

EXPERIMENTAL CHARACTERIZATION OF A DISCRETE GAUSSIAN-MODULATED  
QUANTUM KEY DISTRIBUTION SYSTEM

by

Christian Rios

---

Copyright © Christian Rios 2021

A Thesis Submitted to the Faculty of the

JAMES C. WYANT COLLEGE OF OPTICAL SCIENCES

In Partial Fulfillment of the Requirements

For the Degree of

MASTER OF SCIENCE

In the Graduate College

THE UNIVERSITY OF ARIZONA

2021

THE UNIVERSITY OF ARIZONA  
GRADUATE COLLEGE

As members of the Master's Committee, we certify that we have read the thesis prepared by **Christian Darien Rios**, titled *Experimental Characterization of a Discrete Gaussian-Modulated Quantum Key Distribution System* and recommend that it be accepted as fulfilling the thesis requirement for the Master's Degree.

  
\_\_\_\_\_  
Professor Daniel C. Kilper

Date: 5/28/2021

  
\_\_\_\_\_  
Professor Linran Fan


Date: 5/28/2021


  
\_\_\_\_\_  
Professor Boulat Bash

Date: 5/28/2021

Final approval and acceptance of this thesis is contingent upon the candidate's submission of the final copies of the thesis to the Graduate College.

I hereby certify that I have read this thesis prepared under my direction and recommend that it be accepted as fulfilling the Master's requirement.

  
\_\_\_\_\_  
Professor Daniel C. Kilper  
Master's Thesis Committee Chair  
Wyant College of Optical Sciences

Date: 5/28/21 

ARIZONA

# Table of Contents

	List of Figures, Illustrations, and Tables . . . . .	4
	Abstract . . . . .	5
Ch. 1	<b>Introduction</b> . . . . .	6
	1.1 History of Cryptography . . . . .	6
	1.2 Modern Cryptography . . . . .	11
Ch. 2	<b>Discrete Variable Quantum Key Distribution</b> . . . . .	14
	2.1 Qubits . . . . .	14
	2.2 BB84 Protocol Using Qubits . . . . .	17
	2.3 BB84 Security . . . . .	21
	2.4 Optical BB84 . . . . .	25
Ch. 3	<b>Continuous Variable Quantum Key Distribution</b> . . . . .	28
	3.1 Coherent States . . . . .	28
	3.2 Gaussian-modulated Coherent State Protocol . . . . .	36
Ch. 4	<b>Discrete Gaussian-modulated Quantum Key Distribution</b> . . . . .	40
	4.1 Brief History and Outline of the Chapter . . . . .	40
	4.2 Discrete Gaussian-modulated Coherent State Protocol . . . . .	42
	4.3 Experimental Characterization . . . . .	46
Ch. 5	<b>Phase Stabilization Using Red Pitaya</b> . . . . .	55
	Phase Compensation . . . . .	55
	Experimental Setup . . . . .	59
Ch. 6	<b>Summary and Future Work</b> . . . . .	65
	References . . . . .	68

# List of Figures, Illustrations, and Tables

Fig. 1	The Bloch Sphere . . . . .	15
Fig. 2	Coherent State in Phase Space . . . . .	30
Fig. 3	Coherent State-based 8-QAM . . . . .	32
Fig. 4	Coherent States as a Thermal State . . . . .	43
Fig. 5	Proof of Principle DGM Optical Setup . . . . .	46
Fig. 6	Proof of Principle Constellation Diagram . . . . .	48
Fig. 7	Temperature Phase Scan for a Coherent State with a Mean Photon Number of 5600 Photons . . . . .	52
Fig. 8	Temperature Phase Scan for a Coherent State with a Mean Photon Number of 2800 Photons . . . . .	52
Fig. 9	Normalized Temperature Phase Scan with Drift Correction . . . . .	53
Fig. 10	Complete Discrete Gaussian-modulated QKD system with Phase Compensation . . . . .	59
Fig. 11	Simplified Experimental Setup for Testing Phase Compensation Performance . . . . .	62
Fig. 12	Piezo-induced Phase Scan vs. Phase Lock Comparison . . . . .	63

# Abstract

Quantum Key Distribution (QKD) utilizes the laws of quantum mechanics to enable a verifiably secure distribution of cryptographic key material between distant parties. When properly implemented alongside a one-time pad encryption scheme, QKD can provide unconditional security which is not possible with modern cryptographic systems. One of the most common QKD protocols, the Gaussian-modulated coherent state (GMCS) protocol can never be truly realized due to the stringent requirements of a true Gaussian modulation. This thesis outlines a method for testing a discrete Gaussian-modulated (DGM) QKD protocol which accounts for the discrete nature of its practical implementation. A proof-of-principle experiment for measuring its performance is presented, and a field programmable gate array (FPGA) controlled phase compensation system is designed for practical implementations.

# Chapter 1: Introduction

## 1.1 History of Cryptography

Modern network communication relies almost exclusively on classical cryptography to maintain security. This security depends on the difficulty of computationally hard but solvable problems. Quantum cryptography offers unconditional security backed by physical laws, but the two main methods for implementation are each hindered by their own sets of barriers inhibiting their widespread implementation in a practical environment. Specifically, discrete variable quantum key distribution (DV-QKD) relies on technically difficult single-photon generation and single-photon detectors. Meanwhile, continuous variable quantum key distribution (CV-QKD) uses easily generated coherent states and homodyne detection but is vulnerable to the excess noise contributions of the photodetector electronics and phase variance of a local oscillator. Unlike DV-QKD, the most common approaches to CV-QKD lack a robust security proof. Discrete Gaussian-modulated quantum key distribution (DGM-QKD), offers a hybrid approach, addressing several of these barriers to implementation. This thesis presents work developing an experimental DGM-QKD demonstration.

Whether it involves the decryption of sensitive information during war times or the protection of privacy for personal letters, the security of information has been a topic of interest throughout history. Cryptology studies the science of secure communication and can be split into two branches: cryptography and cryptanalysis. Cryptography studies the methods of hiding and sharing information in messages, while cryptanalysis develops the techniques to find this hidden information.

The goal of communication is to share information between two or more distant parties. Rather than refer to information transfer between two points A and B, cryptography often personifies these points as Alice and Bob, the sender and receiver, respectively. This originates from a paper in 1978 by Rivest, Shamir, and Adleman [1]. The notation was expanded upon in 1988 to include the cryptanalytic eavesdropper, Eve, in a paper by Bennet, Brassard, and Robert [2]. A number of other characters have been introduced over time with varying expertise, capabilities, and motivations in order to describe more complex scenarios.

Cryptology has been a constant race between cryptography and cryptanalysis. One side seeking to develop the next more sophisticated encryption, while the other utilizes developments in algorithms and technology to breach the next layer of security.

The race began roughly 4000 years ago in the Egyptian town of Menet Khufu where rarer and unusual hieroglyphs were used to replace more common and more widely known ones on the tomb of Khnumotep II [3]. Although it is speculated that this was merely to impart dignity and authority rather than obscure the facts about his life, this is the first recorded usage of a simple substitution cipher. Until the 1970's, simple substitutions and transpositions had been the basis for most cryptographic ciphers.

A cipher is a method for encrypting a message from its original content, also called the plaintext, into an encrypted form, a ciphertext. Every cipher also has a key in some form that dictates how the ciphertext was encrypted and how to decrypt the ciphertext back into plaintext. In the case of a transposition cipher, letters from the original plaintext are shuffled out of order in a way described by the key. In a substitution cipher, the key dictates how each letter is transformed to form the plaintext. A prominent example of this is the Caesar cipher [4]. In the Caesar cipher, all letters are replaced by a letter three letters later in the alphabet. Specifically, 'A' be replaced by 'D', and 'B' will be replaced by 'E' and so on. The letters in the last three positions of the alphabet will map back to the start such that 'X', 'Y', and 'Z' will map to 'A', 'B', 'C' respectively. The Caesar cipher is a specific case of a monoalphabetic substitution cipher.

By today's standards, this kind of substitution cipher can be easily broken by analyzing the frequency of letters in the ciphertext and comparing them against the frequency of letters from that language. For example, the most commonly used English letters are 'E', 'T', and 'A'. About 29% of all letters used come from this 3-letter subset [5]. By mapping the probabilities of 'E', 'T', and 'A' to the most frequently occurring ciphertext letters, it is possible to further analyze the next most common letters of the ciphertext alphabet or look for patterns in the ciphertext until the message is uncovered. Unless the frequency of each letter in an alphabet is equally likely, letter frequency analysis will eventually break the cipher. This introduces the idea of using multiple ciphers within the same message. The use of multiple monoalphabetic ciphers within the same message is known as a polyalphabetic substitution cipher. Here, the key dictates how each letter or subset of letters from the plaintext should be encoded. In general, the key length is not known, but methods for estimating the key length do exist. If the key length is known, then the

polyalphabetic substitution cipher only increases the complexity of the decryption for the monoalphabetic substitution cipher by a factor of  $n$ , where  $n$  is the length of the key.

The flaws of these simple ciphers were used to build the requirements of a truly secure cipher scheme. In a truly secure scheme, each key should be used minimally to prevent frequency analysis from mapping letter frequency to the cipher alphabet. Ideally, each key is used at most once and it is randomly selected to ensure an even and uncorrelated distribution. However, this requires that the key be at least as long as the message itself. This type of encryption scheme is called the one-time pad and was first proposed in 1917 by Joseph Mauborgne and Gilbert Vernam [6]. It was not until 1948 that Shannon proved the one-time pad to be unconditionally secure [7]. No form of cryptanalysis can ever decipher a properly implemented one-time pad. However, the one-time pad has a number of practical concerns barring its widespread implementation. It is possible to compromise a one-time pad if the key used is not truly random or if the same key is ever used for more than one message. Also, both communicating parties must possess the key beforehand in order to communicate. Since the key length must at least match the length of the message, many keys must be shared between the parties and securely stored prior to communication. Thus far, these requirements have made the one-time pad impractical in a real-world environment. However, new methods for the distribution of secure keys between distance parties such as quantum key distribution may finally realize these requirements for the one-time pad.

Cryptology remained much the same until the 1900's, employing variations and combinations of different substitution and transposition ciphers. Eventually mechanical devices such as the German Enigma machine were employed on the side of cryptography to automate these ciphers [3]. These automated devices allowed for the generation of much longer keys with a much

larger complexity factor  $n$ . Since much of cryptanalysis was done by hand, this automated method was often effective up until the emergence of computers and information theory which have shaped the current theatre. With a theoretical background to quantize, study, and analyze information and with the complex automation allowed by computers, more sophisticated forms of cryptography and cryptanalysis developed which resemble the current classical protocols that we use today.

## 1.2 Modern Cryptography

In the 1970's, the US National Bureau of Standards released the Data Encryption Standard (DES). This was the first time a national cryptographic protocol was released to the public. It used a 56-bit long key for encryption [8]. Soon after in 1976, Diffie and Hellman published their Diffie-Hellman key exchange protocol [9]. Their protocol introduced the notion of the asymmetric key, also called a public key which allowed for one-way encryption.

