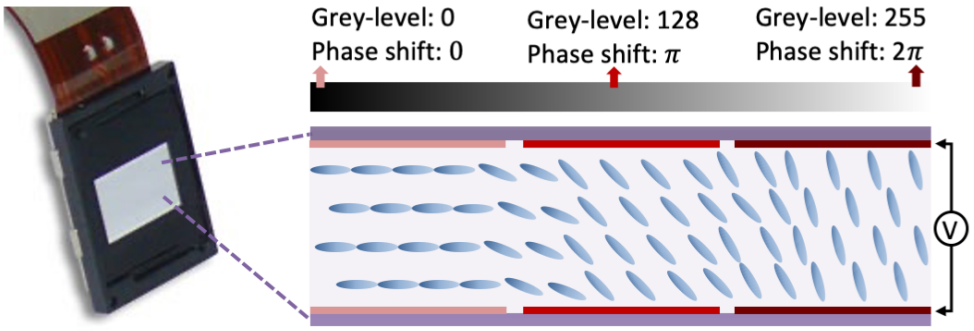

Fig. 2.4 An illustration of a liquid crystal SLM. A zoomed in schematic shows how the grey-level encoded in a hologram translates into an electric field applied across the pixel arrays. The electric field orients the liquid crystals, changing the refractive index and thus the phase of an incident wave.

The display of the Holoeye Pluto SLM used has a 1920×1080 pixel resolution. Each pixel is 8μm with a 50 Hz refresh rate and an 8-bit encoding capacity, corresponding to a 0 to 2π phase shift. As such, grey-scale computer holograms ranging from 0 (black) to 255 (white) can be displayed on the SLM, with the grey-level corresponding to the voltage applied in order to achieve the desired phase shift. A summary of the several methods for encoding these holograms can be found in Ref. [114]. This electrically controlled birefringence allows for rapid control and generation of OAM modes. Additionally, the holograms can be digitally re-positioned offering great control over the quality of the generated modes.

Modes of light that carry OAM can then be generated using SLMs by encoding a grey-scale phase-map associated with the desired mode. The transmission function used to describe the required phase-mapping for OAM modes is given by,

$$T(\phi) = e^{i\ell\phi}, \tag{2.11}$$

where ℓ is the azimuthal index describing the topological charge and ϕ is the azimuthal angle. A Gaussian beam ($\ell = 0$) interacting with a hologram encoded with this transmission function would generate a helical beam carrying OAM proportional to ℓ, as seen in Fig. 2.4. The topological charge ℓ can be easily varied making SLMs extremely versatile in dynamic phase OAM generation.

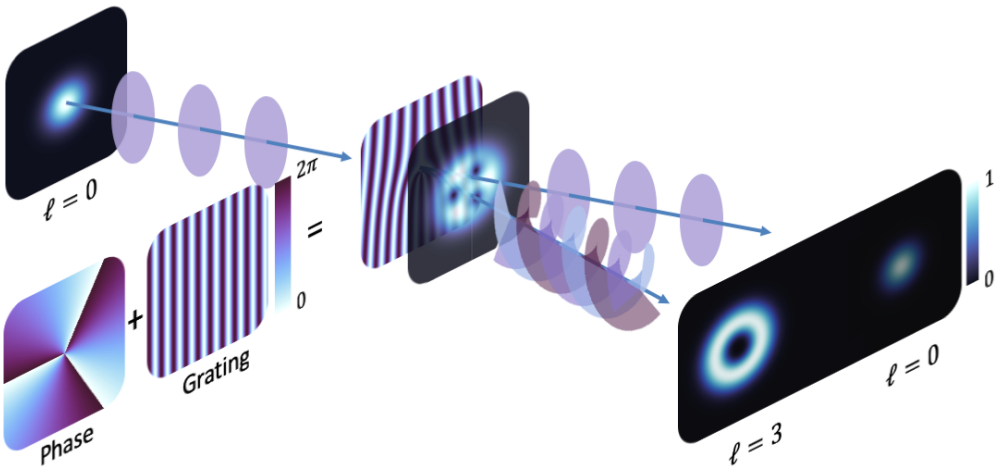

Fig. 2.5 Generation of OAM modes using a SLM. An azimuthal phase hologram encoded on the SLM will impart a helical wavefront to an incident beam. A diffraction efficiency of 80% means that the unmodulated light will interfere with the generated mode along the propagation axis. The addition of a grating to the spiral phase hologram (forming a forked hologram) allows for the spatial separation of the desired mode from the unmodulated incident beam.

However, SLMs are diffractive optical elements and as a result not all incident light is modulated by the the hologram. This is due to the structure of the liquid crystal display and the diffraction efficiency of the device (which in our case is only 80% efficient). Consequently, the unmodulated (zeroth order) beam will also propagate along the same axis as the diffracted first order, interfering and distorting the quality of the desired mode. This is easily overcome by superimposing a periodic grating on the phase-map hologram. The grating separates the zeroth and first diffraction order, in which the desired first order mode can then be isolated (see Fig. 2.4). The transmission function with the grating becomes

$$T(\phi) = e^{i\ell\phi + 2\pi\left(x/t_x + y/t_y\right)}, \tag{2.12}$$

where x and y are Cartesian positions and t_i is the respective grating period. These holograms are called forked diffraction gratings, due to their characteristic fork prongs which are proportional to the azimuthal index. The grating can be used to control the axis of propagation of the desired mode. Moreover, multiple modes can also be multiplexed on the same hologram, each with a unique grating, such that each mode is sent to a different position in space [115]. Using this technique, a Gaussian beam incident on a multiplexed hologram, with the desired transmission function for $\ell = 1, 2, 3$ each with unique grating, allows for the generation of all three modes in one step.

Due to the reciprocity of light, a SLM can also be used to remove OAM from an incident beam. For example, a beam with a topological charge ℓ incident on a forked hologram, encoded with the conjugate transmission function $T^*(\phi) = e^{-i\ell\phi}$, will be modulated back into a Gaussian mode ($\ell = 0$) resulting in an on-axis intensity. This is a well established technique for detecting OAM modes of a particular charge [116]. When combining this method with a single-mode fibre (SMF), for which a Gaussian mode offers the maximum coupling efficiency, we realise a match-filtering detection system. Various match filters can also be multiplexed with unique gratings, such that the filters yielding an on-axis intensity correspond to OAM components of the unknown spatial mode. This reverse process enables us to perform projective measurements on an unknown spatial mode, effectively characterising the state via modal decomposition [117].

Next, we explore mathematically why this is possible. We begin by exploiting the orthonormality of the basis modes to determine the correlation coefficients c of each contributing basis mode. To calculate this modal overlap, we simply take the inner product between the input field $\psi(\mathbf{r})$ and the basis modes $\phi(\mathbf{r})$ [118],

$$c = \langle \phi | \psi \rangle = \iint \phi^*(\mathbf{r}) \psi(\mathbf{r}) \, d^2r, \tag{2.13}$$

where $r = (x, y)$ is the spatial coordinate in the transverse plane and $*$ indicates the complex conjugate. Here, the complex conjugate of a basis mode (i.e., $\phi^*(\mathbf{r})$) is what we refer to as the match filter [116]. Furthermore, the overlap probability describing the correlation between the two modes is given by $|c|^2$, where orthogonal modes correspond to a zero correlation $|c|^2 = 0$. The integral can be performed optically by a lens, equivalent to performing the Fourier transform of the product field $\phi^*(\mathbf{r})\psi(\mathbf{r})$. This yields the state,

$$A(k_x, k_y) = \iint \phi^*(x, y) \psi(x, y) e^{-i(k_x x + k_y y)} \, dxdy, \tag{2.14}$$

where k_x, k_y are the transverse wave vectors in Cartesian coordinates. The field evaluated at the center, $(k_x, k_y) = (0, 0)$, results in

$$A(0,0) = \iint \phi^*(\mathbf{r}) \psi(\mathbf{r}) \, d^2r = c, \tag{2.15}$$

whereby the on-axis field intensity at the focal plane describes the modal overlap weighting $I(0,0) = |A(0,0)|^2 = |c|^2$.

Using the techniques discussed, we experimentally demonstrate the generation and detection of OAM modes with SLMs. The experimental setup is shown in Fig. 2.6(a). The modes were both generated and decomposed using amplitude and phase modulation on SLMs. A collimated horizontally polarised HeNe laser beam was directed to a SLM encoded with the desired OAM

transmission function, resulting in the first diffraction order possessing the required structure. The generated mode was imaged onto the second SLM, encoded with a match filter. The optical inner product between the generated mode and a match filter was performed by the Fourier transformation of a lens. The on-axis intensity at the Fourier plane was recorded with a CCD camera. Here, maximum on-axis intensity indicates that the prepared and measured modes correlate and an on-axis null indicates no correlation (see Fig. 2.6(b)). The results for the generation and detection of OAM modes raging between $\ell = [-4, 4]$ are depicted as a density matrix, shown in Fig. 2.6(c). Here, the diagonal elements in the density matrix indicates that the detection of the OAM modes correspond with the modes generated. The off diagonal elements indicate the overlap between orthogonal modes. System aberrations resulting in negligible cross-talk may be seen in the off diagonal elements closest to the diagonal.

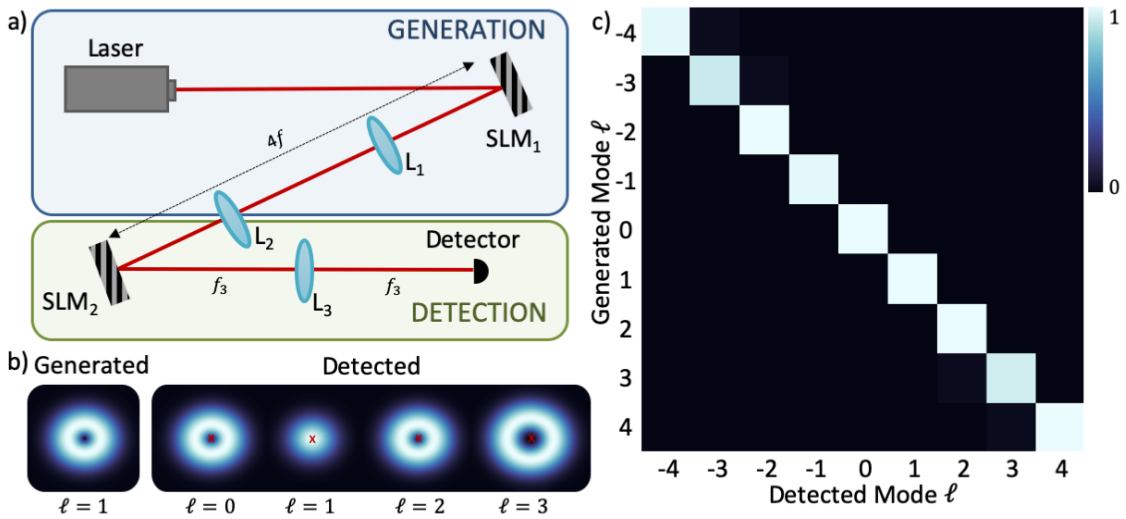

Fig. 2.6 Modal decomposition using SLMs. (a) Simplified experimental setup used to generate and detect OAM modes. (b) Example of the detected intensity profiles for the generated $\ell = 1$ beam incident on various match filters. Match filters yielding an on-axis intensity correspond to OAM components of the unknown spatial mode. (c) Experimental results for the generation and detection of OAM modes raging between $\ell = [-4, 4]$

Overall, the dynamic phase control offered by SLMs has proven to be an effective tool for both the generating and decomposition OAM modes. The ability of generating and uniquely detecting specific modes is essential in quantum communication, where by each mode can then be encoded with information.

2.2 Geometric phase control

In addition to the dynamic phase, a geometric phase can be introduced to a system. This phase results from an adiabatic altering of parameters in a closed loop path [119]. Pancharatnam observed this extra phase acquired by light waves from the cyclic evolution of light polarisation, which he deemed was due to the geometrical properties of the system [120]. Later, Berry generalised this description for a non-relativistic quantum system adiabatically traversing a closed loop path in parameter space [121]. Specifically, when the Hamiltonian of the system undergoes an adiabatic evolution along a closed curve Ω in the parameter space (i.e., a state undergoes a set of operations which bring the state's parameters back to the initial state), then a state that remains an eigenstate of the system develops a geometrical phase which depends only on Ω.

Of interest to this dissertation, the geometric phase incurred from polarisation considerations is often referred to as the Pancharatnam-Berry phase (a popular review can be found in Ref. [122]). In particular, it describes the phase change due to the cyclic evolution of the polarisation state of a light beam and is dependent only on the shape of the corresponding closed loop path on the Poincare sphere, but applies only if the polarisation state is parallel transported along its trajectory.

We consider the manifestation of this Pancharatnam-Berry phase from the intensity-preserving linear optical transformations of a set of waveplates. However, since the birefringence of the optical medium introduces a dynamic phase, the action of the waveplates cannot be purely described as parallel transport, and hence is described by non-geodesic paths [123]. In such cases, the total phase for a closed path is the sum of the geometric phase and the dynamic phase. However, it has been shown that paths produced by a set of waveplates can be decomposed into geodesics if the initial and final states are connected via eigenstates of the waveplates [124]. With such a construction any closed path produced by a set of waveplates can be expressed as consisting of purely geodesics, with the total phase incurred being purely geometric.

This is illustrated in Fig. 2.7, showing the mapping of a set of waveplate operators transporting the state of the system along a geodesic on the Poincare sphere, as long as the states are connected by an eigenstate of the waveplate (see Ref. [125]). Here, we consider the mapping of horizontal polarisation (A) to left circular polarisation (B) by means of a QWP at $-\pi/4$, and then to right circular polarisation (C) by a HWP at an arbitrary angle α. Another QWP at $-\pi/4$ maps the polarisation back to the initial horizontal polarisation state (A'), forming a closed loop path, but with a geometric phase. At the end of the path, the state at A' is phase-shifted relative

to the initial state at A, with the relation being,

$$\langle \psi_A | \psi_{A'} \rangle = e^{\frac{-i\Omega}{2}} = e^{-i\alpha}. \tag{2.16}$$

Here, the incurred geometrical phase is proportional to half the solid angle, $\Omega = 2\alpha$, bounded by the geodesic triangle ABC on the sphere. If the angle of the HWP is increased by β then the area enclosed by the path will increase by 2β, thus increasing the magnitude of the geometric phase by β. It follows that the induced geometric phase is inherently unbounded, i.e., it can be increased indefinitely. This has many applications in optics including phase and frequency shifters and interferometers.

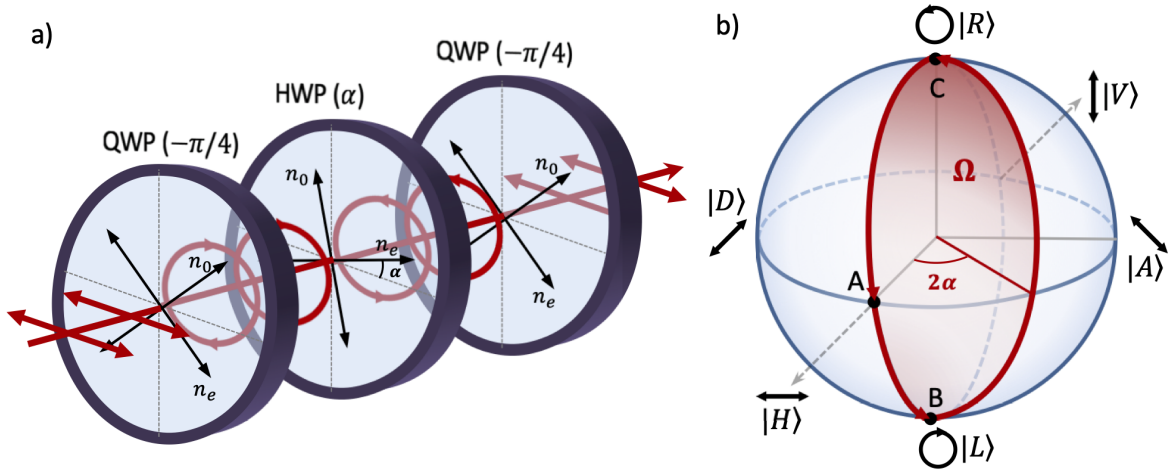

Fig. 2.7 Intuitive illustration of the geometric phase acquired by light transversing a set of waveplates. (a) Horizontally polarised light is mapped to left circular polarisation by means of a QWP($-\pi/4$), then to right circular polarisation by a HWP(α) rotated at some arbitrary angle and finally back to horizontal polarisation by a further QWP($-\pi/4$), with an additional geometric phase. (b) This mapping forms a closed loop path, depicted in polarisation parameter space. The geometric phase imparted is equal to half the solid angle $\Omega = 2\alpha$ enclosed by the path loop.

Note that, in this case, the geometric phase occurs sequentially, evolving in time. However, spatially-varying geometric phase control has been shown to be possible across individual points of the transverse profile of a beam, using optically inhomogeneous and anisotropic media like orientated liquid crystals in q-plates (QPs) [126–129]. A novel approach is to use metasurfaces [130, 131] which utilise nanostructures to shape the light wavefront at will [132, 133].

2.2.1 Generating vector modes with q-plates

The generation of OAM modes with SPPs or SLMs results in separable degrees of freedom, in that the polarisation and OAM components can be treated independently. Vector modes, however, have a non-separable polarisation and OAM coupling. Here, an operation on one degree of freedom affects the outcome of the other [98]. These spin-orbit coupled modes thus require a different generation method. Initial techniques relied on linear dichroism [134] or axial birefringence [135, 136] in intra-cavity implementations to constrain a laser cavity to oscillate, producing a cylindrically symmetric vector mode. A combination of dynamic phase control offered by SLMs and interferometers have also been used to generate these modes, but phase instability is a challenge [137], however, this technique is later used to generate high-dimensional vector modes, by superimposing a scalar and vector mode using a path interferometer. More recently, spatially varying geometric control has been used to generate vector modes with QPs [126] and metamaterials [130]. The principle of operation is similar to that described for HWPs but with locally varying birefringence in anisotropic materials [126]. Traditionally, this is achieved using liquid crystals with spatially varying orientations. The development of the QP has afforded many applications including optical trapping [138], quantum walks [107] and robust QKD communication [103].

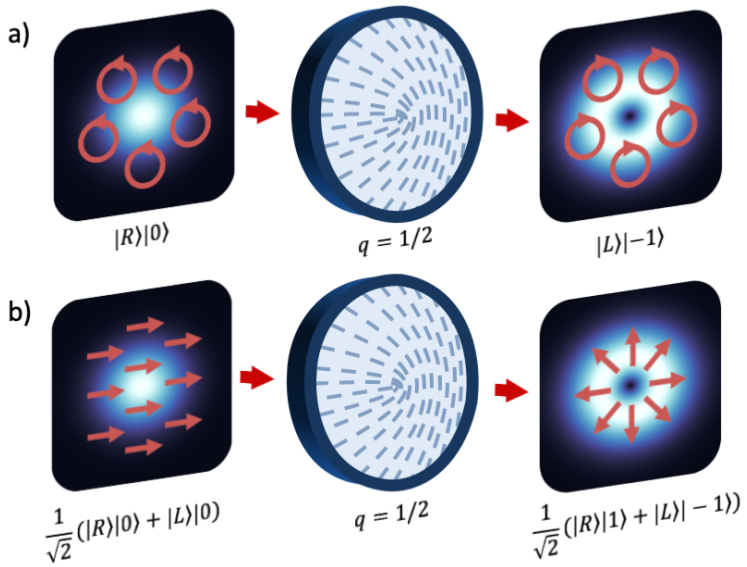

Fig. 2.8 Illustration of spin-orbit coupling using a q-plate with spatially varying fast axes. Geometric phase control is used to generate (a) scalar modes with homogeneous polarisation and (b) vector modes with with inhomogeneous polarisation.

Next, we consider the operational principles behind how the QP achieves spatially varying geometric phase control. This may be thought of as a grid of tiny waveplates varying in

orientation, such that the direction of the slow and fast axes of each grid coordinate can be independently specified, as seen in Fig. 2.8. An incident wave will then experience a different refractive index and thus a different polarisation change at each point. The relative phase acquired across the entire wave is azimuthally dependent, causing the wave to twist in a helical form and gain OAM. The orientation of the optic axis, in polar coordinates, is given by a geometrical parameter [139]

$$\alpha(r,\phi) = q\phi + \alpha_0. \tag{2.17}$$

Here, q is the azimuthal index and α_0 is the angle specifying the initial orientation formed by the optical axis from the x-axis. Assuming that the individual liquid crystals behave like HWP rotated by the parameter $\alpha(r,\phi)$, the operator describing the q-plate action in the linear basis is then,

$$\begin{aligned} U_{QP}(\alpha(r,\phi)) = &\quad R(-\alpha(r,\phi))\,U_{HWP}(0)R(\alpha(r,\phi)) &(2.18)\\ = &\begin{pmatrix} \cos(2\alpha(r,\phi)) & \sin(2\alpha(r,\phi)) \\ \sin(2\alpha(r,\phi)) & -\cos(2\alpha(r,\phi)) \end{pmatrix}. &(2.19)\end{aligned}$$

A global phase can be factored out which is equivalent to setting $\alpha_0 = 0$, this results in a tuned q-plate with the operator,

$$U_{QP}(q,\phi) = \begin{pmatrix} \cos(2q\phi) & \sin(2q\phi) \\ \sin(2q\phi) & -\cos(2q\phi) \end{pmatrix}. \tag{2.20}$$

A more intuitive understanding is exemplified by considering the action of a q-plate on right and left circularly polarised light. The output fields after the QP, calculated according to Eq. 2.3, are

$$\begin{aligned} E_{out} = &\quad U_{QP}|L\rangle = e^{i2q\phi}|R\rangle, &(2.21)\\ E_{out} = &\quad U_{QP}|R\rangle = e^{-i2q\phi}|L\rangle. &(2.22)\end{aligned}$$

It follows that the polarisation of the output field has the opposite handedness compared to the initial field. Additionally, the output field acquires an overall geometric phase $e^{\pm i2q\phi}$, resulting in an OAM transfer of $\ell = \pm 2q\hbar$ per photon, depending on polarisation handedness of the input field (see Fig. 2.8(a)). Hence, the operation of a QP on circularly polarised light, using Dirac

notation, is given by

$$U_{QP}|L\rangle|\ell\rangle = |R\rangle|\ell+2q\rangle, \tag{2.23}$$

$$U_{QP}|R\rangle|\ell\rangle = |L\rangle|\ell-2q\rangle. \tag{2.24}$$

Therefore, any arbitrarily polarised light field will be transformed according to,

$$U_{QP}(\alpha|R\rangle|\ell\rangle+\beta|L\rangle|\ell\rangle) = \alpha|L\rangle|\ell-2q\rangle+\beta|R\rangle|\ell+2q\rangle, \tag{2.25}$$

where α and β are arbitrary weighing functions satisfying $\alpha^2+\beta^2=1$. Using an arbitrary polarisation other then circular polarisation, will result in the generation of a vector mode, in which the spin and orbital angular momentum components will be classically entangled and non-separable. For example, as depicted in Fig. 2.8(b), horizontally polarised light incident on a QP will generate the radial vector mode, with an equal superposition of left and right circular polarisation. Therefore, by exploiting the linearity of waveplates discussed earlier, we can generate any state on the HOPS. Our vector mode basis, $|\psi_{\ell,\theta}\rangle = 1/\sqrt{2}(|R\rangle|\ell\rangle + e^{i\theta}|L\rangle|\ell\rangle)$, can be produced using a combination of waveplates and QP as shown in Table 2.2, of which the reverse order serves as a detector for the vector modes.

Output state	$\|\psi_{\ell,0}\rangle$	$\|\psi_{\ell,\pi}\rangle$	$\|\psi_{-\ell,0}\rangle$	$\|\psi_{-\ell,\pi}\rangle$
HWP(θ_1)	-	$\pi/4$	-	$\pi/4$
QP(q)	1/2	1/2	1/2	1/2
HWP(θ_2)	-	-	0	0

Table 2.2 Generation of vector modes from horizontally polarised light, using a combination of HWPs and q-plates. The waveplate angles are specified relative to the fast axis.

The action performed by the q-plate is called spin to orbit conversion, whereby this mapping allows for the control of the output OAM using the input polarisation, or vice versa. This control, as we will see, is very useful for transferring the information contained in one degree of freedom into the other [140], perfect for the realisation of quantum communication.

2.2.2 Dove prisms for spatial image rotation

The concept of geometric phase applies equivalently to spatial image rotation as it does to light polarisation [141]. This has important applications in classical and quantum protocols necessitating polarisation preserving phase control. The Dove prism (DP) is a key optic element offering image rotation control, particularly for the OAM degree of freedom [142]. Here, the DP operation flips the spatial profile in a transverse direction, leaving the spatial profile unchanged in the opposite transverse direction. This mode transformation can be interpreted as a geometric phase effect [143]. In particular, we interpret the rotation shift of the spatial profile as evolution of this geometric phase in time. It should be noted that a rotated DP can also introduce unwanted polarisation changes for highly focused beams [144]. The DP operation makes for useful techniques in OAM manipulation, including interferometric methods for measuring the OAM of single photons [145] and the measurement of LG beams superpositions [146].

One may best appreciate the interpretation by considering the evolution of the helicity vector $\tilde{\mathbf{k}} = (-1)^n \mathbf{k}_n$, where $\mathbf{k}_n$ is the propagation vector after n reflections [147]. Here, the helicity vector accounts for the inversion introduced by each internal DP reflection. Light transversing through the imaging system of the DP can then be mapped onto a unit sphere, similar to the Poincare sphere, whereby connecting the points forms a closed loop path representing the angle accrued by the rotation of the image. This is shown in Fig. 2.9, which illustrates the equivalence of the geometric phase shift for OAM carrying beams after transmission through DPs. In Fig. 2.9(b) an extra mirror inversion is necessary in order to compare it with the initial state. The effect of the mirror inversion can be accounted for by a change in the sign of the geometric phase [147]. The image rotation is equivalent to $2\pi - 2\gamma$ or $\pi - 2\gamma$ for systems with even or odd number of DP reflections, respectively. In both cases, this corresponds to a geometric phase dependent on twice the angle of the DP. There is also a spatial dependence on the image rotation that is related to the topological charge of the beam. Hence, a DP rotation of γ results in an induced geometric phase of $e^{i2\gamma\ell}$ [144].

The operator describing the action of the DP with respect to the orthogonal OAM states, $|-\ell\rangle = [0 \;\; 1]^T$ and $|\ell\rangle = [1 \;\; 0]^T$, can be written as,

$$U_{DP}(\gamma, \ell) = \begin{pmatrix} e^{-2i\gamma\ell} & 0 \\ 0 & e^{2i\gamma\ell} \end{pmatrix}. \tag{2.26}$$

The ability of a DP to rotate the cross-sectional phase profile of a beam allows for the control of the relative phase difference between OAM modes. This makes DPs specifically useful for the manipulation of OAM degree of freedom in vector modes.

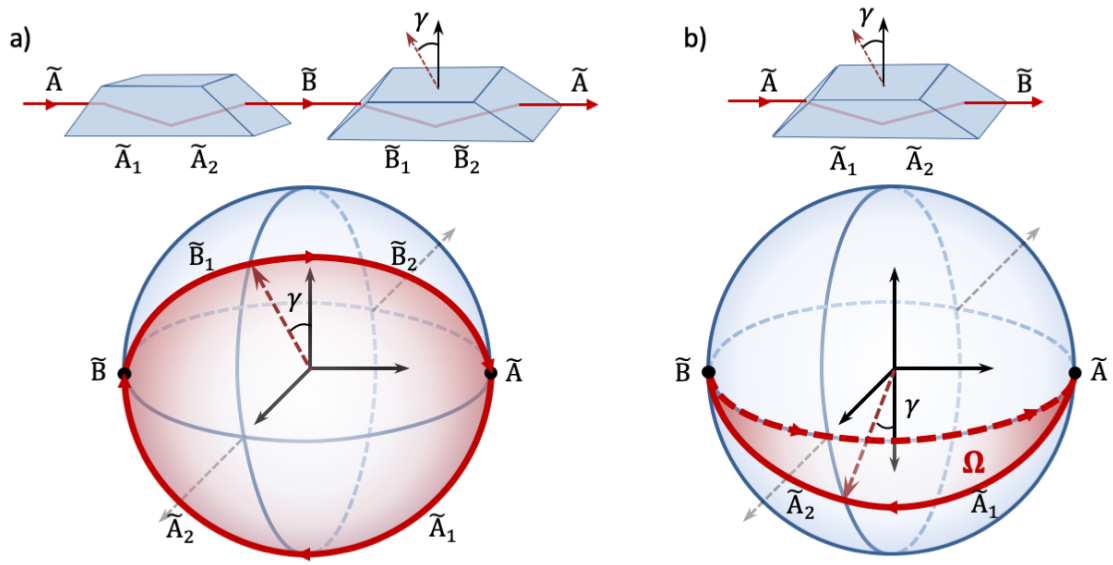

Fig. 2.9 Illustration of the equivalence of the geometric phase shift for OAM carrying beams, in helical vector $\tilde{\mathbf{k}}$-space, after transmission through (a) two consecutive DPs oriented with a relative angle γ and (b) a DP oriented at γ with a (dashed) closing geodesic, performed by a mirror.

Next, we characterise the operation of both the QP and DP inline with the above. Considering the OAM subspace spanned by $|\ell| = 1$, we generate spin-orbit coupled modes according to Table 2.2, using a combination of waveplates and a q-plate to control the geometric phase of light. The different states were then deterministically detected using a combination of multi-path interference and geometric phase control, adapted from Ref. [148] (see Fig. 2.10(a)). A DP was used to impart a relative phase between the OAM superpositions. The mode was mapped into two paths (a and b) using a polarisation grating, which projects the photons into left and right circular polarisation dependent paths. The output mode is path dependent,

$$|\psi_{1,0}\rangle = |R\rangle_a\,|1\rangle_a + e^{4i\gamma}|L\rangle_b\,|-1\rangle_b\,, \tag{2.27}$$

where the subscript a and b refer to the polarisation dependent paths. The photon paths were then interfered at a 50:50 beam splitter (BS). The polarisation information is thus path dependent and henceforth we will drop the polarisation kets in the expression. The resulting state after the BS is

$$|\psi'_{1,0}\rangle = (1-e^{4i\gamma})\,|1\rangle_c + i(1+e^{4i\gamma})\,|-1\rangle_d\,, \tag{2.28}$$

where the subscript c and d refer to the output paths of the beam splitter. By appropriately adjusting the DP angle, constructive interference will occur in one of the two output ports.

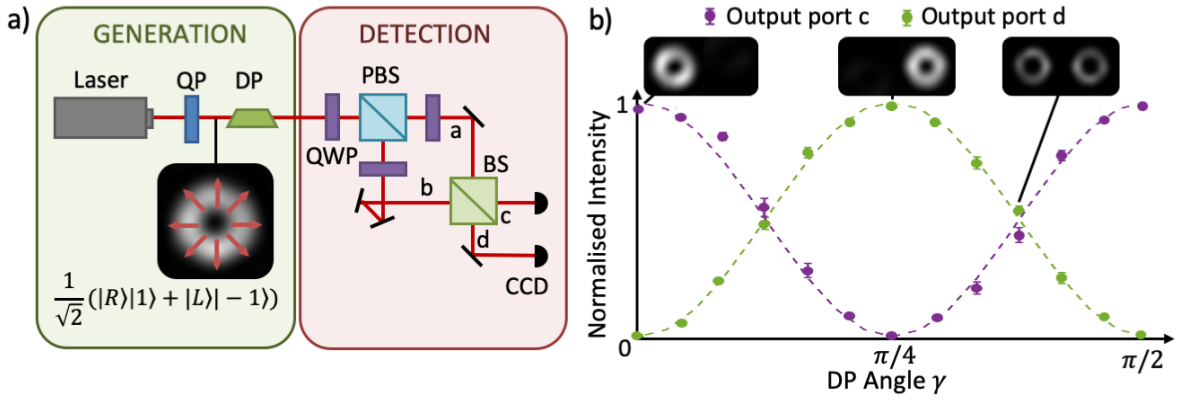

Fig. 2.10 (a) Experimental setup and (b) results for vector mode generation and detection of $|\psi_{1,0}\rangle$ and $|\psi_{1,\pi}\rangle$, using a combination of multi-path interference and geometric phase control. By appropriately adjusting the DP angle γ, constructive interference will occur in one of the two output ports, as seen in the insets above the graph.

