Towards High Dimensional Quantum Key Recycling using Photonic Spatial Modes

THESIS

submitted in partial fulfillment of the
requirements for the degree of

BACHELOR OF SCIENCE
in
PHYSICS

Author :	Pim Eppo Veefkind
Student ID :	s2324822
Supervisor :	Dr. Wolfgang Löffler
Second corrector :	Prof. dr. Serge O. Fehr

Leiden, The Netherlands, July 8, 2021

Towards High Dimensional Quantum Key Recycling using Photonic Spatial Modes

Pim Eppo Veefkind

Huygens-Kamerlingh Onnes Laboratory, Leiden University
P.O. Box 9500, 2300 RA Leiden, The Netherlands

July 8, 2021

Abstract

In this thesis, we work towards a demonstration of quantum key recycling (QKR) using photonic spatial modes. To that end, we first extend the security analysis of QKR provided in Fehr and Salvail's 2016 paper *'Quantum Authentication and Encryption with Key Recycling'* to accommodate for higher dimensional states and to allow for lossy environments. We then show how QKR can be realised using photonic spatial modes and we propose a setup that facilitates it up to a distance of 10 m with a 10% error probability as we confirm by simulation. Next, the theoretical predictions are tested using the classical analogue to single photons, the laser. We show that theory and experiment coincide to such a degree that theoretical expectations are experimentally viable. Finally, we discuss what modifications are required to genuinely demonstrate quantum key recycling using photonic spatial modes.

Contents

Chapter 1

Introduction

The rapid digitisation of society is one, if not the most influential transformation of the past decades. Consequently, safeguarding online data and communications has become pivotal for the functioning of contemporary society. Currently, classical encryption algorithms suffice, but all but one suffer the fundamental shortcoming of being merely computationally secure. That is, security is not theoretically guaranteed but rather depends on the inability of contemporary computers to solve the complex underlying problems. However, this could change, especially in the light of the advent of the quantum computer [1]. The only exception is the classical one time pad which is seldomnly used because it requires a fresh key the length of the message for every message [2]. One solution to this quantum threat also emanates from the quantum realm and concerns quantum encryption schemes, which, contrasting their classical counterparts, are theoretically secure. The most famous of these is quantum key distribution (QKD) using BB84-encrypted qubits [3], with which secure communication over distances in the order of hundreds of kilometers has already been established [4].

Another such algorithm is quantum key recycling (QKR). The main idea behind QKR is to make the key from the one time pad recyclable which is classically impossible. Utilizing the quantum-mechanical phenomenon of superposition, QKR is able to detect eavesdroppers therefore necessitating refreshing the key only if such an eavesdropper is detected. If this is not the case, the key can be recycled lifting the constant refreshment criterion off the classical one time pad making it practically viable. Although its discovery predates QKD [5], the idea remained on the shelves until Gottesman [6] proposed a scheme with partly reusable keys in 2003. A rigorous security analysis was provided in 2005 by Damgård, Pedersen and Salvail [7]. In contrast to the original scheme, the scheme they proved secure requires sender and receiver to be in possession of a quantum computer which was at the time, and still is, technologically infeasible. In 2016 [8], Fehr and Salvail combined the relative simplicity of the original scheme with a security analysis to create a version that is both theoretically secure and realisable with contemporary technology. Since, various extensions and improvements on the scheme have been proposed to increase noise tolerance and efficiency [9–11]. The main advantage QKR holds over QKD is that of message authentication, the ability to verify that a message originates from the intended sender. QKD cannot possibly provide this as it does not involve a shared key and therefore there is no way to differentiate between the intended sender and an impersonator.

Conventionally, QKR requires the communicating parties, commonly referred to as Alice and Bob, to share a private key in advance. The first part of this key, the basis key $\theta \in \{0,1\}^n$, in combination with a randomly generated bitstring $X \in \{0,1\}^n$ is used to prepare the qubits in a state X_i in basis θ_i. These bases are usually the computational and Hadamard bases such that the qubit has uniform probability of being in a state $|0\rangle, |1\rangle, |+\rangle$ and $|-\rangle$. The qubits are then sent to Bob together with a classical message[*] and a classical tag computed from the message and the string X using a message authenticated code (MAC) [12].[†] These can all be intercepted, measured and amended by a malicious eavesdropper Eve who controls the communication channel. Bob then measures the qubits in accordance with θ such that he obtains a string X_B which should be identical to X_A. Using this string he also computes a tag using the same MAC. Finally, he compares the computed tags. If they are identical, classical communication can be initiated using the randomness communicated in X. If not, communication is aborted until a new private key is shared. The protocol is graphically represented in Fig. 1.1. Although promising, an experimental realisation of QKR has never been realised.

This thesis works towards implementing QKR using photonic spatial modes which facilitate qudits up to near arbitrary dimension [13]. To accomplish this, Fehr and Savail's original scheme is first extended in order to allow

[*] This is a random dummy message and not the message Alice actually wants to remain secret.

[†] The MAC computes a tag from the second part of the shared key and the concatenation of X and the message. The map is such that it is impossible to gain information on the shared key from the tag.

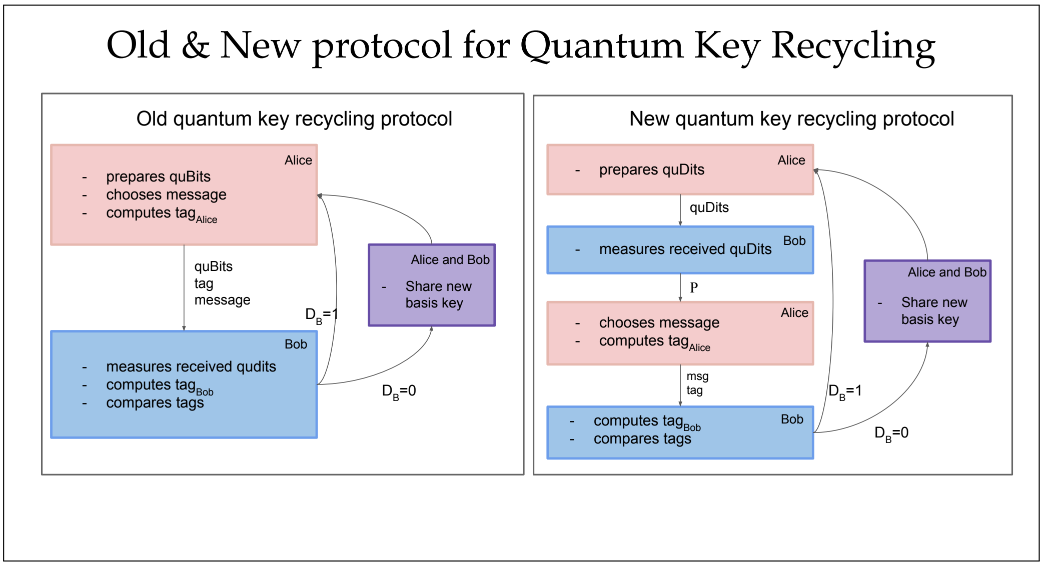


Figure 1.1: *Schematic overview of the protocol presented in [8] (left) and the amended version (right). D_B represents Bob's decision based on the similarity between the tags. In the new protocol, P is a string with information on received quDits.*

for higher dimensional states and to make it robust against the loss-prone environment of experimental reality. The former is achieved by introducing the quantum Fourier transform (QFT)-basis [14, 15] as the natural generalization of the two dimensional Hadamard basis used in the original proof. Similar to these bases, the computational and quantum Fourier bases are mutually unbiased, meaning, in addition to orthonormality of the two bases individually: $|\langle i|\text{QFT}\,|j\rangle\rangle\,|^2 = \frac{1}{D}, \forall i,j \in \{0,1,..,D\}$. It is shown that this generalization does not invalidate the proof. On the contrary, it strengthens the protocol as Eve's knowledge on the key is inversely proportional with the square root of the dimensionality of the qudits. Loss is incorporated by introducing an extra step into the protocol, thereby making it interactive. In this version, at first, Alice only sends over the qudits of which Bob measures those that actually reach him. Bob communicates to Alice which qudits he has received. Alice then calculates the tag using only the elements of X that correspond to qudits that Bob has received. Once again, it is derived that this amendment does not invalidate the proof. By this extension, the scheme is primed for experimental implementation using photonic modes, where losses will be extremely prevalent.

The next chapter discusses how the photonic spatial degrees of freedom are suitable for qudit encryption.[*] A method is introduced to create mutually unbiased sets within these degrees of freedom using position binning. Attention is then diverted to the more practical questions of state creation, state propagation and state detection. Here, a basic familiarity with paraxial optics, complex electric fields and the Fourier property of lenses is assumed as well as the equivalence of photonic probability distributions and classical intensity profiles.[†] Using optical components we sequentially design a setup that can facilitate QKR up to a maximal distance of about 15 meters with an estimated 10% error probability while preserving mutual unbiasedness between the states, at least in simulation. Finally, it is discussed what changes could increase, respectively decrease, the aforementioned results.

In the final chapter we present the experimental realisation of the aforementioned setup. It is shown that the simulations are generally accurate and that the error probabilities are also experimentally feasible. This is all however still performed in a classical setting using intensity distributions instead of single photons. Nevertheless, these results are expected to extrapolate to the quantum realm as the single photon setup equivalent is certainly more challenging from an engineering point of view, but is expected not to introduce any new physics.

[*] These were chosen because they are easy to work with in terms of basis transformation (lens/SLM) and detection of different states (CCD-array). Ultimately, the time-energy degrees of freedom might be more suitable because they allow for in-cable transmission [16]. They are however experimentally cumbersome to work with especially since all states need to be measured at every iteration in order for the protocol to work. Approaches where states are measured in turn and the final result is obtained by applying statistics do not suffice.

[†] As such, they will often be used interchangeably.

Chapter 2

Security analysis high-dimensional & interactive QKR

In this chapter, we present the encryption scheme and provide a proof for its security. It is an extension to Serge Fehr and Louis Salvail's 2016 paper *'Quantum Authentication and Encryption with Key Recycling'* [8] in which they originally proved QKR to be theoretically secure. The amendments include a generalization to arbitrary qudit dimension as well as a modification to the protocol itself to allow for losses between sender and receiver.

In analogy to the original proof, the security is proven in three steps. First, some important mathematical and quantum-cryptographic concepts are introduced and some elementary inequalities derived. Then, these are used to discuss a few versions of a quantum guessing game that will aid in the proof of security of the protocol. Following the introduction of the amended scheme, it is shown that it is still possible to bound the knowledge obtained on the key by a malicious adversary, therefore proving that the modifications do no invalidate the proof.

2.1 Preliminaries

Here, mathematical and cryptographical concepts are introduced to aid our discussions in sections 2.2 and 2.4.

Using the quantum Fourier transform (QFT) [14], we will first define the QFT-basis:

Definition 2.1 (QFT-basis) *Given some Hilbert space of dimension D with orthonormal basis $\{|x_1\rangle, ..., |x_D\rangle\}^*$, one can always construct an orthonormal basis ($\{|y_1\rangle, ..., |y_D\rangle\}$) that is mutually unbiased towards it using the quantum Fourier transform [15]. This is the QFT-basis and its j^{th}-state is given by*

$$|y_j\rangle = \frac{1}{\sqrt{D}} \sum_{k=0}^{D-1} e^{2\pi ikj/D} |x_k\rangle .$$

The operator that transforms between the bases is called QFT and is a unitary operator.

Also, it is possible to re-express the generalized Bell-state $|\phi^+\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} |x_j x_j\rangle$ conveniently using the QFT-operator:

Lemma 1 *The generalized Bell-state can be expressed in terms of the QFT as*

$$|\phi^+\rangle = \frac{1}{\sqrt{D}} \sum_j |x_j x_j\rangle = \frac{1}{\sqrt{D}} \sum_j QFT |x_j\rangle \otimes QFT^\dagger |x_j\rangle .$$

proof.

$$\frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} QFT |x_j\rangle \otimes QFT^\dagger |x_j\rangle = \frac{1}{D^{\frac{3}{2}}} \sum_j \sum_k e^{2\pi ijk/D} |x_k\rangle \otimes \sum_l e^{-2\pi ijl/D} |x_l\rangle =$$

$$\frac{1}{D^{\frac{3}{2}}} \sum_{j,k,l} e^{2\pi ij(k-l)/D} |x_j x_l\rangle = \frac{1}{D^{\frac{3}{2}}} \sum_{j,k} |x_k x_k\rangle = \frac{1}{\sqrt{D}} \sum_k |x_k x_k\rangle$$

Here, the fourth equality is by the general argument that $\sum_{x=0}^{D-1} e^{2\pi ixn/D}, (n, D) \in \mathbb{Z}$ is nonzero only if n is zero or an integer multiple of D. In all other cases, the terms are equidistantly spaced along the unit circle yielding a zero sum. In this specific case, the sum over j is nonzero only if $k = l$.

Definition 2.2 (Schatten$_\infty$-norm) *For any matrix A, the schatten$_\infty$, or standard operator-norm $\|A\|$ outputs the biggest singular value of that matrix: $\|A\| = \sqrt{\max_\lambda(A^\dagger A)}$. It has the following properties [17, 18]:*

- submultiplicativity: $\|AB\| \leq \|A\| \|B\|$
- triangle inequality: $\|A + B\| \leq \|A\| + \|B\|$
- satisfaction of: $\|A\|^2 = \|AA^\dagger\| = \|A^\dagger A\|$
- conservation under unitary transformation: $\|UAU^\dagger\| = \|A\|$

[*] This basis is often referred to as the computational basis in this context.

- for any semi-definite matrix: $\|P\| = \lambda_{max}$[*]
- For semi-definite matrices P,Q with $P < Q$: $\|P\| < \|Q\|$[†]
- if $tr(B) = 1$,for any projection matrix: $tr(PB) \leq \|P\|$[‡]
- for any block diagonal matrix $M = A \oplus B$: $\|M\| = max\{\|A\|, \|B\|\}$.

Definition 2.3 (Schatten$_1$-norm) *For any two matrices A, B, the schatten$_1$-norm, also trace norm, is defined as*

$$\delta(A, B) = \frac{1}{2}\|A - B\|_1 = \frac{1}{2}\sqrt{(A - B)^\dagger (A - B)}.$$

This measure is frequently used in the context of density matrices. In that case, it grants a measure of the similarity between two states ρ, σ. Importantly, it shares the property of conservation under unitary transformation with the Schatten$_\infty$-norm.

Using the properties listed in definition 2.2 two useful lemmas can be derived:

Lemma 2 *Consider four projection, therefore semi-definite operators, P,P', Q and Q' with $P \leq P'$ and $Q \leq Q'$, it holds that*

$$\|PQ\|^2 \leq \|P'Q'\|^2.$$

proof.

Recalling property 6 of 2.2, and considering that $P^2 = P^\dagger P = P$ we have

$$\|PQ\|^2 = \|Q^\dagger P^\dagger PQ\| = \|Q^\dagger PQ\| \leq \|Q^\dagger P'Q\| = \|P'Q\|^2 = \|P'QQ^\dagger P'^\dagger\| =$$

$$\|P'QP'^\dagger\| \leq \|P'Q'P'^\dagger = \|P'Q'\|^2.$$

Definition 2.4 (Set of orthogonal permutations) *The set $\{\pi^k\}$ is the set containing N orthogonal permutations of the string $(0, 1, ..., N - 1)$. Here, orthogonality implies $\pi^i(n) \neq \pi^j(n)$ for $i \neq j$.*

An example of such a set is the set of cyclic permutations for $N = 3$: $\{(0, 1, 2), (2, 0, 1), (1, 2, 0)\}$. In contrast, $\{(0, 1, 2), (2, 0, 1), (2, 1, 0)\}$ are non-orthogonal permutations as $\pi^1(1) = \pi^2(1)$.