In public key cryptography, every party possesses two keys: one key that they keep secret and another that they share with the public. The premise behind this kind of asymmetric key protocol is that certain mathematical expressions are easy or hard to evaluate depending on which terms are known beforehand. By storing information that would make the expression easy in the secret key, a form of security is established. Factoring large prime numbers is one example of such an asymmetric problem. It is easy to compute a product given two prime factors, however it is very difficult to compute the prime factors from their product. In an asymmetric protocol, the prime factors may compose the secret key while their product composes the public key.

These new forms of cryptography introduced the metric of computational complexity to evaluate their security. A protocol can be deemed computationally secure if solving for the key would require more time and computational power than can reasonably be utilized. However, a computationally secure protocol might be insecure in a matter of years or decades. The future computational security of protocol depends on advancements in computational resources, mathematics, and information theory. By 1998, it was demonstrated that a DES-generated key

could be broken in under 72 hours [10]. The unpredictability of these advances drives cryptography to always push the cutting edge of computational security.

Rivest, Shamir, and Adleman developed their own public key protocol, RSA (named after its authors), shortly after the publication of Diffie-Hellman [1]. It uses much longer keys up to 4096 bits long. It is still widely used and computationally secure by today's standards, but it is slow to implement like most secure public key protocols. Due to its speed, it is mostly used to encrypt short messages and share secure keys used by other forms of cryptography.

At this point, our cryptanalyst Eve is maybe a little disheartened. Computational security is a daunting barrier for the would-be eavesdropper. Eve should not lose hope though for she will one day be able to gain access to the information she seeks. Classical information can be copied and stored indefinitely. Eve must simply be patient and await new developments in science and technology. At this later date, Eve can apply new methods and more computational power to uncover the secrets of past messages. Assuming new improvements continue to exist, no computationally secure protocol will remain secure indefinitely. The only currently known method to ensure the secrecy of a message is to utilize a one-time pad scheme. It is the only known unconditionally secure protocol, meaning that it is unbreakable regardless of any future improvements in science and technology.

This guarantee of robust security is the ultimate goal of the aspiring cryptographer, and developments in the field of quantum mechanics have made possible the distribution of the secret keys necessary for implementing the one-time pad protocol. The product of performing Quantum Key Distribution (QKD) is a truly random secret key shared between two distant parties guaranteed by physical laws. Much to the dismay of Eve, not even an eavesdropper would be able to obtain information about a secret key generated through QKD if properly implemented. Using these

secret keys, a true one-time pad scheme may be able to be implemented in real-time in a practical environment.

# Chapter 2: Discrete Variable Quantum Key

## Distribution

### 2.1 Qubits

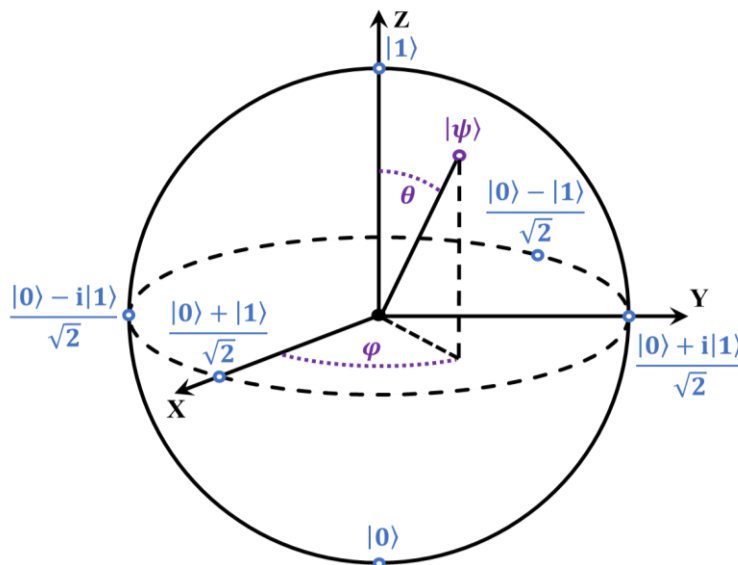
Quantum key distribution (QKD) relies on the distribution of quantum states to operate. The qubit is the most basic of these states, modeling a two-level quantum system. A qubit can be represented by its wavefunction in bra-ket notation

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle, \quad (2.1)$$

where  $\alpha$  and  $\beta$  are complex amplitudes. In order to obtain information about the quantum system, the qubit must be measured. To measure a qubit, a basis must first be selected. If we were to choose the  $|0\rangle$  and  $|1\rangle$  basis to measure the state  $|\psi\rangle$  in, then the probability of obtaining a measurement of  $|0\rangle$  is  $|\alpha|^2$ , and the probability of obtaining a measurement of  $|1\rangle$  is  $|\beta|^2$ . These complex amplitudes  $\alpha$  and  $\beta$  are normalized by the following expression

$$|\alpha|^2 + |\beta|^2 = 1. \quad (2.2)$$

Once a qubit has been measured, it collapses into one of the states composing the measurement basis. At this point, measuring the collapsed qubit in the same basis will always yield



**Fig. 1: The Bloch Sphere.** The poles and four common equal superposition states are labeled in blue. An arbitrary qubit state  $|\psi\rangle$  can be visually represented on the sphere using the angles  $\theta$  and  $\varphi$  as labeled in purple.

the same result. In other words, once a measurement has been performed, no further information about  $\alpha$  or  $\beta$  can be obtained by repeating the measurement. Note that a qubit contains more information than its probabilities alone. For example, measuring one pair of equal superposition states  $\frac{|0\rangle+|1\rangle}{\sqrt{2}}$  and  $\frac{|0\rangle+i|1\rangle}{\sqrt{2}}$  in the  $|0\rangle$  and  $|1\rangle$  basis both yield the same result, but this information cannot be captured by the probability distribution alone.

A more complete qubit representation is by a vector in a spherical coordinate system called the Bloch sphere. The wavefunction can be rewritten as

$$|\psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{i\varphi}\sin\frac{\theta}{2}|1\rangle \quad (2.3)$$

with polar angle  $\theta$  and azimuthal angle  $\varphi$ . The north and south poles of the sphere correspond to the states  $|0\rangle$  and  $|1\rangle$  respectively. Points along the equator represent equal superposition states as used in the previous example.

A qubit's measurement is not just restricted to the  $|0\rangle$  and  $|1\rangle$  basis. The symmetry of the Bloch sphere allows rotations to be performed. Physically, this means measuring the qubit in a rotated basis. This allows measurement schemes to differentiate between the states along the equator of the Bloch sphere for example.

In order to describe a system of multiple qubits with wavefunctions  $|\psi_1\rangle = \alpha_1|0\rangle + \beta_1|1\rangle$  and  $|\psi_2\rangle = \alpha_2|0\rangle + \beta_2|1\rangle$ . The combined wavefunction is described by their outer product

$$|\psi_{1,2}\rangle = |\psi_1\rangle \otimes |\psi_2\rangle. \quad (2.4)$$

$$|\psi_{1,2}\rangle = \alpha_1\alpha_2|00\rangle + \alpha_1\beta_2|01\rangle + \beta_1\alpha_2|10\rangle + \beta_1\beta_2|11\rangle. \quad (2.5)$$

If a two-qubit system cannot be decomposed into two independent single-qubit systems, then the qubits are considered to be entangled. An example of this is one of the Bell states:

$$|\psi_{1,2}\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}. \quad (2.6)$$

If one performs a measurement on either qubit in the pair, the Bell state collapses to either  $|00\rangle$  or  $|11\rangle$  and the state of the other qubit is immediately known despite only measuring one qubit. This property is particularly useful if two distant parties, each sharing one part of the entangled pair, wish to communicate securely. With a basic concept of qubits, we can now review a qubit-based version of the first QKD protocol, BB84, originally developed by Bennett and Brassard in 1984 [11].

## 2.2 BB84 Protocol

Inspired by Stephen Wiesner's idea to use quantum states as a counterfeit-proof form of currency, Bennett and Brassard developed a novel method to use quantum states in a communication protocol to distribute a string of random bits also called a secret key between two parties, Alice and Bob [12, 13]. The protocol has since been named BB84 after the authors and its year of publication. BB84's security is proven by showing that attempts to intercept the information by a potential eavesdropper, Eve, will introduce errors in Bob's detection statistics, potentially alerting the presence of Eve's interception. A paranoid Alice and Bob must assume that any error is due to Eve's presence and can use the total error rate of the protocol to bound Alice's potential information about the secret key. If Alice and Bob share enough information and the total error is sufficiently low, Alice and Bob can distill a secret key proven secure by physical laws.

Any QKD protocol consists of two main steps: preparation, transmission, and measurement of quantum states followed by classical post-processing. In BB84, the classical post-processing step can be further broken down into the sifting, parameter estimation, information reconciliation, and privacy amplification steps. Prior to enacting the protocol, Alice and Bob agree on a pair of orthogonal bases to use in the protocol. The bases are as follows:

$$|H\rangle = |0\rangle \tag{2.7.1}$$

$$|V\rangle = |1\rangle \tag{2.7.2}$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \tag{2.7.3}$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (2.7.4)$$

where  $|H\rangle$  and  $|V\rangle$  correspond to Alice encoding a classical bit of 0 and  $|V\rangle$  and  $|-\rangle$  correspond to Alice encoding a classical bit of 1. Note that the states of the second basis are not orthogonal to the states composing the first. The relationships between  $|H\rangle$  and  $|V\rangle$  and  $|+\rangle$  and  $|-\rangle$  are given by:

$$|H\rangle = \frac{|+\rangle + |-\rangle}{\sqrt{2}} \quad (2.8.1)$$

$$|V\rangle = \frac{|+\rangle - |-\rangle}{\sqrt{2}} \quad (2.8.2)$$

$$|+\rangle = \frac{|H\rangle + |V\rangle}{\sqrt{2}} \quad (2.8.3)$$

$$|-\rangle = \frac{|H\rangle - |V\rangle}{\sqrt{2}}. \quad (2.8.4)$$

Along with the symmetric nature of the Bloch sphere, Eq. 2.8.1 – Eq. 2.8.4 show that the basis selection is arbitrary provided that any state from an orthogonal basis pair is an equal superposition of states from the other pair. Now that a fitting pair of bases has been selected. The details of each step of the protocol are as follows:

1) Preparation, transmission, and measurement: Alice randomly prepares a qubit in one of the four states described in Eq. 2.7.1 – Eq. 2.7.4 and sends that qubit to Bob through a quantum channel. Bob randomly selects one of the two orthogonal bases and measures his received qubit in that basis. This step is repeated N times. Alice and Bob now share a list of N pairs. For Alice, this

is a list of what basis she used to encode the qubit and the bit encoded on that qubit. For Bob, this is a list of what basis was used to measure each qubit and the outcome of that measurement.