The results for the prepared and measured vector states, characterising the q-plate and DP, is shown in Fig. 2.10(b). The graph shows the normalised intensity recorded using a CCD camera, for the detection of the vector states, $|\psi_{1,0}\rangle$ and $|\psi_{1,\pi}\rangle$. This shows that by using the acquired tools for geometric phase control, we can generate and detect orthogonal superpositions of our vector basis, essential for realising a quantum communication protocol.

2.3 Conclusion

In this chapter, we have explored the use of dynamic and geometric phase control for generating and detecting spatial modes of light. The dynamic phase control offered by waveplates was characterised for the ability to introduce a phase shift between the orthogonal components of a photon's electric field and thus manipulating its polarisation state. We experimentally investigated digital holography, through amplitude and phase modulation encoded on SLMs, as a technique to both generate and decompose OAM modes. Additionally, we used a system comprising of a SLM, encoded to produce a Gaussian beam in the desired diffraction order, coupled into a single mode fibre to perform digital projective measurements. This is analogous to an inner-product in quantum mechanics and reveals the OAM content of the photons. The dynamic phase control offered by the SLMs and waveplates proved to be an effective tool for generating, manipulating and detecting OAM modes with interesting applications in quantum communication.

Additionally, we also examined the geometric phase control offered by a q-plate to generate spin-orbit coupled modes. We showed that this is very useful for transferring the information contained in one degree of freedom into the other. Furthermore, we experimentally characterised the operation of a q-plate and a Dove prism to manipulate the spin and orbital components of light. Using a combination of multi-path interference and geometric phase control, we showed that we could deterministically generate and detect orthogonal superpositions of vector modes.

The toolbox presented here covers the essential optical elements and techniques required for the realisation of quantum cryptographic protocols, with particular interest in utilising the high-dimensional state space offered by the OAM degree of freedom.

Chapter 3

Entangled source characterisation

As previously discussed, entanglement is a quintessential property differentiating quantum protocols from their classical counterparts. The formulation of Bell's inequality [82] and later its generalisation, the Clauser-Horne-Shimony-Holt (CHSH) inequality [149], ushered in many practical experiments to test the efficacy of quantum theory and the proposed local hidden variable theories. The slew of experiments that followed, using maximally entangled states, showed the violation of these inequalities, verifying the quantum mechanical predictions of entanglement and nullifying the notion of any hidden variables [150, 151]. This led to a quest for an effective means of generating these states.

Initially, entangled photons were generated from the atomic cascade decay of mercury [151, 152] or calcium atoms [83, 84, 153]. The photons generated in this way are radiate over a full solid angle and their time of emission is also unknown, making their detection very difficult and inefficient. Later, a more suited technique was demonstrated by Burnham and Weinburg [154] showing the simultaneous detection of two spatially separated photons generated from spontaneous parametric down-conversion (SPDC) in an excited non-linear crystal. The momenta and temporal components of the down-converted photons exhibit entangled properties governed by conservation laws, referred to as phase matching conditions. These conditions force the generated photon pairs within a narrow cone of light, constraining the direction of the photon emission. This makes SPDC more favourable over the atomic cascade technique.

In this chapter, we explore the SPDC technique to generate two photon entangled pairs, which will later be necessary for our realisation of quantum cryptographic protocols. We further experimentally verify and characterise the entanglement of our system by performing three quantum measurements including spiral bandwidth measurement, Bell's inequality violation and full state tomography.

3.1 Spontaneous parametric down-conversion

Initially popularised as parametric noise or fluorescence [155, 156], spontaneous parametric down-conversion (SPDC) is a non-linear process in which a high frequency pump excites polarisation dipoles within a non-linear crystal, resulting in the random emissions of entangled signal and idler photons with lower frequencies, as in Fig. 3.1(a). The excitation causes the atoms to populate virtual energy levels permitted by the uncertainty principle and their depopulation results in fluorescent scattering of an entangled pair of photons. If the emitted photons have the same frequency the process is said to be degenerate and propagates as concentric cones centred around the pump axis, otherwise it is said to be non-degenerate.

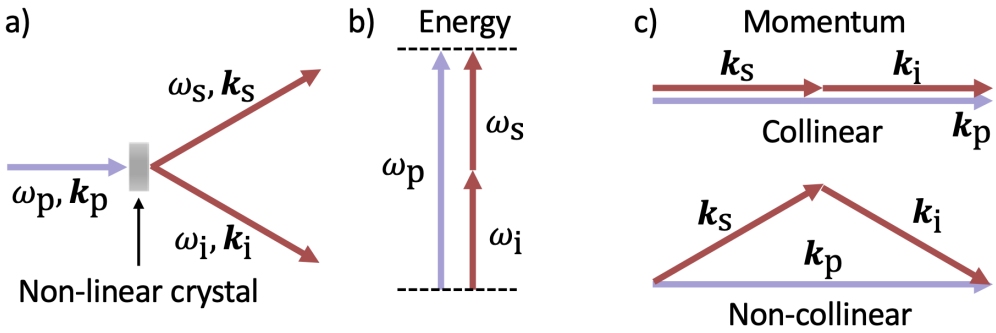

Fig. 3.1 An illustration of spontaneous parametric down-conversion in non-linear crystals. (a) A high frequency pump photon, p, is spontaneously converted into two lower frequency photons, called signal, s, and idler, i, photons for historic reasons. The generated photon pairs propagate with a opening angle α between them. (b) The energy and (c) the momentum of the system are conserved, where ω and $\mathbf{k}$ are the frequency and wavevectors, respectively. These phase matching conditions constraining the generated photon pairs to a collinear or non-collinear emission.

Throughout the process no energy is dissipated or transferred to the photons by the material. Both the energy and the momentum of the system are conserved in the decay process, such that the signal and idler photons must have summed energies and momenta equal to that of the pump photon (see Fig. 3.1(b,c)). This is known as the phase matching conditions, given by

$$\omega_p = \omega_s + \omega_i, \tag{3.1}$$

$$\mathbf{k}_p = \mathbf{k}_s + \mathbf{k}_i, \tag{3.2}$$

where ω and $\mathbf{k}$ are the frequency and wavevectors of the signal (s), idler (i) and pump (p) photons. It then follows that a measurement of the signal photon with a precise energy and direction, causes the correlated idler photon to have a definitive direction and energy. Following

the same reasoning, the total orbital angular momentum of the system is also conserved, resulting in OAM correlations between the down-converted photon pair [157].

It may seem as if there are infinite possibilities that satisfy the above phase matching conditions, however this is not true as each photon will experience a different refractive index due to the dispersion in the non-linear crystal (i.e., variation of the refractive index with a change in frequency) [158]. Providently, the non-linear crystal is also birefringent. This allows for the dispersion to be counterbalanced by the birefringence, achieving two different types of phase matching. When the phase matching produces photon pairs of the same polarisation, orthogonal to that of the pump photon, the process is called Type-I. On the contrary, when the phase matching produces photons of orthogonal polarisation, with one photon and the pump having the same polarisation, we call it Type-II. Herein we use Type-I SPDC phase matching to generate our OAM entangled photons.

By controlling the birefringence of the crystal, either by temperature or tilt angle (depending on the crystal's properties), we can control the phase matching conditions. We make use of a β-Barium Borate (BBO) crystal in which this control is offered by adjusting the propagation axis of the pump photon relative to the crystal's optical axis. A phase mismatch causes the opening angle α between the generated photon pairs to change, characterising the system from collinear to non-collinear. For a collinear system, both photons propagate in the same direction, whereas for a non-collinear system, they move in a divergent manner, in which the diameter of the cone depends on the angle between the pump beam and the optical axis of the crystal.

The efficiency of the process is contingent on the balance between the energy and frequency of the pump source. In other words, the photon pair generation could be improved by increasing the energy of each pulse at the cost of the increased probability of multiple pair generation within the same laser pulse. A thicker crystal will generate a broader OAM spectrum but at the risk of producing more photons pairs per pulse [159]. Furthermore, the pump waist w_p relative to the signal and idler waist $w_{s,i}$ also affects the generated OAM spectrum, where more modes become strongly correlated with an increase in ratio. This ratio is given as $\gamma = w_p/w_{s,i}$, indicating that a larger pump beam is preferable over a tightly focused beam [160]. However, while an the OAM spectrum does increase with γ, it comes at the cost of losses in the photon count rate [159]. The opening angle of the SPDC state has also been shown to affect the number of usable OAM modes [161].

3.1.1 SPDC quantum state

The core theory of the SPDC process can be described in great quantitative detail using the idea of parametric non-linearity, in which the quantum state of a non-linear material remains unchanged when interacting with an optical field [162]. Here, however, we will provide a

semi-quantitative description, describing the spatial structure of the generated quantum state in terms of a mode decomposition of an appropriate OAM basis. The emitted two photon quantum state is given by [162],

$$|\psi_{\text{SPDC}}\rangle = \int d\mathbf{q}_s d\mathbf{q}_i \Phi(\mathbf{q}_s, \mathbf{q}_i) \hat{a}^\dagger(\mathbf{q}_s) \hat{a}^\dagger(\mathbf{q}_i) |0,0\rangle , \tag{3.3}$$

where $|0,0\rangle$ is the multimode vacuum state, $\hat{a}^\dagger(\mathbf{q}_s)$ and $\hat{a}^\dagger(\mathbf{q}_i)$ are the photon creation operators for the signal and idler modes with the respective transverse components $\mathbf{q}_s$ and $\mathbf{q}_i$, of the wave vectors $\mathbf{k}_s$ and $\mathbf{k}_i$. The subscripts s, i merely distinguish the two photons (called the signal and idler photons for historical reasons). Here, $\Phi(\mathbf{q}_s, \mathbf{q}_i)$ describes the mode function of the pump photon (denoted by the subscript p), which results from the conservation of energy and momentum that are inherent in the parametric process.

For a crystal of finite thickness L in the longitudinal direction and transverse length much larger than the pump beam size, $\Phi(\mathbf{q}_s, \mathbf{q}_i)$ is described by

$$\Phi(\mathbf{q}_s, \mathbf{q}_i) = \tilde{E}_p(\mathbf{q}_s + \mathbf{q}_i) \sqrt{\frac{2L}{\pi^2 k_p}} \text{sinc}\left(\frac{\Delta k L}{2}\right) e^{\frac{-i\Delta k L}{2}}, \tag{3.4}$$

where the phase mismatch is given by $\Delta k = \frac{|\mathbf{q}_s - \mathbf{q}_i|^2}{2k_p}$. We note that the equation above has been simplified by replacing the wave vector $\mathbf{k}$ by the transverse component $\mathbf{q}$ and the corresponding corresponding angular frequency ω (for an in depth derivation see Ref. [163]). Further, $\tilde{E}_p(\mathbf{k}_p) = \tilde{E}_p(q)\delta(\omega - \omega_p)$, where $\tilde{E}_p(q)$ is the Fourier transform of $E_p(r)$ the spatial distribution of the pump at the input face of the crystal, which in our case is a Gaussian distribution with a beam waist w_p, given by

$$E_p(r) = \sqrt{\frac{2}{\pi w_p^2}} e^{\frac{-r^2}{w_p}} . \tag{3.5}$$

In principle the spatial mode of the pump beam can be tailored as desired, which will be elaborated in a later chapter.

The produced SPDC state can be decomposed using any complete orthonormal basis. We choose the well-known Laguerre-Gaussian (LG) modes, $LG_p^\ell(\mathbf{q})$, as the complete basis for the vector space of each photon [163]. Here, ℓ is the azimuthal index (a photon with such an azimuthal index possesses orbital angular momentum of $\hbar\ell$), p the radial index, and $\mathbf{q} \in \mathbf{R}^2$ is the 2-dimensional wavevector component transverse to the optical ($\hat{z}$) axis. Note that $LG_p^\ell(\mathbf{q})$, the momentum space representation of an LG mode, is the Fourier transform of a real space LG mode solution. With this, the entangled biphoton state $|\psi_{\text{SPDC}}\rangle$ can be written as a superposition

of LG modes

$$|\psi_{\text{SPDC}}\rangle = \sum_{\substack{\ell_s,\ell_i \\ p_s,p_i}} C^{\ell_s,\ell_i}_{p_s,p_i} |\ell_s, p_s\rangle |\ell_i, p_i\rangle , \tag{3.6}$$

where $|\ell, p\rangle = \int d\mathbf{q} LG^{\ell}_{p}(\mathbf{q})\hat{a}^{\dagger}(\mathbf{q})|0\rangle$ is the state of a photon in an LG mode with indices ℓ, p; $\hat{a}^{\dagger}$ is the usual creation operator, $|0\rangle$ is the vacuum state, and the subscripts s, i distinguish the two photons. The probability amplitudes $C^{\ell_s,\ell_i}_{p_s,p_i}$ fully characterise the entangled biphoton state. The joint probability of finding the signal (idler) photon in the $|\ell_s, p_s\rangle$ ($|\ell_i, p_i\rangle$) state upon a joint projective measurement, is given by $|C^{\ell_s,\ell_i}_{p_s,p_i}|^2$, where

$$C^{\ell_s,\ell_i}_{p_s,p_i} \propto \int d\mathbf{q}_s d\mathbf{q}_i \Phi(\mathbf{q}_s, \mathbf{q}_i) \left[LG^{\ell_s}_{p_s}(\mathbf{q}_s)\right]^* \left[LG^{\ell_i}_{p_i}(\mathbf{q}_i)\right]^* . \tag{3.7}$$

By conservation of momentum, the OAM of the input pump photon equals the sum of the OAM values of the signal and idler photons it gives rise to, $\ell_p = \ell_s + \ell_i$ [157]. Furthermore, assuming a Gaussian pump beam (where $\ell_p = 0 = p_p$) and perfect phase matching conditions, the entangled photons have equal but oppositely charged OAM values, $\ell \equiv \ell_s = -\ell_i$.

Using this description, we will explore the spatial entanglement of two photon states to reach a high-dimensional Hilbert space for the subsequent realisation of robust high-dimensional quantum communication protocols. As will be discussed in the next section, a combination of SLMs and single mode detection fibres are used for coincidence measurements at spatially separated detectors. Since the experimental projective measurement process is sensitive only to different OAM charges and hence implicitly projects onto only the $p = 0$ radial index. The prepared SPDC state becomes

$$|\psi_{\text{SPDC}}\rangle = \sum_{\ell} C_{\ell} |\ell\rangle_s |-\ell\rangle_i , \tag{3.8}$$

with C_ℓ the probability amplitude weighting for the $|\ell\rangle_s|-\ell\rangle_i$ state. Therefore, performing a joint coincidence measurement on the state $|m\rangle_s|-m\rangle_i$ (i.e. projecting onto state $|m\rangle$ and $|-m\rangle$ in the signal and idler arms, respectively) picks out the corresponding amplitude C_m. Therefore, the probability of measuring the state $|\psi_{\text{SPDC}}\rangle$ to be in the ℓ^{th} mode is given by $|C_\ell|^2$. Finally, we will characterise the system to identify the number and degree of OAM entangled modes participating in the output SPDC state of our system.

3.2 Optical setup

Following the above description of the SPDC process, we realise a standard degenerate Type-I SPDC process using a β-Barium Borate (BBO) crystal. Figure 3.2 shows a simple schematic of the experimental setup used to characterise the down-converted photons. Here, a 355 nm mode-locked ultraviolet pulsed laser with an average power of 350 mW was incident on the crystal, producing 710 nm down-converted photons. The pulse frequency of the laser is 80 MHz, containing approximately 10^9 photons per pulse. Since the SPDC process is notoriously inefficient with an average rate of 1 photon pair in every 10^5 pulses, this equates to a down-conversion efficiency of 10^{-14} per photon.

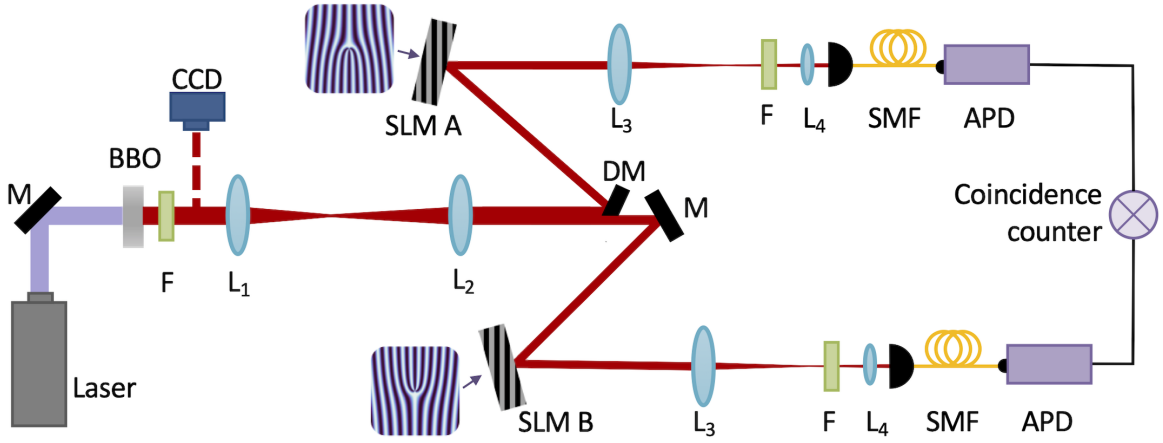

Fig. 3.2 Experimental setup for the characterisation of generated entangled photon pairs from spontaneous parametric down-conversion. A 355 nm mode-locked ultraviolet pulsed laser was used to pump a β-Barium Borate (BBO) crystal, producing 710 nm down-converted photons pairs. The photon pairs were spatially separated using a D-shaped mirror (DM) and imaged to separate spatial light modulators (SLMs) using lens f_1 and f_2. The SLMs were used to perform measurements by modulating the photons with various OAM modes. These planes were then imaged using f_3 and f_4 to single mode fibres (SMFs). Band pass filters (F) were placed after the crystal and before the SMFs to only allow the 710 nm photons. Each SMF was connected to an avalanche photon detector (APD) and measured in coincidence with a 12.5 ns simultaneous arrival time window. A CCD camera was used to image the crystal plane for alignment.

Initially, we characterised the transition of the down-converted light from a collinear to a non-collinear ring-like geometry, by adjusting the optical axis of the crystal relative to the propagation axis of the pump photon. The far-field intensity profile of down-converted field was imaged from the crystal plane to a CCD camera, using a pop-up mirror and lens. A 710 nm band-pass filter with 10 nm bandwidth was placed after the crystal and another was placed before the camera to only allow the down-converted 710 nm photons. The experimental images

are shown in Fig. 3.3(b), where the most probable correlated photons positions are located at opposite edges of the ring, indicated by red dashed circles. Since we were interested in exploring the high-dimensionality of the OAM Hilbert space, we performed our experiments in the non-collinear regime to increase the number of accessible OAM modes. We calculated our ratio to be $\gamma = 2$ which is a reasonable ratio according to Ref. [160], balancing the count rate efficiency and the OAM spectrum.

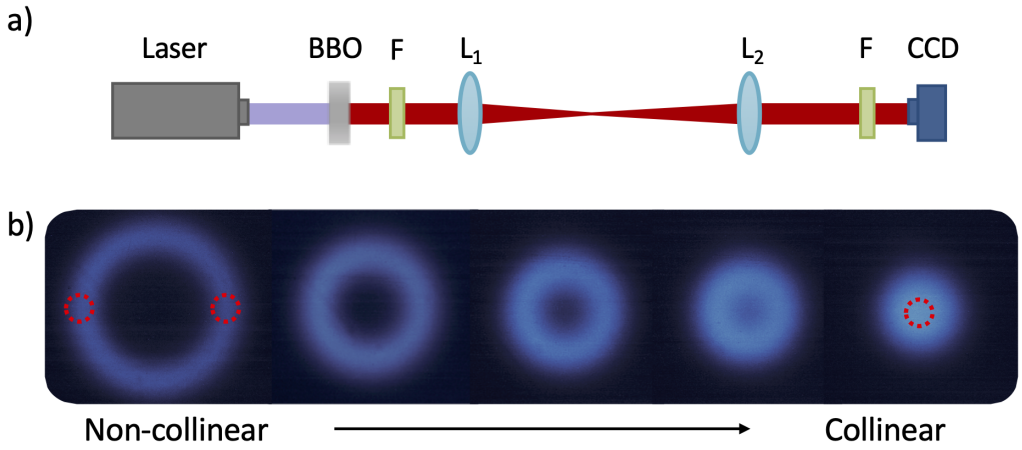

Fig. 3.3 Imaging the generated entangled photon pairs at the crystal plane. (a) Experimental setup used to image the crystal plane with lens f_1 and f_2 to a CCD camera. (b) Experimental far-field intensity profiles of the SPDC cone, for small adjustments to the optical axis angle of the crystal relative to the propagation axis of the pump photon. This characterises a transition from a ring-like non-collinear geometry to a collinear geometry. Correlated photons positions are indicated by red dashed circles.

We spatially separated the entangled photons from the down-converted cone using a D-shaped mirror (DM). The crystal plane was then imaged (f_1 = 200 mm, f_2 = 400 mm) onto two SLMs. This allows the photons to be projected into our orthogonal OAM basis set using grey scale forked holograms, which we used to characterise and decompose the output SPDC state. The resulting modes were then imaged (f_3 = 500 mm, f_4 = 2 mm) and coupled into single mode fibres (SMFs) to only extract the Gaussian component. A 710 nm band-pass filter was also placed in front of each fibre coupler. The fibre outputs were connected to Perkin Elmer avalanche photodiodes (APDs) for single photon detection. A HydraHarp 400 coincidence counter was then used to reconcile overlapping photon signals in both arms by setting a time window (gating time) between the arrival times of the photon pair. This gating time was set to 12.5 ns (i.e., the pulse interval time of the laser), minimising the probability of multiple photons arriving within the same gating time.

3.2.1 Back projection and alignment

It is useful to characterise the detection system independently from the state generation system, as both systems can affect the measurable correlation of the entangled photons. As a result we investigate the quality of our detection system using the retrodictive advanced wave representation proposed by Klyshko [164]. This description is a useful tool for analysing the detection probability of photons arriving at detector B given photon detection at detector A. Using geometric optics arguments, Klyshko showed that the two-photon detection system can be treated equivalently as though the photon measured at detector A propagates back in time to the crystal, where it interacts with the crystal as if it were a mirror, reflecting the photon to detector B. The light incident on a mirror is reflected at angle identical to the incident angle, thus simulating the momentum phase matching conditions. This picture has been very useful in predicting two-photon correlations from SPDC in various entanglement experiments, including high-dimensional quantum key distribution systems [33] and ghost imaging [165–170]. Additionally, a compelling application involves the engineering of quantum states, in which the effect of shaping the pump beam profile incident of the crystal can be examined [171, 172].

We use this model to characterise and isolate the effects of the detection system by replacing the crystal and one detector with a mirror and a classical light source, respectively. Figure 3.4 shows these changes. More specifically, we replaced detector A with a 710 nm diode laser with a Gaussian profile. The beam was imaged through the system onto the mirror at the crystal plane and then imaged to detector B. We modulated the beam in arm A to a particular state and performed the projective measurement detection in arm B. Experimentally, this method is called back-projection, where the classical light source corresponds to the wave propagating back in time to the crystal [167].

To understand this intuitively, let us consider the example of a Gaussian $\ell_p = 0$ pump beam exciting a non-linear crystal, resulting in a down-converted photon pair, where $\ell_A + \ell_B = 0$. In the down-converted regime, a measurement of $\ell_A = 1$ encoded on SLM A, will only result in a correlation with a measurement of $\ell_B = -1$ encoded on SLM B. Now, applying the back-projection technique, the light beam from source A can be modulated by SLM A to have the OAM state $\ell_A = -1$. The helicity of the beam is inverted at the mirror (crystal plane) to $\ell_A = 1$ and reflected to SLM B. Performing the measurement of $\ell_B = -1$ encoded on SLM B results in a Gaussian which couples into the SMF as a detection. If the mode generated at SLM A was changed to $\ell_A = 5$, then the beam would not couple into the SMF as the beam would have an helicity of $\ell = 4$, registering no light at the detector.

By encoding the phase conjugate of SLM A on SLM B, we can be assured that the light from fibre A is coupled into fibre B. We use this technique to maximise the coupling of light into the fibres with respect to spatial modes. Moreover, the detection of the reflected photon

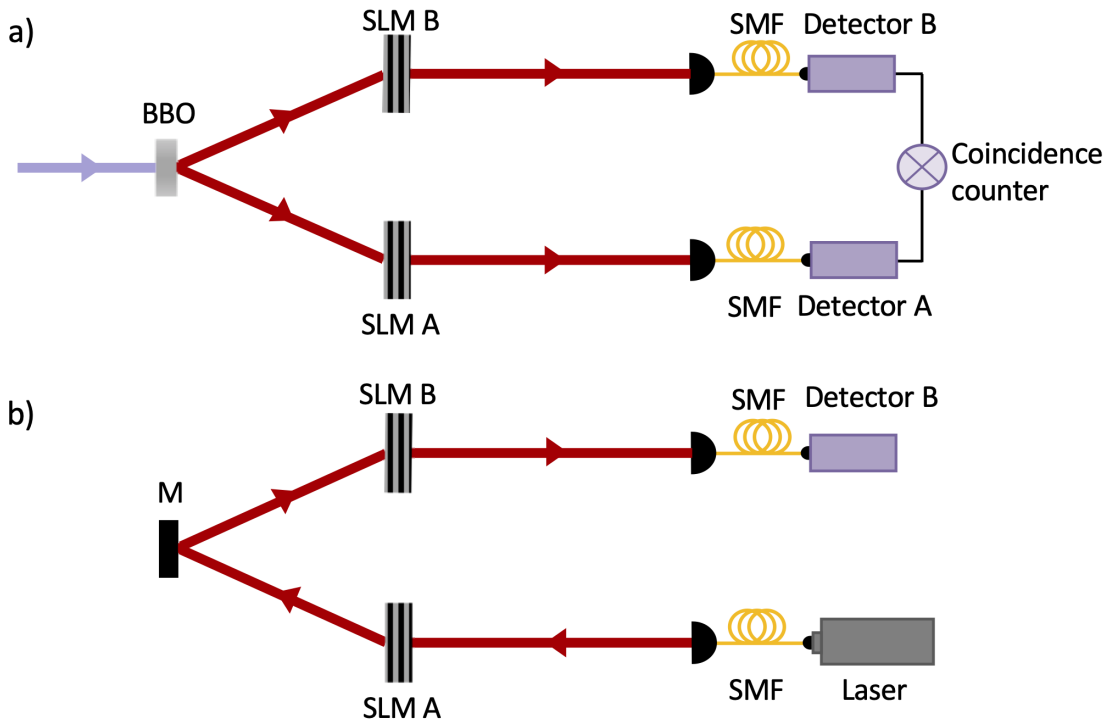

Fig. 3.4 Simplified schematic highlighting the changes made to (a) a general down-conversion entanglement setup, in order to operate the system in (b) back-projection as described by Klyshko. Detector A was replaced with a 710 nm diode laser and the non-linear crystal (BBO) was replaced with a mirror (M). The laser light was coupled to a SMF, after which it was sequentially imaged to each SLM and then coupled into detector B. This model was used to align and characterise the effects of the detection system.

can be optimised to ensure rigorous alignment and in effect anticipate the behaviour of the two photon correlations. We used the back-projection technique to align and optimise our detection system before performing measurements on the down-converted photons.

3.3 Quantum measurements

A non-collinear SPDC setup was used to examine the fundamental properties of the down-converted photon pairs. Correspondingly, we explore various experimental techniques and measures to quantify and characterise the entanglement of the system with respect to the OAM degree of freedom. These measures include: the spiral bandwidth as a measure of OAM spectrum produced, the violation of Bell's inequality as a indication of entanglement and finally a full quantum state tomography to decompose the entangled state.

3.3.1 Spiral bandwidth

Since we are interested in using the OAM degree of freedom as our encoding basis for quantum cryptography, it is imperative that we characterise the degree of OAM entanglement produced by our SPDC source. It follows that this is directly related to the number of OAM modes contributing to the output SPDC state. As we have mentioned, the probability distribution of OAM modes produced through the SPDC process is reliant on the generation conditions at the source and the detection efficiency of the measuring system. A thinner crystal or an increase in the pump beam waist will produce a broader OAM spectrum [163]. Likewise, the number of OAM modes produced can be controlled by manipulating the phase matching conditions of SPDC process [161]. As a result, these parameters impose a limit on the number of modes that can be physically measured, which is referred to as the spiral bandwidth of the system [159]. A broad spiral bandwidth is crucial for high-dimensional quantum cryptography requiring increased information capacity per photon [72, 173].

The spiral bandwidth is calculated as the full-width-half-maximum (FWHM) of the OAM probability distribution, c_ℓ. In effect, it is a measure of the number of OAM modes generated with strong correlations. We quantify the spiral bandwidth of our system by sequentially encoding forked holograms, i.e., azimuthal phase mode functions $e^{i\ell\phi}$, onto the SLMs. More specifically, the hologram encoded on SLM A was kept constant, while iteratively moving through a sequence of varying OAM forked-holograms on SLM B. This process was repeated for a set of ℓ values on both SLMs. Each measurement was recorded over a 10s integration time, well above the time resolution of the detectors (which we set at 12.5 ns), obtaining a statistically accurate coincidence measurement. By performing these projective measurements on each photon, coupling only the fundamental mode (Gaussian) of the single mode fibres and measuring the coincidence rate, we were able to measure the mode availability generated by our system.

The experimental results are shown in Fig. 3.5, where we iterate through $\ell = [-20, 20]$ on each SLM. Figure 3.5(a) shows the measured coincidence counts as a indication of the experimental probabilities c_ℓ. The results are consistent with the conservation of OAM in the SPDC process [157]. The diagonal elements show a depreciating trend from $\ell = 0$, inline with the expected OAM spectrum. Experimentally the off diagonal elements are highly sensitive to misalignment, resulting in an error of less than 5% of their corresponding diagonal element. Figure 3.5(b) shows the diagonal elements. From this we calculated FWHM as an indication for the number of highly correlated OAM modes detectable by the system. This was calculated to be FWHM = 18, indicating an encoding space an order of magnitude larger than the popular two-dimensional polarisation states.

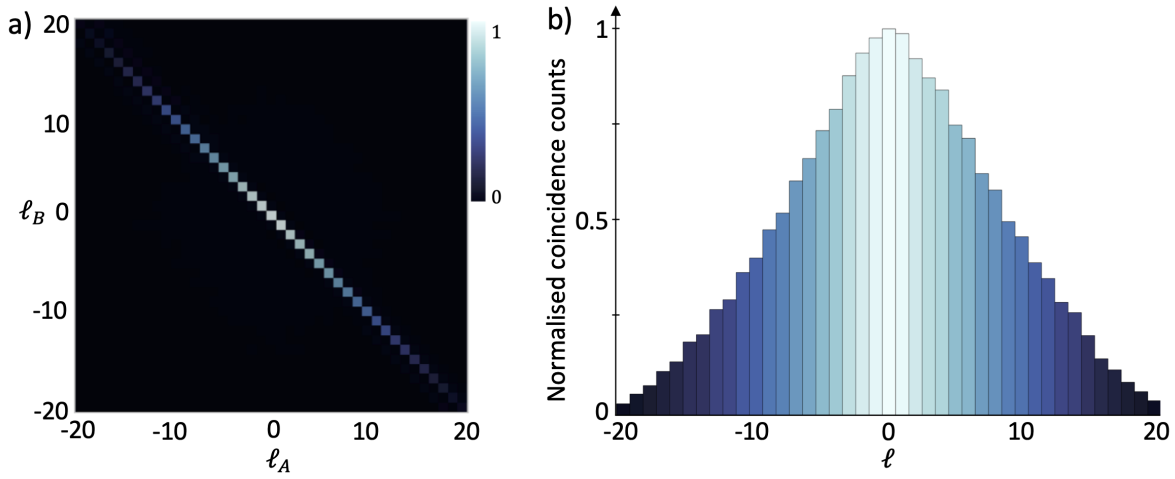

Fig. 3.5 Experimental spiral bandwidth measurements. (a) Density plot of the normalised coincidence counts per second for OAM topological charge ℓ in each arm. (b) The diagonal elements representing the spiral bandwidth were used to calculate the full-width-half-maximum. This was determined to be FWHM = 18, indicating the number of highly correlated OAM modes.

3.3.2 Bell inequality violation with OAM

Next, we explore the non-local correlations between the spatially separated entangled photon pairs. We will demonstrate the violation of the Clauser-Horne-Shimony-Holt (CHSH) inequality [149], an experimentally relevant adaption of the Bell's inequality, which was developed to test for the predicted local hidden variable theory underpinning quantum mechanics [174].