[*] λ_{max} is the largest eigenvalue of P.

[†] For two semi-definite matrices A, B, $A \leq B$ means subtracting A from B yields another semi-definite matrix.

[‡] Importantly, the trace of density matrices is 1.

Lemma 3 *given a set of projection matrices $\{P_1, P_2, ..., P_N\}$ and a set $\{\pi^k\}$ as described in 2.4, it holds that*

$$\sum_k \|P_k\| \leq \sum_k \max_i \{\| \sqrt{P_i}\sqrt{P_{\pi_k}(i)}\|\}.$$

proof.

Let us first store the square roots of the projection operators in a $(N \times N)$-block-matrix as $M = \begin{pmatrix} \sqrt{P}_1 & 0 & \dots & 0 \\ \sqrt{P}_2 & \vdots & & \vdots \\ \vdots & \vdots & & \vdots \\ \sqrt{P}_N & 0 & \dots & 0 \end{pmatrix}^{N \times N}$. Here, the entries represent blocks that are either the square root of a projection matrix or completely 0. It is then easy to verify that

$$M^\dagger M = \begin{pmatrix} \sum_i P_i & 0 & \dots & 0 \\ 0 & 0 & & \vdots \\ \vdots & & \ddots & \vdots \\ 0 & \dots & \dots & 0 \end{pmatrix} \text{ and } MM^\dagger = \begin{pmatrix} \sqrt{P}_1\sqrt{P_1} & \dots & \sqrt{P}_1\sqrt{P}_N \\ \vdots & \ddots & \vdots \\ \sqrt{P}_N\sqrt{P}_1 & \dots & \sqrt{P}_N\sqrt{P}_N \end{pmatrix}.$$

Clearly, $\|\sum_i P_i\|$ is the biggest (and only) nonzero eigenvalue of $M^\dagger M$. Combining this with the notion that the sum of projection matrices is also a projection matrix and property 5 of 2.2* we have

$$\|M^\dagger M\| = \|\sum_i P_i\| = \|MM^\dagger\|.$$

This can be decomposed: $MM^\dagger = \sum_k D_k$ where $(D_k)_{ij} = \delta_{j,\pi^k(i)}\sqrt{M_i}\sqrt{M_j}$. Here, the equivalence is assured by the orthogonality of the permutations [19]. For some intuition, consider the cyclic $N = 3$ case once more where

$$\begin{aligned} MM^\dagger = &\begin{pmatrix} \sqrt{P_1}\sqrt{P_1} & 0 & 0 \\ 0 & \sqrt{P_2}\sqrt{P_2} & 0 \\ 0 & 0 & \sqrt{P_3}\sqrt{P_3} \end{pmatrix} + \begin{pmatrix} 0 & 0 & \sqrt{P_1}\sqrt{P_3} \\ \sqrt{P_2}\sqrt{P_1} & 0 & 0 \\ 0 & \sqrt{P_1}\sqrt{P_3} & 0 \end{pmatrix} \\ &+ \begin{pmatrix} 0 & \sqrt{P_1}\sqrt{P_2} & 0 \\ 0 & 0 & \sqrt{P_2}\sqrt{P_3} \\ \sqrt{P_3}\sqrt{P_1} & 0 & 0 \end{pmatrix} \end{aligned}.$$

Also by the orthonormality of the permutations, there is exactly 1 nonzero entry in every row and column of any D_k and hence, using a unitary

*Valid because a projection matrix is necessarily semi-definite transformation, they can all be transformed into block diagonal matrices $D'_k = UD_kU^\dagger$. By the 4th and 8th property of the operator norm we have

$$\sum_k \|D_k\| = \sum_k \|D'_k\| = \sum_k \max\{\|\sqrt{P_i}\|\|\sqrt{P_{\pi_k}(i)}\|\}.$$

Finally, using the triangle inequality we can relate this to the projection matrices to and obtain

$$\sum_k \|P_k\| = \|MM^\dagger\| \leq \|\sum_k D_k\|.$$

Completing the proof.

Remark. The proof is valid for any choice of π^k. Besides the cyclic permutation another important such choice can be obtained by performing the logical bitwise Xor operation between the element number k and the position number within that element i: $\pi^k(i) = i \oplus k$.
Such a set only exists if $N = 2^n$ with $n \in \mathbb{N}$. In this case, the Hamming distance between $\pi^0(i)$ and $\pi^k(i)$ is given by the number of ones in the binary representation of k [20]. Here, the Hamming distance is defined as $h(a,b) = \sum_{j=0}^{n} |a_j - b_j|$ with a, b two bitstrings of length n. The claim follows as

$$h(\pi^0(i), \pi^k(i)) = \sum_{j=0}^{n} |i_j - (i_j + k_j)| = \sum_j k_j.$$

Consequently, the number of permutations with Hamming distance d is given by the binomial distribution: $N_{d=d} = \begin{pmatrix} n \\ d \end{pmatrix}$. We also note that the Hamming distance distribution is independent of i, the entry of every string that is evaluated.

Definition 2.5 (Guessing probability) *Given quantum information E and classical measurement outcomes $\mathcal{X}$, we will define*

$$\text{Guess}(\mathcal{X}|E) := \max_M (P[M(E) = x]).$$

Hence, Guess$(X|E)$ is the maximum probability of obtaining some $x \in \mathcal{X}$ from E by performing the best possible measurement M on E for obtaining that particular x. It has the following elementary properties [8]:

- Guess$(\mathcal{X}|Q(E)) \leq$ Guess$(\mathcal{X}|E)$ where Q is a CPTP map. Essentially, this states the guess cannot be improved by performing some action on E.

- $\text{Guess}(\mathcal{X}|ZE) \leq \sum_z P_Z(z)\text{Guess}(\mathcal{X}|E, Z = z)$, where Z is a classical distribution.
- $\text{Guess}(X|E, \Lambda) \leq \text{Guess}(\mathcal{X}|E)/P(\Lambda)$, where Λ is an event.
- There exists σ_E such that: $\rho_{XE} \leq \text{Guess}(\mathcal{X}|E) \cdot (I_X \otimes \sigma_E) = \text{Guess}(\mathcal{X}|E) \cdot |\chi| \cdot (u_\chi \otimes \sigma_E)$, where μ_χ is the uniform distribution of length $|\chi|$.[*]

Keeping the last definition in mind, we can move away from mathematics and introduce the crypthographic concept of a hash-function.

Definition 2.6 (Hash-function) *A keyed hash-function H is any function that, given some key $k \in \mathcal{K}$ and message $msg \in \mathcal{MSG}$ outputs a fixed length tag $y \in \mathcal{Y}$ such that:*

$$H(k, msg) \to y$$

Such a function is said to be message-independent if, for a uniform distribution k, the distribution of y is independent of msg. If additionally this distribution is uniform, the hash function is considered uniform.

Remark. Intuitively, it can be understood that such hash functions are useful in authentication schemes. Imagine two parties in possession of a shared key. Post interchanging the message, they can compute tags based on the message and their shared key. By comparing tags, they can exclude message-tampering. Since the message can have any length and is usually longer than y, the map is non-injective implying several messages will map to the same y. Consequently, with a small probability ϵ_{MAC} tampering with the message produces the same tag due to the non-injectivity. For a good MAC, this probability is extremely small.

Finally, it is necessary to define some sort of measure for the security of the key. Without going into details, a convenient measure for this is the notion of v-key-privacy:

Definition 2.7 *A hash function H is said to offer v-key-privacy if for any state ρ_{KXYE} with the properties that $\rho_{KX} = \mu_k \otimes \rho_X$, $y = H(K, X)$ and $\rho_K \leftrightarrow \rho_{XY} \leftrightarrow \rho_E$[†] it holds that:*

$$\delta(K, \mu_k|YE) \leq \frac{v}{2}\sqrt{\text{Guess}(X|YE) \cdot |\mathcal{Y}|}$$

[*] For two semi-definite matrices A, B, $A \leq B$ implies subtracting A from B yields another semi-definite matrix

[†] Here, the arrows imply that the states form a Markov-chain state [21]. Practically, it means that E contains no information on k other than through X and Y which can contain information on k.

Here, μ_k is the uniform distribution of k and the privacy is considered ideal if $v = 1$. Also, Guess$(X|YE)$=Guess$(X|E)$ in case H is message-independent. It can be shown that there exist hash functions that satisfy this definition of v-key-privacy [8].

2.2 A Quantum Guessing Game

In this section, different variants of a quantum guessing game are introduced that are closely related to the final security proof. In case of the two player game, it shows that Bob can retrieve Alice's string with 100% accuracy if Alice prepares and sends qudits according to the protocol described in 2.3 and there has been no eavesdropping. All other scenario's are ultimately used to bound expressions in 2.4.

Two Players

Consider a game played by two players, Alice and Bob, according to the following rules:

- Bob prepares m qudits, n of which are sent to Alice.
- Alice performs a measurement on the received qudits according to a string θ uniformly selected from $\{0,1\}^n$. If $\theta_i = 0$, the i$^{\text{th}}$ qudit is measured in the computational basis. In case $\theta_i = 1$, the qudit is measured in the associated QFT-basis. The result is a string $X_A \in \{0,...,D-1\}^n$
- Alice sends θ to Bob.
- Bob performs some measurement on his remaining $m - n$ qudits. This measurement may depend on θ. The result is a string $X_B \in \{0,...,D-1\}^n$
- Alice and Bob compare strings. Bob wins if $X_A = X_B$.

Without specifying either measurement operator (A^θ_X,B^θ_X) or Bob's qudit preparation, the probability for equal strings conditioned on some θ is given by

$$P[X_A = X_B|\theta = \theta_{fixed}] = \sum_X \text{tr}[A^\theta_X \otimes B^\theta_X)\rho_{AB}].$$

Here, the sum over X is the sum over all possible measurement outcomes where $X_A = X_B$. ρ_{AB} is the state prepared by Bob. By the uniformity of θ, the probability averaged over all θ is then given

$$P[X_A = X_B] = \frac{1}{2^n} \sum_{\theta} \sum_{X} \mathrm{tr}[(A_X^\theta \otimes B_X^\theta)\rho_{AB}].$$

Proposition 2.1 *The game described in the section above can be won by Bob with probability:*

$$P[X_A = X_B] = 1$$

proof.

In order to achieve this, Bob should prepare $2n$-qudits into n Bell-state paires, of which one of each pair is sent to Alice. Since this is a pure state the switch is made from density matrix to ket-notation where $\rho_{AB} = |AB\rangle\langle AB|$. Explicitly $|AB\rangle$ is given

$$|AB\rangle = \frac{1}{\sqrt{D}} \sum_{d=0}^{D-1} |dd\rangle_{1,2} \otimes ... \otimes \frac{1}{\sqrt{D}} \sum_{d=0}^{D-1} |dd\rangle_{n-1,n} .$$

Also, as we are working with the computational basis only, we will abbreviate the state $|x_j\rangle$ to $|j\rangle$. Since the pairs are not entangled with one other, it suffices to consider only one pair as $P[X_A = X_B] = P^1 [X_A = X_B]^n$. Alice's measurement operator is fixed: $A_X^\theta = \mathrm{QFT}^\theta |X\rangle\langle X| \mathrm{QFT}^{\theta\dagger}$. Therefore, if Bob chooses $B_X^\theta = \mathrm{QFT}^{\theta\dagger} |X\rangle\langle X| \mathrm{QFT}^\theta$ and we take into consideration the results from Lemma 1 that $(\mathrm{QFT} \otimes \mathrm{QFT}^\dagger)|\phi^+\rangle = |\phi^+\rangle$ *

$$\sum_X \mathrm{tr}\left((A_X^\theta \otimes B_X^\theta)\rho_{AB}\right) = \sum_X \frac{1}{D}\mathrm{tr}\left(|AB\rangle \sum_d \mathrm{Q}_A^{\theta\dagger}\mathrm{Q}_B^\theta \langle dd| \mathrm{Q}_A^\theta \mathrm{Q}_B^{\theta\dagger} |XX\rangle M_b\right)$$

$$= \frac{1}{D}\sum_X \mathrm{tr}\left(\sum_d \mathrm{Q}_A^\theta \mathrm{Q}_B^{\theta\dagger} |dd\rangle\langle dd| \mathrm{Q}_A^{\theta\dagger}\mathrm{Q}_B^\theta\right) = \frac{1}{D}\sum_X \mathrm{tr}(|XX\rangle\langle XX|) = 1.$$

Where we have used Q, M_b as a shorthand for QFT, the bra terms of the projection operator. Completing the proof is straightforward from here:

$$P[X_A = X_B] = \left(\frac{1}{2^1}\sum_0^1 1\right)^n = 1$$

Remark. Writing $|ab\rangle$ for the state of one of the Bell-pairs, the state of the qudit possessed by Bob after Alice has measured its Bell-state partner is

*It can easily be shown that this also holds for $\langle\phi^+|$

given [14]:

$$\mathrm{tr}_X(\sum_X A_X^\theta \otimes \mathbb{I}_B) \left|ab\right\rangle \left\langle ab\right| = \mathrm{tr}_A(\left|ab\right\rangle \left\langle ab\right|) = \frac{1}{D} tr_a(\sum_{d,d'} \left|dd'\right\rangle_{ab} \left\langle dd'\right|_{ab})$$

$$= \frac{1}{D} \sum_{d,d'} \left\langle d|d'\right\rangle_a \left|d\right\rangle_b \left\langle d'\right|_b = \frac{1}{D} \sum_d \left|d\right\rangle_b \left\langle d\right|_b = \mu_b \tag{2.1}$$

where tr_A denotes the partial trace over subsystem A. Hence, after Alice has measured, Bob has qudits whose state is the classical uniform distribution. His whole system can then be described as

$$\rho_B = tr_A \left|AB\right\rangle = tr_a(\left|ab\right\rangle_{1,2} \otimes ... \otimes \left|ab\right\rangle_{n-1,n}) = \mu_b \otimes ... \otimes \mu_b = \mu_B. \tag{2.2}$$

Three Players

In order to mimic the presence of an eavesdropper, the game is now be extended from a two player to a three player version. Qudits are prepared by Bob and Charlie together. Both of them keep a part of the resulting state ρ_{ABC}. After Alice has measured her qudits, both receive θ, from which both have to guess X_A. That is, the winning condition is $X_A = X_B = X_C$. Communication between Bob and Charlie ceases once they have prepared ρ_{ABC}. From the two player discussion, one would expect that using a kind of three qudit Bell-state, Bob and Charlie should be able to win. Winning however does heavily rely on the results obtained in lemma 1 and a three-qudit variant thereof does not exist. Instead, perhaps surprisingly, it can be shown that Bob and Charlie cannot consistently win independent of their strategy.

Proposition 2.2 *The winning probability of the three player game as described above can be upper-bounded*

$$P_{win} = P[X_A = X_B = X_C] \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{D}}\right)^n.$$

proof.