2) Sifting: Alice and Bob publicly announce what basis they used for each measurement. By comparing these list and discarding qubits that were not prepared and measured in the same basis, Alice and Bob now shared a sifted key of approximately  $N/2$  bits.

3) Parameter Estimation: Alice and Bob now sacrifice a portion of their sifted key to estimate the quantum bit error rate (QBER). The QBER,  $e$ , is the ratio of Bob's incorrectly decoded bits,  $n$ , to the total number of bits sent.

$$e = \frac{n}{N} \quad (2.9)$$

This error rate is used to calculate the bound of information that can be extracted by Eve. If the QBER is too high, Eve could potentially obtain information about the secret key in this iteration and the protocol is cut short to prevent this. Requirements on the QBER for secure communication will be detailed after the protocol.

4) Information Reconciliation: To remove discrepancies in Alice and Bob's keys, Alice and Bob employ an error correction strategy. Originally, this was done using the Cascade protocol developed by Bennet and Salvail until a more efficient scheme named Winnow was developed by Buttler et al. [14, 15]. More recently, it was discovered that a faster and computationally more efficient method is to employ low density parity check (LDPC) codes [16]. These protocols all require that Alice or Bob disclose a subset of their key in order to verify or correct for errors. An efficient error correction scheme is optimized to correct for the maximum number of errors while disclosing the smallest subset of a key.

5) Privacy amplification: knowing the bound of Eve's potential information, Alice and Bob can apply a cryptographic hash function to compress the error corrected key into a secure key. By design, the hash function reduces Eve's probability of guessing the secret key given her information bound on the original sifted key [18]. By sacrificing more bits in this compression process, Eve's probability of guessing the secret key can be made arbitrarily low, guaranteeing the security of the key. If the protocol has not been aborted by this point, Alice and Bob should both share an identical secret key with a very high probability.

## 2.3 BB84 Security

If Eve were to intercept a qubit from Alice to Bob, she must make several correct choices to avoid introducing error in Bob's measurement and risk detection. First, she must choose a basis with which to measure the qubit. If she chooses randomly from the two bases used in the protocol, then on average she will measure the correct basis 50% of the time. If she guesses correctly, then she knows what state to reproduce and send to Bob in the proceeding step. However, Eve does not know after measurement if her basis measurement was correct. At this point, she must always guess which basis to send Bob. In a classical analogue, Eve could simply duplicate a classical state sent by Alice to Bob. However, due to the no-cloning theorem, a perfect copy of Alice's qubit state cannot be created. As a result, any attempt by Eve to imperfectly clone the sent state will contribute to the error rate calculated in the classical post-processing step. One strategy would be to always send the state that she measures to Bob. In the case when she measures the correct basis, she will always send the correct state to Bob. However, when she guesses incorrectly, she will be sending a random state to Bob contributing up to 25% to the expected QBER. By comparing their measured and expected QBER, Alice and Bob can bound the maximum information possibly attained by Eve and possibly guarantee the protocol's security.

However, if Eve is an expert cryptanalyst with access to sophisticated equipment such as an optimal cloning machine for quantum states, then Eve can do more than simply measure the state sent by Alice and send a random state to Bob. Eve may attempt to imperfectly clone the quantum state sent by Alice by interacting it with an already prepared ancilla state. Eve can then

store her result in a perfect quantum memory to be measured at a later time. If properly implemented, Eve may reduce the impact of her eavesdropping on the measured noise while increasing her information obtained about the secure key. In this case, it is more complicated to evaluate Eve's impact on the QBER, but by using information theory an upper bound of Eve's information can be produced.

In order to robustly demonstrate the security of BB84, one must calculate the upper bound of Eve's information about the secret key. To begin, several assumptions are made about Eve [19]:

1. Eve can perfectly monitor the classical communication channel between Alice and Bob.
2. Eve has unlimited computational resources. This may include arbitrarily large computational power or even perfect quantum memories.
3. Eve has control over the quantum channel and her capacity to manipulate the channel is only limited by physical laws. Eve's control only extends to this quantum channel. She cannot manipulate any component local to either Alice or Bob.

Beyond these assumptions, there are three classes of attacks which determine to what extent Eve can manipulate the qubits she intercepts in the quantum channel: individual, collective, and coherent [19].

In the individual attack, Eve interacts individually with each qubit sent by Alice and stores her results in a quantum memory. Eve then performs the appropriate measurement after the results of the sifting procedure are announced by Bob. In the collective attack, Eve's interactions with Alice's sent qubits are the same, but Eve instead uses the information announced during the key distillation procedure to apply the optical collective measurement on the states stored in her quantum memory. In the coherent attack, Eve is allowed to interact collectively with all pulses

sent by Alice and perform the optical joint measurement using information from the key distillation procedure. In DV-QKD, the coherent attack was proven to not be any more effective than a collective attack, allowing DV-QKD to demonstrate unconditional security more easily [20].

By analyzing the mutual information between Alice and Bob and the mutual information between Alice and Eve, we can place a limit on the QBER to establish security. The mutual information between Alice and Bob is given by:

$$I(A: B) = 1 - H(e), \quad (2.10)$$

Where  $e$  is the QBER, and  $H(e)$  is the Shannon entropy:

$$H(e) = -e \log_2(e) - (1 - e) \log_2(1 - e). \quad (2.11)$$

In the case of BB84,  $H(e)$  is also the Holevo information  $\chi(e)$ , an upper bound on an eavesdropper's information for the collective attack [21]. Recall that the strongest attack, the coherent attack is no more effective than the collective attack for BB84. By demonstrating security against the strongest collective attack, we can demonstrate the unconditional security of BB84. If we assume Eve's attack is able extract the maximum information allowed and that any errors in the systems can be attributed to information gained by Eve, then the mutual information between Alice and Eve is equivalent to the Holevo information:

$$I(A: E) = \chi(e) = H(e). \quad (2.12)$$

In order to distill a secret key, the mutual information between Alice and Bob must be greater than the mutual information between Alice and Eve.

$$I(A: B) > I(A: E) \quad (2.13)$$

$$1 - H(e) > H(e) \quad (2.14)$$

$$1 - 2H(e) > 0 \quad (2.15)$$

By applying this constraint to Eq. 2.11, the maximum QBER allowed is 11% to successfully demonstrate the security of the protocol and produce a positive secret key rate (SKR). Lower values of the QBER will result in a more efficient protocol and a higher SKR. This effect can be measured by the difference in mutual information between Alice and Bob and Alice and Eve, also called the secret fraction:

$$r \geq I(A:B) - I(A:E). \quad (2.16)$$

The secret fraction of the symbol rate  $f_s$  is the ideal SKR,

$$K = r \cdot f_s. \quad (2.17)$$

## 2.4 Optical BB84

Since most network communication takes place using light in optical fibers, photons are a natural choice for the implementation of QKD systems. Photons have many degrees of freedom. For example, photon polarization, photon number, or photon arrival time could each be utilized to implement a physical qubit [22]. Plus, light is fast. Technology exists for its rapid detection, and there is a world-spanning optical network architecture already in place.

However, the implementation of a DV-QKD protocol is not without its own limitations hindering practical implementation. The major hindrance for DV-QKD is that single photons are hard to detect at high speeds. Single photon detection often involves burst or avalanche detection schemes that include a dead time after detection, limiting the maximum transmission rate. Optimizing for a short dead time can be complicated to do while maintaining a very high quantum efficiency, low dark counts, and a low jitter time to be effectively used in QKD systems.

Superconducting nanowire single-photon detectors (SNSPD) are a good detector candidate for single photon detection with high quantum efficiencies ( $>70\%$ ), low dark counts ( $< 100$  Hz), and high timing resolution ( $\sim 50$  ps). However, this performance requires cryogenic refrigeration which is neither convenient nor cheap [23]. Avalanche photodiodes (APD) offer a much more compact and cost-effective solution. However, APDs suffer from much lower quantum efficiencies ( $\sim 20\%$ ) at telecom wavelengths [24].

There also exist physical limitations on the achievable distance for optical QKD in fiber due to loss and noise. Higher key rates can be achieved in lower loss environments, typically over shorter lengths of fiber. Several recent experimental demonstrations of BB84 using 1550 nm light highlight this rate vs. distance tradeoff. The shortest of which was performed at a distance of 50 km with a SKR of 1.26 Mbps [25], the median achieved a SKR of 1 kpbs at a distance of 150 km [26], and the longest was performed at a distance of 404 km but with a SKR of only 1.16 bits per hour [26].

Beyond hardware limitations, Eve can take advantage of technical imperfections in an optical QKD system to compromise the security of the protocol. For example, Alice's single-photon source may not be perfect. If instead of always generating only a single photon, Alice's source sometimes generates multiple identical photons, then Eve can split off one of these excess photons and possess perfect copies of the single photon state that Bob receives. After the basis for each measurement is announced, Eve can then measure these extra photons to increase the mutual information she shares with Alice. This form of attack is called a photon-number splitting attack.

This loophole has since been addressed by the addition of "decoy states." These decoy states possess a different photon number than the signal states used in BB84 and are used to verify the expected photon-number statistics of the channel. To do this, Alice chooses randomly from a set of decoy states and the BB84 signal states when she is preparing her quantum state to send to Bob. The decoy state protocol is identical to BB84 except during the parameter estimation step, where Alice additionally announces the intensities or expected photon number of each state she prepared. By comparing the error rates at each intensity level with the expected statistics of the channel, Alice and Bob can determine if Eve has performed a photon-number splitting (PNS)

attack. The idea to use photon-number statistics as a countermeasure against the PNS attack was first proposed by Lütkenhaus and Jahma in 2002 [28].