There have been various demonstrations reporting the CHSH inequality violation using polarisation entangled photons generated by cascade atomic decays [150, 151] or SPDC [175, 176]. These experiments employed correlated polarisation measurements between superposition states of two spatially separated photons. These measurements were performed by passing photon A through a linear polariser rotated at an angle θ_A, and photon B passing through a polariser rotated at θ_B (see the top row of Fig. 3.6). The rotation of the polarisers projects the state to a superposition state described by the equator of the Poincare sphere. In the case of two photon entanglement, the Bell parameter, S, can be defined as

$$S = E(\theta_A, \theta_B) - E(\theta_A, \theta'_B) + E(\theta'_A, \theta_B) - E(\theta'_A, \theta'_B), \tag{3.9}$$

where $E(\theta_A, \theta_B)$ is the photon correlation function between the measurements in arm A and B for different polarisation angle projections θ_i and θ_i'. These correlations are given by

$$E(\theta_A, \theta_B) = \frac{I(\theta_A, \theta_B) - I(\theta_A^\perp, \theta_B) - I(\theta_A, \theta_B^\perp) + I(\theta_A^\perp, \theta_B^\perp)}{I(\theta_A, \theta_B) + I(\theta_A^\perp, \theta_B) + I(\theta_A, \theta_B^\perp) + I(\theta_A^\perp, \theta_B^\perp)}, \tag{3.10}$$

where $\theta_i^\perp = \theta_i + \pi/2$ and $I(\theta_A, \theta_B)$ is the probability of a coincidence measurement for polariser angles θ_A and θ_B, respectively.

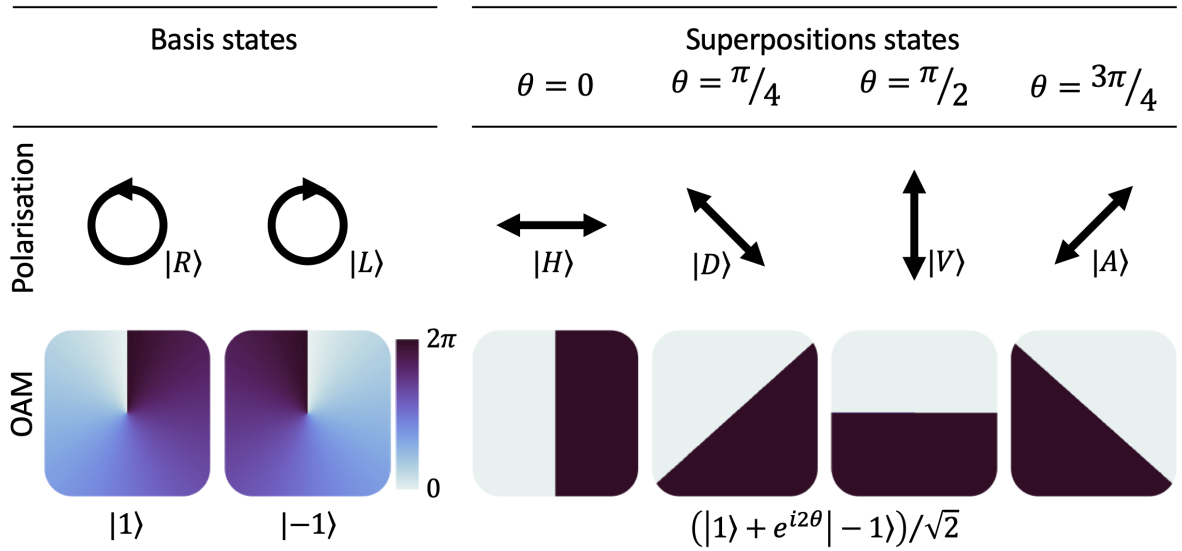

Fig. 3.6 An analogy between Bell inequality violation with polarisation and OAM. Traditionally, correlated polarisation measurements are performed on the two spatially separated photons, by iteratively projecting each photon into each state by varying the angle of a polariser (top row). Similarly, in the OAM basis this can be done using SLMs to project the photons into superpositions of OAM states defined by some relative phase θ (bottom row).

The upper bound for a classical hidden variable theory is $|S| \leq 2$, however, maximally entangled two photon states have been shown to violate this bound for particular polariser angles (i.e., $\theta_A = 0$, $\theta_B = \pi/8$ and $\theta_i' = \theta_i + \pi/4$), with a maximum value of $|S| = 2\sqrt{2}$ in two-dimensions [177]. The violation is indicative of the non-separability of the measured degree of freedom and that the photon pairs exhibit non-local interactions.

In terms of our OAM basis, two orthogonal OAM modes and the corresponding superpositions are needed to perform the two state CHSH inequality measurements [93]. In particular, we need to measure the photon correlations between the OAM superposition. The superposition

in question are described by

$$|\psi_{\theta,\ell}\rangle = \frac{1}{\sqrt{2}}\left(|\ell\rangle + e^{i2\theta}|-\ell\rangle\right). \tag{3.11}$$

Here, by choosing a particular value for ℓ we can detect a superposition of OAM states for a range of θ, which describes the relative phase between modes, analogous to the rotation of polarisation states (see the bottom row of Fig. 3.6).

In order to demonstrate a CHSH violation in terms of OAM, we consider the two photon OAM entangled state produced by SPDC, designating the signal (idler) photon paths with an A (B) subscript, and post select on coincidences for a particular ℓ. The SPDC state in Eq. 3.8 then becomes,

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}\left(|\ell\rangle_A|-\ell\rangle_B + |-\ell\rangle_A|\ell\rangle_B\right). \tag{3.12}$$

We encode the SLM in each arm A and B with the corresponding holograms given by Eq. 3.11, to access the superpositions states of the OAM subspace. The holograms were iteratively rotated, encoding SLM A with the state corresponding to θ_A and varying the state encoded on SLM B corresponding to θ_B. The coincidence count rates were measured for each iteration.

The experimental normalised coincidence counts for the down-converted SPDC photons in the $|\ell| = 1$ OAM subspace, are shown in Fig. 3.7. The coincidence counts are highest when the detection systems (i.e., θ_A and θ_B) are orientated at integer multiples of $\pi/2$ with respect to each other. We calculated the Bell parameter S using Eq. 3.9 to be $S = 2.71 \pm 0.03$. Here, we observed a violation of the CHSH inequality, consequently confirming the quantum correlations and entanglement of our SPDC system in terms of our OAM basis.

3.3.3 Quantum state tomography

Finally, after we have established that our system produces photon pairs entangled in OAM, we wish to characterise and reconstruct the photon state. The process of determining the full state information of an unknown quantum state, commonly referred to as quantum state tomography (QST), was first proposed by Fano [178] with many experimental demonstrations following suit [179, 180]. Originally, these were performed with polarisation and then extended to OAM, with a demonstration of up to $|\ell| = 20$ [181].

Quantum tomography allows the quantum state to be uniquely recovered from a set of measurements, forming a complete basis in the specified Hilbert space. Appropriately, the process requires identical copies of the initial state, as each measurement will change the quantum state. This consists of reconstructing the density matrix $\rho = |\psi\rangle\langle\psi|$ to characterise

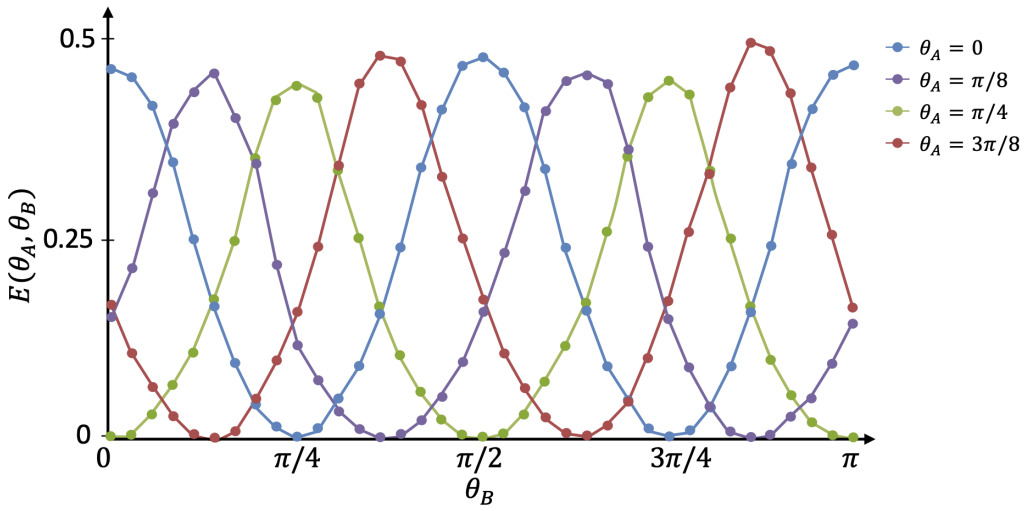

Fig. 3.7 Experimental results for Clauser-Horne-Shimony-Holt (CHSH) inequality. We demonstrate the normalised coincidence counts as a function of the relative angle between superpositions of OAM states. The holograms were iteratively rotated, encoding SLM A with the state corresponding to θ_A and varying the state encoded on SLM B corresponding to θ_B.

the statistical state of the quantum system. The method of reconstruction used here involves linear combinations of the generalised Gell-Mann matrices to describe the density matrix for any given dimension [179]. These Gell-Mann matrices constitute a complete measurement basis set.

Two-dimensional quantum state tomography

The density matrix of a two-dimensional two-photon state can be described by a linear combination of the Pauli matrices, given as [182]

$$\rho = \frac{1}{4}\sigma_0 \otimes \sigma_0 + \sum_{mn} \rho_{mn}\sigma_m \otimes \sigma_n, \tag{3.13}$$

where $\sigma_{m,n}$ are the Pauli matrices for $m,n = 1,2,3$ with corresponding complex coefficients ρ_{mn}. Consequently, a two photon state can be represented by the tensor product of the OAM

Bloch spheres of each photon, and as a result, the density matrix is a 4×4 matrix written as

$$\rho = \begin{pmatrix} a_{11} & a_{12}e^{i\phi_{12}} & a_{13}e^{i\phi_{13}} & a_{14}e^{i\phi_{14}} \\ a_{21}e^{i\phi_{11}} & a_{22} & a_{23}e^{i\phi_{23}} & a_{24}e^{i\phi_{24}} \\ a_{31}e^{i\phi_{31}} & a_{32}e^{i\phi_{32}} & a_{33} & a_{34}e^{i\phi_{34}} \\ a_{41}e^{i\phi_{41}} & a_{42}e^{i\phi_{42}} & a_{43}e^{i\phi_{43}} & a_{44} \end{pmatrix}, \tag{3.14}$$

where a_{ij} and ϕ_{ij} are the amplitudes and the phases that make up the 16 matrix elements, respectively. The diagonal elements express the probability of detecting one photon in the state $|\ell\rangle$ and the other in the state $|-\ell\rangle$. The off-diagonal elements represent superposition states.

Practically, the matrix elements can be determined from a set of joint measurements performed in coincidence, comprising of projections across the OAM eigenstates and the superposition states. Experimentally, these are calculated from the normalised coincidence count rates for a set of measurement states displayed on each SLM. We choose the measurement states to include projections onto the basis states $|\ell\rangle$ and $|-\ell\rangle$, as well as the states described by Eq. 3.11 with $\theta = (0, \pi/4, \pi/2, 3\pi/4)$. This yields 6 iterative projection measurements on each SLM, with a total of 36 measurements. This over complete set of measurements allows us to calculate the 16 matrix elements. The excess information together with statistical methods can be used to minimise photon number fluctuations and detection errors affecting the state reconstruction [183]. This is done using the maximum likelihood estimation, as described in Ref. [184], by minimising the following equation

$$\chi^2 = \left(\sum_i \frac{C_i^{exp} - C_i^{guess}}{\sqrt{C_i^{guess} + 1}} \right)^2, \tag{3.15}$$

on the condition that it yields a density matrix with positive eigenvalues. Here, C_i^{exp} is determined from the experimental coincident counts and C_i^{guess} is predicted from a guessed density matrix for the i^{th} tomographic projection. This guessed matrix, ρ_{guess}, is constructed from a d^2 matrix G, described by a linear combination of Gell-Mann matrices and the identity matrix, as given by

$$\rho_{guess} = \frac{G^\dagger G}{Tr(G^\dagger G)}. \tag{3.16}$$

Here, we minimise χ^2, by picking suitable coefficients of the Gell-Mann matrices. This gives us a close physical description of the density matrix of the measured quantum state. In Fig. 3.8, we visually represent the experimentally reconstructed density matrix for the two-dimensions $|\ell| = 1$ subspace.

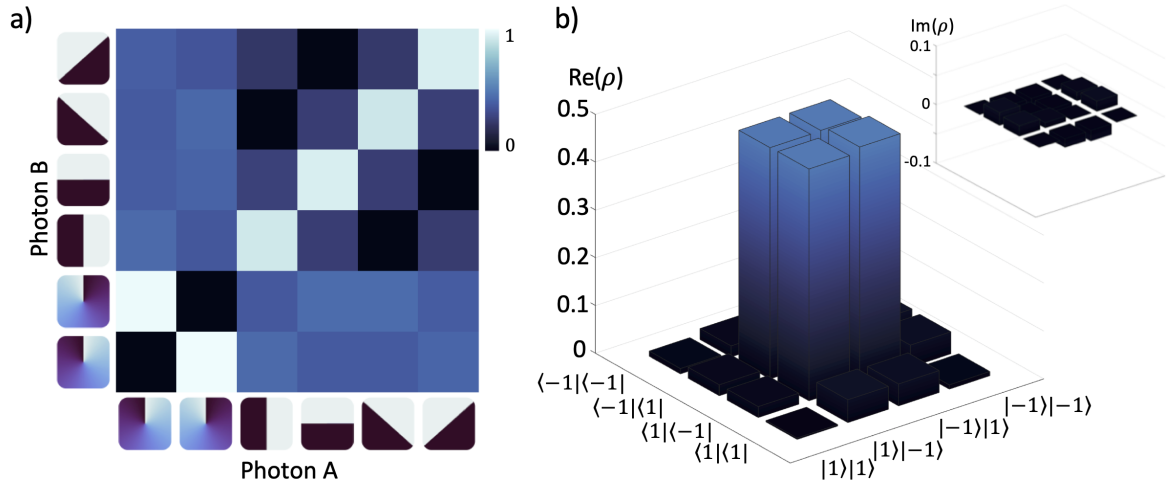

Fig. 3.8 Two-dimensional quantum state tomography of a two photon state, entangled in the $|\ell| = 1$ OAM degree of freedom. (a) Complete set of measured coincidence counts for a pair of entangled photons projected into the measurement state, indicated by the respective phase map. Using this tomographic information, the density matrix describing the state was reconstructed, (b) illustrating both the real and imaginary components.

High-dimensional quantum state tomography

Now, we extend the two-dimensional quantum state tomography to high-dimensions. This generalisation has been presented in Ref. [179] and further demonstrated in Ref. [185]. As before, a d-dimensional single photon state can be represented as a linear combination of the Gell-Mann matrices and the d-dimensional identity matrix, as given by

$$\rho = \frac{1}{d^2}\tau_0 + \sum_n b_n \tau_n, \tag{3.17}$$

where τ_0 is the identity matrix and τ_n is the generalised Gell-Mann matrix with a corresponding complex coefficients b_n. Note that the normalisation requires the sum of the squares of the coefficients to equal unity. Additionally, these coefficients can be determined by a complete set

of measurements, consisting of the OAM basis states $|\ell\rangle$ and superpositions there of, given by

$$|\psi_{\theta,\ell_1,\ell_2}\rangle = \frac{1}{\sqrt{2}}\left(|\ell_1\rangle + e^{i\theta}|\ell_2\rangle\right), \tag{3.18}$$

where $\ell, \ell_1, \ell_2 = (-d, ..., d)$.

Similarly, the density matrix of a two-photon d-dimensional state can then be represented as a tensor product of the two photon states, described by a $d^2 \times d^2$ density matrix,

$$\rho = \frac{1}{d^2}\tau_0 \otimes \tau_0 + \sum_{mn} b_{mn}\tau_m \otimes \tau_n. \tag{3.19}$$

Using this generalisation, we experimentally perform a quantum state tomography in high-dimensions. Figure 3.9 depicts the experimentally measured probabilities forming the complete OAM set in $d = 5$ dimensions. Furthermore, we determined the density matrices of the SPDC states entangled in OAM, for dimensions $d = 2$ to $d = 5$ (see Fig. 3.10). The imaginary components of the coefficients arise from the small but measurable phase Gouy shift between the states caused by not imaging the exact plane of the non-linear crystal.

Extracting information from a tomography measurement

Now that we are able to completely characterise the quantum state of our SPDC source, we can begin to extract useful information from the density matrix to make predictions with regards to the purity and quality of our state. Here, we present useful quantum measures for cryptographic protocols, specifically: fidelity, linear entropy and concurrence [87].

First, we define a parameter describing how well the experimentally reconstructed density matrix approximates the target state. This is called the fidelity of the system, calculated as [186]

$$F = \left(Tr\left[\sqrt{\sqrt{\rho_T}\rho_{guess}\sqrt{\rho_T}}\right]\right)^2, \tag{3.20}$$

where ρ_{guess} is the reconstructed density matrix and ρ_T specifies the density matrix of the target state. A fidelity of $F = 1$ is indicative of identical matrix reconstruction and $F = 0$ indicates no similarity. The definition can be further reduced, for a target state that is pure (i.e., $\rho_T = |\psi_T\rangle\langle\psi_T|$), to a simpler expression

$$F = Tr[\rho_T\rho_{guess}] = \langle\psi_T|\rho_{guess}|\psi_T\rangle. \tag{3.21}$$

We calculated the fidelities for $d = 2$ to $d = 5$ dimensional subspaces, with a high fidelity of $F_2 = 0.98 \pm 0.01$ for $d = 2$, which deteriorates with dimension to $F_5 = 0.77 \pm 0.01$ for $d = 5$

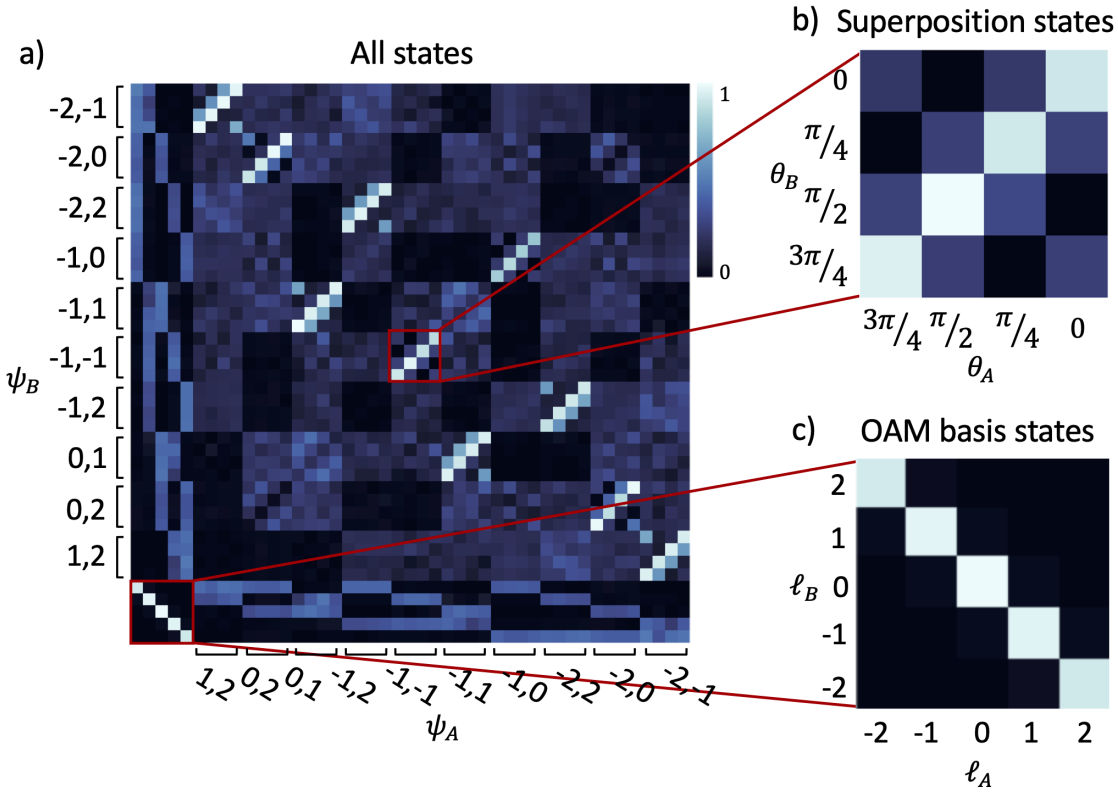

Fig. 3.9 Quantum state tomography of photon pairs entangled in 5-dimensions, $|\ell| = (0,1,2)$. (a) Complete set of experimental coincidence counts (normalised). (b) Shows the coincidence results for an inset of OAM superposition states defined in each arm by $\ell_1, \ell_2 = -1, 1$ and a phase difference of θ_A and θ_B between the respective modes. (c) Shows the measured coincidences for the OAM basis states, ℓ_A and ℓ_B.

dimensions. This indicates a lower measure of overlap between density matrices. This is expected as a result of the finite number of OAM modes and an increase in cross-talk between the measured superpositions.

Next, we describe the measure of the purity of a quantum state [183], the linear entropy, which is given by

$$S_L = \left(1 - Tr[\rho^2]\right). \tag{3.22}$$

The linear entropy for a pure state is 0 since it satisfies $Tr[\rho^2] = Tr[\rho] = 1$. Experimentally, we measure a near zero linear entropy for lower dimensions at $S_{L,2} = 0.03 \pm 0.01$, which increases to $S_{L,5} = 0.27 \pm 0.01$ for $d = 5$ dimensions. This indicates that higher dimensional states are increasingly mixed states. The cross-talk between the modes and the errors incurred for measurements in higher dimensions, result from the unavoidable detection errors in the

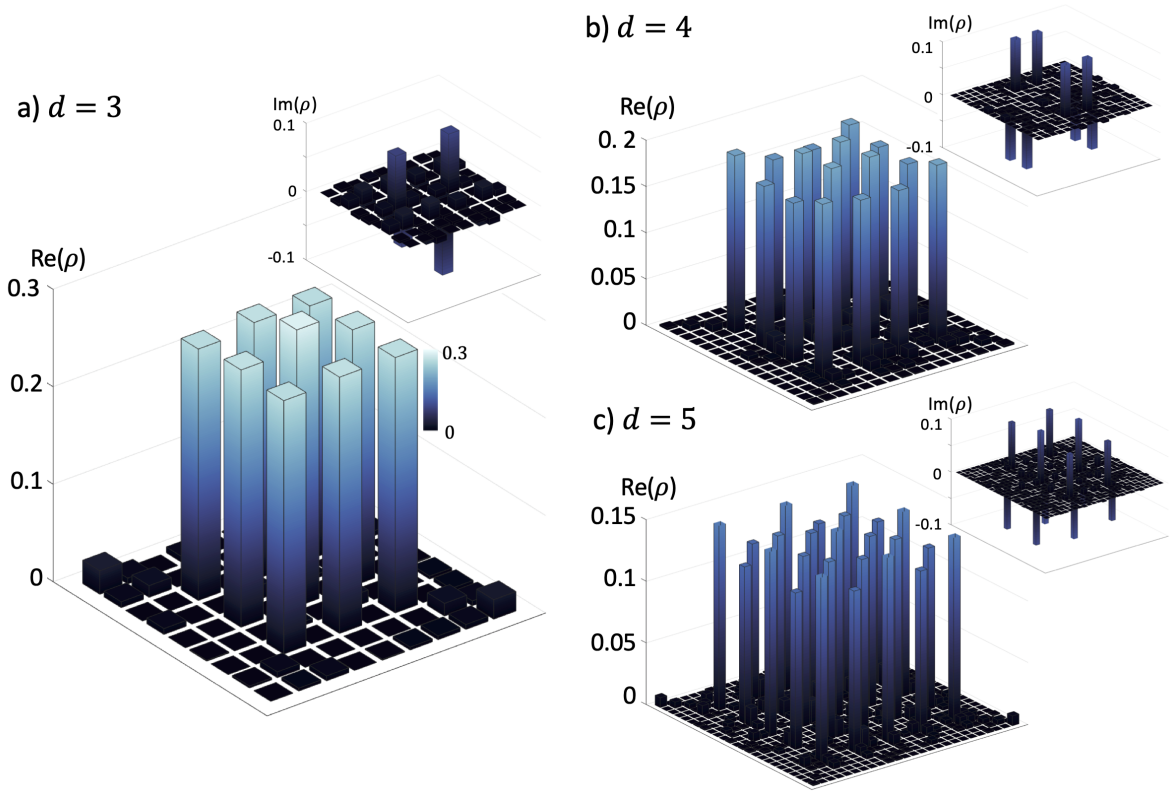

Fig. 3.10 Experimental results for the reconstructed density matrices for dimensions $d = 3, 4, 5$. The axes are labeled using the same convention as in Fig. 3.8. For example, the axes for $d = 3$ would read $\langle 1|\langle 1|, \langle 1|\langle 0|, \langle 1|\langle -1|$... and $|-1\rangle|-1\rangle, |-1\rangle|0\rangle, |-1\rangle|1\rangle$ ..., etc.

coincidence count rates and the fact that the number of measurements required increases with dimension.

Lastly, we define concurrence, C, as a quantitative measure of entanglement for a biphoton qubit state which is expressed as [187]

$$C(\rho) = \max\{0, \sqrt{\lambda_1} - \sum_i \sqrt{\lambda_i}\}, \tag{3.23}$$

with λ_i representing the eigenvalues of the matrix $M = \sqrt{\sqrt{\rho}\tilde{\rho}\sqrt{\rho}}$ with $\tilde{\rho} = \Theta\rho^*\Theta$ and Θ representing an anti-unitary operator satisfying $\langle\psi|\Theta|\phi\rangle = \langle\phi|\Theta^{-1}|\psi\rangle$. A concurrence of $C = 0$ defines a system that is not entangled and $C = 1$ for a maximally entangled state. For our two-dimensional bi-photon state, the measured the concurrence is $C = 0.96 \pm 0.01$ for $d = 2$.

This has since been extended for pure states of arbitrary dimensions (i.e., qudit pure states) in a very intuitive way by looking at the geometry of the tensor products with increasing dimensionality. For bipartite systems larger than a pair of qubits, there is no accepted general

formula for the measure of concurrence. However, there do exist formulas for states with special symmetries, such as Werner and isotropic states [188, 189].

3.4 Conclusion

In this chapter, we investigated the techniques required to generate and detected single photon entanglement, particularly within the OAM degree of freedom. We explored a Type-I SPDC method to generate two photon entangled pairs by exciting a non-linear crystal with a high frequency pump, resulting in the random emissions of entangled lower frequency photons. We illustrated that by controlling the birefringence of the crystal, in our case the tilt of the non-linear crystal with respect to the incident pump, we were able to control the phase matching conditions of the system, thus allowing us to move from collinear to a non-collinear geometry.

The detection system included SLMs coupled to SMFs to perform projective measurements. Using this method we were able to determine the OAM of single photons. We then characterised the detection system independently from the state generation system using the method of back-projection. This made the alignment of single photons much easier, by passing classical light through the setup as if the wave was propagating back in time to the crystal and then to the other detector. We used this technique to maximise the coupling of light from one fibre to the other, such that we optimised our detection system before performing measurements on the down-converted photons.

We performed various quantum measurements to quantify and characterise the entanglement of our system with respect to the OAM degree of freedom. First, we measured the spiral bandwidth as a measure of the OAM spectrum detected and confirmed that OAM is conserved in the SPDC process. This lead us to explore the non-local correlations between the spatially separated entangled photon pairs, such that we performed a CHSH-Bell inequality violation with OAM. Using OAM superpositions states, we determined the Bell parameter to be $S = 2.71 \pm 0.03$. This confirmed the entanglement of the system, such that the OAM correlations could not be described by local hidden variable theories.

Finally, we experimentally perform a quantum state tomography and reconstructed the full state information of OAM entangled photon pairs, for various high-dimensions. Particularly, we determined the density matrices of the system for dimensions $d = 2$ up to $d = 5$. From these results, we calculated useful quantum measures for cryptographic protocols: fidelity, linear entropy and concurrence. These experimental results allow us to further explore and engineer the generation and measurement procedures for OAM based quantum cryptographic applications.

Chapter 4

Quantum random number generation using spatially structured light

The work herein is under peer review, with preprint access in Ref. [190].

The incessant pursuit to enhance the security of communication protocols, in combination with the current advancements in hardware capabilities, has resulted in an increased range of cryptographic applications requiring random seed numbers. These numbers, which are used as the initial choice of basis and measurement states for any quantum communication protocol, must reflect the probabilistic nature of quantum mechanics so as to guarantee the security of the protocol. In this context, we present a quantum random number generator based on random outcomes inherent to the projective measurements on a superposition of quantum states of light.

Firstly, we use multiplexed holograms encoded on a spatial light modulator to spatially map down-converted photons onto a superposition of optical paths. This gives us full digital control of the mapping process which we can tailor to achieve any desired probability distribution. More importantly, we use this method to account for any bias present within our transmission and detection system, forgoing the need for time-consuming and inefficient unbiasing algorithms. Our QRNG achieved a min-entropy of $H_{min} = 0.9991 \pm 0.0003$ bits per photon and passed the NIST statistical test suite.

Furthermore, we extend our approach to realise a QRNG based on photons entangled in their orbital angular momentum (OAM) degree of freedom. This combination of digital holograms and projective measurements on arbitrary OAM combinations allowed us to generate random numbers with arbitrary distributions, in effect tailoring the system's entropy while maintaining the inherent quantum irreproducibility. Such techniques allow access to the higher-dimensional OAM Hilbert space, opening up an avenue for generating multiple random bits per photon.

4.1 Introduction

Our human intuition regarding randomness is often faulty. For example, one would think that if one were to draw enough elements from a truly random source, no patterns in the data would emerge. According to Ramsey theory [191], however, this is not the case: ideal randomness in huge data sets, in which no conceivable patterns in the data exist, is impossible. This, for example, is why ancient cultures observed the various constellations in the night sky.

Random numbers play a vital role in various disciplines where unpredictability is crucial. Monte-Carlo integration [192] makes extensive use of random numbers to effectively sample points within the integration domain when analytical integration fails; randomness is also fundamental in studies of Brownian motion [193] and the path integral formulation of quantum field theory [194]. Uncertainty necessarily needs to be included in models of the financial markets [195] as well as meteorology [196], and even computer games requiring ever-changing scenes or character behaviour make use of randomness [197]. Appropriate to this dissertation, random numbers also underlie current cryptographic methods used to assure the confidentiality and security of our digital communication and storage protocols [1, 26, 27]. The initial choice of basis and measurement states, the key steps in any quantum communication protocol, must be truly random in that the unpredictable nature of the random number generation process assures a secure system. Thus, it goes without saying that understanding, generating and distilling randomness from a variety of sources is fundamental in both scientific and everyday contexts.

Traditionally, random number (RN) generation has been dominated by mathematically complex algorithms that, given a seed, produce a sequence displaying statistical pseudo-random properties [198]. It follows that since these numbers are generated using deterministic algorithms, all security would be lost if an attacker, with access to the system, could figure out the initial seed. Random number generation has since undergone a fundamental shift from depending on deterministic algorithms to random physical sources. However, a system that, at face value, presents probabilistic predictions may not automatically imply intrinsic randomness. The apparent randomness may stem from an incomplete knowledge of the system or a limitation of the formalism, in which a yet to be developed theory could wholly describe the process [81, 199]. In effect, these sequences could be completely predictable to whom ever wants to eavesdrop, given that they have access to the complete information of the system or algorithm. This brings into question the security of its application: a deterministic method will always generate the same pseudo-random number given the same initial seed and conditions, making the generated sequence vulnerable to interception. These methods are thus considered insufficient and insecure, pointing towards the irreproducibility and probabilistic nature of quantum physics as a certification of genuine randomness [200].