In order to prove this, we will first introduce the projection operator Π^θ: $\Pi^\theta = \sum_X Q^\theta \left|X\right\rangle \left\langle X\right| Q^\theta \otimes B_X^\theta \otimes C_X^\theta$. With this definition and property 5 of definition 2.2, P_{win} can be expressed as

$$P_{win} = \frac{1}{2^n} \sum_\theta \mathrm{tr}(\Pi^\theta \rho_{ABC}) = \frac{1}{2^n} \mathrm{tr}(\sum_\theta \Pi^\theta \rho_{ABC}) \leq \frac{1}{2^n} \| \sum_\theta \Pi^\theta \|.$$

Lemma 3 can now be used to rewrite this as

$$P_{win} \leq \frac{1}{2^n} \| \sum_{\theta} \Pi^{\theta} \| \leq \frac{1}{2^n} \max_{k} \|\Pi^{\theta}\Pi^{\pi^k(\theta)}\|.$$

Here, $\pi^k(\theta)$ represents a set of orthogonal permutations of θ. Let us now introduce two new projection operators $B'^{\theta}_X = \sum_X Q^{\theta} |X\rangle \langle X| Q^{\theta\dagger} \otimes B^{\theta}_X \otimes \mathbb{I}_C$ and $C'^{\theta}_X = \sum_X Q^{\theta'} |X\rangle \langle X| Q^{\theta'\dagger} \otimes \mathbb{I}_B \otimes C^{\theta'}_X$. The former, given some θ applied to ρ_{ABC} outputs the probability of $X_A = X_B$, doing nothing to ρ_C. In contrast, the latter leaves ρ_B intact and uses θ' to measure the probability $X_A = X_C$. These operators are bigger* than Π^{θ},$\Pi^{\theta'}$ respectively and hence by lemma 2:

$$\|\Pi^{\theta}\Pi^{\theta'}\|^2 \leq \|B'^{\theta}_X C'^{\theta'}_X\|^2 = \|B'^{\theta}_X C'^{\theta'}_X B'^{\theta}_X\|$$

Introducing $Q\,|X\rangle = |x^{\theta}\rangle$ the right hand side can be computed

$$B'^{\theta} C'^{\theta'} B'^{\theta} = \sum_{x,y,z} |x^{\theta}\rangle \langle x^{\theta}|y^{\theta'}\rangle \langle y^{\theta'}|z^{\theta}\rangle \langle z^{\theta}| \otimes B^{\theta}_x B^{\theta}_z \otimes C^{\theta'}_y .$$

By the orthogonality of the states that is projected onto $B^{\theta}_x B^{\theta}_z = \delta_{x,z} B^{\theta}_x$ and the prior equation can be rewritten as

$$= \sum_{x,y} |x^{\theta}\rangle \, | \langle x^{\theta}| \, |y^{\theta'}\rangle \, |^2 \, \langle x^{\theta}| \otimes B^{\theta}_x \otimes C^{\theta'}_y = D^{-d(\theta,\theta')} \sum_{x} |x^{\theta}\rangle \langle x^{\theta}| \otimes B^{\theta}_x \otimes \mathbb{I}_C. \tag{2.3}$$

Here $d(\theta,\theta')$ is the Hamming distance between θ and θ'. The equality $| \langle x^{\theta}|y^{\theta'}\rangle |^2 = D^{-d(\theta,\theta')}$ follows by the mutual orthogonality of the bases: $| \langle x^{\theta_i}|y^{\theta'_i}\rangle |^2 = D^{-1}$ given $\theta_i \neq \theta'_i$. Recognizing the right side of the equation as B^{θ}_X

$$\|\Pi^{\theta}\Pi^{\theta'}\| = \sqrt{\|B'^{\theta} C'^{\theta'} B'^{\theta}\|} = D^{-d(\theta,\theta')/2}\sqrt{\|B'^{\theta}\|} \leq D^{-d(\theta,\theta')/2}. \tag{2.4}$$

Recalling our discussion of the special permutation case $\pi^k(i) = i \oplus k$:

$$P_{win} \leq \frac{1}{2^n} \sum_{k} \max_{\theta} D^{-d(\theta,\pi^k(\theta))/2} = \frac{1}{2^n} \sum_{\theta'} D^{-d(\theta,\theta')/2} = \frac{1}{2^n} \sum_{d=0}^{n} \binom{n}{d} D^{-d/2} \tag{2.5}$$

Here, the maximum over θ vanishes as the average distance between θ,θ' is independent of the choice for θ.† Applying the binomial theorem [22] to the obtained bound then yields the promised bound.

*Bigger in the sense that $B^{\theta}_X - \Pi^{\theta}$ yields another semi-definite matrix.

†This is argued in the remark following Lemma 3

In the three player case therefore, Bob and Charlie's probability of winning decreases exponentially with the number of qudits they send Alice.

Remark. The original proof has $\theta \in \Theta \in \{0,1\}^n$, with Θ a code of length $|\Theta|$ with minimal distance d_{min}. The difference being that here, eq.2.5 can be directly bounded by realising $\sum_k \max_\theta D^{-d(\theta,\pi^k(\theta))/2} \leq \sum_k D^{-d_{min}/2}$ such that: $P_{win} \leq \frac{1}{|C|} + \frac{1}{D^{d_{min}/2}}$.

Variation I

The game is now slightly amended by giving Bob and Charlie access to (quantum)- information ρ_E. Although slightly abusive, this is often just written as E. In addition, the uniformity condition on θ is dropped.

Proposition 2.3 *With the introduction of quantum information E, Bob and Charlie's odds of winning increase to:*

$$P_{win} \leq \text{Guess}(\theta|E)\left(1 + \frac{1}{\sqrt{D}}\right)^n$$

proof.

By the fourth property of definition 2.5 the joint semi-definite matrix $\rho_{\theta E}$ is bounded: $\rho_{\theta E} \leq 2^n \cdot \text{Guess}(\theta|E) \cdot (\mu_\theta \otimes \sigma_E)$. Here, $\mu_\theta \otimes \sigma_E$ can be thought of as the state before playing the prior variation.[*] Furthermore, since the mapping[†] $\rho_{\theta E} \to \rho_{ABC} \to \rho_{X_A X_B X_C} \to \rho_{1_{X_A=X_B=X_C}}$ is a CPTP map, by property 1 of the guessing probability $\rho_{\theta E} \geq \rho_{1_{X_A=X_B=X_C}} = (1 + \frac{1}{\sqrt{D}})^n$. This concludes the proof:

$$P_{win} \leq 2^n \cdot \text{Guess}(\theta|E)\left(\frac{1}{2} + \frac{1}{2\sqrt{D}}\right)^n = \text{Guess}(\theta|E)\left(1 + \frac{1}{\sqrt{D}}\right)^n$$

Remark. Since $1 + \frac{1}{\sqrt{D}} > 1$ this expression seems to increase exponentially with n. However, Guess$(\theta|E)$ will also be dependent on n. Specifically, if the information provided by E on θ is only marginal: Guess$(\theta|E) \approx \frac{k}{D^n}$ and we reacquire the bound derived in proposition 2.2 multiplied by a factor k.

[*] There was no quantum information present, however one can easily imagine introducing some quantum information that provides no information on θ, therefore not affecting the result.

[†] This mapping is from $(\{0,1\}^n \otimes \mathcal{H}_E)$ to $\{0,1\}$ where it is 1 when $X_A = X_B = X_C$

Variation II

In the next variation, Bob and Charlie are granted the power to decide which portion of the n qudits send to Alice are actually measured as to simulate loss. After preparing ρ_{ABC}, Bob and Charlie create a list P containing $|P|$[*] qudits from ρ_A. The choice of P is shared with Alice who only measures those qudits that are entries of P and discards the rest. The winning conditions is changed to $X_A^P = X_B = X_C$, where X_A^P is the string obtained by Alice after measuring the qudits specified by P.

Proposition 2.4 *With the novel rule, the bound on the quantum game decreases to*[†]

$$P_{win} \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{D}} \right)^{|P|}. \tag{2.6}$$

proof.

We observe that as long as θ looks uniform to Bob and Charlie, by symmetry, there are no $x \in X_A$ that are easier to guess than others. Therefore, by decreasing the number of qudits they cannot gain an advantage other than that the number of qudits they have to guess is reduced from n to $|P|$. This transforms the game in the original game but with $n = |P|$, wich we already bounded.

Remark. One can easily combine the bounds obtained in variation I and variation II to obtain a bound in case both variations are considered simultaneously. Although not performed explicitly here, one can apply the argument of variation I to the bound of variation II to obtain:

$$P_{win} \leq 2^n \cdot \text{Guess}(\theta|E) \left(\frac{1}{2} + \frac{1}{2\sqrt{D}} \right)^{|P|} \tag{2.7}$$

This expression, by the remark following 2.2 decreases exponentially with $|P|$.

Variation III

For the last variation, let us return to a two player setting. This time, Bob now does not receive θ after Alice's measurements. He is however in pos-

[*] Obviously $|P| \leq n$

[†] We observe that if $|P|$ is chosen a small integer, P_{win} can be reasonably large. In a setting where Bob/Charlie is the adversary, this points towards a blockade attack. One can however easily imagine a game where Alice accepts to play if only if $|P| > p_{min}$

session of the quantum information and qudit reduction measure as introduced priorly.

Proposition 2.5 *Bob's odds of winning given the newly introduced rules are the same as in the prior variation, that is:*

$$P_{win} \leq 2^n \cdot \text{Guess}(\theta|E)(\frac{1}{2} + \frac{1}{2\sqrt{D}})^{|P|}$$

proof.

We remark that there is little use for Bob to wait for Alice to finish her measurements before starting his own. Therefore, any playable strategy is contained within preparing ρ_{AB}, and immediately measuring ρ_B. Now, this is a subset of playable strategies in the prior variant as Bob and Charlie can do the same there. Namely, prepare ρ_{ABC}, immediately measure ρ_B to obtain X_B and copy X_B to X_C. Since this exhausts the strategies in this variant, the previously acquired bound must apply here.

2.3 Overview of the Protocol

Now that we have sufficient knowledge on the relevant concepts, it is possible to introduce the loss-allowing, high dimensional quantum key recycling protocol. To simplify the analysis, a noiseless environment is assumed. Because such an assumption is unrealistic from an experimental point of view, error correction as employed in the original proof [8] will still be required for experimental implementation.

Before execution, it is assumed that Alice and Bob share a private key $k_{sec} = k||\theta$ that is the concatenation of the MAC-key $k \in \{0,1\}^m$ and the basis-key $\theta \in \{0,1\}^n$.

The first step is for Alice to generate a random string $X_A \in \{0, 1, ..., D - 1\}^n$ and perform a QFT on every qudit $|x\rangle$ if $\theta_i = 1$. Hence the resulting state

$$\text{QFT}^{\theta_1} |x_1\rangle \otimes ... \otimes \text{QFT}^{\theta_i} |x_i\rangle \otimes ... \otimes \text{QFT}^{\theta_n} |x_n\rangle = \text{QFT}^{\theta} |X_A\rangle = |B\rangle .$$

From here, we also define the density matrix associated with this state: $\rho_B = |B\rangle \langle B|$. This state is then sent to Bob over a public channel potentially controlled by a malicious eavesdropper Eve.

Bob performs measurements as specified in the subsection 'Two Players' on the qudits he has received to obtain X_B. Since we assumed a noiselessness environment, Bob can retrieve the state of any arriving qudit with 100% accuracy. However, since we did not exclude losses, $|X_B|$ may be much smaller than $|X_A|$. To account for this, Bob creates a list P containing the numbers of the qudits he has received.[*] This list is then forwarded to Alice who computes a tag $\tau_A = \mathrm{MAC}(k, msg||X_A^P))$. Here, X_A^P only contains those X_i specified by P and MAC is a message authentication code which inherits the properties of the Hash function (2.6), in particular uniformity and ideal v-key-privacy (definition 2.7). Alice now sends the tag over to Bob together with the message msg. From this, Bob computes his tag $\tau_B = \mathrm{MAC}(k, msg||X_B)$. Finally, he creates a decision bit D according to $D_B = \mathrm{truth}(\tau_A = \tau_B)$, meaning that $D_B = 1$ if $\tau_A = \tau_B$ and 0 otherwise. If $D_B = 0$ communication is aborted until the key is refreshed. Otherwise, the protocol can be repeated. The procedure is also graphically presented in 2.1.

In case $D = 1$ the message is authenticated and, as we will see soon, the interference of an eavesdropper can be excluded. Exploiting the communicated randomness, the scheme can be transformed from an authentication scheme to an encryption scheme as demonstrated in the original paper [8].

2.4 Bounding the Key

For the protocol to be secure, it should be impossible, or almost impossible, to gain knowledge on either part of the key k_{sec}. In that case, overall security of the proof is guaranteed by the MAC. Hence, it is sufficient to show that it is not possible for an eavesdropper to gain significant knowledge on the key during an execution.[†]

In order to do this, it is important to track the information at any point during the execution. Mapping the information at the black dots in Fig. 2.1[‡]

$$k\theta X_A\underline{BE} \to k\theta X_A\underline{B'\tilde{C}} \to k\theta X_A^P X_B\underline{P\tilde{C}\tau_A} \to k\theta X_A^P \tau_B\underline{\tau_A PC'D} \tag{2.8}$$

Here, E is Eve's quantum system before executing the protocol, $\tilde{C}$ is the state in Eve's quantum memory after Alice has sent the qudits. $\tilde{C}$ therefore

[*] It is assumed that this is somehow possible. How exactly this is achieved is irrelevant.

[†] This is, obviously, under the assumption that the eavesdropper starts without knowledge on the key.

[‡] Once again, the notation is used $\rho_A = A$ as actually $k\theta X_A\underline{BE}$ should be $\rho_{k\theta X_A\underline{BE}}$ etc.

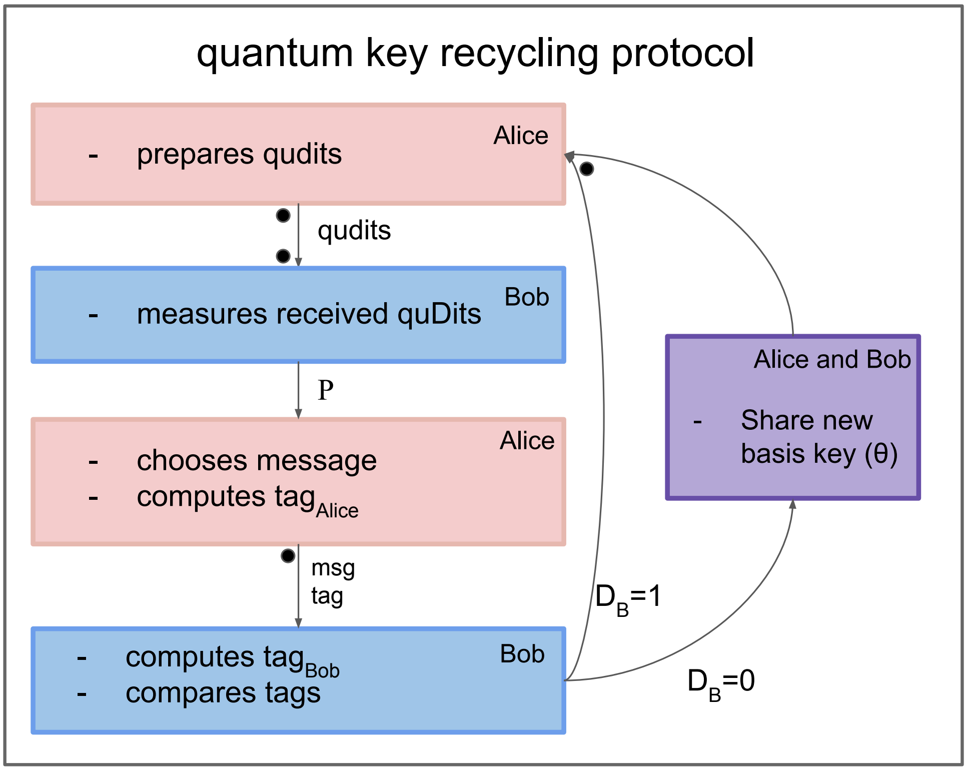


Figure 2.1: *Schematic representation of the authentication scheme. Protocol starts in the upper left corner. Arrows represent transfer of specified information over a public channel controlled by Eve. D_B is the decision made by Bob to accept or reject based on whether $\tau_A = \tau_B$. The black dots are important steps in the informational flow.*

consists of E and the qudit information she keeps (C), possibly entangled. B' is the state, contrived from B, that does reach Bob. Finally, C' is the final state of Eve's quantum memory that she might have changed due to τ_a and P. The underlining means the information is available to Eve. Also, We'll define θ' as the post-execution basis key and E' all information available to Eve at the end of an execution. Here, $\theta' = \theta$ if $D = 1$ and freshly chosen if $D = 0$.