# Chapter 3: Continuous Variable Quantum

## Key Distribution

### 3.1 Coherent States

Another approach to QKD is to use coherent states or Glauber states which can be easily generated from a laser source. By definition, coherent states are eigenstates of the annihilation operator.

$$\hat{a}|\alpha\rangle = \alpha|\alpha\rangle \quad (3.1)$$

The real and imaginary components of  $\alpha$  can be represented as quadrature components in phase space:

$$\alpha = q + ip. \quad (3.2)$$

To better understand coherent states and how to measure them, it is helpful to first understand a basic set of operators. The first operators of interest are the creation and annihilation operators which can be defined by their action on the number state  $|n\rangle$ , also called the Fock state:

$$\hat{a}^+|n\rangle = \sqrt{n+1}|n+1\rangle \quad (3.3.1)$$

$$\hat{a}|n\rangle = \sqrt{n}|n-1\rangle \quad (3.3.2)$$

$$\hat{a}^\dagger \hat{a} |n\rangle = \hat{n} |n\rangle = n |n\rangle, \quad (3.3.3)$$

where  $\hat{n}$  is the number operator. The second operator pair of interest are the quadrature operators:

$$\hat{q} = \hat{a} + \hat{a}^\dagger \quad (3.4.1)$$

$$\hat{p} = -i(\hat{a} - \hat{a}^\dagger). \quad (3.4.2)$$

When considering photonics systems, a number state is the photon number state in which the exact number of photons is present in a mode and the quadrature operators are the quantum analog of the optical field quadratures. The operators above are given in terms of the annihilation and creation operators, but these terms can be reversed to provide a more convenient notation for the annihilation and creation operators for coherent states which we will use later:

$$\hat{a} = \frac{1}{2} (\hat{q} + i\hat{p}) \quad (3.5.1)$$

$$\hat{a}^\dagger = \frac{1}{2} (\hat{q} - i\hat{p}). \quad (3.5.2)$$

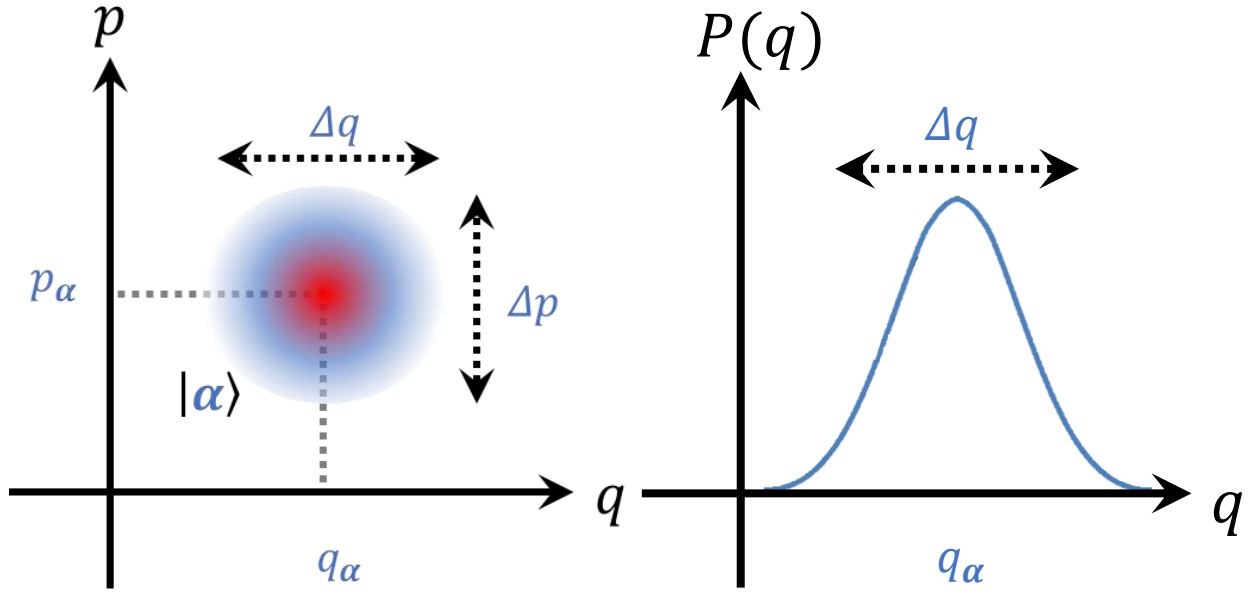
Coherent states are considered quasi-classical states. They exhibit the special property that the product of their uncertainties in each quadrature is always minimized.

$$\Delta \hat{q} \Delta \hat{p} \geq 1 \quad (1.6)$$

The derivation of the product on the left-hand side of Eq 3.6 can be found by starting with the variance of a single quadrature:

$$V(\hat{q}) = \langle \hat{q}^2 \rangle - \langle \hat{q} \rangle^2. \quad (3.7)$$

The calculation of the expectation value  $\langle \hat{q} \rangle$  is straightforward.



**Fig. 2: Left: a coherent state  $|\alpha\rangle$  visually represented in phase-space. The quadrature components of  $\alpha$  are given on each axis. Right: the probability distribution of the  $q$ -quadrature of state  $|\alpha\rangle$  is a gaussian.**

$$\langle \hat{q} \rangle = \langle \alpha | \hat{q} | \alpha \rangle = \langle \alpha | \hat{a} + \hat{a}^\dagger | \alpha \rangle = \langle \alpha | \hat{a} | \alpha \rangle + \langle \alpha | \hat{a}^\dagger | \alpha \rangle \quad (2.8)$$

$$\langle \hat{q} \rangle = \alpha + \alpha^* = (q + ip) + (q - ip) = 2q$$

Next, we calculate the expectation value  $\langle \hat{q}^2 \rangle$ :

$$\langle \hat{q}^2 \rangle = \langle \alpha | \hat{q}^2 | \alpha \rangle = \langle \alpha | (\hat{a} + \hat{a}^\dagger)^2 | \alpha \rangle \quad (3.9)$$

$$\langle \hat{q}^2 \rangle = \langle \alpha | \hat{a}^2 | \alpha \rangle + \langle \alpha | (\hat{a}^\dagger)^2 | \alpha \rangle + \langle \alpha | \hat{a} \hat{a}^\dagger | \alpha \rangle + \langle \alpha | \hat{a}^\dagger \hat{a} | \alpha \rangle$$

$$\langle \hat{q}^2 \rangle = \alpha^2 + (\alpha^*)^2 + \alpha^* \alpha + 1 + \alpha^* \alpha$$

$$\langle \hat{q}^2 \rangle = q^2 - p^2 + 2iqp + q^2 - p^2 - 2iqp + 2(q^2 + p^2) + 1$$

$$\langle \hat{q}^2 \rangle = 4q^2 + 1.$$

Note that these quantities are all given in terms of shot noise units. Combining the results of Eq.

3.8 and Eq. 3.9 into Eq. 3.7, we can now evaluate the variance of a single quadrature:

$$V(\hat{q}) = 4q^2 + 1 - 4q^2 = 1. \quad (3.10)$$

The end result is the minimal uncertainty, also called the shot noise, of one quadrature operator of a coherent state. A similar analysis of  $V(\hat{p})$  yields the same result. From here, it is straightforward to verify that a coherent state satisfies the relationship given in Eq. 3.6 when the right-hand side is equal to 1. As a result, a coherent state cannot be represented by a single point in phase space but must be represented by a probability distribution.

One method of encoding information on coherent states is to displace the coherent state in the two-dimensional phase space. Displacements are performed by the displacement operator:

$$D(\alpha) = e^{\alpha \hat{a}^\dagger - \alpha^* \hat{a}}. \quad (3.11)$$

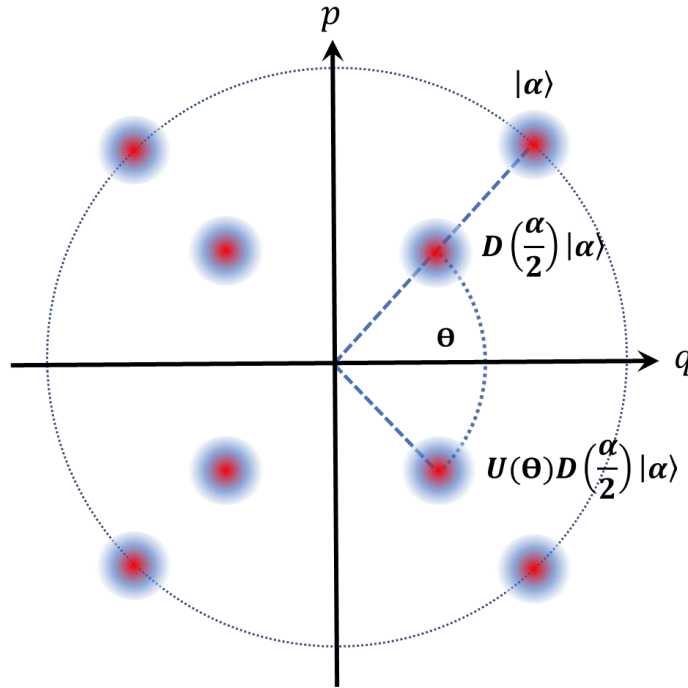
A coherent state  $|\alpha\rangle$  can be represented by the displacement operator acting on the vacuum state:

$$|\alpha\rangle = D(\alpha)|0\rangle \quad (3.12)$$

In general, a displacement operator  $D(\beta)$  will shift an arbitrary coherent state  $|\alpha\rangle$  by the real and imaginary components of  $\beta$  along the respective axes in phase space. A specific case of the displacement operator can be implemented by attenuating a coherent state. Attenuation will displace the coherent state in the direction of the origin by an amount proportional to the degree of attenuation.

Another method for encoding information is to rotate a coherent state in phase space. Rotations can be performed by the phase shifting operator:

$$U(\varphi) = e^{-i\varphi \hat{n}} \quad (3.13)$$



**Fig. 3: Coherent state implementation of 8-QAM. Any coherent state  $|\alpha\rangle$  can be used to generate a full QAM scheme using combinations of attenuators and phase-shifts to generate the additional points in the constellation diagram.**

The action of the phase shifting operator on a coherent state is to rotate the position of the coherent state in phase space about the origin by an amount  $\varphi$ :

$$U(\varphi)|\alpha\rangle = |e^{-i\varphi}\alpha\rangle \quad (3.14)$$

A phase shift can be applied by slightly altering the path length between the coherent state and its phase reference. In fiber, this is typically done using a piezoelectric device to stretch or contract a short length of fiber. This phase shift can only be measured relative to a phase reference with a constant or known phase relation. The phase reference can take the form of a local oscillator created from the same laser source or even temporally adjacent signal states.

By attenuating and phase shifting an existing coherent state, it is possible generate a new coherent state with a probability distribution centered on any point within a fixed distance from

the origin. An example of how a set of constellation points can be generated from a single coherent state is given in Fig. 3. In optical communications, each constellation point can be assigned a symbol containing  $I$  bits of information:

$$I = \log_2 m, \quad (3.15)$$

where  $m$  is the number of symbols and the size of the constellation. Now that we understand how coherent states can be used to store information, let us examine how to extract information from these states.