Broadly speaking, two subcategories of QRNGs exist: trusted device QRNGs, in which a simple but fixed system outputs RNs at a generally high rate and low cost. This system, however, assumes that the device's manufacturer is fully trusted. On the other hand, device-independent 'self-testing' QRNGs exist, in which the quantum randomness is verified using an entanglement witness or non-local Bell inequality violation. Such devices, however, are often extremely inefficient and require initial random seeds [201]. What is certain, however, is that most QRNGs arise from the field of optics, including optical parametric oscillators [202], spontaneous Raman scattering [203], amplified spontaneous emission [204, 205], laser phase noise [206] and quantum vacuum fluctuations [207]. The most common practice involves extracting random bit sequences from the Poissonian statistics intrinsic to the photon emission and detection processes [208–211]. An in-depth review of RNGs based on optical sources can be found in Ref. [212].

More recently, non-local correlations exhibited between entangled particles have been shown to have intrinsically random properties [213, 214], in that measuring these correlations it is possible to non-deterministically extract the inherent random sequences. The simplest of experiments utilising non-locality involves a single photon state $|1\rangle_A|0\rangle_B$ incident on one of two input ports, A or B, of a lossless 50:50 beam splitter. The final state at the output ports of the beam splitter can be expressed as a quantum entangled superposition,

$$|\psi\rangle = \frac{1}{\sqrt{2}}(|1\rangle_C|0\rangle_D + |0\rangle_C|1\rangle_D), \tag{4.1}$$

where the subscripts C and D represent the reflected and transmitted output ports of the beam splitter, respectively. Single photon detectors placed at each output thus perform a projection measurement on the quantum state, such that when detector C (D) registers a photon, we know that the state has collapsed to state $|1\rangle_C|0\rangle_D$ ($|0\rangle_C|1\rangle_D$). A random bit '1' is generated when a photon is registered at detector C and a '0' is generated by a detection at detector D. This implies that single photons incident on the beam splitter, will either be transmitted or reflected, with a probability of $1/2$. In the context of quantum mechanics, it is impossible to predict which port the photon will exit. It follows that the randomness is accessed by projection measurements on a quantum superposition state. This process is non-deterministic and intrinsically random, making it a suitable process for QRNG.

Furthermore, there are various quantum state parameters in which non-locality has been observed and optically implemented to generate random numbers, including polarisation entangled states [215], photon arrival time [216], path branching [217], photon counting detection [218, 219] and observed statistics in bipartite Bell scenario [220]. While these protocols are effective in generating high quality random numbers with assured unpredictability,

practical limitations arise from the efficiency to generate and detect these quantum superposition states. Optical components and detectors are not ideal and may introduce unwanted bias into the system affecting the randomness of the generated sequence. These noises can be detrimental to the system, particularly for cryptographic applications, where they may be known or controlled by an advisory trying to eavesdrop on the system.

Although these protocols are effective in generating high quality unpredictable bits, limitations exist. Firstly, optical transmission and detection systems are often inherently asymmetric and introduce unwanted, detrimental bias in the generated bits. This affects the overall randomness of a string. To counter this, post-measurement algorithms do exist to balance the ratio of 0s to 1s. The simplest algorithm, von Neumann [221], involves grouping two successive bits together, forming four possible pairs 00, 01, 10 and 11. If the two bits are the same, they are discarded and if they are different, the first bit is kept as part of the unbiased sequence. This algorithm is terribly inefficient, resulting in a sequence that is at most 25% the length of the original sequence. While there are complex protocols with improved efficiencies [222], unbiasing measures are still inefficient and preclude real-time, clean RN generation. So, a system allowing for dynamic control of the bias during the generation process - without compromising the 'quantumness' of the protocol - is beneficial (in fact, unbalancing the ratios of 0s to 1s has some important cryptographic applications [223, 224]). The protocol, presented herein is such a system.

Additionally, in many optical QRNGs, the rate at which the random numbers are generated is bounded by the fact that each detection will at most generate only one random bit. Coupled with the low efficiency of single photon sources and the low photon counting abilities and detector dead times, these schemes remain very slow for most practical applications. While detectors with shorter dead times and more efficient single photon sources can be used, a proactive solution has been to try and increase the number of bits generated per detection event. This has been proposed using single qubit quantum walks [225] and more recently, implemented by measuring the arrival positions of photons [226].

To this end, here we propose a quantum photonic scheme focusing on photons entangled in their OAM degrees of freedom to generate random numbers. We first demonstrate a path branching setup in which, in place of the archetypal beam splitter, a spatial light modulator (SLM) is employed to completely probabilistically direct an incident photon from a down-converted SPDC pair into one of two optical paths (with the other photon functioning as a herald). The use of an SLM allows for projective measurements providing full control by digital holograms over the probability of the incident photon choosing either path. Specifically, one can create and remove bias on-the-fly by scaling the digital hologram masked on the SLM screen.

Next, we consider the potential of using two photon states which are entangled in their OAM degree of freedom. By projecting a photon onto OAM-dependent paths (with the other still acting as the heralding photon), we are able to generate sufficiently random bits given various OAM combinations. The SLM employed in this OAM-based QRNG still easily allows dynamic system unbiasing (based on the initial spiral bandwidth of the down-converted photon pair). Furthermore, OAM opens up the high-dimensional state space. This approach can hence be extended to generate multiple bits per photon detection, overcoming the low bit-rate limitations set by the generation and detection efficiencies of the equipment.

4.2 Quantifying randomness

The concept of randomness has been a deep philosophical problem where numerous philosophers have argued the concept of something truly random existing, however we will not attempt to solve such a debate. It is, however, impossible to design a random number generator without knowing the properties of the output we wish to achieve. As such we attempt to define randomness in the context of quantum cryptography and in doing so, we explore various methods used to characterise the randomness of a QRNG system.

Knuth, a pioneer in random number generation put forth the idea that there is no such thing as a random number [227]. While this seems absurd, he reasoned that in the extreme case, it's like asking whether the number 0 is more inherently random than the number 1. He proposed that in order to define randomness we should rather consider a sequence of independent random numbers. As such, we use the term random number and random sequence interchangeably, to mean a sequence of random numbers. It should also be noted that we will only consider the randomness of binary numbers because if a sequence of binary numbers is confirmed to be random, then it is also true of its transformation to any other base interval.

In the simplest of examples, a random sequence could be explained as a series of fair coin flips, where the sides of the coin are labelled 1 and 0 and are equally probable. It then follows that we expect a series of coin flips to be uniformly distributed, lacking any correlation or bias, however, this can be tailored to any desired probability distribution. More importantly, the result of any previous or future coin flip has no effect on the outcome of the present flip, the flips can be said to be independent of each other. Additionally, a random sequence should have full (forward and backward) irreproducibility. As such, the following working definition is proposed: A random key is a sequence of bits that is independent, unpredictable, and follows the desired probability distribution, such that it can not be reproduced.

Before designing and subsequently characterising a quantum random number generator, one needs a basic understanding of the mathematics behind the 'randomness' of a string of

numbers as well as how to measure its uncertainty. An ideal random string of length n, in base d where d is the dimensional of the system, is a sequence of n values independently drawn according to a discrete uniform distribution from the set $[0, 1, \cdots, d-1]$. The sequence elements necessarily need to be drawn independently of one another: it should be impossible to predict the subsequent element in the sequence, even with sight of all previous elements [228]. In base 2, the situation corresponds with n trials of throwing a two-sided unbiased coin. Despite the fact that humans tend to have an intuitive understanding of the concept of 'randomness', its study remains ongoing and there are hence alternative ways of defining and understanding it. For example, *Kolmogorov randomness* posits that a string is only fully random if a computer programme needed to reproduce the string is longer than the string itself [229], whereas information theory typically takes random numbers to be those which maximise a chosen measure of the information entropy of the numbers [230].

Statistical hypothesis testing is one of the most widely used methods to assess whether a sequence is indeed random [231, 232]. Given an appropriate model of the random number generator as well as a dataset of strings arising from it, hypothesis testing applies unbiased analytical tests to the dataset to gauge whether the generator itself tends to output sufficiently random strings. We use the term "sufficiently random" because no amount of hypothesis testing can definitely prove that the process, by which the sequence was generated, is inherently random and irreproducible. While this method is the most popular due to its accessibility and computation time, it does not give a quantifiable measure of randomness. To an extent, the tests only offer a elementary 'pass or fail' assessment to improve our confidence that the generator is producing numbers that have characteristics reminiscent of randomness [233]. However, the increasing consequence of secure communication protocols and the many physical techniques used to generate the required random number seeds, necessitates a set of evaluation metrics for randomness [234]. The intrinsic entropy of a quantum system has been shown to be related to the random outcomes of projection measurements on a quantum superposition state [235], and as such we use entropy as our measure of randomness. While there is no widely accepted entropy estimation standard, we explore Shannon entropy as a quantifiable and comparable measure of the randomness of the generation process.

4.2.1 Statistical test suites

Statistical hypothesis testing takes a sample sequence from a RNG and subjects it to variety of analytical tests. These tests assess the sequence for particular properties that a true random sequence should exhibit. Each test outputs a probability value that, if higher than a preset threshold, can highlight potential flaws and in the process rescind RNGs that are not fit for specific applications. Seeing that a random sequence can appear to have varying properties

of non-randomness, a single statistical test is inadequate, necessitating a battery of tests for determining if a sequence is random.

There are many statistical test suites available, such as the John Walker's ENT [236], Dieharder [237] or the well known NIST-800 22a Statistical Test Suite [18]. While each test suite is different, they all are formulated to check for specific characteristics of a random sequence. Particularly, they test for uniformity (i.e., the occurrence of a 0 or 1 is equally probable at every point in the sequence) and consistency (i.e., a random subsequence should also be random).

It should be noted that while there are many available tests, any finite set of tests can overlook hidden correlations since an infinite number of tests exist for finding said correlations. As such, no particular test suite can be deemed complete and no amount of testing can guarantee that a RNG is unfailing [233]. Nevertheless, the test suites do increase our confidence in the randomness of the generated sequence and can help detect any weaknesses that the RNG may have.

While statistical tests do not offer a means to quantify randomness, we will be subjecting our generated random numbers to a statistical test suite as a means to confirm that they are random. Having considered the many statistical test suites available, the NIST Statistical Test Suite (NIST 800-22a) was chosen, mainly for the pragmatic reason that it is recognised as the industry standard and formulated from comprehensive theoretical and experimental analysis. It is also comprised of the most stringent tests designed to test RNGs for cryptographic applications [18].

NIST Statistical test suite

The NIST Statistical Test Suite contains 15 analytical tests developed to examine binary sequences for qualities exhibiting randomness. These tests can be summarised into the most basic types:

- Frequency tests: calculates the proportion of 0s and 1s for the whole sequence, as well as subsequences extracted at random.
- Runs tests: examines if the number of runs (i.e., successive sequences of the 1s (0s) are bounded by 0s (1s)) is consistent with that of an ideal random sequence. In other words, it verifies if the RNG is oscillating too slow or too fast between 0s and 1s.
- Spectral tests: detects periodic features in the sequence.
- Autocorrelation tests: checks the sequence for correlations with a shifted version of itself.
- Maurer's Universal Statistical test: checks if the sequence can be condensed without losing information.

The measured statistics of each test are converted to a p-value using a reference distribution (usually a χ^2 distribution). P-values can be interpreted as the likelihood that an ideal RNG would have generated a sequence less random than the tested sequence [238]. This means that an ideally random sequence results in a p-value of 1, and conversely a p-value is 0 describes a sequence that appears to not be random at all. Therefore, we can evaluate the test results by comparing the p-value to a significance level α, set by the required security level of the application at hand. The significance level can be thought of as the probability that the test will deny a perfectly random sequence as being random, such that a p-value greater than α accepts the hypothesis and a p-value less than α rejects the hypothesis. Thus, for a confidence threshold of $\alpha = 0.01$, on average one in 100 sequences from an ideal RNG will fail the tests by chance. However, it should be noted that statistical tests usually only test the outputted sequences (and don't include any modelling of the random number generator itself) and hence, at best, can be viewed as sanity checks against obvious flaws rather than being definitive proof of randomness. Moreover, the tests cannot be used as a comparative measure, in that a random sequence that receives higher p-values cannot conclusively be said to be more random than one that received lower p-values. In the end, the p-value determines if the RNG passes that specific test, given that it falls within an threshold value set by the examiner.

4.2.2 Entropy as a measure of randomness

Statistical tests suites can be used to provide a guarantee of statistical properties, however they cannot absolutely assure that the generation process is naturally random and unrepeatable. Thus, it remains essential to assess and quantify the randomness of the generation process behind a random number sequence [239].

A notion closely related to that of entropy in information theoretical contexts is that of *self-information*, which can intuitively be understood as the amount of information learned when observing a value x of a random variable X. The pioneer of information theory, Claude Shannon, required self-information to meet a few intuitive axioms [240]:

- An event certain to occur yields no new information: $I(p = 1) = 0$
- The more unlikely an event is to occur, the more information it's observance gives, with this increase in information being continuous and positive: $I(p_1) \leq I(p_2)$ if $p_2 \leq p_1$, with $I(p) \geq 0 \; \forall \; p \in [0,1]$
- The information gained from observing two independent events is the sum of their individual self-information: $I(p_1 \times p_2) = I(p_1) + I(p_2)$

Up to a multiplicative factor, there is a unique function which meets these axioms: given a random variable X, with possible outcomes x_i and a probability distribution $P_X\{x_i\} = p_i$ for $i = 1, 2, ..., d$, the self-information, $I_X(x_i)$, is given by [240, 230]

$$I_X(x_i) = -\log_d(p_i). \tag{4.2}$$

For our case, $d = 2$, hence I_X is measured in *bits*. With this in mind, Shannon defined the Shannon entropy, $\mathrm{H}(X)$, of the random variable X to be the expectation value of self-information, i.e.

$$\mathrm{H}(X) = -\sum_i p_i \log_2(p_i). \tag{4.3}$$

Shannon entropy is a measure of how informative a random variable X is: it can easily be seen that perfectly random events (i.e. those where p_i is the same for all outcomes x_i) maximise H, whereas perfectly predictable events (those for which p_i is either always 0 or 1) minimise it. Hence, it indicates the associated uncertainty in trying to predict the observed outcome, such that a higher entropy results in a greater uncertainty in predicting the outcome. Additionally, if the entropy is close to $\log_2 d$, where d is the dimension of the system corresponding to the number of possible outcomes, it means we have a nearly uniform distribution and can almost extract all of the random bits from the system.

For example, consider a fair coin toss with $d = 2$ possible outcomes, heads or tails. We need $\log_2 2 = 1$ bits to represent each outcome, either 0 or 1 respectively. If each outcome is equally probable, then the entropy of a coin toss is maximum. It follows that it is impossible to predict the outcome of the coin toss better than purely guessing, resulting in each outcome of the coin toss containing one bit of information. In contrast, a coin toss using a biased coin that always lands heads up, will have an entropy of zero as the outcome can be perfectly predicted each time. Evidently, a uniform probability distribution then requires all bits to encode the information and non-uniform distributions require less bits. In effect, an event that occurs more often is less informative then a less frequent event.

In principle, entropy is a bridge between the highly simplified description of a coin toss game in terms of a single probability and the extremely complicated description of the game in terms of the probability of a sequence of individual tosses. While there is no widely established entropy estimation standard, NIST is in the process of developing a new set of evaluation standards [241]. In information theory, Shannon entropy is used to quantify the uncertainty inherent in a sequence of possible outcomes and as we will see, it provides us with the mean number of random bits that can be extracted from a single measurement result.

In our quantum system, the randomness manifests in the purely probabilistic outcomes of projective measurements on a state ρ. Furthermore, in a quantum setting, the notion of

Shannon entropy above can be extended to that of the Von Neumann entropy S [242], given by $S = -\mathrm{Tr}(\rho \log \rho)$. This formula holds given any arbitrary state ρ, expressed in any basis. However, ρ necessarily admits the spectral decomposition $\rho = \sum_i c_i |i\rangle \langle i|$, with $|i\rangle$ the state's eigenvectors and c_i real [243]. The state ρ is hence diagonal when expressed in its eigenvector basis, with diagonal entries $\{c_i\}$, and it can be shown that the formula for S reduces to that for the Shannon entropy given in Eq. 4.3, i.e.

$$S(\rho) = -\sum_i c_i \log_2(c_i). \tag{4.4}$$

Furthermore, the entropy of a state is an intrinsic property and hence basis-independent. However, Eq. 4.4's simplicity highlights the value of expressing a state in its eigenvector basis: ρ is a probabilistic mixture of pure eigenstates $|i\rangle \langle i|$ with the diagonal elements c_i quantifying the various contributions. Hence, the set $\{c_i\}$ completely determines the randomness of our system.

When working in cryptography or randomness extraction, another oft-used entropy measure, is the so-called 'min-entropy', defined as

$$\mathrm{H}_{\min} = -\log_2(\max_i\{p_i\}), \tag{4.5}$$

i.e. the negative base-2 logarithm of the largest probability p_i. This yields a worst case bound on the entropy, i.e., the lower limit of randomness that can be extracted. It can be shown that this measure always bounds the Shannon entropy from below and will hence be considered in what follows since it is a more cautious estimate of a system's randomness.

4.3 Experimental realisation

The optical setup we employed, shown in Fig. 4.1, is a variation of a widely-adopted QRNG scheme based on path branching, as outlined in [217]. Originally, this RN generator was built by using a beam splitter (BS) to create a state consisting of a superposition of two states labelled with path information. To allow for more control over both the incident beam as well as the random number statistics, we instead used a phase-only Holoeye Pluto-2 spatial light modulator (SLM) to probabilistically split the incident photons into the two paths, mimicking the action of a beam splitter.

A 355 nm mode-locked Vanguard UV laser, directed onto a non-linear β-barium borate (BBO) crystal, resulted in a pair of degenerate Type-I entangled photons. The entangled photons

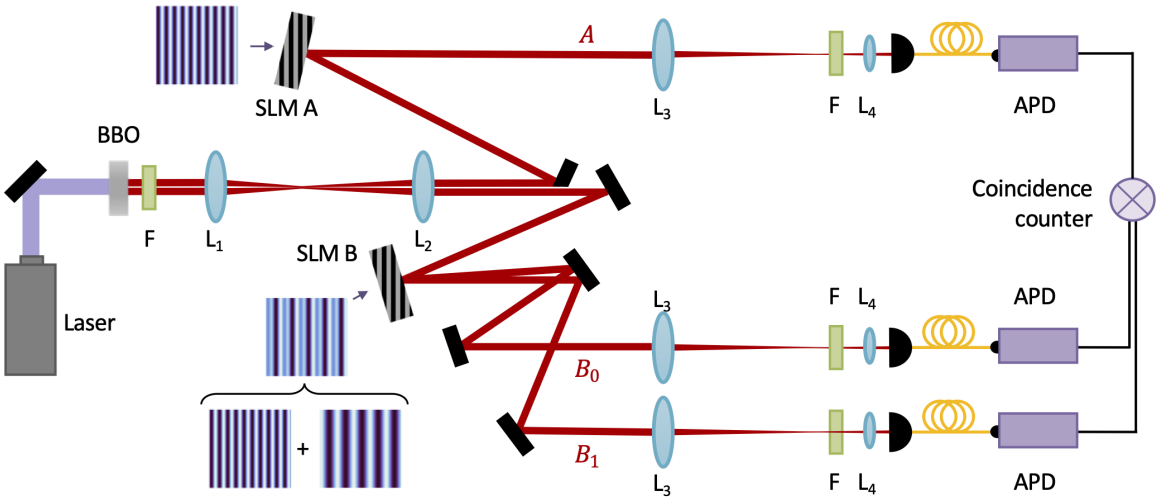

Fig. 4.1 Experimental setup for generating random numbers by projecting photons onto a superposition of paths using a spatial light modulator (SLM). After down-conversion, the photon pair is split into two paths. The path A photon acts as the heralding photon for that in path B, which itself is further split into paths B_0 and B_1, by way of an SLM. A random bit is generated by detecting a coincidence between photon A, and either the photon in path B_0 or B_1. F = filter, L_1 = 200 mm, L_2 = 400 mm, L_3 = 500 mm, L_4 = 2 mm.

were then spatially separated into paths A and B using a D-shaped mirror. The crystal plane was imaged onto an SLM placed in each arm.

To separate the modulated light (in the first order) from unmodulated light, a holographic diffraction grating was added to SLM A. Photons in path A functioned as the heralding photons. SLM B, however, was masked with a juxtaposition of TWO diffraction gratings, each with different periodic spacings, instead of a single grating. This causes a photon in path B, incident on SLM B, to be directed down one of two paths, B_0 or B_1 (see Fig. 4.1). This choice of paths occurs completely probabilistically, with the probabilities themselves controlled by modulating the respective grating depths (i.e. the diffraction efficiencies) of the gratings comprising the juxtaposed SLM B mask: altering the grating depths alters the proportion of incident light diffracted into the first order of either grating.

To be more specific, if one is given a diffraction grating hologram with a maximum possible phase depth of 2π within some local region, subsequently scaling the phase range of the pixel at transverse position (x,y) by a factor of $M(x,y)$ (where $M \in [0,1]$) splits the diffracted light into multiple orders according to [113]

$$|c_n(x,y)|^2 = \mathrm{sinc}^2\left(\pi(n - M(x,y))\right), \tag{4.6}$$

where n is the diffraction order, and $|c_n|^2$ the fraction of power in said n^{th} order [244]. For the first order ($n = 1$), reducing the phase depth across the entire hologram directs a greater proportion of the incident photons out of the first order. Thus, in the case of two juxtaposed gratings corresponding to paths B_0 and B_1, we can digitally control any bias in the system to achieve the desired ratio of photons in each path. This makes it easy to account for experimental imperfections in the system such as asymmetric detector efficiencies and different optical losses in each arm. Furthermore, this also eliminates the need to consider cumbersome randomness distillation algorithms.

After the SLMs, lenses in the three paths coupled the photons to fibres connected to PerkinElmer avalanche photodiodes (APDs), which output an electronic pulse signal for every detection event observed. A Hydraharp 400 time-tagged each pulse (with a resolution of 1 ps), creating a record of both the time as well as the path in which the detection event occurred. To extract photon coincidences, one then simply reconciles the overlapping APD pulses separately arising from a photon detection in either arm B_0 or B_1, with a pulse in arm A. Photon A, as the trigger, causes either of the other two detectors to register a corresponding entangled photon, if the arrival time lies within a small interval. This is a close approximation to a localised single photon state [245].

The resultant data was post-processed to generate random bits: two detectors were said to have detected a pair of entangled photons in coincidence if a single photon was tagged at each respective detector, with the corresponding arrival times differing by a maximum of 25 ns (minimising false coincidence count positives). If detectors A and B_0 each registered a photon with the arrival times differing by less than 25 ns, a '0' was appended to our random bit string. Likewise, a '1' was added for a detector $A - B_1$ coincidence. This entire process was fully automated using *LabVIEW*.

Finally, it should be noted that an unbiased system will register the same number of events in each of the B arms, the sum of which should ideally equal the number of events in arm A. Also, although the down-conversion efficiency of the crystal and the extraction algorithm itself affect the protocol's efficiency, the most significant bottleneck in the RN generation rate is usually the single photon APDs [201].

QRNG using entangled OAM modes

Our proposed random number generator, which operates on the quantum level, measures aspects of pairs of photons entangled via spontaneous parametric down conversion (SPDC) [246]. As discussed in the previous chapter, we choose the well-known Laguerre-Gaussian (LG) modes, $LG_p^{\ell}(\mathbf{q})$, as the complete basis for the vector space of each photon [163]. Since, our experimental projective measurement process is sensitive only to different OAM charges

and hence implicitly projects onto only the $p = 0$ radial index. Designating the signal (idler) photon paths with an A (B) subscript, the prepared SPDC state is hence

$$|\psi_{\text{SPDC}}\rangle = \sum_{\ell} C_{\ell} |\ell\rangle_A |-\ell\rangle_B , \tag{4.7}$$

with C_ℓ the probability amplitude weighting for the $|\ell\rangle_A |-\ell\rangle_B$ state. Therefore, performing a joint coincidence measurement on the state $|m\rangle_A |-m\rangle_B$ (i.e. projecting onto state $|m\rangle$ and $|-m\rangle$ in the signal and idler arms, respectively) picks out the corresponding amplitude C_m. Therefore, the probability of measuring the state $|\psi_{\text{SPDC}}\rangle$ to be in the ℓ^{th} mode is given by $|C_\ell|^2$.

Using this description, we explore the spatial mode entanglement of two photon states to generate random numbers. This only requires changing the single mode fibre in path A to a multi mode fibre. This couples the multiple OAM states generated by the SPDC state, not only the Gaussian component. By projecting photon B onto one of two OAM dependent paths, such that ℓ_0 photons are mapped to B_0, and ℓ_1 photons are mapped to path B_1, we can generate random numbers for various ℓ_0 and ℓ_1 combinations. The probability ratio of generating 0s and 1s is thus given by $|C_{\ell_0}|^2/|C_{\ell_1}|^2$. When the ratio is equal to 1 the proportion of 1s and 0s is equal, indicating maximum randomness. We use this to tailor the ratio according to the discrete OAM contributions C_ℓ from our SPDC system, while simultaneously insuring the unpredictability and irreproducibility of the system.

4.4 Results and discussion

4.4.1 Random numbers from path information

Random sequences were first generated using the experimental setup of Fig. 4.1. An ideal random sequence should be unbiased in the ratio of its bits. However, this was, perhaps unsurprisingly, not the case initially: experimental disparities between the arms gave unequal coincidence detection probabilities, p_0 and p_1, between the detector pairs $A - B_0$ and $A - B_1$, respectively. The bias ratio, $R = p_0/p_1$, would be 1 for a perfectly unbiased system. Initially, this ratio was found to be $R = 0.8518 \pm 0.0014$ (so arm B_1 was slightly favoured), resulting in a min-entropy of $\text{H}_{\text{min}} = 0.8889 \pm 0.0012$ bits, as per Eq. 4.5. While a small error in certain contexts, the batteries of randomness tests typically pick up on such small biases of this magnitude. A generated RN sequence (which was 1Mb in length), when subjected to the NIST test suite, failed to pass three of the 15 statistical tests as per Fig. 4.2(a), with p-values well below the chosen significance level of $\alpha = 0.01$ (a level typical for cryptographic applications [228]). Such a discrepancy in the system, even if relatively small, greatly affects

the randomness of the generation process, requiring many QRNG protocols to apply numerical unbiasing techniques to extract clean randomness from imperfect data [222]. Such an extra step is often inefficient and retards the generation rate by necessitating the consumption of some quality random bits.

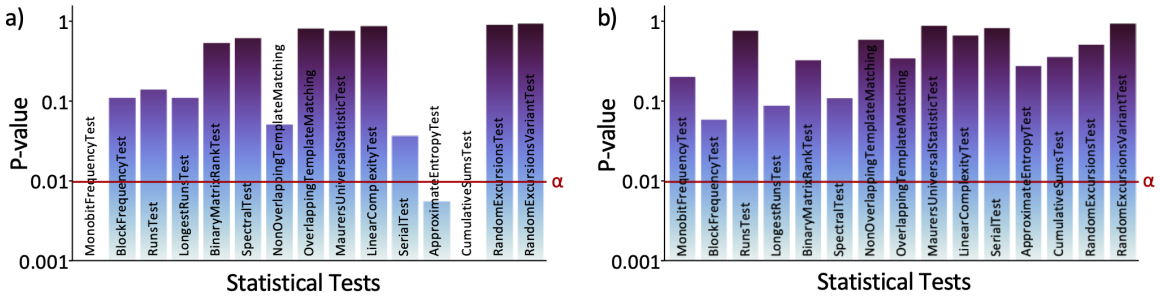

Fig. 4.2 NIST statistical test suite results for a 1 Mb sequence generated by a) the initial QRNG, with inherent experimental disparities, and b) the unbiased QRNG, compensated by adjusting the SLM phase grating. P-values above the significance level set at $\alpha = 0.01$, pass the test, confirming the absence of patterns in the string.

To overcome this, we alter the diffraction efficiency of the more favoured arm (B_1) by changing the phase grating depth of the SLM hologram, as per Eq. 4.6. The SLM employed here was calibrated to display 8-bit grey scale images representative of a total possible phase change of 2π. Scaling the grating depth of arm B_1 by a factor $M \in [0,1]$ decreases the probability p_1 only, and hence the overall bias. So, $p_1 \to p_1' = p_1|c_1|^2$, while $p_0 \to p_0' = p_0$. After renormalising the probabilities such that $p_0' + p_1' = 1$ (since scaling M causes photons to leak into higher diffraction orders, which are discarded), we have

$$p_1' = \frac{p_1|c_1|^2}{p_0 + p_1|c_1|^2} = \frac{\text{sinc}^2(\pi(1-M))}{R + \text{sinc}^2(\pi(1-M))}. \tag{4.8}$$

The min-entropy of the altered system is then $\text{H}_{\text{min}} = -\log_2(\max\{p_0', p_1'\})$. The effect of a change in grating depth, M, on the entropy of a system with an initial bias ratio R is depicted in Fig. 4.3(a), with experimental results shown in Fig. 4.3(b). The data points in (b) concur with the expected trend of a system with an initial bias of $R = 0.8518 \pm 0.0014$. Given this, to maximise the entropy, the count rate (detection probability) of arm B_1 needs to decrease to match that of arm B_0. This was calculated to occur when the grating in arm B_1 is scaled by a factor of $M = 0.7812$. Finally, it follows that since the typical resolution of the SLM is $1/256$ (corresponding to a phase variation of 2π) for our 8-bit grey scale holograms, we can alter the

grating depth of the system to achieve a min-entropy error of approximately

$$\delta \mathrm{H}_{\min} \approx \delta M \left.\frac{\partial \mathrm{H}_{\min}}{\partial M}\right|_{\substack{R=0.8518,\\ M=0.7812}} = \frac{1}{256} \times 1.0727 \approx 0.0043. \tag{4.9}$$

In practice, the detection probabilities of both arms were altered such that a bias ratio of $R' = p'_0/p'_1 = 0.9988 \pm 0.0014$ was achieved, corresponding to a min-entropy of $\mathrm{H}_{\min} = 0.9991 \pm 0.0003$ bits per photon for the corrected system.

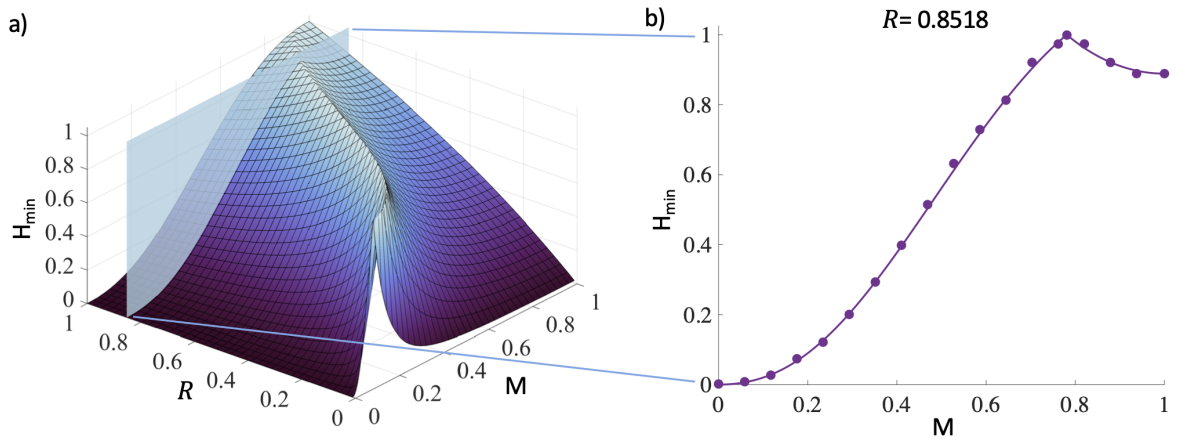

Fig. 4.3 a) The min-entropy theoretically derived from our QRNG as a function of both the grating scaling, M, and the bias ratio, R. For the initial bias in the system, with $R = 0.8518 \pm 0.0014$, inset b) shows how the min-entropy depends on the grating scaling. The grating scaling at which the min-entropy is maximised occurs at $M = 0.7812$, at which point the min-entropy is $\mathrm{H}_{\min} = 0.9991 \pm 0.0003$ bits per bit. This is confirmed by the experimental measurement points; the error bars are too small to be shown at this scale.

The application of this step resulted in a bit bias ratio small enough for the generated string (which, unprocessed, was 1 Mb long) to pass the NIST statistical test suite, Fig. 4.2(b): the p-values for the various tests were all greater than the chosen significance level of $\alpha = 0.01$. This absence of patterns in the string gives credence to the randomness hypothesis for our random number generator. However, although increasing our confidence in the generator, such statistical tests cannot be used as a comparative measure between different generators.