Theorem 2.1 *The interactive QKR protocol as proposed in section 2.1 is secure as an eavesdropper's knowledge on θ, respectively k is upper-bounded by*

$$\text{Guess}(\theta'|E') \leq \frac{1}{2^n} + \text{Guess}(\theta|E)$$

$$\delta(k, \mu_k|\theta' E') \leq 2\epsilon_{\text{MAC}} + \frac{\sqrt{2}}{2}\sqrt{2^n \cdot \text{Guess}(\theta|E)(\frac{1}{2} + \frac{1}{2\sqrt{D}})^{|P|}|\mathcal{T}|}.$$

proof.

For the first claim, recall that Eve's post-execution quantum register E' contains: $E' = C'\tau_A PD$. Using the 2^{th} property of the guessing probability:

$$\text{Guess}(\theta'|E') \leq P(D=0)\text{Guess}(\theta|C'\tau_A P, D=0) +$$

$$P(D=1)\text{Guess}(\theta'|C'\tau_A P, D=1) \leq \frac{1}{2^n} + \text{Guess}(\theta|C'P\tau_A)$$

Where we have used $P(D=0), P(D=1) < 1$ to obtain the final inequality and the fact that the key gets refreshed if and only if $D = 0$. Next, recall that by the information chain in eq.2.8, C' is acquired from $\tilde{C}$ which is in turn acquired from CE. Also, P is extracted from B'. Finally, C and B' are obtained from E and B. Hence, by using property 1 of the guessing probability (2.5) four times:

$$\text{Guess}(\theta|C'P\tau_A) \leq \text{Guess}(\theta|\theta\tilde{C}P\tau_A) \leq \text{Guess}(\theta|\tilde{C}P)$$
$$\leq \text{Guess}(\theta|\tilde{C}B') \leq \text{Guess}(\theta|EB)$$

Here, it is also used that θ cannot depend on τ_A by the message-independence of the MAC. Finally, recalling from eq.2.1 and eq.2.2 that after Alice has measured ρ_A, $\rho_B = \mu_B$* and therefore we obtain $\rho_{B\theta E} = \mu_B \otimes \rho_{\theta E}$. Since B is completely uniform, it cannot provide information on θ which completes the proof.

Moving on to the second claim, let us first define $\tilde{D}$, the idealized version of D. That is, the two are identical but for when $D = 1$ while $X_A^P \neq X_B$ or message/tag/P-tampering has occurred that yielded the same tag by accident. This only happens with probability ϵ_{MAC} as defined in the remark following definition 2.6, which is very small for a good MAC. The two can be related via

$$\delta(k, \mu_k|\theta' TDPC') \leq \delta(k, \mu_k|\tilde{\theta}' T\tilde{D}PC') + 2\epsilon_{MAC}.$$

*The result was obtained in a situation where a generalized Bell-state was prepared after which one of the qudits was measured to produce ρ_B which is the equivalent of B in this game. Altough prepared differently, the resulting states are the same which is why we can use it here.

Here, $\tilde{\theta}'$ is the post-execution basis key associated with the idealized decision $\tilde{D}$. Last, let us assume knowledge on tag/message tampering is contained within Eve's post execution quantum system C' such that by v-key-privacy:

$$\delta(k, \mu_k | \tau_A \tilde{\theta}' 1_{X_A^P = X_B} PC') \leq \frac{1}{2}\sqrt{\text{Guess}(X_A | \tilde{\theta}' 1_{X_A = X_B} PC') |\mathcal{T}|}$$

Splitting the guessing term using its 2^{th} property and immediately upper bounding on $P[X_A^P \neq X_B], P[X_A^P = X_B] \leq 1$:

$$\text{Guess}(X_A^P | T\tilde{\theta}' 1_{X_A^P = X_B} PC') \leq \text{Guess}(X_A^P | \tilde{\theta}' PC', X_A^P \neq X_B) + \text{Guess}(X_A^P | \tilde{\theta}' PC', X_A^P = X_B)$$

For the case $X_A^P \neq X_B$, described by the first term, $\tilde{\theta}'$ is freshly chosen implying X_A^P cannot depend on it. Furthermore, by the same chain as before we find that:

$$\text{Guess}(X_A^P | PC') \leq \text{Guess}(X_A^P | P\tilde{C}) \leq 2^n \cdot \text{Guess}(\theta | E)(\frac{1}{2} + \frac{1}{2\sqrt{D}})^{|P|}$$

Here, the final bound is acquired from the direct correspondence with the third variation of the guessing game (2.2). That is, one player is to guess X_A^P only having access to some priorly existing quantum information.

For the second term, regarding X_C as the measurement outcome of optimally measuring C given θ*:

$$P[X_A^P = X_B]\text{Guess}(X_A^P | \theta PC) \leq P[X_A^P = X_B^P] P[X_A^P = X_C^P] \leq P[X_A^P = X_B^P = X_C^P]$$

This is then exactly the situation described in remark below 2.2 of the quantum guessing game. Hence, similar to the first term:

$$\text{Guess}(X_A^P | \tilde{\theta}' C, X_A^P = X_B) \leq 2^n \cdot \text{Guess}(\theta | E)(\frac{1}{2} + \frac{1}{2\sqrt{D}})^{|P|}$$

Obtaining the final bound on $\delta(k, \mu_k)$ is now only a matter of retracing steps.

Hence, under the assumption of a key appearing completely uniform to an eavesdropper and a secure MAC, the security of high dimensional QKR in a lossy environment as a theoretically secure authentication scheme has been proven. Conversion to the associated theoretically secure encryption scheme can now proceed similarly as described in section 5.2 of [8].

*In the case described by the second term θ is not refreshed and therefore $\tilde{\theta}' = \theta$

Chapter 3

QKR using photonic spatial modes

In this chapter, we develop an implementation of QKR using photonic spatial modes that complies with the security protocol as laid forth in chapter 2. To that end, we first show how mutually unbiased sets of near arbitrary dimension can be constructed using photonic spatial modes [13]. Then, we address the practical questions regarding the design of a realistic setup. These include state creation, state propagation and state detection. In addition to a theoretical discussion, simulations of the different steps are provided using the python library 'Diffractio' for the propagation of classical electric fields. By the direct correspondence between probability distributions and normalized electric field intensity[†], the behaviour of photons. Combining these results, the chapter concludes by providing a simulation of a setup that can facilitate QKR over a distance of 5 m with a maximal single state error probability of approximately 10%.

3.1 Mutual Unbiasedness using photonic spatial modes

The proof provided in chapter 2 implicitly assumes the existence of a mutually unbiased bases (MUB). In particular, the transition from eq.2.3 to eq.2.4 in proposition 2.2 relies on it. Throughout chapter 2, these were assumed to be the computational and QFT-bases but that choice is entirely arbitrary. In fact, any two sets of states can be used as long as they satisfy mutual unbiasedness:

[†] That is, if the field describes monochromatic (laser) light.

Definition 3.1 *Two sets $\{a_1, a_2, ..., a_D\}$ and $\{b_1, b_2, ..., b_D\}$ are considered mutually unbiased if the following conditions are satisfied [23]:*

$$\langle a_i | a_j \rangle = \langle b_i | b_j \rangle = \delta_{ij}, \forall i, j \in \{1, ..., D\}$$
$$| \langle a_i | b_j \rangle |^2 = \frac{1}{D}, \forall i, j \in \{1, ..., D\}$$

Here, the elements of the sets can either be vectors or functions depending on the specific space in question.

In paraxial optics in a linear medium, ignoring polarisation, the field at any plane perpendicular to the optical axis can be expressed as a complex field [24]. These fields will then propagate along the optical axis. We can use this field to define states, which we require to be normalizable. Hence, to construct these states, we have a L^2-space meaning the elements will be square integrable functions $f : \mathbb{R}^n \rightarrow \, , n \in \{1, 2\}$. Here, the value of n depends on the number of transverse dimensions. That is, the number of dimensions perpendicular to the optical axis that are considered. In experiment, this will always be $n = 2$, but $n = 1$ yields less cumbersome formulae for theoretical analysis.

Consequently, the spatial space is (uncountable)-infinitely dimensional and one therefore cannot expect to find a finite dimensional bases for it to conduct QKR with. Instead, one has to construct two mutually independent sets whose elements span a subspace of the complete spatial space. This creates the potential for 'state leakage' into the set's orthogonal complement. The consequences of this are addressed in section 3.3.

The position set

For now, let us focus our attention towards finding sets of functions $\{f_1(x), ..., f_D(x)\}$ and $\{g_1(x), ..., g_D(x)\}$ that satisfy the condition of mutual unbiasedness. To this end, the inner product needs to be explicitly defined

$$\langle a(x) | b(x) \rangle = \int_{-\infty}^{\infty} a(x)^\dagger b(x) dx.$$

The most convenient such set concerns one constructed from D position bins of size d that are equidistantly spaced a distance d' apart. They are graphically represented in Fig. 3.1a and will from now be referred to as the position set or position basis.* Further defining $\tilde{d} = d + d'$, the j-th

*The latter is abusive as the set does not span the entirety of the space.

such state can be mathematically expressed as

$$|p_j(x)\rangle = \frac{1}{\sqrt{d}} \int_{j\tilde{d}}^{j\tilde{d}+d} \delta(x-x')dx'. \tag{3.1}$$

Although intuitively obvious, for completeness sake, they can easily be proven to be orthonormal. Here, without loss of generality, the x-axis is chosen such that the left side of the j^{th}-bin lies at the origin.

$$\int_{-\infty}^{\infty} \int_0^d \delta(x-x')dx' \int_{k\tilde{d}}^{k\tilde{d}+d} \delta(x-x'')dx''dx = \frac{1}{d} \int_0^d \int_{k\tilde{d}}^{k\tilde{d}+d} \delta(x''-x')dx''dx'$$

Here, it was used that $\int_{-\infty}^{\infty} \delta(x-a)\delta(x-b) = \delta_{ab}$. Realising that $x'' = x' + (k-j)\tilde{d}$, the subsitution $u = x'' - (k-j)\tilde{d}$ is made such that

$$= \frac{1}{d} \iint_0^d \delta(x' - (u + (k-j))\tilde{d})dx'du$$

In the special case $k = j$ this evaluates to:

$$\frac{1}{d} \iint_0^d \delta(x'-u)dx'du = \frac{1}{d} \int_0^d du = 1.$$

As when evaluating the inner integral, u lies within the range of x'. In contrast, if $k \neq j$, the inner integral will evaluate to zero as $u + (k-j)d'$ does not lie within $[0, x']$ as $d < \tilde{d}$ for $d' > 0$. Hence, we conclude that $\langle p_j(x)|p_k(x)\rangle = \delta_{jk}$.

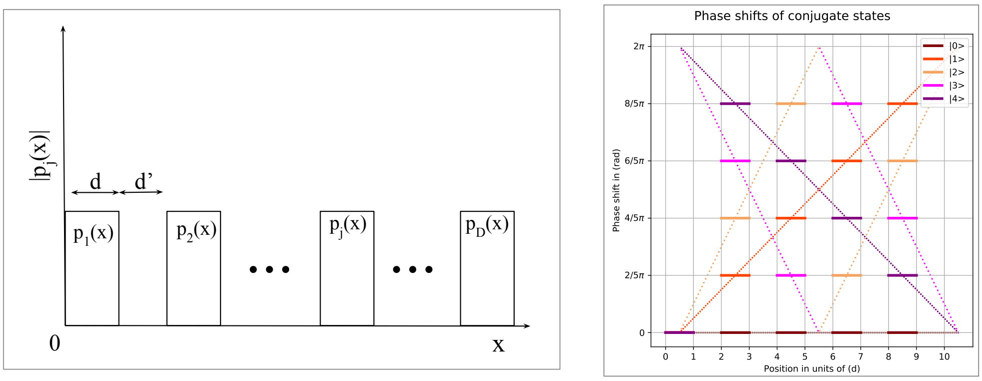
Finding a conjugate set

Having constructed one orthonormal set, the job is now to find a second one that is mutually unbiased towards it. It is important to note that this choice is not unique.* The easiest states to consider are superpositions of the positions bins with constant phase factors for any of the bins: $|m(x)\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D} p_j(x)e^{2\pi i\phi_j}$, for which mutually unbiasedness with the position set is straightforwardly derived

$$|\langle p_j(x)|m(x)\rangle|^2 = |\langle p_j(x)|\frac{1}{\sqrt{D}} \sum_{k=0}^{D} p_k(x)e^{i\phi_k}\rangle|^2 = \frac{1}{D}|\langle p_j(x)|p_j(x)e^{i\phi_j}\rangle|^2 = \frac{1}{D}.$$

*In fact, finding and testing more of such conjugate sets is a promising route to improving overall performance, see section (3.4)

Position and conjugate set



***(a)** Sketch boxcar function that make up the position set. Given the proper normalisation they are orthonormal.*

***(b)** Phase shift of conjugate set with $d' = d$ for $D = 5$. Lines represent the plane waves that the states are named after.*

***Figure 3.1:** Amplitude and phase distribution of the position and momentum sets respectively.*

Consequently, if a D-sized orthonormal set of these superposition states is constructed, it is automatically mutually unbiased towards the position basis. We require that

$$\langle m_m(x)|m_n(x)\rangle = \frac{1}{D}\sum_j p_j^*(x)e^{-i\phi_{jm}}\sum_k p_k(x)e^{i\phi_{kn}} = \frac{1}{D}\sum_j e^{i(\phi_{jn}-\phi_{jm})} = \delta_{mn}.$$

It is physically appealing[*] for all states to have linear phase ramps $\phi_{jm} = 2\pi j \cdot a_m$ where a_m is the phase ramp of such a state. With this restriction, it is obtained that

$$\frac{1}{D}\sum_{j=0}^{D-1} e^{2\pi i j(a_n - a_m)} = \frac{1}{D}\sum_{j=0}^{D-1} e^{2\pi i j \frac{c}{D}} = \delta_{mn}.$$

Where we have made the substitution $a_n - a_m = \frac{c}{D}$. The last equality holds only if $c \in \mathbb{Z}$.[†] The fact that the 2π-periodicity of the purely complex exponential requires $0 \leq a_n - a_m < 1$ for every unique state, in combination

[*] because these states are at least somewhat reminiscent of plane waves, which work well in combination with lenses.

[†] Where the sum (multiplied by the prefactor)is 1 if c is an integer multiple of D and 0 for any other integer.

with the objective of finding a set of length D, then fully fixes c to take on values $\{0, ..., D-1\}$. Hence, apart from the freedom to choose the ramp of the first state[*], the states are fully determined. Making the choice to set the a_m-th state's ramp to 0, the other ramps become: $a_n = \frac{c}{D}$. Naming the states after their respective value for c, the resulting states take on the form:

$$|m_k(x)\rangle = \frac{1}{\sqrt{D}} \sum_{j=0}^{D-1} e^{2\pi ijk/D} |p_j(x)\rangle = QFT(|p_k(x)\rangle) \tag{3.2}$$

This leads us to conclude that we have found suitable bases within the spatial freedom of the photon to conduct QKR with. Also, there is a convenient method of constructing the conjugate states with the help of the quantum Fourier transform. In addition, this choice is unique under the assumptions of constant, linearly increasing phase shifts between the positions states. In the remainder of the thesis the conjugate states will often be referred to as momentum state because of the linear phase ramp reminiscent of optical plane waves, which have a well defined momentum.