In the case of DV-QKD, single photons states are usually distinguished by their photon number, polarization, or time bin. These attributes of single photon states allow their state to be measured directly on a single detector or to be sorted to allow a single detector to distinguish between them. In CV-QKD, measurement of quadrature is not so straightforward. To describe the measurement of a coherent state, we will begin by defining a classical local oscillator (LO) as in [29]:

$$\alpha_{LO} = |\alpha_{LO}|e^{i\theta}, \quad (3.16)$$

where  $|\alpha_{LO}|$  is the amplitude of the classical field and  $\theta$  is the phase of the classical field relative to a particular coherent state. This classical field will be combined with a coherent state (represented by the annihilation operator given in Eq. 3.5.1) on a balanced beam splitter defined by:

$$BS_{50-50} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad (3.17)$$

The two outputs resulting from this combination are given by  $\hat{a}_1$  and  $\hat{a}_2$ .

$$BS_{50-50} \begin{pmatrix} \hat{a} \\ \alpha_{LO} \end{pmatrix} = \begin{pmatrix} \hat{a}_1 \\ \hat{a}_2 \end{pmatrix} \quad (3.18)$$

$$\hat{a}_1 = \frac{1}{\sqrt{2}}(\hat{a} + \alpha_{LO}) \quad (3.19.1)$$

$$\hat{a}_2 = \frac{1}{\sqrt{2}}(\hat{a} - \alpha_{LO}) \quad (3.19.2)$$

Recall the number operator from Eq. 3.3.3. The number operators  $\hat{n}_1$  and  $\hat{n}_2$  for each beam splitter output are:

$$\hat{n}_1 = \hat{a}_1^\dagger \hat{a}_1 = \frac{1}{2}(\hat{a}^\dagger + \alpha_{LO}^*)(\hat{a} + \alpha_{LO}) \quad (3.20.1)$$

$$\hat{n}_1 = \frac{1}{2}(\hat{a}^\dagger \hat{a} + \alpha_{LO}^* \alpha_{LO} + \alpha_{LO} \hat{a}^\dagger + \alpha_{LO}^* \hat{a})$$

$$\hat{n}_2 = \hat{a}_2^\dagger \hat{a}_2 = \frac{1}{2}(\hat{a}^\dagger + \alpha_{LO}^*)(\hat{a} - \alpha_{LO}) \quad (3.20.2)$$

$$\hat{n}_2 = \frac{1}{2}(\hat{a}^\dagger \hat{a} + \alpha_{LO}^* \alpha_{LO} - \alpha_{LO} \hat{a}^\dagger - \alpha_{LO}^* \hat{a})$$

The number operator can be physically implemented by measuring the power at either output of the balanced beam splitter. Taking the difference of these powers is analogous to applying the number-difference operator:

$$\begin{aligned} \Delta \hat{n} &= \hat{n}_1 - \hat{n}_2 = \alpha_{LO} \hat{a}^\dagger + \alpha_{LO}^* \hat{a} \quad (3.21) \\ &= |\alpha_{LO}| (e^{i\theta} \hat{a}^\dagger + e^{-i\theta} \hat{a}) \\ &= |\alpha_{LO}| \frac{1}{2} (e^{i\theta} (\hat{q} - i\hat{p}) + e^{-i\theta} (\hat{q} + i\hat{p})) \end{aligned}$$

$$\begin{aligned}
&= |\alpha_{LO}| \frac{1}{2} (\hat{q} (e^{i\theta} + e^{-i\theta}) + i\hat{p} (-e^{i\theta} + e^{-i\theta})) \\
&= |\alpha_{LO}| (\hat{q} \cos \theta + \hat{p} \sin \theta)
\end{aligned}$$

Based on the relative phase  $\theta$  of the LO, a measurement can be performed to extract a single quadrature component. This phase can be varied to control which quadrature is measured.

$$\Delta\hat{n} = |\alpha_{LO}| \hat{q}, \quad \theta = 0 \quad (3.22.1)$$

$$\Delta\hat{n} = |\alpha_{LO}| \hat{p}, \quad \theta = \frac{\pi}{2} \quad (3.22.2)$$

This form of measurement is known as homodyne detection when the frequency of the signal and the LO are identical. Accurate homodyne detection relies on precise control or knowledge of the phase relationship between the signal and the local oscillator. Additionally, the ratio of the detector electronic noise to the shot noise must be kept low.

## 3.2 Gaussian-modulated Coherent State Protocol

In 2002, Grosshans and Grangier developed a promising alternative to BB84. Often referred to as the Gaussian-modulated Coherent State (GMCS) protocol, this scheme eliminated the need to generate, manipulate, and measure single photons. By deviating from the use of single photons, it alleviated technical limitations on both the signal source and detector. Instead of the traditional single photon source, any narrow-linewidth laser source can be attenuated to generate an appropriate coherent state. Since each signal state requires a strong local oscillator to mitigate the effects of detector noise, detection occurs at much higher powers which enables the use of a much wider range of photodiodes, potentially even those employed in classical coherent communications. An overview of the GMCS protocol will now be presented following the same format as the BB84 protocol.

1) Preparation, transmission, and measurement: Alice generates two random numbers  $q_A$  and  $p_A$  from a gaussian distribution with variance  $V_A$ . Alice then prepares the coherent state  $|q_A + ip_A\rangle$  in an optical pulse and transmits this state to Bob. Bob then measures randomly either the phase or amplitude of the coherent state to extract information about either the p- or q-quadrature of the signal state.

In general, a quantum channel is both noisy and lossy. In other words, there exists an amount of excess noise  $\xi$  beyond the shot noise, and the channel transmittance  $T$  is less than 1 which must be accounted for. Both of these channel properties impact the reliability of Bob to

accurately measure the states that Alice prepares. Eve can potentially mask her eavesdropping attempts behind the unreliable nature of the channel. As the excess noise increases, Eve's Holevo information grows as well. As the channel transmittance decreases, Bob's ability to measure Alice's prepared state decreases, and the mutual information between Alice and Bob  $I_{AB}$  also decreases. A combination of these two factors may create a situation where the protocol is insecure. Hence, it is necessary for Alice and Bob to estimate these parameters during the parameter estimation step of the protocol.

2) Sifting: Bob publicly announces which basis he used for each measurement. Similar to BB84, half of the information encoded by Alice is discarded. Alice and Bob now have two correlated sets of gaussian variables.

3) Parameter estimation: Alice and Bob now sacrifice a portion of their sets to estimate the channel transmissivity and the excess noise of the channel. Estimating these parameters allows Alice and Bob to bound the mutual information between Alice and Eve and determine the security of the protocol. If the mutual information between Alice and Bob is less than the mutual information between Alice and Eve, then the protocol is terminated here.

4) Information reconciliation: Alice and Bob now transform their continuous Gaussian variables into a discrete, errorless bit string. This process can be done via either sliced reconciliation or multidimensional reconciliation [30,49]. These techniques are optimized to detect and correct errors while minimizing the information publicly disclosed for correction when an error is detected. Efficient sliced reconciliation schemes have been proposed using polar codes, Bose-Chaudhuri-Hocquengem (BCH) codes, and LDPC codes [31, 32, 33]. In particular, multi-edge type (MET) LDPC codes perform well in high loss conditions.

These methods can be employed in one of two ways: either Bob corrects his bits according to information released by Alice in a process called direct reconciliation, or Alice corrects her bits according to information released by Bob in which is known as reverse reconciliation. When using direct reconciliation, there exists a limit on the channel loss since Alice must correct any errors by disclosing information about her key. If the channel loss is greater than 3 dB, Eve could potentially gain more information about Alice's secret key than Bob would gain through measurement. In this case, no secret key can be generated. If reverse reconciliation is used instead, only information about Bob's key is announced. Since Alice knows the state she prepared, the parameters of the channel, and Bob's measurement basis, she will always know more about Bob's measurements than Eve who only knows partial information about Alice's prepared state, the channel parameters, and Bob's measurement basis. This allows the 3 dB loss limit to be overcome when using reverse reconciliation [17].

5) Privacy amplification: From this point on, the protocol is identical to BB84. From their errorless bit string, Alice and Bob can use standard classical privacy amplification techniques as described in the BB84 protocol in section 2.2

The premise behind the security of GMCS is to mask a distribution of coherent states as a thermal state to any would-be eavesdropper, but this relies on several assumptions which are not yet feasible. The first requirement is that the distributions of the complex random numbers be drawn from a Gaussian distribution of a given variance. This requires a random number source which follows a true Gaussian distribution. In reality, a random number source can only attempt to emulate a Gaussian by truncating number outcomes below some probability. Furthermore, sampling from a true Gaussian by modulating with a finite extinction ratio is not possible. And in practice, only a finite number of points can be used for modulation. For these reasons,

implementations of a secure GMCS protocol are not practical, and attempts to implement GMCS in a practical environment are not secure.

It is possible to approximate a discretized Gaussian modulation as a true Gaussian while maintaining its security. Near the shot noise limit, it is difficult to differentiate a true Gaussian from a discrete one provided the discretization is small enough. For example, if a Gaussian distribution is truncated to 7 standard deviations and discretized into steps of 0.25 shot noise units, then a discrete Gaussian consisting of 253 points would be sufficient to maintain security [33]. This requires that each state in a discretized GMCS protocol can be reliably generated and measured.

In the next chapter, a discrete version of the GMCS protocol will be presented. Methods for calculating the bounds on Eve's Holevo information and the mutual information between Alice and Bob based on experimental data will also be presented. Finally, a proof-of-principle experimental setup capable of characterizing a discrete Gaussian protocol will be shown alongside theoretical calculations of the error introduced by a Gaussian approximation.

# Chapter 4: Discrete Gaussian-modulated Quantum Key Distribution

## 4.1 Brief History and Outline of the Chapter

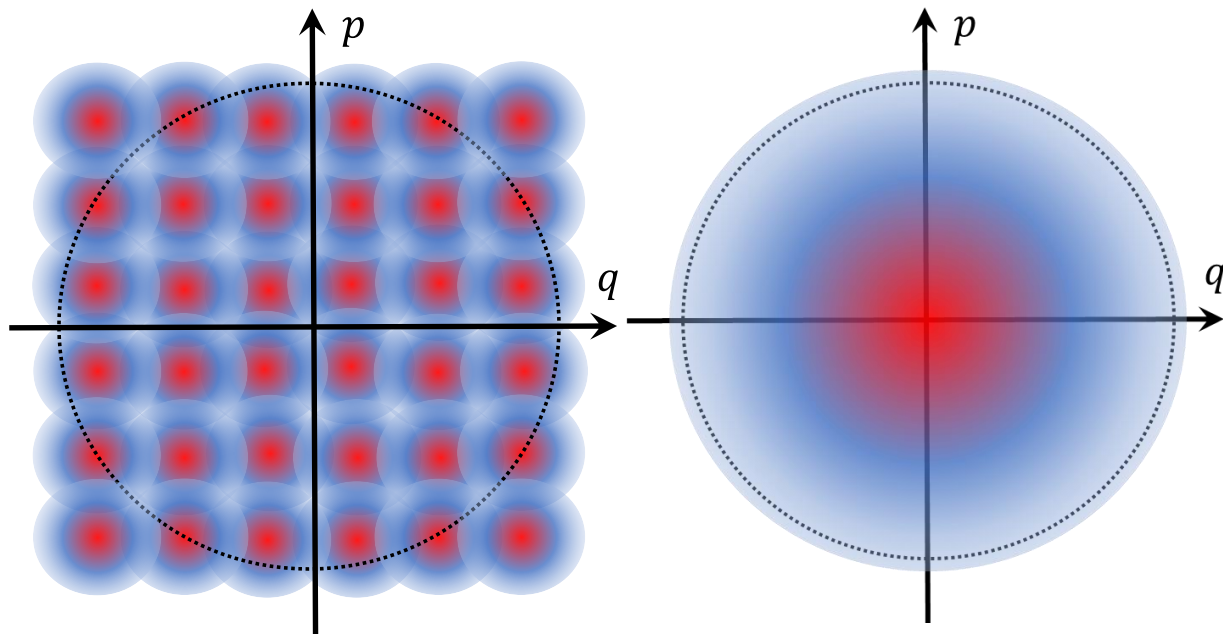
The idea of discretely modulated CV-QKD was first proposed in the late 1990's and early 2000's [34, 35, 36]. Since then, several discrete protocols have been proposed alongside security proofs against specific types of collective attacks, but these protocols have so far not been able to match the key rates provided by the GMCS protocol [37, 38]. These protocols attempt to leverage the efficient modulation and error correction techniques of DV-QKD to overcome the typical deficiencies of CV-QKD. These efficient methods are enabled by the small, finite constellation sizes typical of DV-QKD. In 2012, a discrete Gaussian-modulated coherent state (DGM) protocol was proposed by Leverrier et al. which used a finely discretized Gaussian to approximate a true Gaussian distribution in hopes of achieving a key rate similar to GMCS [33]. However, their proposal did not include a proof of security. It was not until recently that both a proof of security against collective attacks and a bound for Eve's Holevo information were established for a general discrete modulation QKD protocol [39, 40, 41].