Our system achieved a bit generation rate of 24 kHz for Gaussian mode detection using single mode fibres, reaching up to 0.46 MHz with multi-mode fibres. Although, optics-based QRNGs have achieved higher bit rates [201], such studies often require unbiasing post-processing procedures which significantly reduced their effective bit rate. Our use of SLMs forwent such unbiasing requirements.

While the bit rate could be increased using more efficient sources and equipment, it still remains practically limited by the time resolution of the detectors. Furthermore, one of the most efficient ways of increasing the bit rate of a randomness generator is by measuring a high-dimensional Hilbert space [201], in which more than one bit of entropy is extracted per detection event. The inclusion of SLMs to dynamically control efficiencies in a higher-dimensional optical QRNG could easily allow for automatic, real-time unbiasing. This in turn potentially allows for the real-time generation of random strings, a feature missing in most contemporary randomness generator studies.

4.4.2 Random numbers from OAM

Finally, we explore the proposed protocol in which we spatially project onto transverse profiles of single photons to realise a QRNG based on the OAM entanglement of down-converted photon pairs. To do this, the SLM in arm B was masked with superpositions of Laguerre-Gaussian mode holograms and appropriate diffraction gratings to separate the incident photons into OAM-dependent paths (as well as account for inherent bias in the system). By performing these projective measurements on the photons in arm B and coupling only the desired Gaussian mode using single mode fibres, allows us to post-select the desired photon state - a well established spatial mode detection technique [116]. The detection of the photons in arm A, by way of a multi-mode fibre, ensures that we are able to herald the detection of the photons in arm B without having to modulate photons in arm A and losing the coincidence counts between the detectors.

First, the mode availability in each arm of the RN generator was characterised by spiral bandwidth measurements, i.e., iteratively performing a set of OAM projections in each pair of arms. The normalised coincidence counts for each arm are given in Fig. 4.4. The full-width-half-max values of 19 in each arm indicate a large number of the various OAM basis modes were correlated. Using these experimental coincidence counts, it is possible to estimate the entropy of the system given chosen OAM projections in the arms. Indeed, after balancing the juxtaposed gratings on SLM B such that it is equally likely for an incident photon to choose either arm B_0 or B_1 (as we have shown above), if we project a photon in path B_0 onto an ℓ_{B_0} eigenstate, and an independent photon in path B_1 onto an ℓ_{B_1} eigenstate (they're independent since a photon in path B only traverses one of the two subpaths), the min-entropy is $\mathrm{H}_{\min} \equiv \mathrm{H}_{\min}(\ell_{B_0}, \ell_{B_1})$, since the probabilities p_0, p_1 in general depend on the modes we project the paths into, namely ℓ_{B_0}, ℓ_{B_1}, in addition to the projection mode in arm A, ℓ_A. So, $p_0 \equiv p(0|\ell_{B_0}, \ell_{B_1}, \ell_A)$, and similarly for p_1. Photon A, however, simply functions as a heralding photon and when estimating the min-entropy conditional on ℓ_{B_0}, ℓ_{B_1}, we in essence use marginal

probabilities with the photon A mode 'traced out', i.e. summed over, so

$$p(0/1|\ell_{B_0},\ell_{B_1}) = \sum_{\ell_A} p(0/1|\ell_{B_0},\ell_{B_1},\ell_A) \tag{4.10}$$

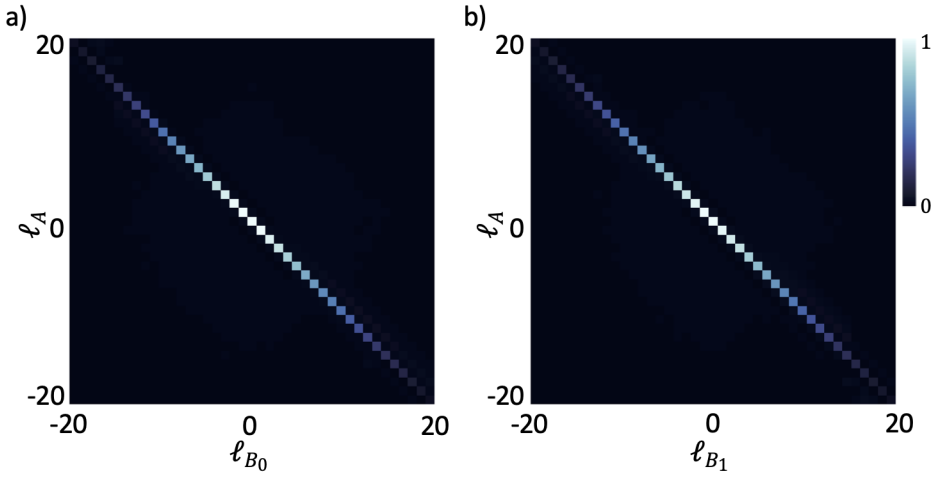

Fig. 4.4 Normalised coincidence counts for a) arm B_0 and b) arm B_1, for different projected OAM values. Each arm had a FWHM value of 19, indicative of a high degree of OAM correlation between the A and B photons.

Furthermore, the probability of measuring a 0 does not depend on the chosen projection mode for arm B_1, since we only measure a 0 if the photon traversed arm B_0, in which case it doesn't matter what value was chosen for ℓ_{B_1}. We hence assert that

$$p(0|\ell_{B_0},\ell_{B_1}) \equiv p(0|\ell_{B_0}), \tag{4.11}$$

and similarly when observing a 1. Finally, since the probability of observing a 0 or 1 is proportional to the spiral bandwidth coincidence counts of each arm, we can estimate $p(0|\ell_{B_0})$ and $p(1|\ell_{B_1})$ by respectively summing the coincidence counts in Fig. 4.4(a) and (b) over the ℓ_A values (assuming a reasonable cutoff) and normalising by their combined sum. Similarly, the estimated normalised bit generation rate is found by summing the coincidence counts over ℓ_A for both ℓ_{B_0} and ℓ_{B_1} contributions and normalising by the maximum bit generation rate of all OAM combinations. Correspondingly, we arrive at the min-entropy values and the generation rates, conditional on ℓ_{B_0},ℓ_{B_1}, as given in Fig. 4.5(a).

We experimentally generate various random number strings for a subset of OAM projections, i.e., $\ell_{B_0} = 4$ and $\ell_{B_1} = [-20,20]$. The experimental bit generation rates and min-entropy values, are shown in Fig. 4.5(b) and (c), corresponding to their estimated values. From this, we see

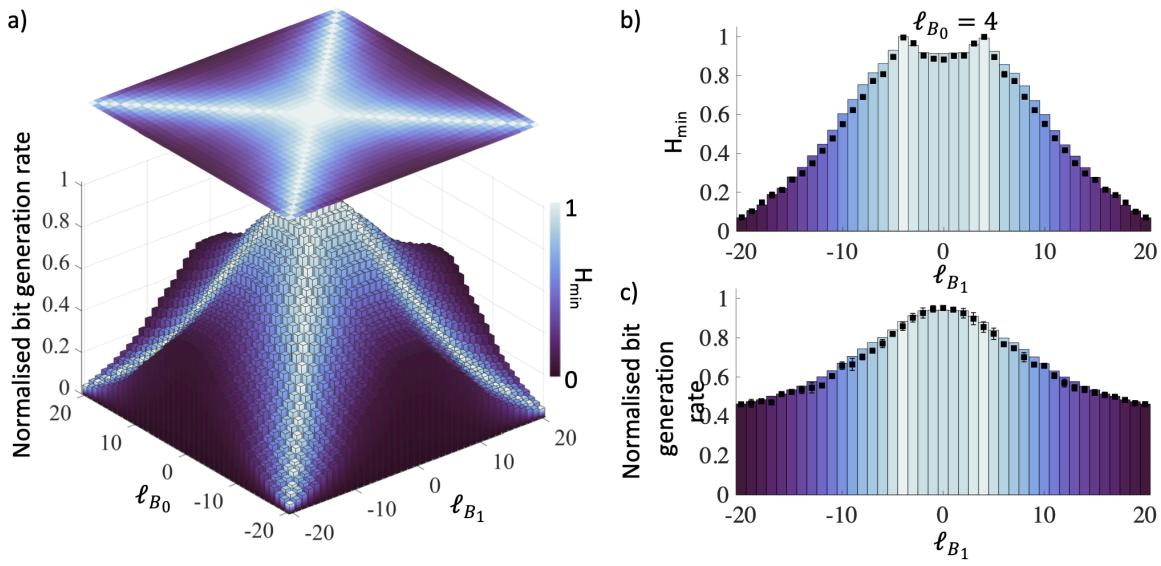

Fig. 4.5 a) Min-entropy (colour) and normalised bit generation rate (z-axis) as function of OAM projection combinations, calculated from the spiral bandwidth measurements. Experimental results for a subset of OAM values, $\ell_{B_0} = 4$, $\ell_{B_1} = [-20, 20]$, showing the b) min-entropy and c) bit generation rates extracted from generated random number strings. The bars correspond to the estimated values from a).

that projecting the two B subpaths onto OAM states with equal topological charge magnitudes (i.e. $|\ell_{B_0}| = |\ell_{B_1}|$) results in the highest achievable min-entropy of 1 bit per detection. This is unsurprising considering OAM momentum conservation, which ensures an equal probability of the conjugate OAM state in either arm. Since the SPDC state roughly follows a normal distribution in the OAM modes, projecting onto higher OAM charges results in a lower detection probability and hence a lower bit generation rate, as in Fig. 4.5(c). Accordingly, projecting the photon states onto increasingly mismatched OAM values (i.e. states with larger differences in their absolute OAM values) lowers the corresponding bit generation rate and entropy.

Thus, by projecting the photons onto any combination of OAM values one can tailor the ratio of 0s to 1s and consequently alter the observed entropy of the system. This comes at the cost of a reduced bit generation rate. One can conceive of a system in which this OAM projection could be used, similar to altering the phase grating depth, to unbias any inherent asymmetries of the system or perhaps to discretely tailor the ratio of 0s and 1s to a desired distribution, in which case a measured sequence NOT following said distribution highlights the potential presence of an adversary. This could be done all the while maintaining the irreproducibility inherent in the quantum system.

For cryptographic and randomness purposes, often a uniform probability distribution, in which each outcome (here the OAM state) is equally likely to be observed upon measurement.

However, the OAM distribution of the down-converted state strongly depends on the profile of the pump field incident on the non-linear crystal. Further advances in the area of pump shaping could be incorporated to finely tailor the distribution and engineer the entropy [157]. The engineering of such a probability distribution from SPDC has been previously investigated, both theoretically and experimentally [247, 248], where the spiral bandwidth of the entangled photons has been shown to be dependent on the ratio of the pump waist to the photon pair waist.

Finally, given that orbital angular momentum values lie in a higher-dimensional Hilbert space (of dimension d), their easy manipulation suggests the possibility of exploiting their higher-dimensional state space to build a multi-bit QRNG. The amount of entropy one could then gain from each photon is $\log_2 d$. Any such demonstration would obviously be contingent on the ability of the system to discriminate between basis modes comprising a d-dimensional superposition of OAM states. While a setup similar to the one presented here (namely spatially separating photons with an SLM), a more efficient approach would perhaps entail using mode sorting to conformally map a photon's input OAM charge to a lateral spatial position [145] and the subsequent detection of such positions with an array of single photon detectors. This is an experimentally-feasible proposition.

4.5 Conclusion

In previous chapters, we carefully studied the quantum mechanical principles of entanglement and superposition. Using this knowledge, we proposed a QRNG based the random behaviour intrinsic to projective measurements on a superposition of quantum states of light. Many of the existing QRNG protocols extract random numbers from Poissonian statistics intrinsic to photon emission and detection processes. Our approach is no different.

Our demonstration above was two-fold. Firstly, we demonstrated the integration of digital SLMs for holographic control of the randomness in an otherwise traditional optical QRNG scheme based on path information. This replaced the need for a traditional static beam splitter and easily allowed for the dynamic control of photon path direction and efficiencies. The latter can be easily tailored by simple hologram scaling, offering the ability to remedy any inherent asymmetries in the system and eliminating the need for inefficient or sluggish post experiment randomness extraction techniques. The strings generated from this RNG passed the complete NIST statistical test suite, despite being raw themselves.

Secondly, using holograms composed of gratings and spiral OAM masks, we implemented a QRNG based on the orbital angular momentum degree of freedom of entangled down-converted photon states. The use of spatial light modulators to project onto combinations of OAM charges allowed us to alter the bit generation rate as well as finely tune the bit bias of the generated

string, and in effect the entropy of the system while maintaining the irreproducibility of the quantum system.

This work is an important first step in realising an OAM-based, higher-dimensional QRNG. Two properties of an ideal QRNG would be a high bit generation rate, as well as real-time randomness generation (with no randomness extraction procedure required). The protocol here already includes the keys to the former, and modifying it to forgo the projective, iterative 'scanning' nature and instead incorporate equipment capable of discriminating the various OAM contribution immediately, opens up the latter.

Chapter 5

High-dimensional quantum secret sharing with spin-orbit structured photons

The work herein has been published in Ref. [101].

With the advent of quantum computing the current state of communication protocols is at risk. The way information is shared between a network of nodes has to transition to the quantum realm, in which the security is no longer subject to computational complexity but rather the probabilistic laws of quantum mechanics. Quantum secret sharing is a viable solution, allowing three or more parties to share secret information which can only be decrypted through collaboration. It complements quantum key distribution as a valuable resource for securely distributing information between multiple parties.

Here we realise the first experimental high-dimensional single photon QSS protocol using hybrid spin and orbital angular momentum states to access a high dimensional encoding space. To illustrate the versatility of our approach, we first demonstrate the protocol in two dimensions, extending the number of participants to ten, and then demonstrate the protocol in three dimensions with three participants, the highest realisation of participants and dimensions thus far. We demonstrate that our method is easily scalable in both dimension and participants. We reconstruct secret keys depicted as images with a fidelity of up to 0.979. Moreover, our scheme exploits the use of conventional linear optics to emulate the quantum gates needed for transitions between basis modes on a high dimensional Hilbert space, allowing us to exceed the 1 bit per photon limit of two-dimensional protocols. Our work offers a practical approach for sharing information across multiple parties, a crucial element of any quantum network.

5.1 Introduction

In a world where cloud computing environments dominate our lives, secure communication and key distribution between multiple parties is a growing concern. This includes the secure sharing of encryption keys, missile launch codes, bank account information and social media profiles. In popular cryptography methods either a single copy of the encryption key is kept in one location for maximum secrecy or multiple copies of the same key are kept in different locations for greater reliability, but at an increased security risk. Secret sharing, a multiparty communication technique, is a promising solution. In principle, a secret sharing protocols divides a secret and shares it among N parties, which can then be securely reconstructed through collaboration. This makes it ideal for storing and sharing information that is highly sensitive, achieving both high levels of privacy and reliability [249, 250].

However, with the current development in quantum computation, classical secret sharing implementations are becoming inadequate and do not provide the necessary resilience to eavesdropping attempts. Therefore, to increase the security, secret sharing has to be realised in a quantum regime, in which the security of the shared information is no longer subject to mathematical or computational complexity but rather quantum mechanical principles, particularly the no-cloning theory[9]. Quantum secret sharing (QSS) posses the salient feature of enabling multiple parties to share a secure key without compromising the secrecy of the information and further enabling the detection of eavesdropping [74, 251].

The first quantum secret sharing (QSS) scheme proposed the use of particle entangled states [29]. In this protocol, three parties (Alice, Bob and Charlie) randomly choose between two measurement bases and independently measure their particle, similar to the BB84 protocol used for QKD [11]. If their measurement results are correlated, Bob and Charlie can use their measurement bases and outcome information to determine the result of Alice's measurement, otherwise the round is discarded. Since approximately half the instances will be discarded the intrinsic efficiency is about 50%. This protocol was improved to accommodate an arbitrary number of parties based on multi-particle qubit entanglement states [252], and later to multi-particle d dimensional entanglement states [253].

Although much theoretical, in both the discrete-variable [254–262] and continuous-variable regime [263, 264], and (to a lesser extent) experimental [265, 47, 48] attention has focussed on QSS using multi-particle entangled states, progress has been limited by the intrinsic hurdle that the number of parties involved is bound by the number of entangled particles. Multi-photon entanglement is notoriously inefficient and the difficulty of obtaining the required quantum correlations grows rapidly. The efficiency of preparing even tripartite or four-partite entangled states is very low [266, 267], making particle entanglement-based QSS inefficient and unscalable.

As a result of these limitations, two-dimensional QSS schemes using single photon states have been proposed [49, 43] and implemented [50, 268] for a scalable number of parties. The advantage arises in its circular structure, where each party performs sequential unitary operations on the same single photon, instead of several entangled photons which require convoluted setups. The security was found to be less robust as compared to quantum key distribution (QKD) and susceptible to cheating strategies in that dishonest parties could infer some information about the choice of bases of another party [269, 270]. To address this deficiency, multi-party high-dimensional single photon QSS protocols were theoretically proposed [51–54] but with few suggestion as to how they might be (practically) implemented in the laboratory [271–273]. Challenges in high-dimensional state preparation, transformation and detection, the key steps of any QSS protocol, have so far presented barriers to experimental realisation.

Here we realise the first experimental high-dimensional single photon QSS protocol using photons that are vectorially structured in their orbital angular momentum (OAM) and polarisation. Our approach requires only simple linear optical elements: spin-orbit coupling optics to prepare the initial state, waveplates with dove prisms to encode the secret in the sequential phase transformation of each party, and a deterministic detector for all basis elements in the high-dimensional vector space. We successfully implement this protocol in two-dimensions for ten parties, and three-dimensions with three parties - the highest realisation of participants and dimensions thus far. Our approach is scalable in the number of participants, highly efficient and provably secure.

5.2 Single photon quantum secret sharing protocol

We begin by extending the single photon QSS protocol [51] to prime dimensions and then we outline the general structure of a N-party QSS scheme using a single photon state. In this protocol multiple participants perform local operations on a single photon encoded in prime d dimensions. Suppose a participant R_1, also known as the distributor, wants to share a secret key amongst multiple parties, $R_2, \ldots, R_N$, then the QSS protocol can be summarised in four steps (see Fig. 5.1):

1. **State preparation:** The distributor, R_1, prepares an initial single photon state $|e_0^{(0)}\rangle$ from a set of mutual unbiased bases (MUB) in the desired prime dimension d. In our protocol, the MUBs are formulated from the logical basis, $|\ell\rangle$, as follows:

$$|e_k^{(j)}\rangle = \frac{1}{\sqrt{2}} \sum_{\ell=0}^{1} \omega^{\frac{1}{2}\ell(j+2k)} |\ell\rangle , \tag{5.1}$$

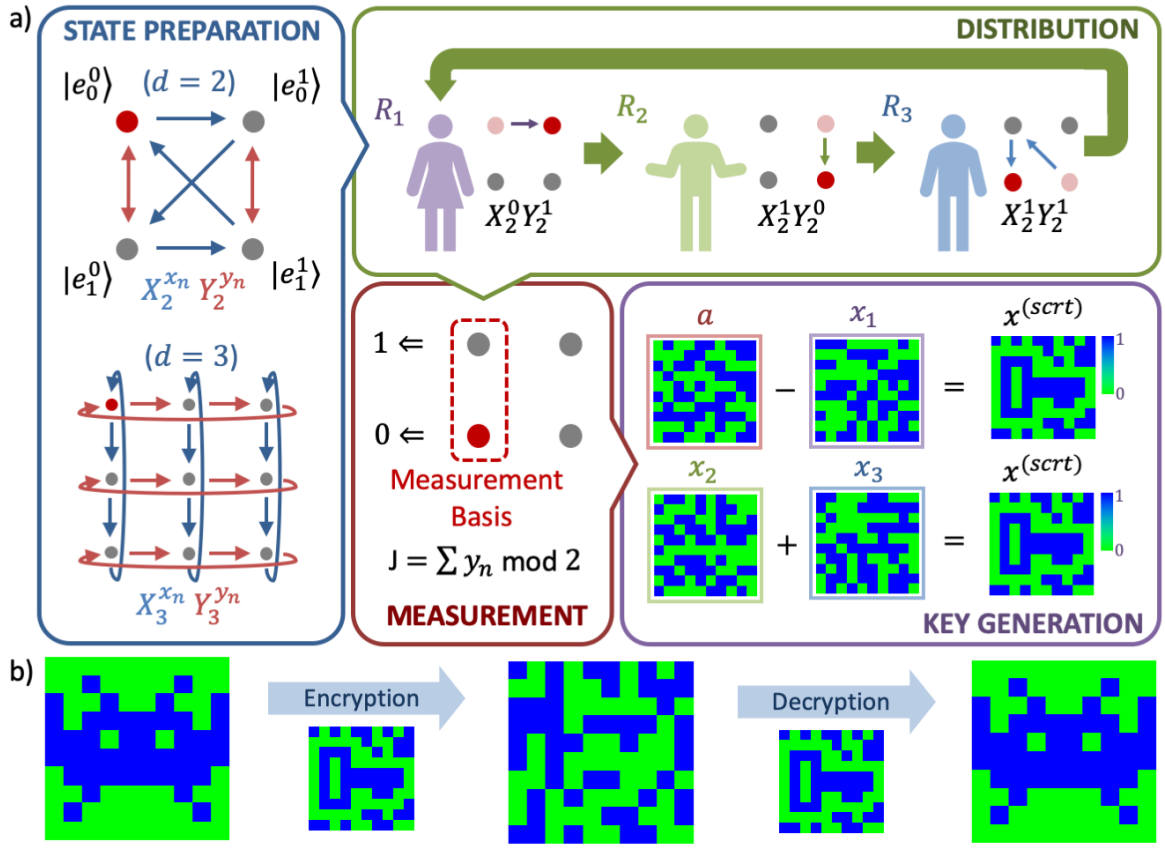

Fig. 5.1 General scheme for a 3 party single qubit QSS scheme. (a) The distributor, R_1, prepares an initial state from a set of $d = 2$ MUBs. The qubit is then sequentially distributed to each party, who in turn performs a unitary phase operation given by $X_d^{x_n} Y_d^{y_n}$. The choice of X^{x_n} is analogous to a change in local states within the basis, and a choice of Y^{y_n} corresponds to a change of basis. The last participant sends the qubit back to the distributor. The distributor requests that parties R_2 and R_3 broadcast their choice of y_n and performs a measurement in a basis that leads to a deterministic result. The distributor can generate a secret key $x^{(scrt)}$ by using the measurement result to reset their choice of x_n. The other parties, upon collaborating and broadcasting their choice of x_n, can also generate the same secret key $x^{(scrt)}$. We also show the state preparation for $d = 3$ dimensions. (b) The distributor can securely encrypt a message by applying a simple XOR encryption operation using their generated secret key. The encrypted message, after being distributed, can be decrypted by each participant using their own secret key. At no point is the secret key shared among any participants.

in two dimensions and in odd prime dimensions (d') they are generalised as [51],

$$|e_k^{(j)}\rangle = \frac{1}{\sqrt{d'}} \sum_{\ell=0}^{d'-1} \omega^{\ell(k+j\ell)} |\ell\rangle , \tag{5.2}$$

where k maps onto a mode from the j^{th} MUB and $\omega = \exp(\frac{i2\pi}{d})$. Note that $\ell, j, k \in \{0, \ldots, d-1\}$.

2. **Distribution:** The distributor modulates the photon initially in the state $|e_0^{(0)}\rangle$ with the operators $X_d^{x_1} Y_d^{y_1}$, where $x_1, y_1 \in \{0, \ldots, d-1\}$ are chosen randomly and indicate how many times the operators should be applied. The photon is then sent sequentially to each participant $R_2, \ldots, R_N$, who upon receiving the single photon, randomly choose $x_n, y_n \in \{0, \ldots, d-1\}$, such that they apply the corresponding unitary operations $X_d^{x_n} Y_d^{y_n}$.

   To map between the MUB basis states, each party has access to two operators: X_d and Y_d. The operator X_d is defined as,

$$X_d = \sum_{\ell=0}^{d-1} \omega^{\ell} |\ell\rangle \langle\ell| , \tag{5.3}$$

   for prime dimensions. We adapted the protocol [51] for two dimensions such that the operator Y_d is defined as

$$Y_2 = \sum_{\ell=0}^{1} \omega^{\frac{1}{2}\ell} |\ell\rangle \langle\ell| , \tag{5.4}$$

   in two dimensions and in odd prime dimensions (d') as

$$Y_{d'} = \sum_{\ell=0}^{d-1} \omega^{\ell^2} |\ell\rangle \langle\ell| . \tag{5.5}$$

   The operator $X_d^{x_n}$ cycles through x_n modes in the same basis, while the operator $Y_d^{y_n}$ cycles through y_n MUBs, as shown in Fig. 5.1(a). Using both operators in sequence results in the mapping between all MUB states which is crucial in the implementation of the single photon secret sharing protocol.

3. **Measurement:** After receiving the single photon from the last participant, the distributor request that parties $R_2, \ldots, R_N$ broadcast their choice of y_n in a random order, keeping their value of x_n a secret. By considering the sum of all y_n, the distributor chooses a measurement basis from the MUB set in such a way that the measurement leads to a deterministic result. In prime dimensions this is equivalent to applying the local unitary

operator Y_d^J and measuring the photon in the basis $|e_k^{(J)}\rangle$, where

$$J = \sum_{n=1}^{N} y_n \bmod d. \tag{5.6}$$

The final measurement result obtained by the distributor is labelled $a \in \{0,\ldots,d-1\}$. Since the measurement is performed in a basis that yields a correlated result, the efficiency of the protocol is 100% [54]. If Eq. 5.6 holds, the participants have a strongly correlated selection of x_n, satisfying

$$\sum_{n=1}^{N} x_n + C = a \bmod d. \tag{5.7}$$

where we define $C = \lfloor \frac{1}{2} \sum_{n=1}^{N+1} y_n \rfloor$ for two dimensions, which accounts for the additional X_2 operator imparted by every odd number of Y_2 operators, and $C = 0$ in odd prime dimensions, due to the cyclic property of the operators in d' dimensions.

4. **Key generation:** The distributor resets his value of $x_1^{(scrt)} = (a - x_1 + C) \bmod d$ according to the measurement result a. Consequently, if participants $R_2,\ldots,R_N$ collaborate and reveal among themselves their choice of x_n, they can reconstruct the distributors secret value $x_1^{(scrt)} = \sum_{n=2}^{N} x_n \bmod d$, which was previously only known to the distributor R_1. By repeating this procedure, the distributor can share a secret key among the rest $N-1$ participants. Using the secret key, the distributor can securely encrypt a message and distribute it to the participants, who in turn can use their own secret key to decrypt the message, as in Fig. 5.1(b).

Participant R_1 checks the security, such that he randomly selects a subset of rounds. The degree of security specifications determines the size of the subset. In order to increase the security, as justified in [54], R_1 must make sure that the subset of valid rounds includes a round in which each participant broadcasts his choice of y_n last. Each participant reveals their inferred value $x^{(scrt)}$ for the subset of rounds, which is compared to the value determined by the distributor. If there is a discrepancy any dishonest eavesdropping or cheating strategy is exposed.

In the next step, we investigate the necessary tools to implement a high-dimensional single photon QSS scheme. We explore vector modes and how we can implement unitary phase operators using simple linear optics.

5.3 Experimental realisation

Here we introduce the tools (operations) needed for single photon secret sharing in prime dimensions. Lastly, we show how the protocol can be implemented in both $d = 2$ and $d = 3$ dimensions using polarisation and OAM control.

5.3.1 Two-dimensional realisation

If we consider the polarisation subspace coupled with the OAM subspace, spanned only by $|\ell|$, we can construct a two dimensional mode set, i.e., $\mathcal{H}_2$=span($\{|R\rangle|\ell\rangle, |L\rangle|-\ell\rangle\}$) as illustrated in Fig. 5.2(a). The basis states can be mapped as orthogonal column vectors,

$$|R\rangle|\ell\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad |L\rangle|-\ell\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}. \tag{5.8}$$

This allows us to map the MUBs (see Fig. 5.2(b)) as row vectors in matrix form as follows:

$$\mathrm{M}_1 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \mathrm{M}_2 = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}. \tag{5.9}$$

The first step in implementing the protocol is preparing the photon in the initial state within our MUB set. We generated the initial state, $|e_0^{(0)}\rangle = \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle)$ denoted by $|\Psi_0\rangle$, from a horizontally polarised photon incident on a spin-orbit coupling q-plate [126, 274]. The Jones representation of horizontally polarised light incident on a q-plate is given by,

$$\hat{U}_{QP}|H\rangle = \begin{pmatrix} \cos(2q\phi) & \sin(2q\phi) \\ \sin(2q\phi) & -\cos(2q\phi) \end{pmatrix} |H\rangle \tag{5.10}$$

$$= \frac{1}{\sqrt{2}}(|R\rangle|\ell\rangle + |L\rangle|-\ell\rangle). \tag{5.11}$$

where $2q = \ell$, $|H\rangle = \frac{1}{\sqrt{2}}(|R\rangle + |L\rangle)$ and $|\ell\rangle = e^{i\phi\ell}$. Hence, a q-plate is sufficient in preparing an initial state within our MUB set.

The next step is to find a way to independently move between each MUB state by applying the required operators. It follows from Eq. 5.9, that the operators required to move between all

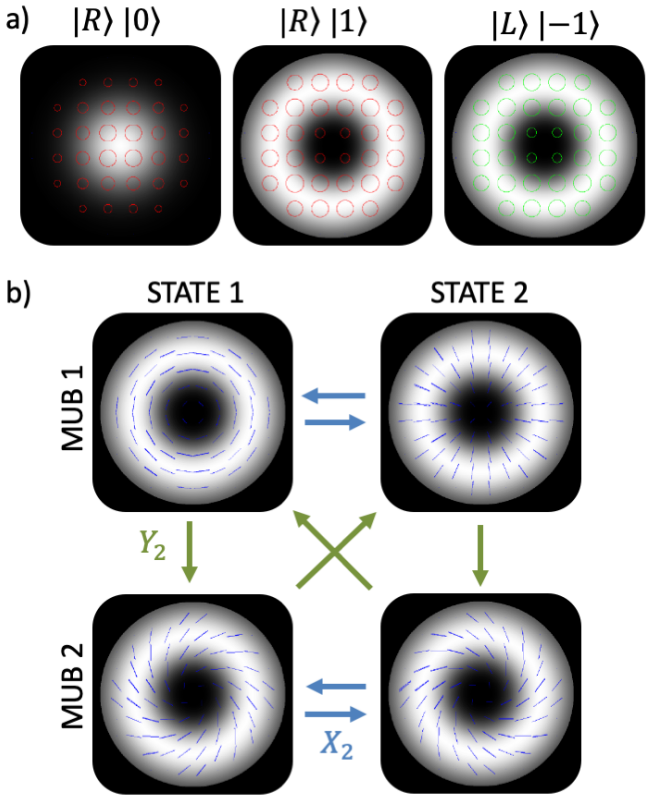

Fig. 5.2 Illustration of the spin-orbit coupled modes that form our computational basis, from which we construct our MUBs in $d = 2$ dimensions. (a) Right circularly polarised light is shown in red, left circularly polarised light is shown in green and linear polarisation in blue. (b) We realise the operators in $d = 2$ using a half waveplate (HWP). A HWP at $\theta = \pi/4$ realises the X_2 operator, cycling between the states within the same basis; at $\theta = \pi/8$ we realise the Y_2 operator, moving between MUBs. Note that the Y_2 operator is not cyclic, due to the extra X_2 operator that is imparted by every odd number of Y_2.

MUBs can be expressed as,

$$X_2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad Y_2 = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}. \tag{5.12}$$

The operator of X_2 is analogous to a change in local states within the basis and Y_2 corresponds to a change of basis. However, it should be noted that, the transformations between MUBs are not cyclic for two-dimensions. This is a particular property of MUBs in odd primed dimensions [275]. Since each Y_2 operator introduces a i phase shift, then every odd number of Y_2 operators introduces an extra X_2 operator. This must be accounted for when extracting the

secret key. Both operators are easily implemented by a half waveplate (HWP). It is straight forward to see that a HWP acting on the initial state $|e_0^{(0)}\rangle$, induces a relative phase difference, $e^{i4\theta}$, between the circular polarisation states. This can be summarised as

$$\hat{U}_{HWP}(\theta) \propto \begin{pmatrix} 1 & 0 \\ 0 & e^{i4\theta} \end{pmatrix}, \tag{5.13}$$

where $\theta \in \{0, \pi/8, \pi/4, 3\pi/8\}$ is the rotation angle of the HWP, corresponding to the transformations $\hat{U}_{HWP}(\theta) = \{X_2^0 Y_2^0, X_2^0 Y_2^1, X_2^1 Y_2^0, X_2^1 Y_2^1\}$. In this way, Fig. 5.2(b) shows that we can move independently between all MUBs.