3.2 State creation using a Spatial Light Modulator

Having acquired a method of constructing mutually unbiased bases in the spatial degree of freedom, it is now necessary to focus attention away from theoretical questions and start addressing more practical ones. The first of these is the matter of state creation. Explicitly, this implies manipulating an electric field such that it takes on forms specified in eq.3.1 and eq.3.2. Considering the phase jumps introduced in the momentum basis, full control over the phase profile is required. In addition, if there is no premature fixing on section 3.1's d and d' parameters, amplitude control is also required. One way to achieve this is using a spatial light phase modulator (SLM). Such a device applies an arbitrary phase shift $\phi(n,m)$ to any of its $(N \times M)$ pixels of size (l_x, l_y). Mathematically this can be expressed as[†]

$$E_{out}(x,y) = \sum_{i=0}^{N} \sum_{j=0}^{M} \int_{il_x}^{(i+1)l_x} \int_{jl_y}^{(j+1)l_y} E_{in}(x,y) e^{i\phi(n,m)} \delta(x-x')\delta(y-y') dx'dy'.$$

[*] Choosing the first state is essentially adding a global phase factor which is of no physical relevance.

[†] Altough certainly very insightful, this expression is very cumbersome to work with.

It is immediately clear that such a device grants direct control over the light's phase profile on length scales l: $l_{x/y} < l < Nl$. Complete amplitude control is obtained by applying an extra phase ramp to a part of the incoming light. This phase ramp bends part of the light with an angle $\theta = \arctan(\frac{\lambda}{nl_{x/y}})$, where n is the number of pixels used for a phase cycle. [*] The light that has been bent is said to be 1^{th}-order light and The unaffected light is said to be 0^{th}-order in accordance with standard grating terminology [24]. One can formally show that by using a phase-only SLM like this, any desired light profile can be constructed in the 0^{th}- or 1^{th}-order [25].[†] Since real SLMs are non-ideal, not all light will be deflected into the first order even with a full 2π-phase cycle. Hence, the 1^{th}-order will be used to create the states and the 0^{th}-order will contain all left-over light.

By estimating the angle θ using typical values $\lambda = 0.633\,\mu\text{m}$[‡], $n = 5$, $l_x = 10\,\mu\text{m}$ it is found that $\theta \approx 1°$. Consequently, taking a typical SLM width $Nl_x = 1\,\text{cm}$, full separation between the 0^{th}- and 1^{th}-order light happens only after 50 cm. Even then, introducing optical elements that only affect the 1^{th}-order will be hard. Hence, a filtering system is introduced, that, using a 4f-imaging system and an adjustable slit gets rid of any non 1^{th}-order light. The design is schematically represented in figure 3.2.

Using this design, state creation can be simulated. In figure 3.3 this is performed in five dimensions with the states from 3.1 displayed on the SLM. The light is evolved using the Diffractio module which uses the Rayleigh-Sommerfeld approximation for propagation.

In Fig. 3.3b we see that, using this method, states can be created that are reasonably close to the boxcar functions of 3.1. Due to diffraction effects, the square fields produced by the SLM have, upon arriving at the imaging plane, lost their sharp edges. A quick visual inspection lead us to conclude that they are better approximated by gaussians. Importantly, this is of no consequence to security as the states still show a high degree of orthonormality (Fig.3.3d), which is ultimately what matters, not the exact shape of the field. In addition, this figure also shows all squares of inner products between position and momentum states to be close to $\frac{1}{5}$ as expected. Specifically, the mean is 0.189 with a standard deviation of 0.01 which is

[*] To deflect all light going through the pixels to whom the ramp is applied this cycle goes from 0 to 2π.

[†] The proof is omitted here as the experimental realization does not live or die with this result.

[‡] This choice stems from the fact that helium-neon lasers, a very common laser, emits with this wavelength.

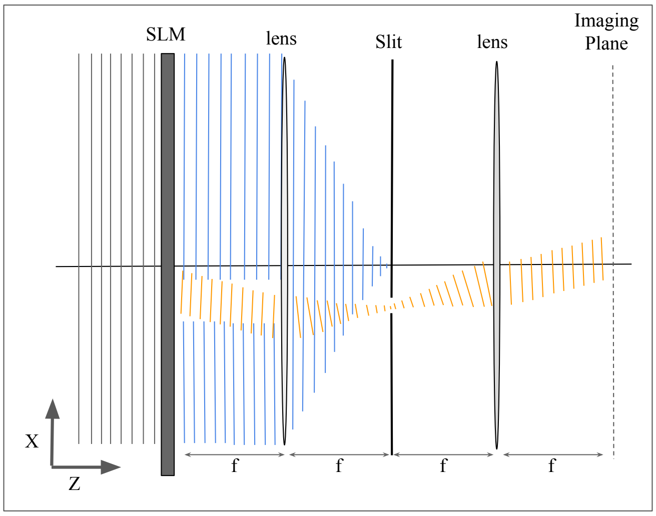


Figure 3.2: *1^{th}-order filtering using a 4F-imaging system. The phase ramp is applied to the orange light which is deflected into the first order.By the properties of such a system, the field in the imaging plane is exactly the same but for a mirroring in the x-direction, both in amplitude and phase, as the 1^{th}-order light in the SLM-plane. [24].*

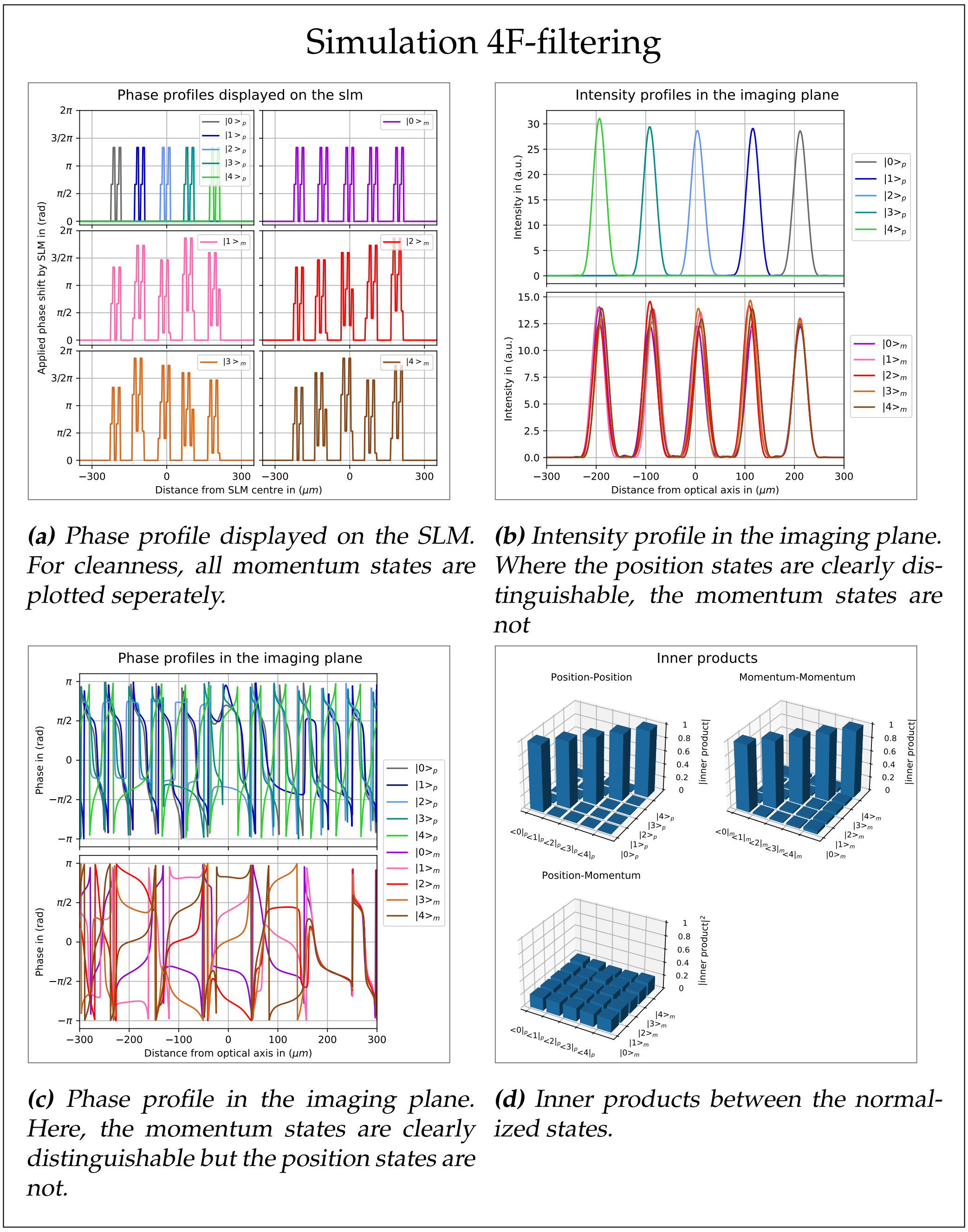
reasonably unbiased. As a final comment, Fig. 3.3c shows the momentum states to be much more distinguished in their phase profiles. This is expected because their intensity profiles are so similar. From an information theoretic point of view, the waves representing different states need to carry that information somewhere. If it is not carried in the amplitude it needs to be contained within the phase.

One (legitimate) concern regarding the applicability of the simulation is the fact that it was performed using a plane wave SLM input. Viable source candidates however, most likely lasers, will be gaussian-shaped in the transverse dimensions [26]. For the light incident on the SLM

$$|E_{SLM}(x,y)| \propto e^{-\frac{x^2+y^2}{2\sigma^2}} \approx 1 - \frac{x^2+y^2}{2\sigma^2}.$$

Here, σ is the beam width at the SLM and the approximation is valid for small $x^2 + y^2$. If the condition on the source is now placed that $\sigma > 5 \cdot \frac{D}{2}(d + d') - \frac{d'}{2} = 5 \cdot x_{max}$*, in our one dimensional case ($y = 0$) this

[*] This is the constrained that the standard deviation be five times bigger than the distance from the outer position bins to the centre.



(a) *Phase profile displayed on the SLM. For cleanness, all momentum states are plotted seperately.*

(b) *Intensity profile in the imaging plane. Where the position states are clearly distinguishable, the momentum states are not*

(c) *Phase profile in the imaging plane. Here, the momentum states are clearly distinguishable but the position states are not.*

(d) *Inner products between the normalized states.*

Figure 3.3: *Simulation of state creation using a phase-only SLM and a 4f-lensing system for the following parameters:* $d = 40\,\mu\text{m}$, $d' = 60\,\mu\text{m}$, $l_x = 8\,\mu\text{m}$, $n = 3$, $f = 20\,\text{cm}$ *and slit size* $5\,\text{mm}$. *The transverse (X) direction has size* $1\,\text{cm}$ *and contains* $10{,}000$ *points.*

gives

$$\frac{|E_{SLM}(x_{max})|}{|E_{SLM}(0)|} \approx \frac{1-(\frac{x_{max}}{5\sqrt{2}x_{max}})^2}{1} = 0.98. \tag{3.3}$$

Hence, under this assumption on the source, the plane wave approximation is sufficient and the simulation realistic.

3.3 Propagation through the eavesdroppable zone

In this section, the propagation of the light between the communicating parties is discussed. First, the effect of diffraction is discussed and a relation derived between the realistic transmission distance and the initial beam width. Then, theoretical evidence is provided that mutual unbiasedness is preserved during propagation which is then also confirmed by simulations.

Diffraction and divergence

The setup described in Fig. 3.2 creates mutually unbiased states that could in principle be sent directly to Bob. Any propagating beam however is subject to beam widening in the transverse dimensions caused by diffraction. For gaussian beams, the widening of the beam width is given by [26]:

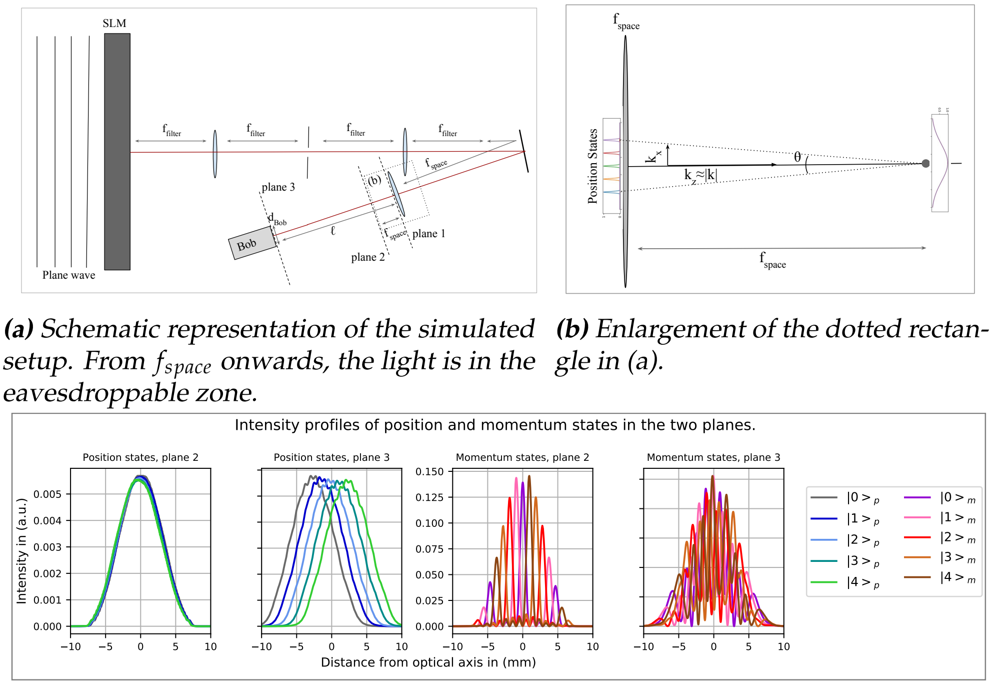
$$w(z) = w_0\sqrt{1+(\frac{z\lambda}{\pi w_0^2})^2}$$

Here, $w_0 = 2\sigma$ is the original beam width and z is the propagated distance measured from the focus. Considering the small initial beam widths at the focus (imaging plane) of only about 30 µm, the effect of diffraction will be very profound. Taking $z = 5\,\text{m}$, the beam width will have grown to: $w(5m) = 60\,\mu\text{m}\sqrt{1+(\frac{5\,\text{m}\cdot 0.5\,\mu\text{m}}{\pi\cdot 60\,\mu\text{m}^2})^2} \approx 1.3\,\text{cm}$. Therefore even this tiny propagation distance already requires Bob to have measurement or focal equipment of significant size. Perhaps surprisingly, to overcome this issue, the initial beam width has to be increased. A convenient way to achieve this is using a lens. By its Fourier property [24], for the absolute value of the field we obtain

$$|E(x)| = \mathcal{F}(e^{-\frac{x^2}{2\sigma_{old}^2}}) = e^{-\frac{1}{2}\sigma_{old}^2 k_x^2}.$$

By a geometric argument based on 3.4b, $x = \frac{k_y}{|k|} f = \frac{k_y \lambda f}{2\pi}$, and by simple substitution, we obtain $\sigma_{new} = \frac{\lambda f}{2\pi\sigma_{old}}$. Computing this using some typical values: $\sigma_{new} \approx \frac{0.5\,\mu\text{m}\cdot 0.5\,\text{m}}{2\pi\cdot 30\,\mu\text{m}} = 1.3\,\text{mm}$, and therefore:
$w(5\,\text{m}) = 2.6\,\text{mm}\sqrt{1 + (\frac{5\,\text{m}\cdot 0.5\,\mu\text{m}}{\pi\cdot 2.6\,\text{mm}^2})^2} = 2.6\,\text{mm}$, which is smaller by almost one order.