The work in this thesis involves the specific protocol outlined in [39] by Kaur, Guha, and Wilde using homodyne detection. The end-goal of this work is to realize this protocol in an experimental demonstration. A summary of the DGM protocol will be presented here, followed by an experimental setup modeling this protocol. Finally, a method for obtaining a data set representative of Bob's measurement outcomes is presented. From these outcomes, it is possible to estimate the secure key rate of the DGM protocol.

## 4.2 The Discrete Gaussian-modulated Protocol

In this section, the DGM protocol of [39] is presented in the same format as the BB84 and the GMCS protocols. The protocol is split into two major parts. The first involves the preparation, transmission, and measurement of quantum states. The second part is classical post-processing which here will focus on parameter estimation as both the classical information reconciliation and privacy amplification steps have already been discussed in previous protocols. The sifting step will also be omitted here as it is not necessary in this protocol. This DGM protocol is based on  $m^2$  coherent states where  $m$  is a pre-selected integer. Larger values of  $m$  will allow for finer discretization and better performance, more closely matching the ideal GMCS protocol (see Fig. 4). First, let  $X$  be a Gaussian random variable with zero mean, with a variance equal to  $N_S$ , and with outcomes  $x \in \{1, 2, 3, \dots, m^2\}$ . Now, let  $\alpha_x$  be a complex number corresponding to  $x$ . The protocol is as follows:

- 1) Preparation, transmission, and measurement: Alice chooses a value of  $x$  according to the probability distribution  $r(x)$  and prepares the coherent state  $|\alpha_x\rangle$ . The probability distribution  $r(x)$  is designed such that the weighted collection of coherent states  $\alpha_x$  form a constellation that appears as a thermal state with a mean photon number  $N_S$ . Such a thermal state appears as a Gaussian in phase space with the most probable number of photons being zero, but the mean is non-zero, given by  $N_S$ . Alice notes the value of  $x$  in the variable  $x_j$  where  $j$  indexes the symbol or transmission round in which a symbol or pulse is transmitted in each round. Alice also records the



**Fig. 4: On the left is a phase space map for a collection of densely packed coherent states ( $m=6$ ). If the number of coherent states  $m^2$  that compose this collection is sufficiently large, then a probability distribution can be selected such that the average of this distribution can be disguised as a thermal state as shown on the right.**

real and imaginary components of  $\sqrt{2}\alpha_j$  into the variables  $q_j$  and  $p_j$  respectively. Next, Alice picks a random phase  $\varphi_j \in \{0, \frac{\pi}{2}, \pi, \frac{3\pi}{2}\}$  to apply as an additional phase shift to her prepared coherent state. Alice then sends this state to Bob across a quantum communication channel. Alice then communicates to Bob which phase shift she applied to her state. Bob uses this information to reverse Alice's phase shift. This symmetric phase manipulation is helpful in reducing the number of estimated parameters during the parameter estimation step. After the phase has been reversed, Bob performs homodyne detection and records his result in the variable  $y_j^q$ . This step is repeated  $n$  times.

2) Parameter estimation: Alice and Bob now sacrifice a fraction  $\delta$  of their symbols to estimate channel parameters. Specifically, Alice and Bob calculate the elements of the covariance matrix  $\gamma_{11}$ ,  $\gamma_{12}$ , and  $\gamma_{22}$  from the following equations.

$$\gamma_{11} \equiv \frac{1}{\delta n} \sum_{j=1}^{\delta n} (q_j - \bar{q})^2, \quad (4.1.1)$$

$$\gamma_{12} \equiv \frac{1}{\delta n} \sum_{j=1}^{\delta n} (q_j - \bar{q})(y_j^q - \bar{y}), \quad (5.1.2)$$

$$\gamma_{22} \equiv \frac{1}{\delta n} \sum_{j=1}^{\delta n} (y_j^q - \bar{y})^2, \quad (6.1.3)$$

where:

$$\bar{q} \equiv \frac{1}{\delta n} \sum_{j=1}^{\delta n} q_j, \quad \bar{y} \equiv \frac{1}{\delta n} \sum_{j=1}^{\delta n} y_j^q. \quad (7.2)$$

By announcing the data from  $\delta n$  rounds of Alice's  $q_j$  and Bob's  $y_j^q$ . From the covariance matrix, Alice and Bob calculate the upper bound on Eve's Holevo information  $\chi_{EB}$  from the following equation:

$$\chi_{EB} = g(v_1) + g(v_2) - g(v_3), \quad (4.3)$$

where

$$v_1 = \gamma_{11} + 1, \quad (4.4.1)$$

$$v_2 = \gamma_{22} \pm \varepsilon_1, \quad (4.4.2)$$

$$v_3 = (\gamma_{11} + 1) \left( \gamma_{11} - \frac{(\gamma_{11} + 2)}{\gamma_{11}(\gamma_{22})} (\gamma_{12} \pm \varepsilon_2)^2 \right). \quad (4.4.3)$$

The function  $g(x)$  is defined by:

$$g(x) = (x + 1) \log_2(x + 1) - x \log_2 x. \quad (4.5)$$

The epsilon terms  $\varepsilon_1$  and  $\varepsilon_2$  are small errors introduced by approximating a true Gaussian with a discrete one. As the constellation size  $m^2$  increases and mean photon number of the thermal state

$N_S$  decreases, the magnitude of these errors decreases and Eve's bound approaches that of the GMCS protocol. Once Alice and Bob have bounded Eve's Holevo information, they can measure their own mutual information from the signal-to-noise ratio (SNR):

$$I_{AB} = \frac{1}{2} \log_2(1 + SNR). \quad (4.5)$$

The SNR can be calculated from the total channel transmittance  $T$  and the excess noise  $\xi$ . These parameters can be calculated from the covariance matrix elements in the same way as for the GMCS protocol when  $N_S$  is used as the modulation variance:

$$SNR = \frac{TN_S}{1 + \xi}, \quad (4.6)$$

$$T = \frac{\gamma_{12}^2}{N_S^2 + 2N_S}, \quad (4.7)$$

$$\xi = \gamma_{22} - TN_S - 1. \quad (4.8)$$

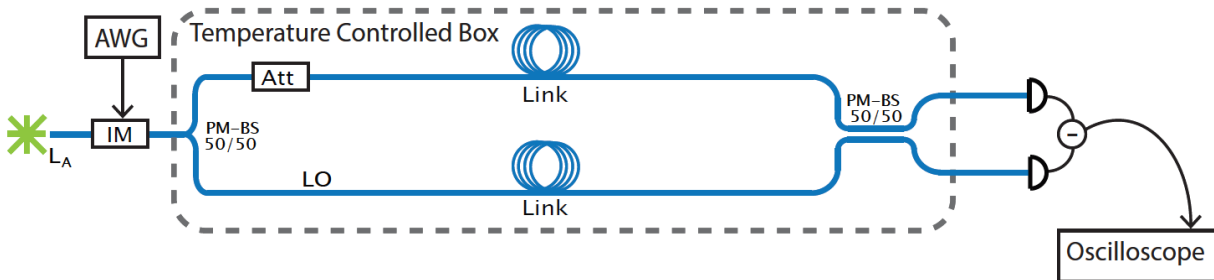
The secret key rate  $K$  can then be calculated by:

$$K = f_{sym}(1 - \delta)(\beta I_{AB} - \chi_{EB}), \quad (4.8)$$

where  $f_{sym}$  is the symbol rate and  $\beta$  is a value between 0 and 1 representing the efficiency of the post-processing. The fraction of symbols sacrificed for parameter estimation  $\delta$  is also accounted for. If Alice and Bob's mutual information  $I_{AB}$  is greater than the upper bound on Eve's Holevo information  $\chi_{EB}$ , then the protocol is secure. Otherwise, the protocol is terminated.

Finally, the data from the  $\delta n$  rounds of symbols used for parameter estimation is discarded, and the remaining  $q_j$  and  $y_j^q$  compose the raw key to be used for secure key generation. Alice and Bob then perform the standard information reconciliation and privacy amplification using techniques previously discussed in chapters 2 and 3.

### 4.3 Experimental Characterization



**Fig. 5: Optical DGM proof-of-principle experimental setup.**  $L_A$ : Alice’s laser source, AWG: arbitrary waveform generator, IM: intensity modulator, PM-BS: polarization-maintaining beam splitter, Att: optical attenuator.

An optical proof-of-principle setup for the DGM protocol is shown in Fig 5. The 1550 nm continuous-wave output of a narrow linewidth semiconductor laser (Clarity NLL-1550-LP) is coupled in polarization maintaining (PM) fiber and carved into pulses using an intensity modulator (EOSpace AX-65S-10-PFAP-R5). These pulses are 10 ns wide with a rep rate of 25 MHz. These pulses are split on a 50/50 PM beam splitter. One arm is designated for the signal states and attenuated to the desired coherent state amplitude using a variable fiber attenuator, while the other arm serves as the LO. Both the attenuated signal and LO are recombined on a 50/50 PM beam splitter and then measured on a homodyne detector (Thorlabs PDB425C). The pair of beam splitters and the fiber connecting them are placed inside a temperature-controlled housing which serves to passively stabilize the phase between the signal and LO.