Once the initial state is sent through a set of even N consecutive HWPs, allowing each party to apply their unitary operator, the final state of the photon will be:

$$|\Psi_N\rangle = \frac{e^{i\Omega}}{\sqrt{2}} \left[|R\rangle |\ell\rangle + e^{i\Phi} |L\rangle |-\ell\rangle \right], \tag{5.14}$$

where $\Omega = (-i)^N e^{-2i(\sum_{n=1}^{N}(-1)^{n+1}\theta_n)}$ and $\Phi = 4\sum_{n=1}^{N}(-1)^{n+1}\theta_n$. The distributor then applies the corresponding operator for $\phi_J \in \{0, \pi/2\}$ using a HWP, such that performing the measurement in the basis $\frac{1}{\sqrt{2}}(|R\rangle |\ell\rangle + e^{i\phi_J} |L\rangle |-\ell\rangle)$ leads to deterministic result.

Next, we discuss the detection system used to distinguish between all MUB states. The different states can be deterministically detected using a combination of geometric phase control and multi-path interference, as seen in Fig. 5.3(a). The photon was mapped onto two polarisation dependent paths (a and b) using a combination of quarter waveplates (QWP) and a polarising beam splitter (PBS). A QWP oriented at $\frac{\pi}{4}$ transforms the polarisation of the photons from circular to linear polarisation, followed by the PBS which separates the photons into two polarisation dependent paths ($|H\rangle$ and $|V\rangle$). A quarter wave plate oriented at $\frac{\pi}{4}$ in each arm transforms the polarisation back to circular polarisation, such that the state of the qubit becomes,

$$|\Psi_N\rangle = \frac{e^{i\Omega}}{\sqrt{2}} [|R\rangle_a |1\rangle_a + e^{i\Phi} |L\rangle_b |-1\rangle_b], \tag{5.15}$$

where the subscripts a and b refer to the polarisation dependent paths. The photon paths were interfered at a 50:50 beam splitter (BS), setting the dynamic phase difference between the two paths to $\pi/2$. An extra reflection was added to one path so that the number of reflections, and thus the polarisation of the two output paths, was automatically reconciled. Henceforth, we will drop the polarisation kets in the expression as the polarisation information is path dependent.

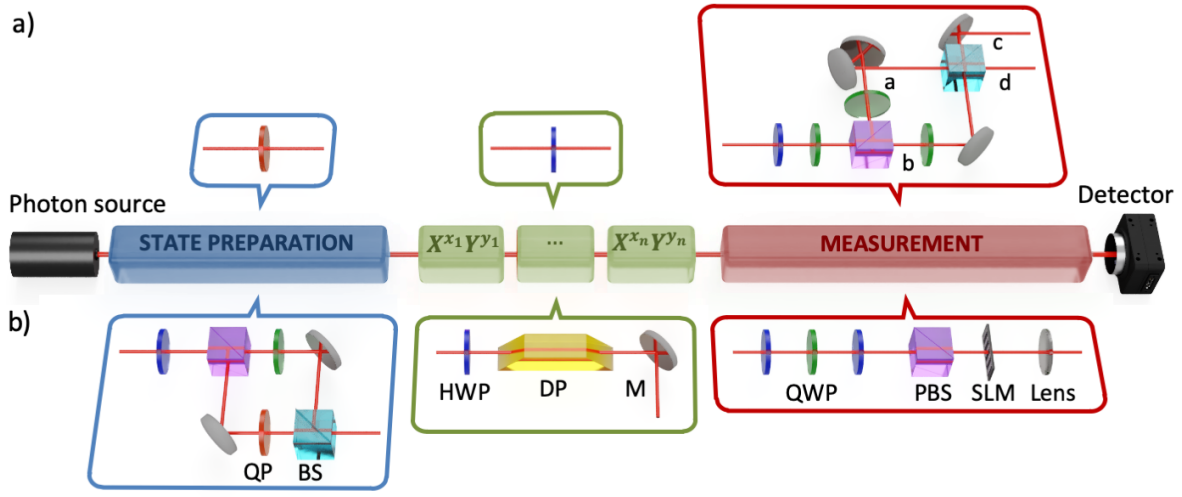

Fig. 5.3 Generalised experimental setup of a single photon quantum secret sharing scheme, showing the state preparation, distribution and measurement steps for (a) $d = 2$ and (b) $d = 3$ dimensions. The initial states are generated using a combination of geometric phase optics (i.e., a q-plate (QP)). The initial state is then sequentially communicated to each participant, who perform a unitary phase operator employed using simple linear optics such as a half waveplate (HWP) and a dove prism (DP). A HWP in the measurement step was used to perform the measurement in the same basis each time. The different states can be deterministically detected (a) using a combination of geometric phase control and multi-path interference using beam splitters (BM) and polarising beam splitter (PBS), or (b) via modal decomposition using a spatial light modulator (SLM). M are mirrors.

The resulting state after the BS is

$$|\Psi'_N\rangle = \frac{e^{i\Omega}}{2}[(1-e^{i\Phi})\,|1\rangle_c + i(1+e^{i\Phi})\,|-1\rangle_d], \tag{5.16}$$

where the subscript c and d refer to the output paths of the beam splitter. From this equation we see that the detection scheme is in fact deterministic for given values of Φ, such that all the light will be in either path c or d.

Next, we extend the two dimensional implementation to three dimensions, using a similar linear optics setup.

5.3.2 Three-dimensional realisation

We now consider a mode set that spans a three dimensional (qutrit) space of spin-orbit coupled modes, i.e., $\mathcal{H}_3$=span($\{\ |R\rangle\,|0\rangle), |R\rangle\,|\ell\rangle\,, |L\rangle\,|-\ell\rangle\}$) as depicted in Fig. 5.2(a). If we map the

basis states as orthogonal column vectors, i.e.,

$$|R\rangle|0\rangle = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \quad |R\rangle|\ell\rangle = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}, \quad |L\rangle|-\ell\rangle = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}, \tag{5.17}$$

then the MUBs can be mapped as row vectors in matrix form as

$$\mathrm{M}_1 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{pmatrix}, \quad \mathrm{M}_2 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \omega \\ 1 & \omega & 1 \\ \omega & 1 & 1 \end{pmatrix}, \quad \mathrm{M}_3 = \frac{1}{\sqrt{3}} \begin{pmatrix} 1 & 1 & \omega^2 \\ 1 & \omega^2 & 1 \\ \omega^2 & 1 & 1 \end{pmatrix}, \tag{5.18}$$

where $\omega = \exp(\frac{i2\pi}{3})$.

The initial state was prepared using a interferometric combination of a q-plate, HWP and beam splitter, as in Fig. 5.3(b). We further engineer the required operators by using a half waveplate in combination with a dove-prism as illustrated. As before, the HWP induces a relative phase difference, $e^{4i\theta}$, between the circular polarisation degree of freedom and the DP imparts a phase, $e^{-2i\gamma\ell}$ which proportional to the OAM state. A mirror after the dove prism is needed to invert the final OAM state. The unitary transformation, in the basis from Eq. 5.17 can be summarised as

$$\hat{U}(\theta,\gamma) \propto \begin{pmatrix} 1 & 0 & 0 \\ 0 & e^{-2i\gamma\ell} & 0 \\ 0 & 0 & e^{(2i\gamma\ell+4i\theta)} \end{pmatrix}, \tag{5.19}$$

where $\theta \in \{0, \pi/6, 2\pi/6\}$ is the rotation angle of the HWP and $\gamma \in \{0, \pi/3, 2\pi/3\}$ is the rotation angle of the DP. The DP allows us to realise the X_3 gate, cycling between the states within the same basis, and the HWP allows us to realise the Y_3 gate, cycling between the MUBs (see Fig. 5.4).

The detection system included mapping our vector basis to a scalar basis using a set of half waveplates and quarter waveplates. We measured the detection probabilities of each MUB state by performing optical inner-product measurements using match filters encoded on the SLM via modal decomposition. The detection modes where encoded as phase and amplitude holograms on a Holoeye Pluto spatial light modulator (SLM) - a well established technique for spatial mode detection [116]. Alternatively, using a quantum Fourier transform (QFT) to map between

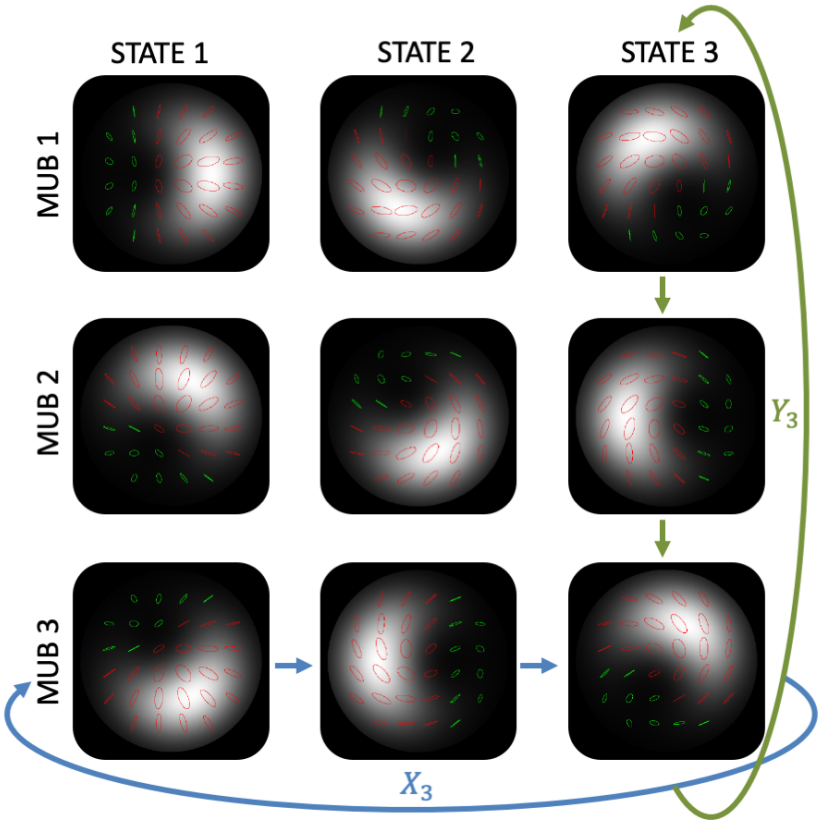

Fig. 5.4 Illustration of the spin-orbit coupled modes that form our MUBs in $d = 3$ dimensions. Right circularly polarised light is shown in red and left circularly polarised light is shown in green. Here we see the cyclic nature of the operators in $d = 3$. A dove prism (DP) allows us to realise the X_3 gate, cycling between the states within the same basis, and a half waveplate (HWP) allows us to realise the Y_3 gate, cycling between the MUBs.

the MUB superpositions of OAM modes to the OAM standard basis, one can deterministicaly sort the MUBs and thereafter sort the OAM modes. In three dimensions, a QFT for OAM has been proposed [276]. The technique exploits the tritter [277], by using path and phase control. Once the mapping between the MUB and OAM basis is achieved, mode sorters can be used deterministicly to measure the OAM modes [145]. Mode sorting has been extensively used for both scalar [278] and vector modes [148].

5.4 Results

Here we present the results for our implementation of the quantum secret sharing protocol with single photon states in $d = 2$ and $d = 3$ dimensions. For practical purposes, the experiment was first performed with a classical light source and a ccd camera. Later, the light source was

attenuated to an average photon number of $\mu = 0.02$ per pulse. Although weak coherent states cannot be used without photon splitting strategies this could, in principle, be overcome by preparing and testing the transmission properties of some decoy states. In the single photon regime, the measurement system includes coupling the photons through fibres to avalanche photon detectors (APD).

5.4.1 Two-dimensional results

The two dimensional detection results of our vector basis ares shown in Fig. 5.5. This was performed by rotating the angle θ of the HWP and measuring the intensity of each output port using a ccd camera at each port (see Fig. 5.5(a)) and in the single photon regime, using single photon detectors (see Fig. 5.5(b)).

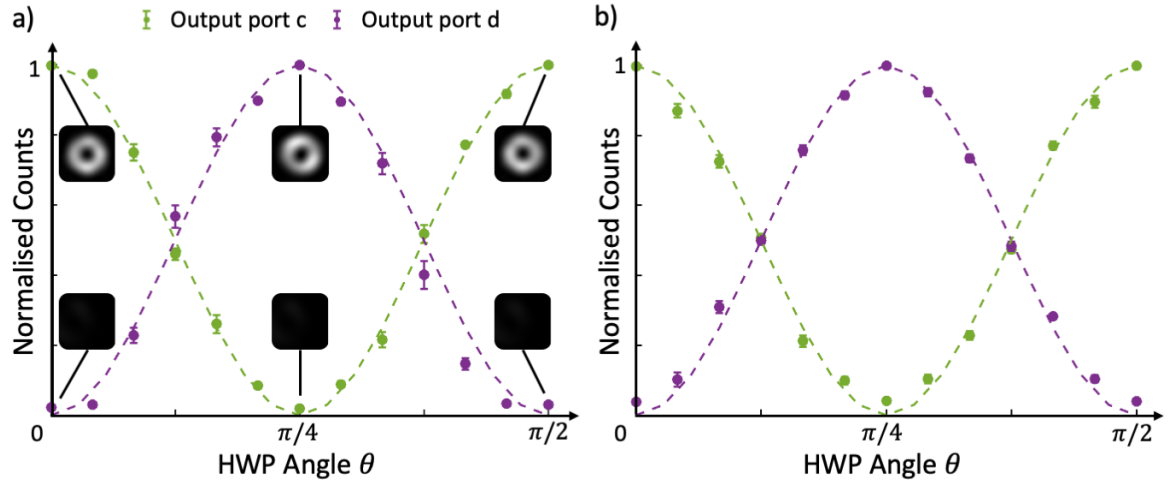

Fig. 5.5 Detection of superposition of vector states. Each graph shows the detection (normalised counts) of the photons in a superposition of the vector states $|\Psi'_N\rangle$, generated by rotating the HWP angle θ, using (a) ccd camera and (b) photodiodes in the single photon regime. Each data point was generated by averaging over 35 measurements. The dashed lines show the theoretical curve.

There is an excellent agreement between the experimental results (data points) and the theory (dashed curves). The Visibility, V, of the detection scheme in each output port was calculated using the equation:

$$V = \frac{|\mathcal{I}_{max} - \mathcal{I}_{min}|}{\mathcal{I}_{max} + \mathcal{I}_{min}}, \tag{5.20}$$

where $\mathcal{I}$ is the normalised counts in each arm. Spatial filtering was applied to the data obtained using the ccd camera to remove unwanted noise, resulting in $V = 0.958 \pm 0.005$. In our system, the errors are introduced by the additive imperfections in the half waveplates causing slight

misalignment in the setup. The visibility for the single photon regime was measured to be $V = 0.924 \pm 0.003$, which can be accounted for by the photon loss in fibre coupling and detector dark counts. Nonetheless, such values imply the use of a well-aligned and stable interferometer.

For phase-coding setups, the fidelity of the detection system is related to the interference visibility by [1],

$$F = \frac{1+V}{2}. \tag{5.21}$$

Hence, the fidelity of the system was calculated to be $F = 0.979 \pm 0.005$ for the classical implementation and $F = 0.962 \pm 0.003$ for the single photon regime. Using this deterministic detector, we can detect any arbitrary superposition of our vector basis with high fidelity.

5.4.2 Three-dimensional results

To demonstrate the feasibility of our secret sharing scheme in three dimensions, we verify that the $d+1$ MUBs are each orthogonal with respect to each other by measuring the scattering probabilities. The crosstalk matrix is shown theoretically in Fig. 5.6 (a) and experimentally in Fig. 5.6 (b) and Fig. 5.6 (c), for the classical and single photon regime respectively. To obtain the results we first prepared the initial superposition state $|e_0^{(0)}\rangle$ and applied the X_3 and Y_3 gates to iterate through the various basis modes and MUB mode sets. Using a set of waveplates, we mapped the circular polarisation photon states to the horizontal polarisation state and performed projective measurements via modal decomposition.

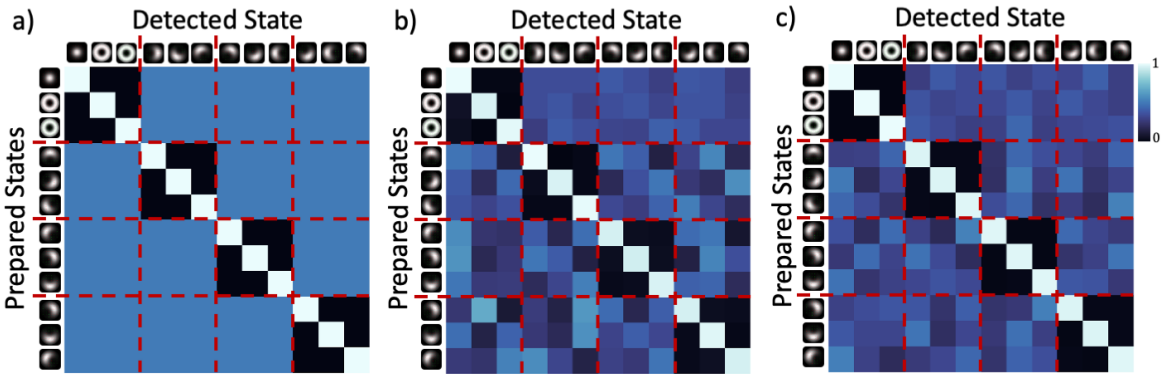

Fig. 5.6 Crosstalk matrices shown theoretically in (a) and experimentally in (b) and (c), for classical light and the single photon regime respectively. This shows the scattering probabilities for modes prepared and detected in identical bases (diagonal) and the overlap between modes from mutually unbiased bases (off diagonal).

From the crosstalk matrices, we measured an average fidelity of $F = 0.946 \pm 0.003$ when using classical light and similarly we measured $F = 0.938 \pm 0.001$ in the single photon regime.

In our system, the errors are introduced by imperfections, including the rotation of the dove prism and half waveplates causing slight misalignment in the setup.

5.4.3 Security analysis

From the measured detection fidelities, we performed a security analysis on our QSS scheme for $d = 2$ and $d = 3$ dimensions. The results of the analysis are summarised in Table 5.1.

Measures	**d=2**		**d=3**	
	Classical	**Quantum**	**Classical**	**Quantum**
F	0.979	0.962	0.946	0.938
QBER	0.021	0.038	0.054	0.062
I	0.853	0.767	1.225	1.187

Table 5.1 Summary of the $d = 2$ and $d = 3$ experimental results for our secret sharing protocol, for both the classical regime using the ccd camera as a detector and for the single photon regime using APDs. We show the experimental values of the detection fidelity (F), the quantum bit error rate (QBER) in bits per photon and mutual information (I) between distributor and participants.

The quantum bit error rate (QBER), reflecting the probability of making detection errors, is related to the fidelity by [55],

$$\text{QBER} = 1 - F, \tag{5.22}$$

which is 0 for a perfect system. The detection fidelities translated into an optical QBER between 0.021 and 0.062, well below the 0.110 and 0.156 bounds for unconditional security against coherent attacks in two and three dimensions respectively [279]. Systematic errors can be attributed to detector dark counts and the interferometric phase drift, which influences the prepared relative phases. This forced a phase re-calibration before each run.

From the fidelity we can calculate the mutual information, I. This places a bound on the amount of information that can be shared between the distributor and participants. This bound is only due to the generation and detection fidelities, and not intrinsic to the protocol itself. This is given by [55],

$$I = \log_2(d) + F\log_2(F) + (1-F)\log_2\left(\frac{1-F}{d-1}\right). \tag{5.23}$$

For a perfect system we would expect a value of 1 bit per photon in a $d = 2$ qubit system and 1.58 bits per photon in in a $d = 3$ qutrit system. For $d = 3$ this was measured to be nearly $1.5\times$ the maximum achievable in $d = 2$ dimensions. We note that increasing the dimension of the quantum secret sharing protocol, did result in higher mutual information capacity.

5.4.4 Secret key generation

To corroborate the advantage of our protocol utilising a higher dimensional encoding space, we experimentally shared a secret in both $d = 2$ and $d = 3$ dimensions using the experimental setups described.

In two dimensions, the protocol was performed by $N = 10$ participants - the highest number of participants realised thus far - each equipped with a X_2 and Y_2 gate (half waveplate). We ran the protocol for 100 valid runs, resulting in a generated secret key of 100 bits. The results are shown in Fig. 5.7(a), for the identical secret key retrieved by the distributor and shared between the participants. The distributor's secret key was determined by resetting his choice of x_1 using the measurement results and the participants choice of y_n. The participants shared secret key was calculated by summing the keys of the participants $R_2, ..., R_{10}$, modulus two.

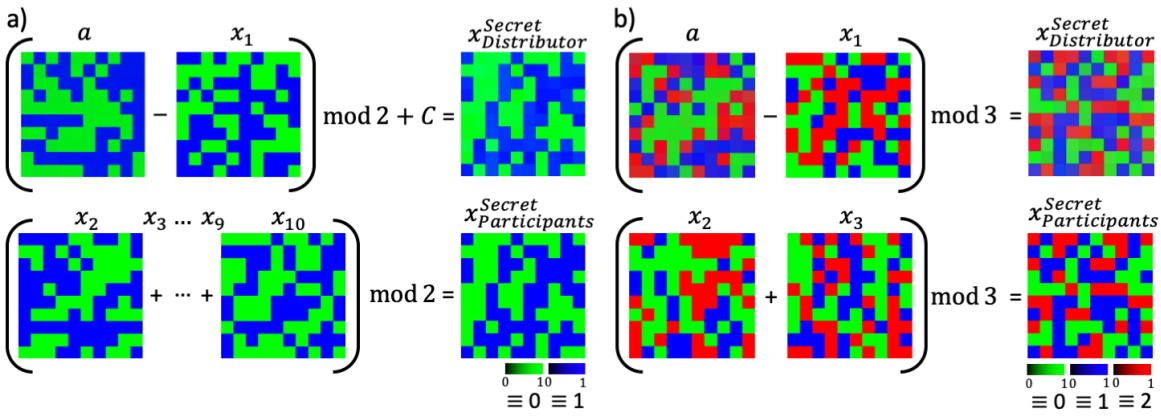

Fig. 5.7 Experimentally generated distributor's and participants' secret keys, in (a) $d = 2$ and (b) $d = 3$ dimensions, by implementing the protocol for 100 valid runs. The colour bars indicate the measured probability of generating a 0, 1 or 2.

Next, exploiting the higher dimensional ($d = 3$) encoding space, we shared a secret key between $N = 3$ participants, each equipped with the X_3 gate (dove prism) and Y_3 gate (half waveplate). The results are shown in Fig. 5.7(b), for the secret code retrieved by the distributor and shared between the participants. The keys are identical as desired. Using the high dimensional protocol for 100 valid runs we generated a secure key that was 158 bits.

5.5 Discussion

Transverse spatial modes of light carrying orbital angular momentum have become ubiquitous for encoding quantum information. Here, OAM modes have proven invaluable for secure and robust communication, and thus have the potential to increase the mutual information and security of quantum channels in QSS. However, despite its many potential advantages, the complete realisation of high-dimensional quantum cryptography with OAM, so far, has been limited by technical difficulties arising in the full manipulation and transmission of this degree of freedom (DoF). To overcome these restraints, photon states encoded in different DoFs, called hybrid entangled states, have attracted a lot of attention [97]. Spin-orbit coupled states, e.g. vector modes, have been used to complete the entanglement purification in photon pairs for polarisation Bell states [280, 281]. Similarly, they have been used to overcome the limiting channel capacity of super-dense coding [282] and to realise a high capacity QKD protocol [283].

We note that although we used a weak coherent photon source, practical deployments require ideal single photon sources to ensure unconditional security. The engineering of such sources is an ongoing field of research [284] and as a result our scheme remains demonstrable. In principle, one could counter photon splitting attacks by preparing and testing the transmission properties of some decoy states, modulating several intensities of weak coherent photons and reserving one intensity as the signal state. Alternatively, state-of-the-art single photon emitters or sub-Poissonian sources like SPDC heralded photons can be used (see our previous QKD demonstration [35]). Nevertheless, even Fock states larger than $n = 1$ have a non-zero detection probability and may pose a security risk, potentially requiring the use of decoy states. We stress that we used an attenuated laser source in which the photon statistics follow a Poisson distribution mainly for the high spatial coherence which is no different to that of a single photon source. Correspondingly, the superposition principle and mutually unbiased basis (the fundamental properties exploited in our scheme) are inherent properties in both sources, making both sources equivalent for state encoding and decoding protocols. In fact, a myriad of high-dimensional QKD schemes have been tested this way, using spatially structured photons in free-space [33] and fibre [285].

The efficiency and secure key rate could be improved for practical deployments, by using commercially accessible detectors with low dark counts, short detector dead times, high resolution and high detection efficiencies. Since our scheme is adaptable to any wavelength, detectors with up to 93% efficiency, a dead time of up to 40ns, a dark count rate of 1 count-per-second and a timing resolution of up to 150ns are available at telecom wavelengths - promising quantum communication speeds in the megahertz regime [286].

Here, we have reported a novel scheme for sharing secure keys between multiple parties by interfacing different DoF, namely spin and orbital angular momentum of single photons in high-dimensions ($d = 3$). Our scheme can be extended to multiple participants and requires conventional linear optical elements making it easily scalable. For a practical implementation waveplates and dove prisms can be rotated using electronically driven rotation mounts [244], whose rotation rate would be the only limiting factor with regards to the generation rates.

The spatial modes used here can be represented by LG modes and thus are the natural modes of quadratic media like free-space and optical fibre making them ideal for practical implementations in long distance communication. So far, free-space quantum channels have been demonstrated with satellite-to-ground links [287], intra-city free-space links [288] and in QKD using similar vector modes [289]. Moreover, our basis modes if chosen carefully, lie within the first two mode groups which may have low group delays and minimal crosstalk. Hence, our scheme can also be exploited over long distances using few mode fibres, as demonstrated up to 1 km for QKD [290]. Applications can also be extended to underwater channels, previously shown for QKD [291]. The main application challenge would be overcoming deleterious effects, like turbulence resulting from local fluctuations in refractive index of refraction [292] which could reduce the QBER.

We iterate that QSS protocols involve the sharing of a random encryption key, as opposed to a predetermined secret message. Where the latter is necessary, quantum secure direct communication (QSDC) is a solution, where secret information is transmitted directly through a quantum channel without prior distribution of a secret key [293–297]. Appropriately, the technique presented here (i.e., using spin-orbit coupled modes as high-dimensional information carriers) has the potential to advance the likes of other quantum communication branches, such as QSDC.

5.6 Conclusion

In conclusion, we successfully implemented two-dimensional single photon QSS for 10 parties. We further extended our scheme to higher dimensions by interfacing independent degrees of freedom, providing a natural extension to high-dimensional QSS. Our approach shows that by using hybrid polarisation and OAM encoding, it is possible to realise a $d = 2$ and $d = 3$ dimensional single photon QSS using conventional linear optical elements. Further, by exploiting the non-separability of polarisation and OAM in our choice of spatial modes, we were able to realise transitions on a high dimensional Hilbert space, mapping between different MUB states, demonstrating the advantage of interfacing independent DoFs. Our practical

scheme is scalable to an unlimited number of participants and can be realised using current technologies, without generating complex multi-particle entangled states.

Chapter 6

Conclusion

In this dissertation, we investigated the potential of using structured light in the realm of quantum cryptography, specifically the generation and distribution of encryption keys. We showed that spatially structuring light to access an infinite encoding space, provides a considerable advantage over two dimensional polarisation encoding. Using simple linear optics we overcame the challenges in high dimensional state preparation, transformation and detection, which had previously presented barriers to experimental realisations. Ultimately, we demonstrated the viability of using structured light as a versatile platform for practical high-dimensional quantum cryptographic implementations.

In Chapter 1, we outlined general quantum cryptographic protocols, including both the generation (i.e. random number generation) and distribution (i.e. secret sharing) of encryption keys. We further investigated the inherent principles, such as the no-cloning theorem and non-locality, which make them superior to their classical counterparts. Next, we explored structured light as a carrier of information. By considering Maxwell's breakthrough that light must also be a carrier of energy and other mechanical effects, we showed that in the paraxial approximation of the Helmholtz equation, the angular momentum of light can be separated into two components: spin angular momentum (SAM), associated with the circular polarisation of photon, and orbital angular momentum (OAM), associated with the transverse spatial profile of the photon. As such, we explored spatial modes carrying OAM due to their potential for infinite accessible states and sought to overcome the current technical difficulties arising in the full manipulation, transmission and detection of this degree of freedom.

In Chapter 2, we circumvented these limitations by exploiting dynamic and geometric phase control for generating, manipulating and detecting spatial modes of light. We assembled a toolbox with various optical elements and techniques, whereby we characterised the operation of these elements and established a good understanding of their operation and the practical

aspects of their experimental implementation. Waveplates were shown to manipulate the polarisation state by introducing a phase shift between the orthogonal components of a photon's electric field. We also experimentally characterised the operation of a q-plate and a Dove prism to manipulate the spin-orbit coupled components of light. We showed that this is effective for transferring the information contained in one degree of freedom into the other. Using the acquired tools in combination with multi-path interference we were then able to show that orthogonal vector modes could be deterministically detected. Furthermore, we investigated digital holography as a technique to both generate and decompose OAM modes. By using a combination of an SLM and single mode fibre we were able to perform an optical inner-products revealing the OAM content of the photons. The techniques and optical elements presented in this chapter allowed us to structure and manipulate light to realise the high-dimensional quantum cryptographic protocols presented in Chapters 4 and 5.

In Chapter 3, we analysed spontaneous parametric down-conversion as a method to generate single photon entanglement, with particular interest in the OAM degree of freedom. We showed that the phase matching conditions (momentum and energy conservation) could be controlled by adjusting the tilt of our BBO crystal, ultimately allowing us to adjust the geometry of the emitted photons. Using the projective measurement system characterised in Chapter 2, we were able to measure the OAM states of single photons. A back-projection method, in which one of the entangled photon paths is replaced with a laser, was used for the alignment of the system. This allowed us to maximise the coupling of light from one fibre to the other, before performing the projective measurements on the down-converted photons. To verify the entanglement of our system various quantum measures were explored with respect to the OAM degree of freedom. The spiral bandwidth, a measure of the OAM spectrum, confirmed that the down-conversion process conserves OAM. This lead us to explore non-local correlations with respect to the OAM degree of freedom, in which we further confirmed the entanglement of the system via a Bell-like inequality violation. Lastly, we reconstructed the density matrices for high-dimensional OAM states by performing quantum state tomography on the photon pairs entangled in the OAM degree of freedom. On the whole, we fully characterised the OAM entanglement of our system and dimension of accessible OAM modes for secure quantum cryptography.

In Chapter 4, we utilised the techniques explored in Chapter 2 and 3 to demonstrate a new quantum random number generator [102]. Our approach is based on popular path branching QRNG schemes, however, we used digital holography to spatially map photons onto two paths. This method allowed the mapping process to be digitally controlled, which we used to account for the transmission and detection asymmetries of our system. Following this, we generated random numbers which passed the standard NIST statistical test suite, without the need for inefficient and deleterious post-processing. Moreover, the digital control

allowed us to extend our QRNG protocol to the high-dimensional OAM degree of freedom, in which we realised a novel QRNG based on the spatial mode entanglement of SPDC photon states. Taking a step further, we showed that the probability distribution of 1s and 0s and thus the entropy (a comparative measure of the quality of randomness) of the system, could be tailored by projecting the photons into arbitrary combinations of OAM contributions, all the while maintaining the irreproducibility of the quantum system. Correspondingly, our QRNG scheme offered full flexibility and control to generate random numbers satisfying any desired probability distribution, paving the way for the realisation of a multi-bit QRNG based on the high-dimensional OAM degree of freedom.