Simulation of the eavesdroppable zone



(a) *Schematic representation of the simulated setup. From f_{space} onwards, the light is in the eavesdroppable zone.*

(b) *Enlargement of the dotted rectangle in (a).*

(c) *Intensity profiles of the position and momentum states at the planes as specified at (a). The mutual diverging of the position states in the eavesdroppable zone is clearly visible. Diffraction however is negligible as the states are sufficiently wide. In contrast, the momentum states do not diverge but all the different peaks diffract widening them considerably. The result is a very chaotic profile.*

Figure 3.4: *Simulation of the propagation of light through the eavesdroppable zone. Parameters are identical to that of Fig 3.3 with the exception of d' which is set* 40 µm*. In addition, $f_{space} = 60\,\text{cm}$ and $l = 10\,\text{m}$. Since $\frac{l}{f_{sp}} \approx 17 < 42$ all light is contained within a* 2 cm *area.*

In addition to diffraction, there are also momentum considerations that pose a restriction if we want Bob's setup to be of workable dimensions. The different position states gain different transverse momenta once they propagate through the lens, posing the risk of diverging past a point where Bob can collect them using a reasonably sized lens. To investigate this concern, the states will be approximated as a beam of size 2σ. This can be done as the ray-approximation neglects diffraction but that has already been dealt with. Looking at Fig. 3.4b, the angle θ is given $\theta = \frac{(D-1)(d+d')}{f}$, and consequently for the transverse distance between the outer edges of the extremal states at a distance l:

$$x_{max} = (l-f)\theta + 2\sigma = (l-f)\frac{(D-1)(d+d')}{f} + 2\sigma < \frac{l(D-1)(d+d')}{f} + 2\sigma < d_{Bob}$$

Here, the last inequality does not follow logically but is a restriction if Bob wants to catch the majority of the light with optical equipment of diameter d_{Bob}. Taking $d = 2\,\text{cm}$ and setting the other parameters like in the previous simulations, the ratio between focal and transmission length can be lower bounded: $\frac{l}{f} < \frac{d_{bob}-2\cdot\sigma}{(D-1)(d+d')} = \frac{2\,\text{cm} - 2\cdot 0.3\,\text{cm}}{4(40\,\mu\text{m}+40\,\mu\text{m})} = 42$. This points towards the biggest problem using spatial degrees of freedom for encryption purposes namely that the required optical equipment size is unrealistic for transmission over significant distance. Although one can probably find ways to increase this bound a bit, the problem seems rather fundamental. Resultingly, the spatial degrees of freedom seem to be of little use beyond demonstrational purposes.

Mutual Unbiasedness during Propagation

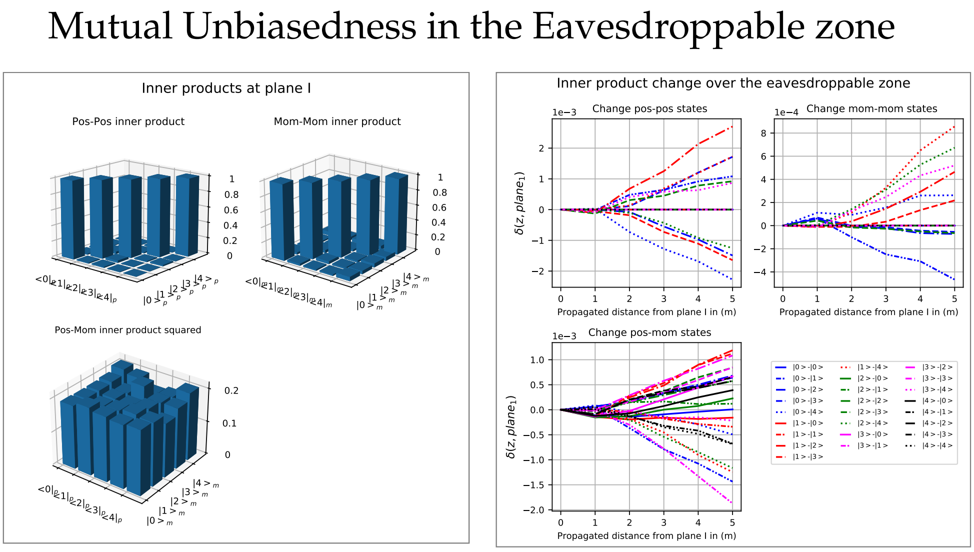
Figure 3.3 shows the mutual unbiasedness of the states, but this by itself is insufficient to claim mutual unbiasedness throughout the eavesdroppable zone. Between state creation and the eavesdroppable zone operations are performed on the light. If these operations are not unitarian for instance due to absorption, inner product is certainly not preserved which affects mutual unbiasedness and therefor the security of the procedure.

Instead, a proof of mutual unbiasedness at plane I of Fig. 3.4a in addition to a proof of preservation of inner product during propagation is required. The former is straightforward, at least in simulation, and is shown in Fig. 3.5a. The latter is a result of the unitarity of linear optics [27], a proof of which is beyond the scope of this thesis. In our context, this theorem states that any action onto a state $\psi \to \psi'$ can be represented by a unitary operator U from which conservation of the inner product immediately follows:

$$\langle \psi_1' | \psi_2' \rangle = \langle \psi_1 | U^{\dagger} U | \psi_2 \rangle = \langle \psi_1 | \psi_2 \rangle$$

Defining the inner product change through the eavesdroppable zone as:

$\delta(z,0) = \langle\psi_1(z)|\psi_2(z)\rangle - \langle\psi_1(0)|\psi_2(0)\rangle$, this can also be tested in simulation. Here, distance is measured from f_{space}, the start of the eavesdroppable zone. Theoretically, this quantity should always evaluate to zero.



(a) Inner products at plane 1. The states are very close to being mutually unbiased.

(b) Evolution of mutually unbiasedness throughout the eavesdroppable zone. A state pair $|i\rangle$ - $|j\rangle$ should be interpreted as $|i\rangle_{p/m}$ - $|j\rangle_{p/m}$ with p/m in accordance with the title of the subplot.

***Figure 3.5:** Simulation of the evolution of mutually unbiasedness in the eavesdroppable zone. From (a) it can be deduced that the states start out almost mutually unbiased. Combining this with information from (b), it is confirmed that the states are (almost) mutually unbiased everywhere in the eavesdroppable zone.*

Interestingly, the inner products are not completely preserved during the simulation. Although changes are only in the order of 10^{-3}, the change is correlated with distance meaning this could pose a serious problem if the setup is elongated. That is, in simulation only [*], because it is assumed that this is merely an error in simulation, considering the rigidness and fundamentality of the theory underlying the preservation of inner products within linear optics and the tiny inner product deviation. In the remainder of this thesis it is therefore assumed that in reality these deviations do

[*] The origin of this peculiar behavior is unknown and certainly deserves to be properly investigated. It might originate from the method the Diffractio module uses to propagate the fields.

not occur.

3.4 State detection

The final step in designing a suitable setup for QKR is corporealizing the grey box labeled 'Bob' in Fig 2.1. The goal of this apparatus is to create a string X_B from the incoming photons that is identical to X_A. By the result presented in the subsection 'Two players' in 2.2 this should be possible with 100% accuracy. The goal therefore is to construct physical manifestations of the operators (B^{θ}_{X}) that can distinguish between the different states. As established in chapter 2, the choice of operator may depend on θ, the key shared between Alice and Bob. This allows us the freedom to adjust the setup in accordance with θ. This might be done without any regard for conservation of mutual unbiasedness as it is assumed the eavesdropper cannot interfere once the light is inside Bob's apparatus.

Discriminating between position states

The first step is to find a method to discriminate between the position states. Recall that the states in the imaging plane in Fig 3.2 have the same intensity and phase profiles as when produced at the SLM.* This plane in turn lies exactly one focal length away from Alice's last lens implying that the field one focal length into the eavesdroppable zone can be described as [24]

$$E(l = f_{space}, x) = \mathcal{F}\left(E_{imag}(\frac{x}{\lambda f_{space}})\right).$$

Defining $l_{ex} = l - 2f_{space}$ then, and placing a lens with focal length $f = f_{space} = f_{sp}$ at the beginning of Bob's apparatus, we can calculate the field a focal distance further on to be

$$E(z = l + f_{sp}, x) = e^{i\frac{k}{2f}(1-\frac{l_{ex}+f_{sp}}{f_{sp}})x^2}\mathcal{F}(E(z = f_{sp}, x)) = e^{i\frac{k}{2f}(1-\frac{l_{ex}+f_{sp}}{f_{sp}})x^2}E_{imag}(-x).$$

Where the phase factor is the result of the interlens distance not being exactly of length $2f_{sp}$. This however is of no consequence if a measurement is performed:

$$P[x_a < x < x_b] = \int_{x_a}^{x_b} e^{-i\phi(x)}E_{imag}(-x)^{\dagger}e^{i\phi(x)}E_{imag}(-x)dx = \int_{x_a}^{x_b} I_{imag}(-x)dx$$

*That is, but for the transformation of the states from boxcar to gaussians by diffraction.

Here, the phase factor has been abbreviated to $\phi(x)$ and $I_{imag}(-x)$ is the intensity in the imaging plane. Since the position states can be clearly discriminated in the imaging plane (Fig. 3.3(b)), this gives a straightforward way to distinguish the position states given a camera with pixels that are at least an order smaller than the width of the gaussians. If this condition is met the position state gaussians are all well seperated and can be accurately resolved. Consequently, illumination of a particular pixel can be traced back to a particular state. Of course, when two intensity profiles overlap, there is an associated error with this. To quantify the similarity between two states for Bob, we'll define the overlap integral:

$$\mathrm{O}(|i\rangle_p, |j\rangle_p) = \int_{-\infty}^{\infty} \tilde{I}_i(x)\tilde{I}_j(x)dx^*$$

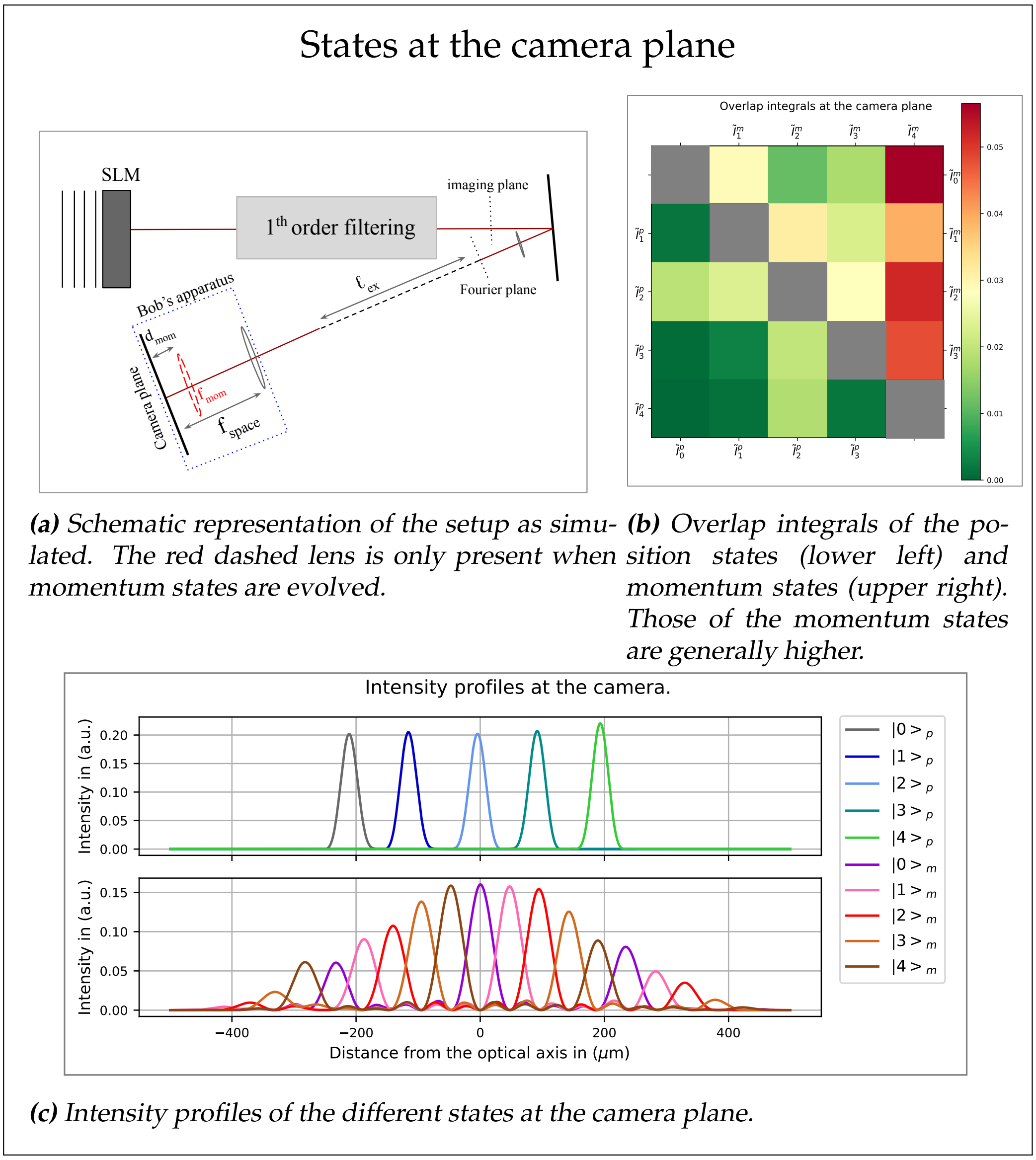
Where $\tilde{I}$ is the normalized intensity at the plane $z = l + f_{sp}$ such that $\mathrm{O} = 1$ for fully overlapping state and $\mathrm{O} = 0$ for perfectly separable states. Judging from the results of 3.3, this should guarantee accurate position state discrimination as is confirmed in simulation in 3.6.

Discriminating between momentum states

In contrast to discriminating the position states, discriminating the momentum states is significantly less trivial. In fact, finding a setup that yields overlap integrals as good as the position states is one of, if not the most important unsolved challenge remaining within the project. The elementary solution involves positioning a lens with focal distance f_m a distance d_m from the camera as in Fig.3.6a. The discrepancy between f_m and d_{mom} corrects for the phase factor obtained during propagation and the fact that the lens is not ideally positioned such that f_{sp} and f_m constitute a 4F-system. Finding optimal values for f_m and d_m is best performed numerically for fixed f_{space} and l. In the simulation of Fig. 3.6, Scipy's least squares method is used for this. From the figure, it can immediately be concluded that this solution is not optimal as there is clear overlap between momentum states. Consequently, Bob will not be able to tell the state of a photon sent in the momentum basis with 100% certainty. From a security perspective, all these errors have to be ascribed to be due to the eavesdropper. As a result, X_A and X_B may be different to such an extent that even noise correction will not suffice in reconciliating the strings, which would mean the key needs to be refreshed without even the pres-

[*] In reality, the camera is not infinitely long and the bounds will be at the outer most pixels.

ence of an eavesdropper*. It is therefore of the utmost importance that future efforts are directed towards decreasing the error probability.



(a) *Schematic representation of the setup as simulated. The red dashed lens is only present when momentum states are evolved.*

(b) *Overlap integrals of the position states (lower left) and momentum states (upper right). Those of the momentum states are generally higher.*

(c) *Intensity profiles of the different states at the camera plane.*

Figure 3.6: *Simulation of the light observed by Bob at the camera plane. Used parameters were identical to those at 3.4. Furthermore it was chosen to fix* $f_{mom} = 100\,\mathrm{mm}$. *Using least square fitting, the ideal momentum lens distance was determined* $d_{mom} = 62\,\mathrm{mm}$.