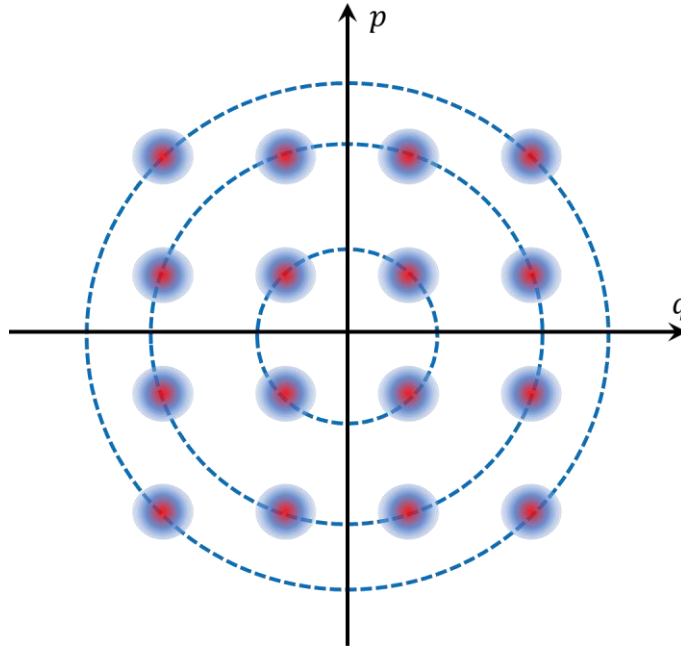
In order to generate the coherent states desired for the DGM protocol, the intensity of the signal arm and its relative phase to the local oscillator must be controlled. In this proof-of-principle setup, the intensity of the signal can be controlled using the attenuator in the signal arm of the

interferometer. The control of the phase is done indirectly by controlling the temperature inside the housing. By shifting the temperature inside the interferometer housing, a small path length difference can be induced between the two arms of the interferometer relative to the difference in their fiber lengths. By inducing a larger shift in the longer arm of the LO, the relative phase between the LO and signal can be adjusted. Precise control of this phase is not necessary if the phase can be scanned much faster than the phase drift. By allowing the temperature inside the box to reach a set point and then switching the temperature controller on or off, a fast phase scan can be applied albeit for a limited time. As the temperature of the housing reaches an equilibrium, the phase scan slows and the phase drift begins to dominate. In a practical DGM QKD implementation, the control of intensity and phase will be performed on-demand by an intensity and phase modulator, chosen according to the probability distribution  $r(x)$ . Temperature scanning was used for simplicity here to characterize the system.

For proof of principle demonstration, our goal is to collect data for a 10 x 10 grid of constellation points for the DGM protocol described in [39]. This data will be representative of Bob's measurement outcomes and can be used to estimate the secure key rate of a practical DGM implementation. The method for data collection will be explained for a 4 x 4 grid, but in principle this can be extended to a 10 x 10 grid and beyond. Fig. 6 shows the states that need to be generated for a 4 x 4 grid of constellation points. The placements of points in these grids depend on the constellation grid size  $m$ . Points are placed along each axis at the roots of the  $m$ -th order Hermite polynomial. In [39], the Hermite polynomial is defined as:

$$H_n(x) = (-1)^n \exp\left(\frac{x^2}{2}\right) \frac{d^n}{dx^n} \left( \exp\left(-\frac{x^2}{2}\right) \right). \quad (4.6)$$

The zeros  $Z_4$  of the 4<sup>th</sup> order Hermite polynomial  $H_4(x)$  are located at:



**Fig. 6: A 4 x 4 grid of coherent states in phase space composing a sample DGM constellation. Each blue dotted line corresponds to a subset of these states with equal coherent state amplitudes. Coherent states in the first quadrant have phases of  $17.62^\circ$ ,  $45^\circ$ , or  $72.38^\circ$  as dictated by the roots of the 4<sup>th</sup> order Hermite polynomial.**

$$Z_4 = \pm 0.742, \pm 2.334. \quad (4.7)$$

The set of constellation points within such a 4 x 4 grid can be organized into 3 subsets of points where each subset falls on a circle of a given radius in phase space. In other words, coherent states belonging to a given subset all possess the same mean coherent state amplitude or average photon number and a unique phase within that subset. The 4 x 4 grid constellation and the described subsets are illustrated in Fig. 6. This means that Alice's weak coherent states must have a mean photon number  $N_\alpha$  between 1.04 and 3.30 photons. In the case of our goal of a 10 x 10 grid where the zeros  $Z_{10}$  of the 10<sup>th</sup> order Hermite polynomial  $H_{10}(x)$  are located at:

$$Z_{10} = \pm 0.485, \pm 1.466, \pm 2.484, \pm 3.582, \pm 4.859, \quad (4.8)$$

the coherent states in the constellation range in mean photon number between 0.686 and 6.872 photons.

In order to properly simulate a thermal state, the coherent states nearest to the center of the constellation diagram must be the most likely to be chosen by Alice in the protocol, as per the discretized Gaussian distribution. It is a challenge to reliably generate and transmit such weak coherent states in a channel that is both lossy and noisy. Fortunately, the mean photon number of the thermal state  $N_S$  being approximated can be scaled to increase the mean photon number requirement of the signal state. By increasing the mean photon number of the thermal state by a factor of 2 for example, the required mean photon number of the signal state also increases by a factor of 2. In general, this factor can be optimized for a given constellation size to achieve the optimal key rate, but it can also be set larger to accommodate a stronger coherent state signals. This comes at a price in terms of the key rate. The approximation error for substituting a collection of weak coherent states as a thermal state is given by  $\varepsilon$ :

$$\varepsilon = \frac{1}{2} \sqrt{\tau(2 + \tau)}, \quad (4.9)$$

where  $\tau$  scales with the mean photon number of the thermal state:

$$\tau \approx 2.36(1 + N_S) \left( \frac{N_S}{\sqrt{N_S(1 + N_S)}} \right)^{2m}. \quad (4.10)$$

If  $N_S$  is large,  $\tau$  scales linearly with further increases in  $N_S$ . This can be mitigated by increasing the constellation size. However, the effect of increasing the constellation size on mitigating this error also decreases as  $N_S$  grows. This means that maintaining a low mean photon number is very important if we wish to obtain a key rate similar to that of the ideal GMCS protocol. The difference in Eve's Holevo information as a result of the discrete Gaussian approximation is given in [39]:

$$f(\varepsilon, N_S) = \varepsilon(2t + r_\varepsilon(t)) \cdot g\left(\frac{P}{\varepsilon t}\right) + 2g(\varepsilon r_\varepsilon(t)) + 2H(\varepsilon t), \quad (4.11)$$

$$r_\varepsilon(t) = \frac{1 + \frac{t}{2}}{1 - \varepsilon t}, \quad (4.12)$$

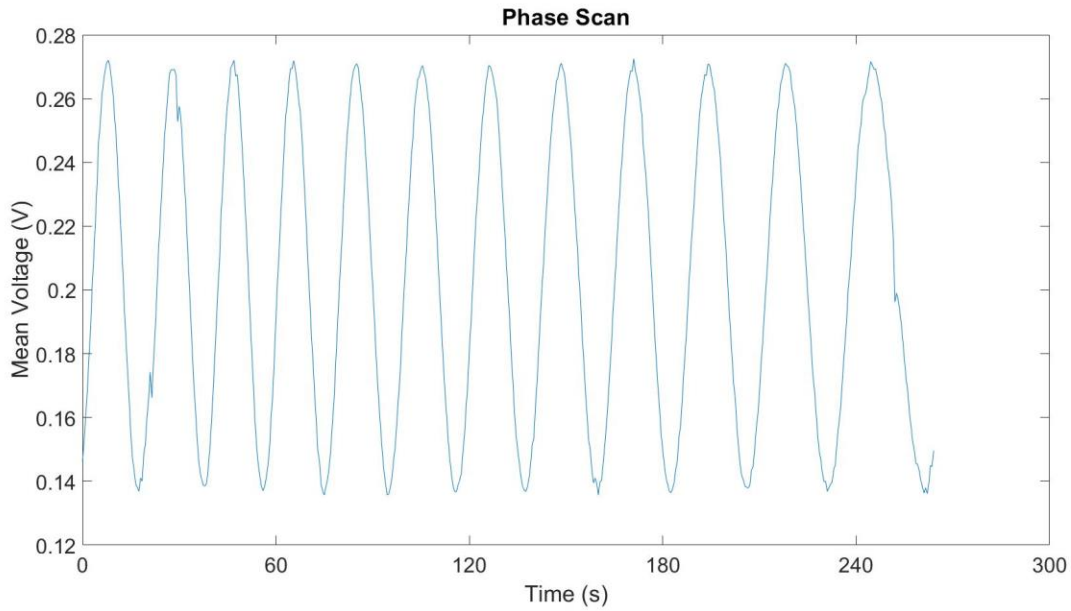
where  $P = 10^7$  is a bound of the mean energy of Eve's observed thermal state and  $t$  can take any value between 0 and  $0.5\varepsilon$ . The functions  $g(x)$  and  $H(x)$  are the same as those presented in Eq. 4.5 and Eq. 2.11, respectively. Eve's Holevo information can now be calculated by the following equation without calculating the individual error terms  $\varepsilon_1$  and  $\varepsilon_2$ :

$$\chi_{EB} = g(\gamma_{11} + 1) + g(\gamma_{22}) - g\left(\sqrt{\frac{\gamma_{11} + 2}{\gamma_{11}}} \gamma_{12}\right) + f(\varepsilon, N_S) \quad (4.13)$$