Lastly, in Chapter 5, demonstrated a novel quantum secret sharing protocol using spin-orbit coupled photons [101]. The secret was encrypted in the sequential phase transformations that each party applied to a single photon, moving between the mutually unbiased basis states. We effectively realised this protocol in two dimensions for 10 participants, using a waveplates as the phase operators and path interference as a deterministic detector for the basis states. Using the experimental techniques explored in Chapter 2, we further demonstrated our protocol in three-dimensions for three parties, by interfacing the OAM and polarisation degrees of freedom. We engineered the required operators by using a waveplate in combination with a dove prism to impart a phase proportional to the spin and OAM components, respectively. Our approach allowed us to exploit the high dimensional capabilities of these spatial modes to realise transitions between basis modes on a high dimensional Hilbert space, which had not yet been demonstrated for QSS. Moreover, this allowed us to exceed the 1 bit per photon limit of two dimensional protocols. We showed that our scheme is scalable to an unlimited number of participants, without the need for complex multi-particle entangled states. Furthermore, it is versatile and practical, using conventional linear optical elements, demonstrating the advantage of interfacing independent degrees of freedom.

6.1 Future work

Our first quantum cryptographic application demonstrated the use of OAM entangled photons pairs to generate a string of random bits. An obvious extension is to investigate the possibility of using the high-dimensional state space accessible by the OAM degree of freedom to realise a multi-bit QRNG based on OAM. Here, the number of detectable OAM modes would influence the bit per photon generation rate. Appropriately, we can engineer the probability distribution of available OAM contributions in the generated SPDC state, which is strongly related to the pump field. To decrease any bias in our multi-bit QRNG scheme, we would need the magnitudes of each OAM contribution to be as equal as possible. This could be done by shaping the initial

pump beam so that its topological information is translated into the amplitudes of the generated entangled states. By employing a Bessel-Gaussian function encoding scheme, a larger spiral bandwidth for the photon pairs could be generated [298]. Using this beam shaping framework, with a view to flattening the spiral bandwidth curve as much as possible, we could realise a multi-bit QRNG using the high-dimensional encoding space offered by the OAM degree of freedom.

An SLM, before the non-linear crystal, could be used to shape the incident beam such that the spiral bandwidth emanating from the crystal is flattened and increased. In this manner, the probability of the down-converted photon pairs created by the crystal could be dynamically controlled to adopt any OAM value within a certain range. A realisable demonstration is contingent on the ability to deterministically detect OAM states. This can be done efficiently using a mode sorter to perform the OAM projective mapping to position. An array of single photon detectors would then be necessary to perform coincidence detections. Therefore, the realisation of a multi-bit QRNG based on OAM is not far from experimental feasibility, which we hope to achieve in the near future.

Additionally, a salient area for future research in the generation of random numbers is the evaluation and quantification of randomness. Although statistical tests offer a form of statistical assurance, they do not guarantee that there are no underlying patterns and they do not provide any insight into the physical generation process. The evaluation specifications for a RNG should necessitate the entropy estimation of the system, however, there is currently no consensus on a single perfect entropy estimate. We hope to investigate this further.

Secondly, we showed that transverse spatial modes of light carrying OAM are valuable for secure and robust quantum channels and have the promise of increased information capacity, however, the real-world deployment of such schemes requires further development. For a practical quantum communication implementation, scintillation processes experienced during propagation through a turbulent medium, affect the state of the encoded photon, resulting in a loss of information. As such the distortion of OAM modes during transmission over large distances poses a huge challenge for quantum communication with OAM, which we aim to further investigate.

Moreover, one of the key principles of any quantum communication protocol is the ability to deterministically detect the output state. While mode sorting has been extensively used to measure the OAM basis, deterministically sorting superpositions of OAM modes has remained elusive in high-dimensions. Using a quantum Fourier transform (QFT) to map between the MUB superpositions of OAM modes to the OAM standard basis is an efficient way to do this, however, it is not simple to implement in high-dimensions, with very few suggestions on how

to practically do so. In three dimensions, a QFT for OAM has been proposed [276], using path and phase control. Realising such a technique would be beneficial to the OAM community, further paving the way for quantum cryptographic protocols with OAM. Building upon the techniques presented within this dissertation, a future research opportunity would be to realise a deterministic detector for OAM superpositions.

On another note, the secret sharing protocol demonstrated is in the regime of discrete-variable quantum information. Aside from the entangled states of single photons, continuous-variable entangled states of optical modes can also be used as quantum resources to implement deterministic quantum secret sharing [263, 264]. Bridging these two approaches would be an interesting avenue to explore. In our implementation we use Laguerre-Gaussian modes ($LG_{\ell,p}$) as our encoding basis which are described by two discrete variables, azimuthal order ℓ and the radial order p. However, Bessel-Gaussian modes ($BG_{k_r,\ell}$) are described by the discrete variable ℓ and the continuous-variable k_r (radial wavevector). Exploiting BG modes, in a similar way as we do the LG basis, would make for fascinating future work, in which we could couple discrete and continuous-variable protocols.

Bibliography

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," *Reviews of Modern Physics*, vol. 74, no. 1, p. 145, 2002.

[2] N. F. Pub, "197: Advanced encryption standard (aes)," *Federal Information Processing Standards Publication*, vol. 197, no. 441, p. 0311, 2001.

[3] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[4] M. Bellare, A. Desai, E. Jokipii, and P. Rogaway, "A concrete security treatment of symmetric encryption," in *Proceedings 38th Annual Symposium on Foundations of Computer Science*, pp. 394–403, IEEE, 1997.

[5] L. K. Grover, "A fast quantum mechanical algorithm for database search," in *Proceedings of the twenty-eighth annual ACM symposium on Theory of computing*, pp. 212–219, 1996.

[6] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in *Proceedings 35th annual symposium on foundations of computer science*, pp. 124–134, Ieee, 1994.

[7] L. Chen, L. Chen, S. Jordan, Y.-K. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, *Report on post-quantum cryptography*, vol. 12. US Department of Commerce, National Institute of Standards and Technology, 2016.

[8] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-quantum cryptography*, pp. 147–191, Springer, 2009.

[9] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," *Nature*, vol. 299, no. 5886, p. 802, 1982.

[10] M. Redhead and L. E. Ballentine, "Incompleteness, non locality and realism. a prolegomenon to the philosophy of quantum mechanics," *American Journal of Physics*, vol. 57, no. 4, 1987.

[11] C. H. Bennett and G. Brassard, "An update on quantum cryptography," in *Workshop on the theory and application of cryptographic techniques*, pp. 475–480, Springer, 1984.

[12] H.-K. Lo, M. Curty, and K. Tamaki, "Secure quantum key distribution," *Nature Photonics*, vol. 8, no. 8, p. 595, 2014.

[13] D. Dieks, "Communication by epr devices," *Physics Letters A*, vol. 92, no. 6, pp. 271–272, 1982.

[14] P. A. M. Dirac, "A new notation for quantum mechanics," in *Mathematical Proceedings of the Cambridge Philosophical Society*, vol. 35, pp. 416–418, Cambridge University Press, 1939.

[15] I. Owens, R. Hughes, and J. Nordholt, "Entangled quantum-key-distribution randomness," *Physical Review A*, vol. 78, no. 2, p. 022307, 2008.

[16] M. Stipcevic, "Quantum random number generators and their applications in cryptography," in *Advanced Photon Counting Techniques VI*, vol. 8375, p. 837504, International Society for Optics and Photonics, 2012.

[17] F. James, "A review of pseudorandom number generators," *Computer Physics Communications*, vol. 60, no. 3, pp. 329–344, 1990.

[18] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," tech. rep., Booz-allen and hamilton inc mclean va, 2001.

[19] V. Bagini and M. Bucci, "A design of reliable true random number generator for cryptographic applications," in *International Workshop on Cryptographic Hardware and Embedded Systems*, pp. 204–218, Springer, 1999.

[20] M. Isida and H. Ikeda, "Random number generator," *Annals of the Institute of Statistical Mathematics*, vol. 8, no. 1, pp. 119–126, 1956.

[21] J. Manelis, "Generating random noise with radioactive sources," *Electronics (US)*, vol. 34, no. 36, 1961.

[22] H. Fürst, H. Weier, S. Nauerth, D. G. Marangon, C. Kurtsiefer, and H. Weinfurter, "High speed optical quantum random number generation," *Optics Express*, vol. 18, no. 12, pp. 13029–13037, 2010.

[23] H. Guo, W. Tang, Y. Liu, and W. Wei, "Truly random number generation based on measurement of phase noise of a laser," *Physical Review E*, vol. 81, no. 5, p. 051137, 2010.

[24] C. Gabriel, C. Wittmann, D. Sych, R. Dong, W. Mauerer, U. L. Andersen, C. Marquardt, and G. Leuchs, "A generator for unique quantum random numbers based on vacuum states," *Nature Photonics*, vol. 4, no. 10, p. 711, 2010.

[25] A. Ivanova, S. Chivilikhin, and A. Gleim, "Using of optical splitters in quantum random number generators, based on fluctuations of vacuum," in *Journal of Physics. Conference Series (Online)*, vol. 735, 2016.

[26] A. K. Ekert, "Quantum cryptography based on bell's theorem," *Physical Review Letters*, vol. 67, no. 6, p. 661, 1991.

[27] C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without bell's theorem," *Physical Review Letters*, vol. 68, no. 5, p. 557, 1992.

[28] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing.," *Theoretical Computer Science*, vol. 560, no. 12, pp. 7–11, 2014.

[29] M. Hillery, V. Bužek, and A. Berthiaume, "Quantum secret sharing," *Physical Review A*, vol. 59, no. 3, p. 1829, 1999.

[30] A. Beige, B. Englert, C. Kurtsiefer, and H. Weinfurter, "Secure communication with a publicly known key," *Acta Physica Polonica A*, vol. 101, no. 3, p. 357–368, 2002.

[31] C. H. Bennett and G. Brassard, "Proceedings of the ieee international conference on computers, systems and signal processing," 1984.

[32] A. Klappenecker and M. Rötteler, "Constructions of mutually unbiased bases," in *International Conference on Finite Fields and Applications*, pp. 137–144, Springer, 2003.

[33] M. Mafu, A. Dudley, S. Goyal, D. Giovannini, M. McLaren, M. J. Padgett, T. Konrad, F. Petruccione, N. Lütkenhaus, and A. Forbes, "Higher-dimensional orbital-angular-momentum-based quantum key distribution with mutually unbiased bases," *Physical Review A*, vol. 88, no. 3, p. 032305, 2013.

[34] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, and A. Zeilinger, "Communication with spatially modulated light through turbulent air across vienna," *New Journal of Physics*, vol. 16, no. 11, p. 113028, 2014.

[35] I. Nape, E. Otte, A. Vallés, C. Rosales-Guzmán, F. Cardano, C. Denz, and A. Forbes, "Self-healing high-dimensional quantum key distribution using hybrid spin-orbit bessel states," *Optics Express*, vol. 26, no. 21, pp. 26946–26960, 2018.

[36] D. Cozzolino, D. Bacco, B. D. Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenlnwe, "Fiber-based high-dimensional quantum key distribution with twisted photons," in *CLEO Pacific Rim Conference 2018*, p. Th5A.1, Optical Society of America, 2018.

[37] A. Sit, R. Fickler, F. Alsaiari, F. Bouchard, H. Larocque, P. Gregg, L. Yan, R. W. Boyd, S. Ramachandran, and E. Karimi, "Quantum cryptography with structured photons through a vortex fiber," *Optics Letters*, vol. 43, no. 17, pp. 4108–4111, 2018.

[38] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, R. w. Boyd, and E. Karimi, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics Express*, vol. 26, no. 17, pp. 22563–22573, 2018.

[39] F. Hufnagel, A. Sit, F. Grenapin, F. Bouchard, K. Heshami, D. England, Y. Zhang, B. J. Sussman, R. W. Boyd, G. Leuchs, and E. Karimi, "Characterization of an underwater channel for quantum communications in the ottawa river," *Optics Express*, vol. 27, no. 19, pp. 26346–26354, 2019.

[40] V. D'ambrosio, E. Nagali, S. P. Walborn, L. Aolita, S. Slussarenko, L. Marrucci, and F. Sciarrino, "Complete experimental toolbox for alignment-free quantum communication," *Nature communications*, vol. 3, p. 961, 2012.

[41] G. Vallone, V. D'Ambrosio, A. Sponselli, S. Slussarenko, L. Marrucci, F. Sciarrino, and P. Villoresi, "Free-space quantum key distribution by rotation-invariant twisted photons," *Physical Review Letters*, vol. 113, no. 6, p. 060503, 2014.

[42] A. Shamir, "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612–613, 1979.

[43] F.-G. Deng, H.-Y. Zhou, and G. L. Long, "Circular quantum secret sharing," *Journal of Physics A: Mathematical and General*, vol. 39, no. 45, p. 14089, 2006.

[44] J.-L. Hsu, S.-K. Chong, T. Hwang, and C.-W. Tsai, "Dynamic quantum secret sharing," *Quantum Information Processing*, vol. 12, no. 1, pp. 331–344, 2013.

[45] B. Bell, D. Markham, D. Herrera-Martí, A. Marin, W. Wadsworth, J. Rarity, and M. Tame, "Experimental demonstration of graph-state quantum secret sharing," *Nature Communications*, vol. 5, p. 5480, 2014.

[46] Y.-G. Yang, Y.-W. Teng, H.-P. Chai, and Q.-Y. Wen, "Verifiable quantum (k, n)-threshold secret key sharing," *International Journal of Theoretical Physics*, vol. 50, no. 3, pp. 792–798, 2011.

[47] Y.-A. Chen, A.-N. Zhang, Z. Zhao, X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, "Experimental quantum secret sharing and third-man quantum cryptography," *Physical Review Letters*, vol. 95, no. 20, p. 200502, 2005.

[48] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, "Experimental demonstration of four-party quantum secret sharing," *Physical Review Letters*, vol. 98, no. 2, p. 020503, 2007.

[49] G.-P. Guo and G.-C. Guo, "Quantum secret sharing without entanglement," *Physics Letters A*, vol. 310, no. 4, pp. 247–251, 2003.

[50] C. Schmid, P. Trojek, M. Bourennane, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, "Experimental single qubit quantum secret sharing," *Physical Review Letters*, vol. 95, no. 23, p. 230505, 2005.

[51] A. Tavakoli, I. Herbauts, M. Żukowski, and M. Bourennane, "Secret sharing with a single d-level quantum system," *Physical Review A*, vol. 92, no. 3, p. 030302, 2015.

[52] V. Karimipour and M. Asoudeh, "Quantum secret sharing and random hopping: using single states instead of entanglement," *Physical Review A*, vol. 92, no. 3, p. 030301, 2015.

[53] S. Lin, G.-D. Guo, Y.-Z. Xu, Y. Sun, and X.-F. Liu, "Cryptanalysis of quantum secret sharing with d-level single particles," *Physical Review A*, vol. 93, no. 6, p. 062343, 2016.

[54] X.-B. Chen, X. Tang, G. Xu, Z. Dou, Y.-L. Chen, and Y.-X. Yang, "Cryptanalysis of secret sharing with a single d-level quantum system," *Quantum Information Processing*, vol. 17, no. 9, p. 225, 2018.

[55] L. Sheridan and V. Scarani, "Security proof for quantum key distribution using qudit systems," *Physical Review A*, vol. 82, no. 3, p. 030301, 2010.

[56] T. Durt, D. Kaszlikowski, J.-L. Chen, and L. C. Kwek, "Security of quantum key distributions with entangled qudits," *Physical Review A*, vol. 69, no. 3, p. 032313, 2004.

[57] H. Rubinsztein-Dunlop, A. Forbes, M. V. Berry, M. R. Dennis, D. L. Andrews, M. Mansuripur, C. Denz, C. Alpmann, P. Banzer, T. Bauer, *et al.*, "Roadmap on structured light," *Journal of Optics*, vol. 19, no. 1, p. 013001, 2016.

[58] M. Erhard, R. Fickler, M. Krenn, and A. Zeilinger, "Twisted photons: new quantum perspectives in high dimensions," *Light: Science & Applications*, vol. 7, no. 3, p. 17146, 2018.

[59] J. C. Maxwell, "Viii. a dynamical theory of the electromagnetic field," *Philosophical Transactions of the Royal Society of London*, no. 155, pp. 459–512, 1865.

[60] O. Bouchet, H. Sizun, C. Boisrobert, and F. De Fornel, *Free-space optics: propagation and communication*, vol. 91. John Wiley & Sons, 2010.

[61] J. H. Poynting, "The wave motion of a revolving shaft, and a suggestion as to the angular momentum in a beam of circularly polarised light," *Proceedings of the Royal Society of London. Series A, Containing Papers of a Mathematical and Physical Character*, vol. 82, no. 557, pp. 560–567, 1909.

[62] D. L. Andrews and M. Babiker, *The angular momentum of light*. Cambridge University Press, 2012.

[63] S. Franke-Arnold, L. Allen, and M. Padgett, "Advances in optical angular momentum," *Laser & Photonics Reviews*, vol. 2, no. 4, pp. 299–313, 2008.

[64] R. A. Beth, "Mechanical detection and measurement of the angular momentum of light," *Physical Review*, vol. 50, no. 2, p. 115, 1936.

[65] L. Allen, M. W. Beijersbergen, R. Spreeuw, and J. Woerdman, "Orbital angular momentum of light and the transformation of laguerre-gaussian laser modes," *Physical Review A*, vol. 45, no. 11, p. 8185, 1992.

[66] G. Molina-Terriza, J. P. Torres, and L. Torner, "Twisted photons," *Nature Physics*, vol. 3, no. 5, p. 305, 2007.

[67] L. Allen, M. Padgett, and M. Babiker, "Iv the orbital angular momentum of light," in *Progress in Optics*, vol. 39, pp. 291–372, Elsevier, 1999.

[68] A. Forbes, *Laser beam propagation: generation and propagation of customized light*. CRC Press, 2014.

[69] F. Gori, G. Guattari, and C. Padovani, "Bessel-gauss beams," *Optics Communications*, vol. 64, no. 6, pp. 491–495, 1987.

[70] M. J. Padgett and J. Courtial, "Poincaré-sphere equivalent for light beams containing orbital angular momentum," *Optics Letters*, vol. 24, no. 7, pp. 430–432, 1999.

[71] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," *Physical Review A*, vol. 61, no. 6, p. 062308, 2000.

[72] S. Walborn, D. Lemelle, M. Almeida, and P. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," *Physical Review Letters*, vol. 96, no. 9, p. 090501, 2006.

[73] A. C. Dada, J. Leach, G. S. Buller, M. J. Padgett, and E. Andersson, "Experimental high-dimensional two-photon entanglement and violations of generalized bell inequalities," *Nature Physics*, vol. 7, no. 9, pp. 677–680, 2011.

[74] C. H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W. K. Wootters, "Teleporting an unknown quantum state via dual classical and einstein-podolsky-rosen channels," *Physical Review Letters*, vol. 70, no. 13, p. 1895, 1993.

[75] D. Bouwmeester, J.-W. Pan, K. Mattle, M. Eibl, H. Weinfurter, and A. Zeilinger, "Experimental quantum teleportation," *Nature*, vol. 390, no. 6660, pp. 575–579, 1997.

[76] D. Tang, T.-j. Wang, S. Mi, X.-M. Geng, and C. Wang, "High-dimensional circular quantum secret sharing using orbital angular momentum," *International Journal of Theoretical Physics*, vol. 55, no. 11, pp. 4963–4971, 2016.

[77] H. F. Chau, "Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate," *Physical Review A*, vol. 66, no. 6, p. 060302, 2002.

[78] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "High-dimensional quantum cryptography with twisted light," *New Journal of Physics*, vol. 17, no. 3, p. 033033, 2015.

[79] A. Vaziri, J.-W. Pan, T. Jennewein, G. Weihs, and A. Zeilinger, "Concentration of higher dimensional entanglement: qutrits of photon orbital angular momentum," *Physical Review Letters*, vol. 91, no. 22, p. 227902, 2003.

[80] G. Molina-Terriza, A. Vaziri, R. Ursin, and A. Zeilinger, "Experimental quantum coin tossing," *Physical Review Letters*, vol. 94, no. 4, p. 040501, 2005.

[81] A. Einstein, B. Podolsky, and N. Rosen, "Can quantum-mechanical description of physical reality be considered complete?," *Physical Review*, vol. 47, pp. 777–780, May 1935.

[82] J. S. Bell, "On the einstein podolsky rosen paradox," *Physics Physique Fizika*, vol. 1, no. 3, p. 195, 1964.

[83] A. Aspect, P. Grangier, and G. Roger, "Experimental tests of realistic local theories via bell's theorem," *Physical Review Letters*, vol. 47, no. 7, p. 460, 1981.

[84] A. Aspect, P. Grangier, and G. Roger, "Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities," *Physical Review Letters*, vol. 49, no. 2, p. 91, 1982.

[85] E. Karimi and R. W. Boyd, "Classical entanglement?," *Science*, vol. 350, no. 6265, pp. 1172–1173, 2015.

[86] P. Achuthan and K. Venkatesan, "General principles of quantum mechanics," *Handbuch der Physik*, vol. 5, no. Part 1, 1958.

[87] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, "Quantum entanglement," *Reviews of Modern Physics*, vol. 81, no. 2, p. 865, 2009.

[88] R. J. Spreeuw, "A classical analogy of entanglement," *Foundations of physics*, vol. 28, no. 3, pp. 361–374, 1998.

[89] A. Luis, "Coherence, polarization, and entanglement for classical light fields," *Optics communications*, vol. 282, no. 18, pp. 3665–3670, 2009.

[90] N. Gisin and H. Bechmann-Pasquinucci, "Bell inequality, bell states and maximally entangled states for n qubits," *Physics Letters A*, vol. 246, no. 1-2, pp. 1–6, 1998.

[91] R. T. Thew, S. Tanzilli, W. Tittel, H. Zbinden, and N. Gisin, "Experimental investigation of the robustness of partially entangled qubits over 11 km," *Physical Review A*, vol. 66, no. 6, p. 062304, 2002.

[92] D. Stucki, H. Zbinden, and N. Gisin, "A fabry–perot-like two-photon interferometer for high-dimensional time-bin entanglement," *Journal of Modern Optics*, vol. 52, no. 18, pp. 2637–2648, 2005.

[93] J. Leach, B. Jack, J. Romero, M. Ritsch-Marte, R. Boyd, A. Jha, S. Barnett, S. Franke-Arnold, and M. Padgett, "Violation of a bell inequality in two-dimensional orbital angular momentum state-spaces," *Optics Express*, vol. 17, no. 10, pp. 8287–8293, 2009.

[94] C. Rosales-Guzmán, B. Ndagano, and A. Forbes, "A review of complex vector light fields and their applications," *Journal of Optics*, vol. 20, no. 12, p. 123001, 2018.

[95] G. Milione, H. Sztul, D. Nolan, and R. Alfano, "Higher-order poincaré sphere, stokes parameters, and the angular momentum of light," *Physical Review Letters*, vol. 107, no. 5, p. 053601, 2011.

[96] M. McLaren, T. Konrad, and A. Forbes, "Measuring the nonseparability of vector vortex beams," *Physical Review A*, vol. 92, no. 2, p. 023833, 2015.

[97] E. Nagali, L. Sansoni, L. Marrucci, E. Santamato, and F. Sciarrino, "Experimental generation and characterization of single-photon hybrid ququarts based on polarization and orbital angular momentum encoding," *Physical Review A*, vol. 81, no. 5, p. 052317, 2010.

[98] E. Karimi, J. Leach, S. Slussarenko, B. Piccirillo, L. Marrucci, L. Chen, W. She, S. Franke-Arnold, M. J. Padgett, and E. Santamato, "Spin-orbit hybrid entanglement of photons and quantum contextuality," *Physical Review A*, vol. 82, no. 2, p. 022115, 2010.

[99] I. B. Djordjevic, "Multidimensional qkd based on combined orbital and spin angular momenta of photon," *IEEE Photonics Journal*, vol. 5, no. 6, pp. 7600112–7600112, 2013.

[100] J. Liu, I. Nape, Q. Wang, A. Vallés, J. Wang, and A. Forbes, "Multidimensional entanglement transport through single-mode fiber," *Science Advances*, vol. 6, no. 4, 2020.

[101] M. de Oliveira, I. Nape, J. Pinnell, N. TabeBordbar, and A. Forbes, "Experimental high-dimensional quantum secret sharing with spin-orbit-structured photons," *Physical Review A*, vol. 101, no. 4, p. 042303, 2020.

[102] M. de Oliveira, N. Bornman, and A. Forbes, "Random numbers from spatially structured light," *In preparation*, 2020.

[103] B. Ndagano, B. Perez-Garcia, F. S. Roux, M. McLaren, C. Rosales-Guzman, Y. Zhang, O. Mouane, R. I. Hernandez-Aranda, T. Konrad, and A. Forbes, "Characterizing quantum channels with non-separable states of classical light," *Nature Physics*, vol. 13, no. 4, pp. 397–402, 2017.

[104] P. Li, Y. Sun, Z. Yang, X. Song, and X. Zhang, "Classical hypercorrelation and wave-optics analogy of quantum superdense coding," *Scientific Reports*, vol. 5, p. 18574, 2015.

[105] Y. Sun, X. Song, H. Qin, X. Zhang, Z. Yang, and X. Zhang, "Non-local classical optical correlation and implementing analogy of quantum teleportation," *Scientific Reports*, vol. 5, p. 9175, 2015.

[106] A. Pinheiro, C. Souza, D. Caetano, J. Huguenin, A. Schmidt, and A. Khoury, "Vector vortex implementation of a quantum game," *JOSA B*, vol. 30, no. 12, pp. 3210–3214, 2013.

[107] B. Sephton, A. Dudley, G. Ruffato, F. Romanato, L. Marrucci, M. Padgett, S. Goyal, F. Roux, T. Konrad, and A. Forbes, "A versatile quantum walk resonator with bright classical light," *PloS One*, vol. 14, no. 4, 2019.

[108] E. Hecht, "Hecht optics," *Addison Wesley*, vol. 997, pp. 213–214, 1998.

[109] B. E. Saleh and M. C. Teich, *Fundamentals of photonics*. john Wiley & sons, 2019.

[110] J. M. Burch, *Introduction to matrix methods in optics*. Wiley-Interscience, 1975.

[111] M. Beijersbergen, R. Coerwinkel, M. Kristensen, and J. Woerdman, "Helical-wavefront laser beams produced with a spiral phaseplate," *Optics Communications*, vol. 112, no. 5-6, pp. 321–327, 1994.

[112] F. Mok, J. Diep, H.-K. Liu, and D. Psaltis, "Real-time computer-generated hologram by means of liquid-crystal television spatial light modulator," *Optics Letters*, vol. 11, no. 11, pp. 748–750, 1986.

[113] C. Rosales-Guzmán and A. Forbes, *How to shape light with spatial light modulators*. SPIE Press, 2017.

[114] T. W. Clark, R. F. Offer, S. Franke-Arnold, A. S. Arnold, and N. Radwell, "Comparison of beam generation techniques using a phase only spatial light modulator," *Optics Express*, vol. 24, no. 6, pp. 6249–6264, 2016.

[115] J. Wang, J.-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, *et al.*, "Terabit free-space data transmission employing orbital angular momentum multiplexing," *Nature Photonics*, vol. 6, no. 7, p. 488, 2012.

[116] A. Forbes, A. Dudley, and M. McLaren, "Creation and detection of optical modes with spatial light modulators," *Advances in Optics and Photonics*, vol. 8, no. 2, pp. 200–227, 2016.

[117] F. S. Roux and Y. Zhang, "Projective measurements in quantum and classical optical systems," *Physical Review A*, vol. 90, no. 3, p. 033835, 2014.

[118] C. Schulze, S. Ngcobo, M. Duparré, and A. Forbes, "Modal decomposition without a priori scale information," *Optics Express*, vol. 20, no. 25, pp. 27866–27873, 2012.

[119] Y. Aharonov and J. Anandan, "Phase change during a cyclic quantum evolution," *Physical Review Letters*, vol. 58, no. 16, p. 1593, 1987.

[120] S. Pancharatnam, "Generalized theory of interference and its applications," in *Proceedings of the Indian Academy of Sciences-Section A*, vol. 44, pp. 398–417, Springer, 1956.

[121] M. V. Berry, "Quantal phase factors accompanying adiabatic changes," *Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences*, vol. 392, no. 1802, pp. 45–57, 1984.

[122] M. J. Escuti, J. Kim, and M. W. Kudenov, "Controlling light with geometric-phase holograms," *Optics and Photonics News*, vol. 27, no. 2, pp. 22–29, 2016.

[123] M. Martinelli and P. Vavassori, "A geometric (pancharatnam) phase approach to the polarization and phase control in the coherent optics circuits," *Optics communications*, vol. 80, no. 2, pp. 166–176, 1990.

[124] J. Courtial, "Wave plates and the pancharatnam phase," *Optics communications*, vol. 171, no. 4-6, pp. 179–183, 1999.

[125] E. J. Galvez, "Applications of geometric phase in optics," *Recent Research Developments in Optics*, vol. 2, pp. 165–182, 2002.

[126] L. Marrucci, C. Manzo, and D. Paparo, "Optical spin-to-orbital angular momentum conversion in inhomogeneous anisotropic media," *Physical Review Letters*, vol. 96, no. 16, p. 163905, 2006.

[127] E. Brasselet, N. Murazawa, H. Misawa, and S. Juodkazis, "Optical vortices from liquid crystal droplets," *Physical Review Letters*, vol. 103, no. 10, p. 103903, 2009.

[128] F. Cardano, E. Karimi, S. Slussarenko, L. Marrucci, C. de Lisio, and E. Santamato, "Polarization pattern of vector vortex beams generated by q-plates with different topological charges," *Applied Optics*, vol. 51, no. 10, pp. C1–C6, 2012.

[129] E. Brasselet, "Tunable high-resolution macroscopic self-engineered geometric phase optical elements," *Physical Review Letters*, vol. 121, no. 3, p. 033901, 2018.

[130] N. Shitrit, I. Yulevich, E. Maguid, D. Ozeri, D. Veksler, V. Kleiner, and E. Hasman, "Spin-optical metamaterial route to spin-controlled photonics," *Science*, vol. 340, no. 6133, pp. 724–726, 2013.

[131] A. Ambrosio, "Structuring visible light with dielectric metasurfaces," *Journal of Optics*, vol. 20, no. 11, p. 113002, 2018.

[132] E. Hasman, G. Biener, A. Niv, and V. Kleiner, "Space-variant polarization manipulation," *Progess in Optics*, vol. 47, pp. 215–289, 2005.

[133] N. Yu and F. Capasso, "Flat optics with designer metasurfaces," *Nature Materials*, vol. 13, no. 2, pp. 139–150, 2014.

[134] J.-F. Bisson, J. Li, K. Ueda, and Y. Senatsky, "Radially polarized ring and arc beams of a neodymium laser with an intra-cavity axicon," *Optics Express*, vol. 14, no. 8, pp. 3304–3311, 2006.

[135] K. Yonezawa, Y. Kozawa, and S. Sato, "Generation of a radially polarized laser beam by use of the birefringence of a c-cut nd: Yvo4 crystal," *Optics Letters*, vol. 31, no. 14, pp. 2151–2153, 2006.

[136] K. Yonezawa, Y. Kozawa, and S. Sato, "Compact laser with radial polarization using birefringent laser medium," *Japanese Journal of Applied Physics*, vol. 46, no. 8R, p. 5160, 2007.

[137] C. Maurer, A. Jesacher, S. Fürhapter, S. Bernet, and M. Ritsch-Marte, "Tailoring of arbitrary optical vector beams," *New Journal of Physics*, vol. 9, no. 3, p. 78, 2007.

[138] M. Padgett and R. Bowman, "Tweezers with a twist," *Nature Photonics*, vol. 5, no. 6, pp. 343–348, 2011.

[139] L. Marrucci, E. Karimi, S. Slussarenko, B. Piccirillo, E. Santamato, E. Nagali, and F. Sciarrino, "Spin-to-orbital optical angular momentum conversion in liquid crystal "q-plates": Classical and quantum applications," *Molecular Crystals and Liquid Crystals*, vol. 561, no. 1, pp. 48–56, 2012.

[140] E. Nagali, F. Sciarrino, F. De Martini, L. Marrucci, B. Piccirillo, E. Karimi, and E. Santamato, "Quantum information transfer from spin to orbital angular momentum of photons," *Physical Review Letters*, vol. 103, no. 1, p. 013601, 2009.

[141] M. Segev, R. Solomon, and A. Yariv, "Manifestation of berry's phase in image-bearing optical beams," *Physical Review Letters*, vol. 69, no. 4, p. 590, 1992.

[142] M. J. Padgett and J. P. Lesso, "Dove prisms and polarized light," *Journal of Modern Optics*, vol. 46, no. 2, pp. 175–179, 1999.