*This would also directly hinder the main goal of QKR, namely to recycle the key.

Optimizing Bob's measurements

From the same figure, it can be observed that all overlap integrals are upper bounded by 0.07. Although this by itself is acceptable, one has to realize how the total error rate is related to this. Generally, to determine which state caused a particular pixel excitation, one divides the pixels into intervals where a particular state dominates. When a photon is detected in that interval it is then assumed to come from the dominant state. The error probability for the i^{th}-state with dominating intervals $\{(x_s^1, x_f^1), ..., (x_s^n, x_f^n)\}$:

$$P_{err}^i = \sum_{k=0}^{n} P[x_s^k < x < x_f^k | i] \frac{P[!i]}{P[!i] + P[i]} = \sum_{k=0}^{n} \int_{x_s^k}^{x_f^k} I_i' dx \frac{\sum_{j \neq i} \int_{x_s^k}^{x_f^k} \tilde{I}_j dx}{\int_{x_s^k}^{x_f^k} \tilde{I}_i dx + \sum_{j \neq i} \int_{x_s^k}^{x_f^k} \tilde{I}_j dx}$$

Here, I' is the intensity normalized over the chosen intervals.[*] $P[i]$ and $P[!i]$ are the probability that an excitation is or is not caused by the dominant state. Compared to the overlap integral, this quantity more accurately represents the error probability. It does however require establishing the intervals where the overlap integral does not. Hence, the overlap integral is sometimes preferred. Realistically, the two will be heavily correlated, implying that optimizing either one will likely suffice. However, strictly, it is the error probability that needs to be minimized.

One possible method for minimizing the error probability concerns post-selection of photons based on which pixel is excited. In particular, the regions where there is no clear dominant state can be excluded and regarded as loss. This strategy is applied to the states shown in Fig. 3.7, which yields error probabilities of at most 10%. Such a strategy would however require another amendment to the security analysis as this kind of non-uniform post-selection with regard to θ is currently not included. Intuitively, such post-selection would necessitate randomly discarding position state photons such that X_B contains approximately as much position as momentum state photons but this needs to be investigated more carefully.

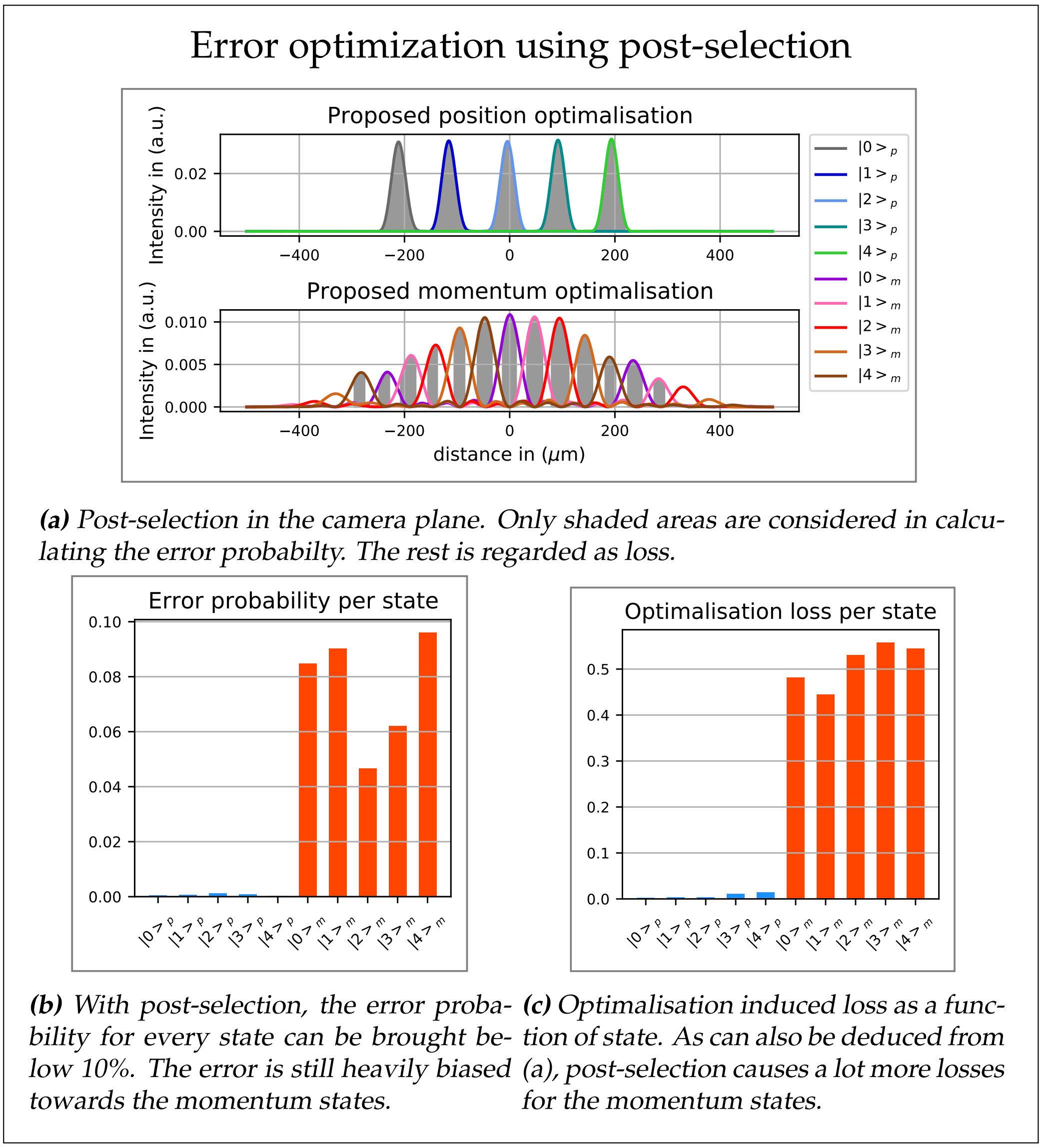
There is a possibility that such post-selection is ultimately not necessary with additional changes to the setup. As priorly mentioned, the momentum states are orthonormal meaning they should be fully separable. Possibly, a path other than the current momentum lens exists to better seperate the momentum state in intensity. We attempted to add higher order poly-

[*] In contrast to $\tilde{I}$ which is normalized over the whole of x.

nomial terms to the phase distribution of the momentum lens

$$\phi_{new}(x) = \phi_{lens}(x) + ax^3 + bx^4 = \frac{\pi}{\lambda f_{mom}} x^2 + ax^3 + bx^4.$$

However, least square fitting converged to $\phi_{lens}(x)$ even with variable d_{mom}. This is, however, far from an exhaustive search so there might be other configurations that yield better results possibly containing several lenses or other optical equipment.



***(a)** Post-selection in the camera plane. Only shaded areas are considered in calculating the error probabilty. The rest is regarded as loss.*

***(b)** With post-selection, the error probability for every state can be brought below 10%. The error is still heavily biased towards the momentum states.*

***(c)** Optimalisation induced loss as a function of state. As can also be deduced from (a), post-selection causes a lot more losses for the momentum states.*

***Figure 3.7:** Simulation of error optimization at Bob's. Momentum errors are reduced to below 10% in return for a 50% loss.*

Chapter 4

Experimental realization

After having optimized the experimental design in the previous chapter, we now turn to the experimental implementation, and compare the results to the simulations. The measurements are all still performed using monochromatic laser light instead of single photons. Nevertheless, it is shown that, besides some minor details, simulation and experiment agree to such an extent that running the encryption scheme is actually feasible.

4.1 Setup

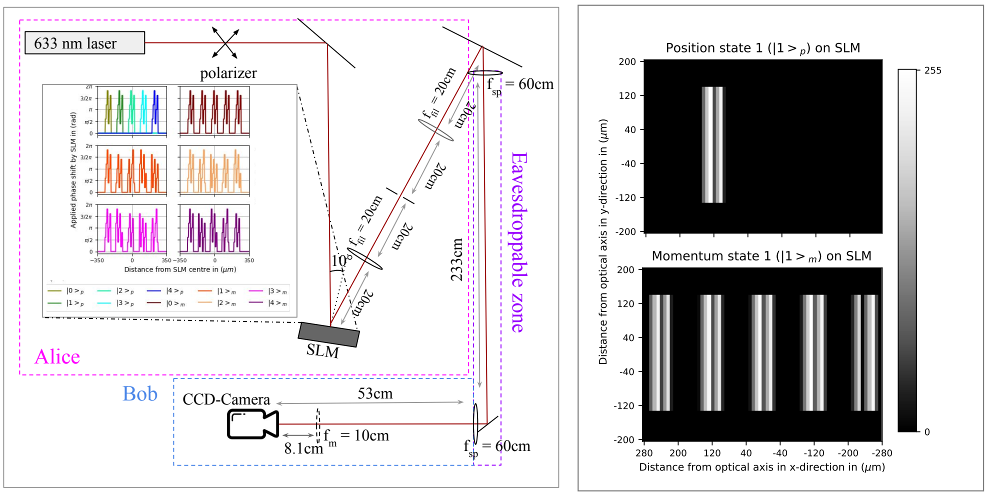
The constructed setup is very reminiscent of that presented in Fig. 3.6. The plane-wave source is provided using a 633 nm helium-neon laser satisfying the constraint posed in Eq. 3.3. The light is then guided towards a (8 µm x 8 µm) spatial light modulator (Holoeye Pluto) under a 10° angle of incidence. The per pixel phase shift on the SLM can be controlled by means of a (1920 x 1080)-greyscale image that is pixel-wise converted to a phase shift $\phi(\text{pix}) = \gamma(w(\text{pix})) \approx \frac{2\pi \cdot w(\text{pix})}{255}$ with $w(\text{pix})$ the brightness of a pixel in the greyscale image. The 1-dimensional states of Fig. 4.1a are displayed along the x-direction. Here, the state parameters are chosen $d = 40\,\mu\text{m}$ and $d' = 60\,\mu\text{m}$.[†] Furthermore, the number of pixels per 2π-revolution is 3. Every pixel further away from the SLM centre also gets zero phase shift.[‡] In the y-direction, the image is displayed on the centre 34 pixels such that the height of the fields (initially $34 \cdot 8\,\mu\text{m} = 270\,\mu\text{m}$) is

[†] For definitions of these parameters 3.1

[‡] This is the vast majority as the SLM is much larger.

roughly conserved under propagation through the lenses.* We developed software based on the python library 'Pygame' that allows fast switching between the states by pressing the associated key to portray the state onto the SLM. The 4f 1^{th}-order filtering system consists of two lenses with focal distance 20 cm and an adjustable diaphragm for optimization of the spatial filtering. In accordance with simulation, f_{space} is chosen 60 cm. Due to practical constraints however, the propagation length is restricted to 2.33 m. This is still significantly larger than $2f_{sp}$ such that the imaging is still non-4F meaning the phase will still acquire a phase shift that requires correction.†

Experimental Setup



633 nm laser
polarizer
Alice
SLM
10°
f_{fil} = 20cm
f_{fil} = 20cm
20cm
20cm
20cm
20cm
233cm
f_{sp} = 60cm
Eavesdroppable zone
Bob
CCD-Camera
53cm
f_m = 10cm
8.1cm
f_{sp} = 60cm
Applied phase shift by SLM in (rad)
Distance from SLM centre in (μm)
Position state 1 ($|1>_p$) on SLM
Momentum state 1 ($|1>_m$) on SLM
Distance from optical axis in y-direction in (μm)
Distance from optical axis in x-direction in (μm)
255
0

(a) *Schematic overview of the setup. The dashed lens f_m is included only if a momentum state is to be measured. The subplot shows the different states on the SLM.*

(b) *Examples of $|1\rangle_p$ and $|1\rangle_m$ as greyscale images. Every pixel outside this interval receives no phase shift.*

To measure at Bob's, a megapixel Spiricon SP620U CCD-camera with pixel-size (4.4 µm x 4.4 µm) is used. The camera plane is chosen 53 cm because it yielded the best result in practice, despite being 7 cm away from the expected focal plane. Finally, Bob's momentum lens is chosen $f_{mom} = 10$ cm.

*This is because, as derived in 3.3, $\sigma_{new} = \frac{f}{2\pi\sigma_{old}\approx\frac{0.63\cdot10^{-6}\cdot0.5}{2\pi135\cdot10^{-6}}} \approx 350$ µm for a typical lens ($f = 0.5$ m) in the setup.

†This is important because one cannot expect to create a 4F-system if l is ever increased. Therefore, this distortion is crucial to preserve a realistic setup.

Like the slit size, its position is manually optimized. The setup is also shown in Fig. 4.2.

4.2 Method & Results

The first measurement series is conducted with the camera positioned in Bob's camera plane and the momentum lens disjointed from the setup. All states were consecutively displayed on the SLM. One screenshot of the intensity profile is saved per state. Camera settings were freely adjusted also within one such measurement series as absolute intensities are largely irrelevant. It is the normalized intensity that is associated with photon probability distribution.[*] Afterwards, the momentum lens is introduced and the method repeated. The resulting normalized intensity distributions, summed over the y-direction, are shown in Fig. 4.2.

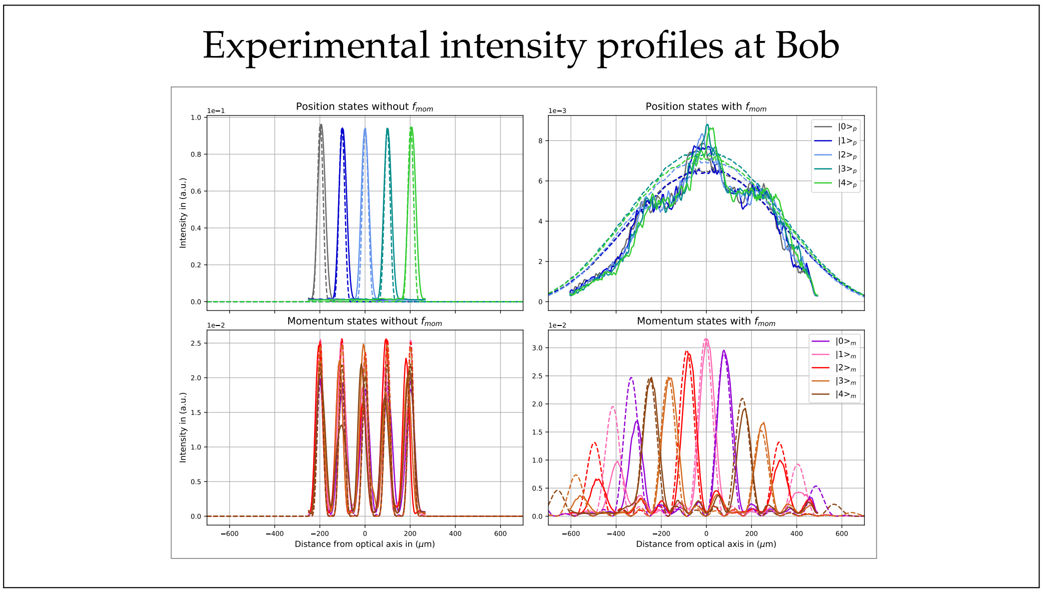


Figure 4.2: *Intensity profiles at the camera plane, both by experiment (solid) and by simulation (dashed). Simulation parameters match experimental parameters as specified in 4.1a. Except for $f_{sp} = 60\,\text{cm}$ as mentioned in the text.*

Besides intensity profiles at Bob, the other important characteristic to varify is mutual unbiasedness. To demonstrate mutual unbiasedness, the

[*] This is necessary because the momentum states are five times as luminous as their position counterpart as more light is reflected into the 1^{th}-order at the SLM.

camera is moved to the plane 43 cm into the eavesdroppable zone, a value that was chosen at random. Since the beam width in the eavesdroppable zone ($\sim$ 1 cm) is larger than the camera width, the camera is positioned slightly left of the optical axis such that the left side of the profile can be imaged. A measurement series is conducted for all states after which the camera is moved over to the right and the procedure is repeated. The resulting intensity distributions are plotted in Fig. 4.3. In addition to summing over the y-direction, this plot is a rolling average over fifty pixels to act as a low-pass filter. This is required as the light intensity in the eavesdroppable zone is reduced by approximately a factor $\frac{1.5\,\text{cm}}{40\,\mu\text{m}} = 375$ for the position states* necessitating a higher gain and integration time amplifying the noise. Since these variations are of little interest, the rolling average is justified.

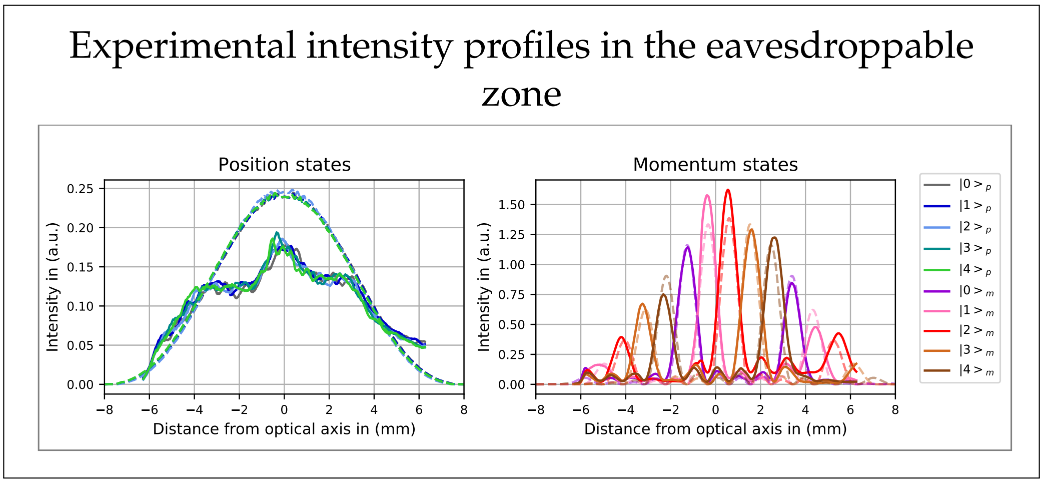


Figure 4.3: *Intensity profiles* 43 cm *into the eavesdroppable zone, both by experiment (solid) and by simulation (dashed). Simulation parameters match experimental parameters as specified in 4.1a. Only the distance f_{sp}-camera is kept at the theoretical* 60 cm*.*

4.3 Discussion

Considering the profiles in Fig. 4.2, it can be concluded that predictions are met to a reasonable degree. Measuring in the position basis, agreement is excellent and thus, in accordance with simulation, the position

*For the momentum state, this factor is harder to find but it will be far less than the position states because every momentum state in the eavesdroppable zone contains a few $\sigma \approx 0.5$ mm peaks.

states will be straightforwardly separable. In the momentum basis, agreement is not ideal which is notably pronounced in the upper left figure that shows quite a deviation from a Gaussian in the experimental case. This is especially troublesome as discriminating momentum states is already tougher theoretically, and any deviation from the the optimized simulation will complexify this even further. It is however currently the case that this predominantly affects the side lobes which could possibly be ignored by post-selection in exchange for an even higher loss. Considering the similarity with simulation in the remaining centre regions, it is expected that simular error probabilities can be obtained as in Fig.3.7a.

One possible explanation for this discrepancy has to do with the odd choice for the camera plane at 53 cm instead of the focal plane of f_{space}. Theoretically, there is no reason for this and such behavior is not observed anywhere in simulation. Of course, it could be that the focal distance of the lens was incorrect, but the deviation is so severe that this seems unlikely. A more probable explanation emanates from the source: although satisfying the condition in eq.3.3, this was only barely met. Consequently, the beam is of such size that diffraction is not entirely negligible. This widening could then have had consequences down the optical path that leads to the different effective focal plane.

Moving onto the eavesdroppable zone, we observe the exact same deviation from simulation as with the momentum lens. This is unsurprising as the momentum lens effectively projects a scaled version of the intensity profile in the eavesdroppable zone onto the camera. The similar discrepancies however do indicate that the process causing the difference originates from Alice, further discrediting the flawed lens hypothesis. Although experiment and simulation agree less here, this does not necessarilly indicate a security breach. As priorly mentioned, the security does not dependent on the exact shape. As long as the conjugate[*] basis changes accordingly such that mutual unbiasedness is preserved the security is guaranteed. As this does seem to have happened[†], one can be reasonably sure that mutual unbiasedness is realized also in the experimental case.

[*] Be it the momentum states if the position states change or vice versa.

[†] An indicator for this is the way the side lobes have changed

Outlook

We worked towards implementing a demonstration of high dimensional quantum key recycling. And, to that end, significant progress has been made: We developed a more experimentally-friendly version of the security proof, designed a setup that has a 10% error rate and verified this using a classical analogue. However, as is so often the case, there lie many more challenges ahead, both theoretically and experimentally.

Theoretically, there is a lot to gain in state optimization. To start, the approach in section 3.1 contains restrictions that are unnecessary. Linearity for example, although convenient in the context of lenses, is not required and there may exist conjugate bases that are more suitable for QKR, especially in combination with Bob's momentum lens replaced by a momentum spacial light modulator. Together, these may decrease overlap between conjugate states at the detector. In addition, the security protocol can be extended to include steps like post-selection (3.7) on measured qudits by Bob. This would make it much easier to eliminate noise.

This is important, because experimentally there is a lot of work that still needs to be done in order to perform a successful demonstration. First, the laser has to be replaced by a single photon source [28] or weak coherent pulses in the form of decoy states have to be used [29]. In addition, the current camera would have to be replaced by a single photon camera, the combination of which would pose significant engineering challenges. Another issue is that of speed, especially with regard to Bob's switching between measuring position and momentum states. Probably, even without a new conjugate basis, the momentum lens has to be upgraded to a SLM to enable fast switching between the two. In case of no new conjugate basis however, a liquid lens [30] is another option to achieve similar results. Of course, accompanying software that portrays the right state and interprets Bob's camera in real time have to be developed.

Looking even further into the future, one could ask whether the spatial degree of freedom is the best photon degree to conduct QKR in. It is certainly a convenient degree in terms of state creation, manipulation, detection and ease of reaching high dimensions, but it is fundamentally plagued by diffraction and divergence as addressed in section 3.3. This shortcoming will likely restrict the range below practical usability. In addition, QKD experiments have been performed using other high dimensional photon degrees of freedom including Energy-time and Angular position- Angular momentum [16, 31]. The Energy-time degree, although experimentally cumbersome, is especially promising because it is suitable for in-fibre transmission which has potentially enormous consequences in terms of range.

In conclusion, there are still major challenges to overcome. Both before a demonstration is realised and wherever the project may lead from there. Nevertheless, I hope to have laid a solid foundation to wherever that may be. Maybe we will see our future communications protected by quantum key recycling. One never knows.

Acknowledgements

A solo-project is seldomly a journey truly traveled alone. Visibly and invisibly one is always guided, supported and accommodated by people that stand along the route. I am no exception.

Before all, I want to express my gratitude towards Dr Wolfgang Löffler for his excellent guidance and supervision during the last half-year. For his self-sacrifice by facilitating experimental projects in Covid-times and for inspiring any time the journey seemed to strand. In addition, I want to thank Prof. dr. Serge Fehr for introducing me to the world of theoretical quantum encryption schemes. I don't understand how you come up with those but I do know there wouldn't be a project without you. You were much more than just a second supervisor.

One can however not live from academics alone and I want to thank everyone that took my mind of the project from time to time. Specifically, I want to thank Filip and Casper for sitting through the most frustrating hours. I'm glad we are still roommates. I'm grateful for my family who come above all.

Finally, I'm eternally grateful to my grandfather who sowed the physical seed. Unfortunately, you are no longer here to see the third generation mature. I know you never believed you would now be watching from above, but just in case: Thank you!

Bibliography

[1] J. R. Lindsay, “Surviving the Quantum Cryptocalypse,” *Strategic Studies Quarterly*, vol. 14, no. 2, pp. 49–73, 2020. [Online]. Available: :https://www.jstor.org/stable/10.2307/26915277

[2] J. A. Buchmann, *Introduction to Cryptography*. New York, NY: Springer US, 2001, oCLC: 851800802. [Online]. Available: http://catalog.hathitrust.org/api/volumes/oclc/43936737.html

[3] M. Razavi and Institute of Physics (Gran Bretanya), *An introduction to quantum communications networks, or, how shall we communicate in the quantum era?*, 2018, oCLC: 1107672847. [Online]. Available: https://iopscience.iop.org/book/978-1-6817-4653-1

[4] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, H. Chen, M. J. Li, D. Nolan, F. Zhou, X. Jiang, Z. Wang, Q. Zhang, X.-B. Wang, and J.-W. Pan, “Measurement-Device-Independent Quantum Key Distribution Over a 404 km Optical Fiber,” *Physical Review Letters*, vol. 117, no. 19, p. 190501, Nov. 2016, publisher: American Physical Society. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevLett.117.190501

[5] C. H. Bennett, G. Brassard, and S. Breidbart, “Quantum cryptography II: How to re-use a one-time pad safely even if P= NP,” *Natural computing*, vol. 13, no. 4, pp. 453–458, 2014, publisher: Springer.

[6] D. Gottesman, “Uncloneable Encryption,” *arXiv:quant-ph/0210062*, Sep. 2004, arXiv: quant-ph/0210062. [Online]. Available: http://arxiv.org/abs/quant-ph/0210062

[7] I. Damgård, T. B. Pedersen, and L. Salvail, "A Quantum Cipher with Near Optimal Key-Recycling," in *Advances in Cryptology â CRYPTO 2005*, ser. Lecture Notes in Computer Science, V. Shoup, Ed. Berlin, Heidelberg: Springer, 2005, pp. 494–510.

[8] S. Fehr and L. Salvail, "Quantum Authentication and Encryption with Key Recycling," 2016. [Online]. Available: https://arxiv.org/abs/1610.05614

[9] B. Škorić and M. De Vries, "Quantum key recycling with 8-state encoding (the quantum one-time pad is more interesting than we thought)," *International Journal of Quantum Information*, vol. 15, no. 03, p. 1750016, 2017.

[10] D. Leermakers and B. Skoric, "Security proof for quantum key recycling with noise." *Quantum Inf. Comput.*, vol. 19, no. 11&12, pp. 913–934, 2019.

[11] Y.-C. Lu, C.-W. Tsai, and T. Hwang, "Quantum Key Recycling with Optimal Key Recycling Rate based on Error Rate," *arXiv:2004.11596 [quant-ph]*, Jun. 2020, arXiv: 2004.11596. [Online]. Available: http://arxiv.org/abs/2004.11596

[12] M. Bellare and P. Rogaway, "Introduction to Modern Cryptography," p. 283, May 2005.

[13] N. H. Valencia, V. Srivastav, M. Pivoluska, M. Huber, N. Friis, W. McCutcheon, and M. Malik, "High-Dimensional Pixel Entanglement: Efficient Generation and Certification," *Quantum*, vol. 4, p. 376, Dec. 2020, arXiv: 2004.04994. [Online]. Available: http://arxiv.org/abs/2004.04994

[14] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, 7th ed. Cambridge University Press, 2016.

[15] T. A. Brun, "Quantum Fourier Transform." [Online]. Available: https://viterbi-web.usc.edu/~tbrun/Course/lecture13.pdf

[16] X. Liu, X. Yao, H. Wang, H. Li, Z. Wang, L. You, Y. Huang, and W. Zhang, "Energy-time entanglement-based dispersive optics quantum key distribution over optical fibers of 20 km," *Applied Physics Letters*, vol. 114, no. 14, p. 141104, Apr. 2019. [Online]. Available: http://aip.scitation.org/doi/10.1063/1.5089784

[17] R. Wang, "Matrix norms," Feb. 2015. [Online]. Available: http://fourier.eng.hmc.edu/e161/lectures/algebra/node12.html

[18] "Matrix norm," Feb. 2021, page Version ID: 1008374867. [Online]. Available: https://en.wikipedia.org/w/index.php?title=Matrix_norm&oldid=1008374867

[19] T. Johansson and P. Q. Nguyen, Eds., *Advances in Cryptology - EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013, Proceedings*, 1st ed., ser. Security and Cryptology. Berlin, Heidelberg: Springer Berlin Heidelberg : Imprint: Springer, 2013, no. 7881.

[20] J. H. v. Lint, *Introduction to coding theory*, 2nd ed., ser. Graduate texts in mathematics. Berlin ; New York: Springer-Verlag, 1992, no. 86.

[21] R. Douc, E. Moulines, P. Priouret, and P. Soulier, *Markov Chains*. New York: Springer, 2019, oCLC: 1152978215. [Online]. Available: https://link.springer.com/10.1007/978-3-319-97704-1

[22] R. A. Adams and C. Essex, *Calculus, A complete course*, 9th ed. Pearson, 2018.

[23] T. Durt, B.-G. Englert, I. Bengtsson, and K. Życzkowski, "ON MUTUALLY UNBIASED BASES," *International Journal of Quantum Information*, vol. 08, no. 04, pp. 535–640, Jun. 2010. [Online]. Available: https://www.worldscientific.com/doi/abs/10.1142/S0219749910006502

[24] J. W. Goodman, *Introduction to Fourier optics*, 2nd ed., ser. McGraw-Hill series in electrical and computer engineering. New York: McGraw-Hill, 1996.

[25] J. A. Davis, D. M. Cottrell, J. Campos, M. J. Yzuel, and I. Moreno, "Encoding amplitude information onto phase-only filters," *Applied Optics*, vol. 38, no. 23, p. 5004, Aug. 1999. [Online]. Available: https://www.osapublishing.org/abstract.cfm?URI=ao-38-23-5004

[26] E. N. Glytsis, "Gaussian_beams.pdf," Mar. 2021. [Online]. Available: http://users.ntua.gr/eglytsis/OptEng/Gaussian_Beams.pdf

[27] M. Reck, A. Zeilinger, H. J. Bernstein, and P. Bertani, "Experimental realization of any discrete unitary operator," *Physical review letters*, vol. 73, no. 1, pp. 58–61, 1994, place: United States.

[28] H. Snijders, J. Frey, J. Norman, V. Post, A. Gossard, J. Bowers, M. van Exter, W. Löffler, and D. Bouwmeester, "Fiber-Coupled Cavity-QED Source of Identical Single Photons," *Physical Review Applied*, vol. 9, no. 3, p. 031002, Mar. 2018. [Online]. Available: https://link.aps.org/doi/10.1103/PhysRevApplied.9.031002

[29] B. Huttner, N. Imoto, N. Gisin, and T. Mor, "Quantum cryptography with coherent states," p. 8.

[30] H. Ren and S.-T. Wu, "Variable-focus liquid lens," *Optics Express*, vol. 15, no. 10, p. 5931, May 2007. [Online]. Available: https://www.osapublishing.org/abstract.cfm?URI=oe-15-10-5931

[31] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. 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, Mar. 2015, arXiv: 1402.7113. [Online]. Available: http://arxiv.org/abs/1402.7113