[143] S. Van Enk, "Geometric phase, transformations of gaussian light beams and angular momentum transfer," *Optics Communications*, vol. 102, no. 1-2, pp. 59–64, 1993.

[144] N. González, G. Molina-Terriza, and J. P. Torres, "How a dove prism transforms the orbital angular momentum of a light beam," *Optics Express*, vol. 14, no. 20, pp. 9093–9102, 2006.

[145] G. C. Berkhout, M. P. Lavery, J. Courtial, M. W. Beijersbergen, and M. J. Padgett, "Efficient sorting of orbital angular momentum states of light," *Physical Review Letters*, vol. 105, no. 15, p. 153601, 2010.

[146] J. Leach, M. J. Padgett, S. M. Barnett, S. Franke-Arnold, and J. Courtial, "Measuring the orbital angular momentum of a single photon," *Physical Review Letters*, vol. 88, no. 25, p. 257901, 2002.

[147] E. J. Galvez and C. D. Holmes, "Geometric phase of optical rotators," *JOSA A*, vol. 16, no. 8, pp. 1981–1985, 1999.

[148] B. Ndagano, I. Nape, B. Perez-Garcia, S. Scholes, R. I. Hernandez-Aranda, T. Konrad, M. P. Lavery, and A. Forbes, "A deterministic detector for vector vortex states," *Scientific Reports*, vol. 7, no. 1, p. 13882, 2017.

[149] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, "Proposed experiment to test local hidden-variable theories," *Physical Review Letters*, vol. 23, no. 15, p. 880, 1969.

[150] S. J. Freedman and J. F. Clauser, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 28, no. 14, p. 938, 1972.

[151] J. F. Clauser, "Experimental investigation of a polarization correlation anomaly," *Physical Review Letters*, vol. 36, no. 21, p. 1223, 1976.

[152] E. S. Fry and R. C. Thompson, "Experimental test of local hidden-variable theories," *Physical Review Letters*, vol. 37, no. 8, p. 465, 1976.

[153] C. A. Kocher and E. D. Commins, "Polarization correlation of photons emitted in an atomic cascade," *Physical Review Letters*, vol. 18, no. 15, p. 575, 1967.

[154] D. C. Burnham and D. L. Weinberg, "Observation of simultaneity in parametric production of optical photon pairs," *Physical Review Letters*, vol. 25, no. 2, p. 84, 1970.

[155] S. Harris, M. Oshman, and R. Byer, "Observation of tunable optical parametric fluorescence," *Physical Review Letters*, vol. 18, no. 18, p. 732, 1967.

[156] D. Kleinman, "Theory of optical parametric noise," *Physical Review*, vol. 174, no. 3, p. 1027, 1968.

[157] A. Mair, A. Vaziri, G. Weihs, and A. Zeilinger, "Entanglement of the orbital angular momentum states of photons," *Nature*, vol. 412, no. 6844, pp. 313–316, 2001.

[158] M. Fox, *Quantum optics: an introduction*, vol. 15. OUP Oxford, 2006.

[159] J. Torres, A. Alexandrescu, and L. Torner, "Quantum spiral bandwidth of entangled two-photon states," *Physical Review A*, vol. 68, no. 5, p. 050301, 2003.

[160] F. Miatto, D. Giovannini, J. Romero, S. Franke-Arnold, S. Barnett, and M. Padgett, "Bounds and optimisation of orbital angular momentum bandwidths within parametric down-conversion systems," *The European Physical Journal D*, vol. 66, no. 7, p. 178, 2012.

[161] J. Romero, D. Giovannini, S. Franke-Arnold, S. Barnett, and M. Padgett, "Increasing the dimension in high-dimensional two-photon orbital angular momentum entanglement," *Physical Review A*, vol. 86, no. 1, p. 012334, 2012.

[162] B. E. Saleh, A. F. Abouraddy, A. V. Sergienko, and M. C. Teich, "Duality between partial coherence and partial entanglement," *Physical Review A*, vol. 62, no. 4, p. 043816, 2000.

[163] F. M. Miatto, A. M. Yao, and S. M. Barnett, "Full characterization of the quantum spiral bandwidth of entangled biphotons," *Physical Review A*, vol. 83, no. 3, p. 033816, 2011.

[164] D. Klyshko, "A simple method of preparing pure states of an optical field, of implementing the einstein–podolsky–rosen experiment, and of demonstrating the complementarity principle," *Soviet Physics Uspekhi*, vol. 31, no. 1, p. 74, 1988.

[165] T. Pittman, Y. Shih, D. Strekalov, and A. V. Sergienko, "Optical imaging by means of two-photon quantum entanglement," *Physical Review A*, vol. 52, no. 5, p. R3429, 1995.

[166] T. Pittman, D. Strekalov, D. Klyshko, M. Rubin, A. Sergienko, and Y. Shih, "Two-photon geometric optics," *Physical Review A*, vol. 53, no. 4, p. 2804, 1996.

[167] R. S. Aspden, D. S. Tasca, A. Forbes, R. W. Boyd, and M. J. Padgett, "Experimental demonstration of klyshko's advanced-wave picture using a coincidence-count based, camera-enabled imaging system," *Journal of Modern Optics*, vol. 61, no. 7, pp. 547–551, 2014.

[168] R. Meyers, K. S. Deacon, and Y. Shih, "Ghost-imaging experiment by measuring reflected photons," *Physical Review A*, vol. 77, no. 4, p. 041801, 2008.

[169] A. I. Lvovsky and T. Aichele, "Conditionally prepared photon and quantum imaging," in *Quantum Communications and Quantum Imaging II*, vol. 5551, pp. 1–6, International Society for Optics and Photonics, 2004.

[170] P.-A. Moreau, E. Toninelli, T. Gregory, and M. J. Padgett, "Ghost imaging using optical correlations," *Laser & Photonics Reviews*, vol. 12, no. 1, p. 1700143, 2018.

[171] Y. Zhang, M. Mclaren, F. S. Roux, and A. Forbes, "Simulating quantum state engineering in spontaneous parametric down-conversion using classical light," *Optics Express*, vol. 22, no. 14, pp. 17039–17049, 2014.

[172] M. Arruda, W. Soares, S. Walborn, D. Tasca, A. Kanaan, R. M. de Araújo, and P. S. Ribeiro, "Klyshko's advanced-wave picture in stimulated parametric down-conversion with a spatially structured pump beam," *Physical Review A*, vol. 98, no. 2, p. 023850, 2018.

[173] P. B. Dixon, G. A. Howland, J. Schneeloch, and J. C. Howell, "Quantum mutual information capacity for high-dimensional entangled states," *Physical Review Letters*, vol. 108, no. 14, p. 143603, 2012.

[174] J. S. Bell, "On the problem of hidden variables in quantum mechanics," *Reviews of Modern Physics*, vol. 38, no. 3, p. 447, 1966.

[175] P. G. Kwiat, K. Mattle, H. Weinfurter, A. Zeilinger, A. V. Sergienko, and Y. Shih, "New high-intensity source of polarization-entangled photon pairs," *Physical Review Letters*, vol. 75, no. 24, p. 4337, 1995.

[176] A. Lamas-Linares, J. C. Howell, and D. Bouwmeester, "Stimulated emission of polarization-entangled photons," *Nature*, vol. 412, no. 6850, pp. 887–890, 2001.

[177] B. S. Cirel'son, "Quantum generalizations of bell's inequality," *Letters in Mathematical Physics*, vol. 4, no. 2, pp. 93–100, 1980.

[178] U. Fano, "Description of states in quantum mechanics by density matrix and operator techniques," *Reviews of Modern Physics*, vol. 29, no. 1, p. 74, 1957.

[179] R. Thew, K. Nemoto, A. G. White, and W. J. Munro, "Qudit quantum-state tomography," *Physical Review A*, vol. 66, no. 1, p. 012303, 2002.

[180] G. M. D'Ariano, M. G. Paris, and M. F. Sacchi, "Quantum tomography," *Advances in Imaging and Electron Physics*, vol. 128, pp. 206–309, 2003.

[181] B. Jack, J. Leach, H. Ritsch, S. Barnett, M. Padgett, and S. Franke-Arnold, "Precise quantum tomography of photon pairs with entangled orbital angular momentum," *New Journal of Physics*, vol. 11, no. 10, p. 103024, 2009.

[182] D. F. James, P. G. Kwiat, W. J. Munro, and A. G. White, "On the measurement of qubits," in *Asymptotic Theory of Quantum Statistical Inference: Selected Papers*, pp. 509–538, World Scientific, 2005.

[183] N. K. Langford, R. B. Dalton, M. D. Harvey, J. L. O'Brien, G. J. Pryde, A. Gilchrist, S. D. Bartlett, and A. G. White, "Measuring entangled qutrits and their use for quantum bit commitment," *Physical Review Letters*, vol. 93, no. 5, p. 053601, 2004.

[184] K. Banaszek, G. D'ariano, M. Paris, and M. Sacchi, "Maximum-likelihood estimation of the density matrix," *Physical Review A*, vol. 61, no. 1, p. 010304, 1999.

[185] M. Agnew, J. Leach, M. McLaren, F. S. Roux, and R. W. Boyd, "Tomography of the quantum state of photons entangled in high dimensions," *Physical Review A*, vol. 84, no. 6, p. 062101, 2011.

[186] R. Jozsa, "Fidelity for mixed quantum states," *Journal of Modern Optics*, vol. 41, no. 12, pp. 2315–2323, 1994.

[187] S. Hill and W. K. Wootters, "Entanglement of a pair of quantum bits," *Physical Review Letters*, vol. 78, no. 26, p. 5022, 1997.

[188] W. K. Wootters, "Entanglement of formation and concurrence.," *Quantum Inf. Comput.*, vol. 1, no. 1, pp. 27–44, 2001.

[189] X. Gao, A. Sergio, K. Chen, S. Fei, and X. Li-Jost, "Entanglement of formation and concurrence for mixed states," *Frontiers of Computer Science in China*, vol. 2, no. 2, pp. 114–128, 2008.

[190] M. de Oliveira, N. Bornman, and A. Forbes, "Holographically-controlled random numbers from entangled twisted photons," *arXiv e-prints*, p. arXiv:2007.07656, 2020.

[191] R. Graham and S. Butler, *Rudiments of Ramsey theory*, vol. 123. American Mathematical Soc., 2015.

[192] N. Metropolis and S. Ulam, "The monte carlo method," *Journal of the American Statistical Association*, vol. 44, no. 247, pp. 335–341, 1949.

[193] P. Mörters and Y. Peres, *Brownian motion*, vol. 30. Cambridge University Press, 2010.

[194] M. Peskin and D. Schroeder, *An Introduction to Quantum Field Theory*. Advanced book classics, Avalon Publishing, 1995.

[195] M. Jeanblanc, M. Yor, and M. Chesney, *Mathematical methods for financial markets*. Springer Science & Business Media, 2009.

[196] T. Palmer, G. Shutts, R. Hagedorn, F. Doblas-Reyes, T. Jung, and M. Leutbecher, "Representing model uncertainty in weather and climate prediction," *Annual Review of Earth and Planetary Sciences*, vol. 33, pp. 163–193, 2005.

[197] A. Schiffler, "Physical entropy in computer games," *Technoetic Arts*, vol. 8, no. 1, pp. 39–45, 2010.

[198] J. von Neumann, "Various techniques used in connection with random digits," in *Monte Carlo Method* (A. S. Householder, G. E. Forsythe, and H. H. Germond, eds.), vol. 12 of *National Bureau of Standards Applied Mathematics Series*, ch. 13, pp. 36–38, Washington, DC: US Government Printing Office, 1951.

[199] J. S. Bell and J. S. Bell, *Speakable and unspeakable in quantum mechanics: Collected papers on quantum philosophy*. Cambridge University Press, 2004.

[200] M. Born, "Statistical interpretation of quantum mechanics," *Science*, vol. 122, no. 3172, pp. 675–679, 1955.

[201] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, "Quantum random number generation," *npj Quantum Information*, vol. 2, no. 1, pp. 1–9, 2016.

[202] A. Marandi, N. C. Leindecker, K. L. Vodopyanov, and R. L. Byer, "All-optical quantum random bit generation from intrinsically binary phase of parametric oscillators," *Optics Express*, vol. 20, no. 17, pp. 19322–19330, 2012.

[203] M. Collins, A. Clark, C. Xiong, E. Mägi, M. Steel, and B. Eggleton, "Random number generation from spontaneous raman scattering," *Applied Physics Letters*, vol. 107, no. 14, p. 141112, 2015.

[204] C. R. Williams, J. C. Salevan, X. Li, R. Roy, and T. E. Murphy, "Fast physical random number generator using amplified spontaneous emission," *Optics express*, vol. 18, no. 23, pp. 23584–23597, 2010.

[205] A. Argyris, E. Pikasis, S. Deligiannidis, and D. Syvridis, "Sub-tb/s physical random bit generators based on direct detection of amplified spontaneous emission signals," *Journal of Lightwave Technology*, vol. 30, no. 9, pp. 1329–1334, 2012.

[206] B. Qi, Y.-M. Chi, H.-K. Lo, and L. Qian, "High-speed quantum random number generation by measuring phase noise of a single-mode laser," *Optics Letters*, vol. 35, no. 3, pp. 312–314, 2010.

[207] M. Jofre, M. Curty, F. Steinlechner, G. Anzolin, J. Torres, M. Mitchell, and V. Pruneri, "True random numbers from amplified quantum vacuum," *Optics Express*, vol. 19, no. 21, pp. 20665–20672, 2011.

[208] C. Vincent, "The generation of truly random binary numbers," *Journal of Physics E: Scientific Instruments*, vol. 3, no. 8, p. 594, 1970.

[209] M. Silverman, W. Strange, C. Silverman, and T. Lipscombe, "Tests for randomness of spontaneous quantum decay," *Physical Review A*, vol. 61, no. 4, p. 042106, 2000.

[210] H.-Q. Ma, Y. Xie, and L.-A. Wu, "Random number generation based on the time of arrival of single photons," *Applied Optics*, vol. 44, no. 36, pp. 7760–7763, 2005.

[211] M. Stipčević and B. M. Rogina, "Quantum random number generator based on photonic emission in semiconductors," *Review of Scientific Instruments*, vol. 78, no. 4, p. 045104, 2007.

[212] M. Herrero-Collantes and J. C. Garcia-Escartin, "Quantum random number generators," *Reviews of Modern Physics*, vol. 89, no. 1, p. 015004, 2017.

[213] A. Acín and L. Masanes, "Certified randomness in quantum physics," *Nature*, vol. 540, no. 7632, pp. 213–219, 2016.

[214] L. Masanes, A. Acín, and N. Gisin, "General properties of nonsignaling theories," *Physical Review A*, vol. 73, no. 1, p. 012112, 2006.

[215] M. Fiorentino, C. Santori, S. Spillane, R. Beausoleil, and W. Munro, "Secure self-calibrating quantum random-bit generator," *Physical Review A*, vol. 75, no. 3, p. 032334, 2007.

[216] M. A. Wayne, E. R. Jeffrey, G. M. Akselrod, and P. G. Kwiat, "Photon arrival time quantum random number generation," *Journal of Modern Optics*, vol. 56, no. 4, pp. 516–522, 2009.

[217] T. Jennewein, U. Achleitner, G. Weihs, H. Weinfurter, and A. Zeilinger, "A fast and compact quantum random number generator," *Review of Scientific Instruments*, vol. 71, no. 4, pp. 1675–1680, 2000.

[218] A. Stefanov, N. Gisin, O. Guinnard, L. Guinnard, and H. Zbinden, "Optical quantum random number generator," *Journal of Modern Optics*, vol. 47, no. 4, pp. 595–598, 2000.

[219] M. Ren, E. Wu, Y. Liang, Y. Jian, G. Wu, and H. Zeng, "Quantum random-number generator based on a photon-number-resolving detector," *Physical Review A*, vol. 83, no. 2, p. 023820, 2011.

[220] S. Pironio, A. Acín, S. Massar, A. B. de La Giroday, D. N. Matsukevich, P. Maunz, S. Olmschenk, D. Hayes, L. Luo, T. A. Manning, *et al.*, "Random numbers certified by bell's theorem," *Nature*, vol. 464, no. 7291, pp. 1021–1024, 2010.

[221] J. von Neumann, "Various techniques used in connection with random digits," *John von Neumann, Collected Works*, vol. 5, pp. 768–770, 1963.

[222] N. Nisan and D. Zuckerman, "Randomness is linear in space," *Journal of Computer and System Sciences*, vol. 52, no. 1, pp. 43–52, 1996.

[223] H.-K. Lo, H. F. Chau, and M. Ardehali, "Efficient quantum key distribution scheme and a proof of its unconditional security," *Journal of Cryptology*, vol. 18, no. 2, pp. 133–165, 2005.

[224] M. Xu, J. Huang, W. Liang, C. Zhang, S. Wang, Z. Yin, W. Chen, and Z. Han, "Adjustable unbalanced quantum random-number generator," *Chinese Optics Letters*, vol. 13, no. 2, pp. 021405–021405, 2015.

[225] A. Sarkar and C. Chandrashekar, "Multi-bit quantum random number generation from a single qubit quantum walk," *Scientific Reports*, vol. 9, no. 1, pp. 1–11, 2019.

[226] Q. Yan, B. Zhao, Q. Liao, and N. Zhou, "Multi-bit quantum random number generation by measuring positions of arrival photons," *Review of Scientific Instruments*, vol. 85, no. 10, p. 103116, 2014.

[227] D. E. Knuth, *The art of computer programming*, vol. 3. Pearson Education, 1997.

[228] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "Nist special publication 800-22 1a: A statistical suite for random and pseudorandom number generators for cryptographic applications," tech. rep., National Institute of Standards and Technology, U.S. Department of Commerce, 2010.

[229] M. Li, P. Vitányi, *et al.*, *An introduction to Kolmogorov complexity and its applications*, vol. 3. Springer, 2008.

[230] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*. MIT press, 2016.

[231] U. M. Maurer, "A universal statistical test for random bit generators," *Journal of Cryptology*, vol. 5, no. 2, pp. 89–105, 1992.

[232] J. Soto, "Statistical testing of random number generators," in *Proceedings of the 22nd national information systems security conference*, vol. 10, p. 12, NIST Gaithersburg, MD, 1999.

[233] K. Charmaine, "Random number generators: An evaluation and comparison of random. org and some commonly used generators," *Management Science and Information Systems Studies. Project Report*, pp. 6–10, 2005.

[234] J. D. Hart, Y. Terashima, A. Uchida, G. B. Baumgartner, T. E. Murphy, and R. Roy, "Recommendations and illustrations for the evaluation of photonic random number generators," *APL Photonics*, vol. 2, no. 9, p. 090901, 2017.

[235] X. Yuan, H. Zhou, Z. Cao, and X. Ma, "Intrinsic randomness as a measure of quantum coherence," *Physical Review A*, vol. 92, no. 2, p. 022124, 2015.

[236] J. Walker, "Ent: a pseudorandom number sequence test program," *Software and documentation available at/www. fourmilab. ch/random/S*, 2008.

[237] R. G. Brown, D. Eddelbuettel, and D. Bauer, "Dieharder: A random number test suite," *Open Source Software Library, under development, URL http://www. phy. duke. edu/~ rgb/General/dieharder. php*, 2013.

[238] K. Marton and A. Suciu, "On the interpretation of results from the nist statistical test suite," *Science and Technology*, vol. 18, no. 1, pp. 18–32, 2015.

[239] K. Marton, A. Suciu, C. Sacarea, and O. Cret, "Generation and testing of random numbers for cryptographic applications," *Proceedings of the Romanian Academy, Series A*, vol. 13, no. 4, pp. 368–377, 2012.

[240] C. E. Shannon, "A mathematical theory of communication," *Bell System Technical Journal*, vol. 27, no. 3, pp. 379–423, 1948.

[241] M. S. Turan, E. Barker, J. Kelsey, K. A. McKay, M. L. Baish, and M. Boyle, "Recommendation for the entropy sources used for random bit generation," *NIST Special Publication*, vol. 800, no. 90B, 2018.

[242] J. Von Neumann, *Mathematische grundlagen der quantenmechanik*, vol. 38. Springer-Verlag, 2013.

[243] M. A. Nielsen and I. Chuang, *Quantum computation and quantum information*. Cambridge University Press, 10th anniversary ed. ed., 2011.

[244] E. Toninelli, B. Ndagano, A. Vallés, B. Sephton, I. Nape, A. Ambrosio, F. Capasso, M. J. Padgett, and A. Forbes, "Concepts in quantum state tomography and classical implementation with intense light: a tutorial," *Advances in Optics and Photonics*, vol. 11, no. 1, pp. 67–134, 2019.

[245] C. Hong and L. Mandel, "Experimental realization of a localized one-photon state," *Physical Review Letters*, vol. 56, no. 1, p. 58, 1986.

[246] Y. Shih, *An introduction to quantum optics: photon and biphoton physics*. CRC press, 2018.

[247] G. Molina-Terriza, J. P. Torres, and L. Torner, "Management of the angular momentum of light: preparation of photons in multidimensional vector states of angular momentum," *Physical Review Letters*, vol. 88, no. 1, p. 013601, 2001.

[248] J. P. Torres, Y. Deyanova, L. Torner, and G. Molina-Terriza, "Preparation of engineered two-photon entangled states for multidimensional quantum information," *Physical Review A*, vol. 67, no. 5, p. 052313, 2003.

[249] R. Ahlswede and I. Csiszár, "Common randomness in information theory and cryptography. part i: secret sharing," *IEEE Transactions on Information Theory*, vol. 39, no. 4, 1993.

[250] B. Schneier, *Applied cryptography: protocols, algorithms, and source code in C*. john wiley & sons, 2007.

[251] A. Karlsson, M. Koashi, and N. Imoto, "Quantum entanglement for secret sharing and secret splitting," *Physical Review A*, vol. 59, no. 1, p. 162, 1999.

[252] A. Sen, U. Sen, M. Żukowski, *et al.*, "Unified criterion for security of secret sharing in terms of violation of bell inequalities," *Physical Review A*, vol. 68, no. 3, p. 032309, 2003.

[253] I.-C. Yu, F.-L. Lin, and C.-Y. Huang, "Quantum secret sharing with multilevel mutually (un) biased bases," *Physical Review A*, vol. 78, no. 1, p. 012344, 2008.

[254] S. Bandyopadhyay, "Teleportation and secret sharing with pure entangled states," *Physical Review A*, vol. 62, no. 1, p. 012308, 2000.

[255] A. C. Nascimento, J. Mueller-Quade, and H. Imai, "Improving quantum secret-sharing schemes," *Physical Review A*, vol. 64, no. 4, p. 042311, 2001.

[256] T. Tyc and B. C. Sanders, "How to share a continuous-variable quantum secret by optical interferometry," *Physical Review A*, vol. 65, no. 4, p. 042310, 2002.

[257] V. Karimipour, A. Bahraminasab, and S. Bagherinezhad, "Entanglement swapping of generalized cat states and secret sharing," *Physical Review A*, vol. 65, no. 4, p. 042320, 2002.

[258] S. Bagherinezhad and V. Karimipour, "Quantum secret sharing based on reusable greenberger-horne-zeilinger states as secure carriers," *Physical Review A*, vol. 67, no. 4, p. 044302, 2003.

[259] L. Xiao, G. L. Long, F.-G. Deng, and J.-W. Pan, "Efficient multiparty quantum-secret-sharing schemes," *Physical Review A*, vol. 69, no. 5, p. 052307, 2004.

[260] D. Fu-Guo, L. Gui-Lu, W. Yan, and X. Li, "Increasing the efficiencies of random-choice-based quantum communication protocols with delayed measurement," *Chinese Physics Letters*, vol. 21, no. 11, p. 2097, 2004.

[261] Y. Li, K. Zhang, and K. Peng, "Multiparty secret sharing of quantum information based on entanglement swapping," *Physics Letters A*, vol. 324, no. 5-6, pp. 420–424, 2004.

[262] L.-F. Han, Y.-M. Liu, J. Liu, and Z.-J. Zhang, "Multiparty quantum secret sharing of secure direct communication using single photons," *Optics Communications*, vol. 281, no. 9, pp. 2690–2694, 2008.

[263] A. M. Lance, T. Symul, W. P. Bowen, B. C. Sanders, and P. K. Lam, "Tripartite quantum state sharing," *Physical Review Letters*, vol. 92, no. 17, p. 177903, 2004.

[264] Y. Zhou, J. Yu, Z. Yan, X. Jia, J. Zhang, C. Xie, and K. Peng, "Quantum secret sharing among four players using multipartite bound entanglement of an optical field," *Physical Review Letters*, vol. 121, no. 15, p. 150502, 2018.

[265] W. Tittel, H. Zbinden, and N. Gisin, "Experimental demonstration of quantum secret sharing," *Physical Review A*, vol. 63, no. 4, p. 042301, 2001.

[266] D. Bouwmeester, J.-W. Pan, M. Daniell, H. Weinfurter, and A. Zeilinger, "Observation of three-photon greenberger-horne-zeilinger entanglement," *Physical Review Letters*, vol. 82, no. 7, p. 1345, 1999.

[267] J.-W. Pan, M. Daniell, S. Gasparoni, G. Weihs, and A. Zeilinger, "Experimental demonstration of four-photon entanglement and high-fidelity teleportation," *Physical Review Letters*, vol. 86, no. 20, p. 4435, 2001.

[268] K.-J. Wei, H.-Q. Ma, and J.-H. Yang, "Experimental circular quantum secret sharing over telecom fiber network," *Optics Express*, vol. 21, no. 14, pp. 16663–16669, 2013.

[269] G. P. He, "Comment on "experimental single qubit quantum secret sharing"," *Physical Review Letters*, vol. 98, no. 2, p. 028901, 2007.

[270] S.-J. Qin, F. Gao, Q.-Y. Wen, and F.-C. Zhu, "A special attack on the multiparty quantum secret sharing of secure direct communication using single photons," *Optics Communications*, vol. 281, no. 21, pp. 5472–5474, 2008.

[271] H. Qin and R. Tso, "Efficient quantum secret sharing based on polarization and orbital angular momentum," *Journal of the Chinese Institute of Engineers*, vol. 42, no. 2, pp. 143–148, 2019.

[272] K.-h. Zhou, Y. Wang, T.-j. Wang, and C. Wang, "Implementation of high capacity quantum secret sharing using orbital angular momentum of photons," *International Journal of Theoretical Physics*, vol. 53, no. 11, pp. 3927–3934, 2014.

[273] M. Smania, A. M. Elhassan, A. Tavakoli, and M. Bourennane, "Experimental quantum multiparty communication protocols," *Npj Quantum Information*, vol. 2, p. 16010, 2016.

[274] L. Marrucci, E. Karimi, S. Slussarenko, B. Piccirillo, E. Santamato, E. Nagali, and F. Sciarrino, "Spin-to-orbital conversion of the angular momentum of light and its classical and quantum applications," *Journal of Optics*, vol. 13, no. 6, p. 064001, 2011.

[275] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "On mutually unbiased bases," *International journal of quantum information*, vol. 8, no. 04, pp. 535–640, 2010.

[276] Y. Jo, H. S. Park, S.-W. Lee, and W. Son, "Efficient high-dimensional quantum key distribution with hybrid encoding," *Entropy*, vol. 21, no. 1, p. 80, 2019.

[277] M. Żukowski, A. Zeilinger, and M. A. Horne, "Realizable higher-dimensional two-particle entanglements via multiport beam splitters," *Physical Review A*, vol. 55, no. 4, p. 2564, 1997.

[278] M. Mirhosseini, M. Malik, Z. Shi, and R. W. Boyd, "Efficient separation of the orbital angular momentum eigenstates of light," *Nature Communications*, vol. 4, p. 2781, 2013.

[279] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," *Physical Review Letters*, vol. 88, no. 12, p. 127902, 2002.

[280] Y.-B. Sheng and F.-G. Deng, "Deterministic entanglement purification and complete nonlocal bell-state analysis with hyperentanglement," *Physical Review A*, vol. 81, no. 3, p. 032307, 2010.

[281] X.-H. Li, "Deterministic polarization-entanglement purification using spatial entanglement," *Physical Review A*, vol. 82, no. 4, p. 044304, 2010.

[282] J. T. Barreiro, T.-C. Wei, and P. G. Kwiat, "Beating the channel capacity limit for linear photonic superdense coding," *Nature Physics*, vol. 4, no. 4, p. 282, 2008.

[283] W.-Y. Wang, C. Wang, and G.-L. Long, "Doubling the capacity of quantum key distribution by using both polarization and differential phase shift," *International Journal of Quantum Information*, vol. 7, no. 02, pp. 529–537, 2009.

[284] M. D. Eisaman, J. Fan, A. Migdall, and S. V. Polyakov, "Invited review article: Single-photon sources and detectors," *Review of Scientific Instruments*, vol. 82, no. 7, p. 071101, 2011.

[285] D. Cozzolino, D. Bacco, B. Da Lio, K. Ingerslev, Y. Ding, K. Dalgaard, P. Kristensen, M. Galili, K. Rottwitt, S. Ramachandran, and L. K. Oxenløwe, "Orbital angular momentum states enabling fiber-based high-dimensional quantum communication," *Physical Review Applied*, vol. 11, p. 064058, Jun 2019.

[286] F. Marsili, V. B. Verma, J. A. Stern, S. Harrington, A. E. Lita, T. Gerrits, I. Vayshenker, B. Baek, M. D. Shaw, R. P. Mirin, *et al.*, "Detecting single infrared photons with 93% system efficiency," *Nature Photonics*, vol. 7, no. 3, p. 210, 2013.

[287] J. Yin, Y. Cao, Y.-H. Li, J.-G. Ren, S.-K. Liao, L. Zhang, W.-Q. Cai, W.-Y. Liu, B. Li, H. Dai, *et al.*, "Satellite-to-ground entanglement-based quantum key distribution," *Physical Review Letters*, vol. 119, no. 20, p. 200501, 2017.

[288] K. J. Resch, M. Lindenthal, B. Blauensteiner, H. Böhm, A. Fedrizzi, C. Kurtsiefer, A. Poppe, T. Schmitt-Manderbach, M. Taraba, R. Ursin, *et al.*, "Distributing entanglement and single photons through an intra-city, free-space quantum channel," *Optics Express*, vol. 13, no. 1, pp. 202–209, 2005.

[289] A. Sit, F. Bouchard, R. Fickler, J. Gagnon-Bischoff, H. Larocque, K. Heshami, D. Elser, C. Peuntinger, K. Günthner, B. Heim, *et al.*, "High-dimensional intracity quantum cryptography with structured photons," *Optica*, vol. 4, no. 9, pp. 1006–1010, 2017.

[290] L. Cui, J. Su, X. Li, and Z. Ou, "Distribution of entangled photon pairs over few-mode fibers," *Scientific Reports*, vol. 7, no. 1, p. 14954, 2017.

[291] F. Bouchard, A. Sit, F. Hufnagel, A. Abbas, Y. Zhang, K. Heshami, R. Fickler, C. Marquardt, G. Leuchs, E. Karimi, *et al.*, "Quantum cryptography with twisted photons through an outdoor underwater channel," *Optics Express*, vol. 26, no. 17, pp. 22563–22573, 2018.

[292] L. C. Andrews and R. L. Phillips, "Laser beam propagation through random media," SPIE, 2005.

[293] F.-G. Deng, G. L. Long, and X.-S. Liu, "Two-step quantum direct communication protocol using the einstein-podolsky-rosen pair block," *Physical Review A*, vol. 68, no. 4, p. 042317, 2003.

[294] F.-G. Deng and G. L. Long, "Secure direct communication with a quantum one-time pad," *Physical Review A*, vol. 69, no. 5, p. 052319, 2004.

[295] G.-L. Long and X.-S. Liu, "Theoretically efficient high-capacity quantum-key-distribution scheme," *Physical Review A*, vol. 65, no. 3, p. 032302, 2002.

[296] F. Zhu, W. Zhang, Y. Sheng, and Y. Huang, "Experimental long-distance quantum secure direct communication," *Science Bulletin*, vol. 62, no. 22, pp. 1519–1524, 2017.

[297] R. Qi, Z. Sun, Z. Lin, P. Niu, W. Hao, L. Song, Q. Huang, J. Gao, L. Yin, and G.-L. Long, "Implementation and security analysis of practical quantum secure direct communication," *Light: Science & Applications*, vol. 8, no. 1, pp. 1–8, 2019.

[298] M. McLaren, J. Romero, M. J. Padgett, F. S. Roux, and A. Forbes, "Two-photon optics of bessel-gaussian modes," *Physical Review A*, vol. 88, no. 3, p. 033818, 2013.