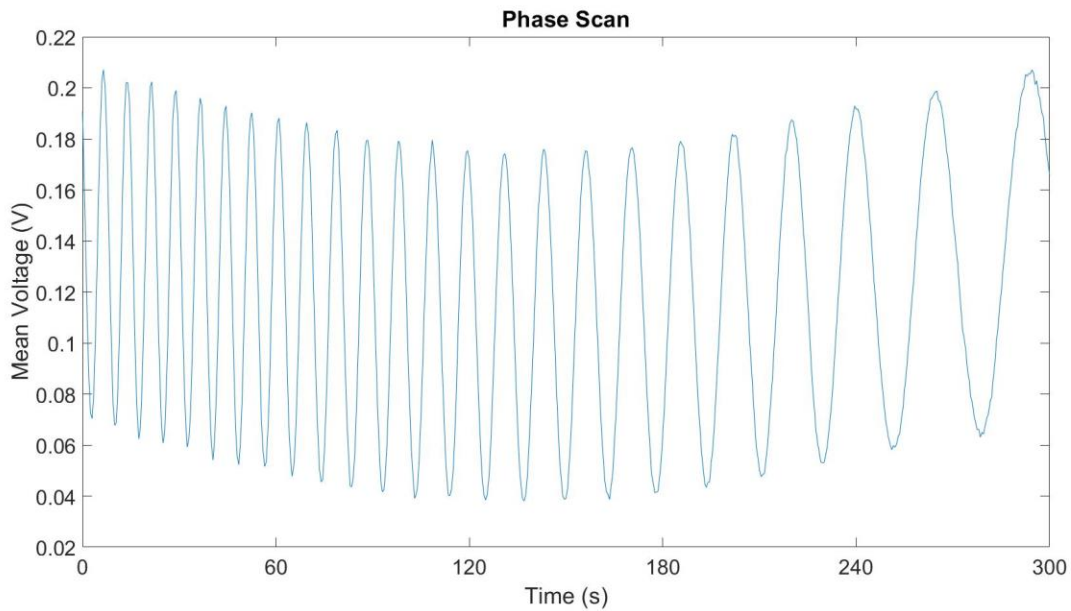
With this formula, Eve's Holevo information can be calculated based solely on Alice's prepared states, Bob's measurements, and the known parameters  $m^2$  and  $N_S$ . To collect a sample of Bob's measurement outcomes, the output of our homodyne detector is captured by an oscilloscope while a temperature-induced phase scan occurs. Each oscilloscope trace spans 1000 ns. With a rep rate of 25 MHz, this means that we expect to find 25 pulses in each oscilloscope trace. These oscilloscope traces are taken frequently, limited by rate at which high resolution traces can be saved which is about 1-2 Hz for our oscilloscope. The means of each oscilloscope trace are then calculated to estimate the phase for each set of pulses. A phase scan curve collected from our proof of principle setup is presented in Fig 7. This phase scan is repeated at a set of mean photon numbers determined by the selection of  $m$  and  $N_S$ . For a 4 x 4 grid with  $N_S = 1$ , phase scans must be obtained for coherent states with mean photon numbers of 1.04, 2.45, and 3.30 photons. For each phase scans at a given amplitude, we can calculate the mean photon number and estimate the relative phase for each oscilloscope trace in the scan. Based on these two parameters, we can identify a collection of Bob's measurements corresponding to each signal in the constellation diagram.

All phase scans that we have collected have a mean photon number too large to be used in a DGM protocol with a positive key rate. The data presented here is for signal states with a mean photon numbers around  $N_\alpha \approx 2800$  photons. We have been able to collect phase scans with mean photon numbers as low as  $N_\alpha \approx 250$  photons and are currently working on collecting phase scans for smaller mean photon numbers. However, as the mean photon number of our targeted coherent states decrease, it becomes more difficult to obtain a stable phase scan and identify coherent states with our desired phase.

Additionally, we sometimes observe a slow drift in the phase scan when collecting data over 5 minutes at lower coherent state amplitudes as in Fig 8. This is characteristic of a slow electronic drift in the difference amplifier circuit of the homodyne detector. This drift is only observed when looking at the difference output of our homodyne detector, which is AC coupled, giving rise to the drift. In separate measurements of the optical power just before each input to our homodyne detector the drift is not observed. Therefore, this drift can be corrected by obtaining a phase scan over multiple periods and tracing the drift in the local maxima and minima values of the phase scan in order to remove it from the data. Once an estimate of the drift is obtained, it can be used to normalize the original phase scan and obtain a drift-free trace. At each maxima, we assume a phase of 0, and at each minima, we assume a phase of  $\pi$ . An example of this correction applied to the data from Fig. 8 is presented in Fig. 9 alongside a set of lines identifying where the mean of the oscilloscope trace corresponds to a phase in the constellation diagram. Once a set of oscilloscope traces with a sufficiently low mean photon number are identified from the normalized phase scan curves, we can use this set of traces as examples of Bob's measurement outcomes. From the means and variances of Bob's measurements, we can calculate the covariance matrix elements and ultimately a key rate.



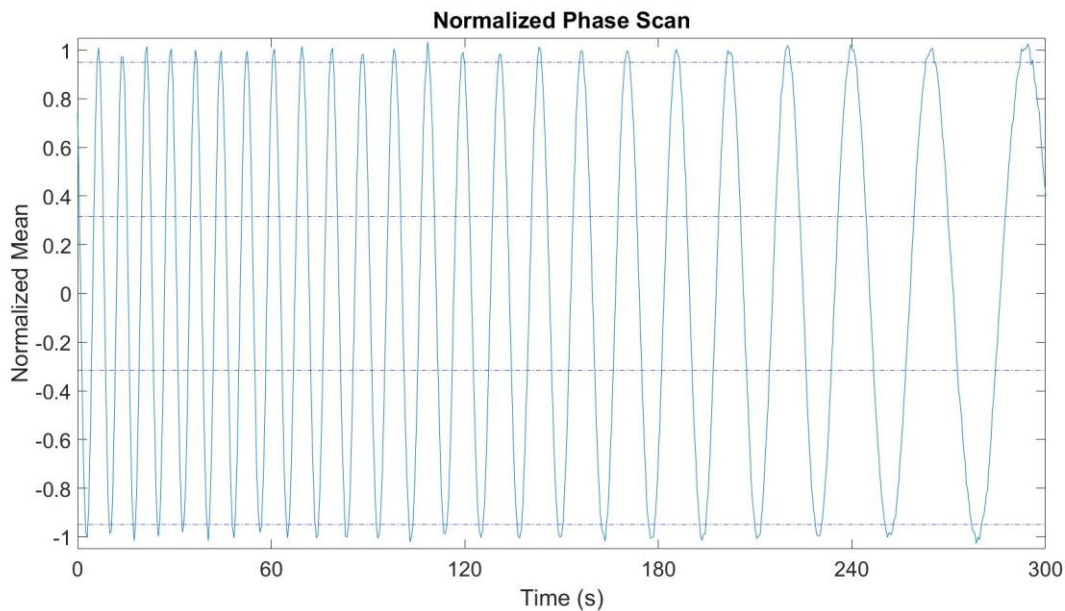
**Fig. 7:** The mean difference voltage measured at the homodyne detector output for a phase scan with an LO power of 18  $\mu$ W and a signal power of 18 nW ( $N_\alpha \approx 5600$  photons).



**Fig. 8:** The mean difference voltage measured at the homodyne detector output for a phase scan with an LO power of 18  $\mu$ W and a signal power of 9 nW ( $N_\alpha \approx 2800$  photons).

The next step towards our proof of principle demonstration of DGM-QKD is to generate the appropriate coherent states composing the DGM constellation diagram. Some coherent states have already been generated, but in order to achieve a positive SKR and eventually one close to that of the GMCS protocol it will be necessary to generate coherent states with lower mean photon numbers.

One improvement that would enable the generation of low amplitude coherent states would be to replace the attenuators in the signal arm with an intensity modulator. A  $10 \times 10$  DGM constellation requires signal states at 15 different amplitudes between 0.686 and 6.872 photons. The range of our current variable attenuator ( $\sim 50$  dB) is not sufficient to attenuate down from the microwatt level down to the picowatt level required to generate coherent states for the DGM



**Fig. 9:** The normalized mean difference calculated from the data presented in Fig. 8. If we pretend this data corresponds to a mean photon number of 2.45 photons from the  $4 \times 4$  grid, then we would be interested in identifying points with phase angles of  $17.62^\circ$ ,  $72.38^\circ$ ,  $107.62^\circ$ , and  $162.38^\circ$ . To do this, horizontal lines corresponding to the cosines of these angles are plotted. We can now search for points near these intersections to identify oscilloscope traces with the desired relative phase. The sign of the phase scan slope can be used with these intersections to distinguish between all 8 points in the constellation subset.

protocol. We need to pair this with another source of attenuation. This could be something simple such as a fixed value attenuator or something capable of quickly switching between a variety of mean photon numbers such as an intensity modulator. In order to obtain phase scans, it would be easier and faster to implement a simple attenuator. However, an intensity modulator will eventually be necessary beyond the proof-of-principle in order to generate coherent states at the desired amplitude on demand.

Another improvement can be made to the phase scan sampling rate. Due to the speed of our oscilloscope on its current settings, it is not possible to collect more than 2 traces per second. If the phase is scanned by  $2\pi$  over the course of 15 seconds, only 30 points would characterize a full phase oscillation. Obtaining a set of points on this curve whose phases very closely match those on the constellation diagram requires potentially many iterations. Relying on temperature sweeps as in the current setup makes obtaining many iterations a very time-consuming process.

One potential avenue that is explored in the next chapter is to add a phase modulator to the signal arm of the interferometer. Being able to tune the relative phase via a phase modulator would allow the application of an arbitrary phase shift to obtain any desired coherent state at a given amplitude. However, targeting each point in the constellation diagram in this way requires that the phase drift due to noise is slow in comparison to our symbol rate, or that some method is employed to compensate for this phase noise. The next chapter explores using a Red Pitaya microcontroller in conjunction with a piezoelectric phase modulator to compensate for phase noise.

# Chapter 5: Phase Stabilization Using Red

## Pitaya

### 5.1 Phase Compensation

In the original implementation of GMCS, Alice generates and transmits a LO to Bob to allow him to perform homodyne detection on her coherent state. Various techniques such as feedforward carrier recovery and optical phase-locked loops exist in classical communications to recover the phase information needed for coherent detection, but these methods are not suitable in QKD where both the signal power and tolerable phase noise are extremely low [42, 43]. Originally, only a single laser was used to generate the signal and LO. The reason for this is that the frequency instability of two lasers causes rapid fluctuations in their phase relationship. If both signal and LO come from the same laser source, a phase drift should then only arise from the difference in optical path length (OPL) between the signal and LO.

If the phase drift is slow enough, several rounds of a QKD protocol can be performed before Alice will need to select several rounds to use to recalibrate and to re-estimate the phase relationship between the LO and signal. As the phase drift increases, recalibration must be performed more frequently at the cost of efficiency. This transforms the problem of phase

compensation into a resource optimization problem: how can the best phase estimation be achieved by sacrificing the fewest signal pulses?

However, once this problem is solved, there are further barriers. Even transmitting a LO places requirements on the launch power of a QKD system. In order to perform coherent detection with a low electronic noise to low shot-noise ratio, the local oscillator pulse must contain at least  $10^8$  photons [44]. For high-speed, long distance communications, the LO launch power becomes a practical constraint. It is possible to separate and amplify the classical local oscillator, but this may introduce additional leakage from the LO into the signal mode and contribute to the noise. Furthermore, transmitting the LO allows Eve to manipulate the LO power and wavelength to her advantage. As such, CV-QKD systems involving a transmitted LO are both hindered by practical constraints and vulnerable to attacks on the LO. Two new methods for phase compensation which address these concerns will now be discussed: the self-referencing method and the self-coherent method.

In the self-referencing method, Bob uses a laser source in his own laboratory to replace the transmitted LO. This source is often referred to as Bob's "local" local oscillator (LLO). By circumventing transmission, Eve no longer has access to the LO, and the LLO can be fully trusted. The power of the LLO can also reliably be controlled by Bob to maintain the same power at all times. However, Alice and Bob must now correct or compensate for the drift in the LLO phase reference which can be difficult if the frequency drift of the two independent laser sources is too fast. Alice can do this if she weaves reference pulses into her own stream of signal pulses. Each reference pulse can be used by Bob to measure the phase offset between his LLO and Alice's reference pulse. Because pulses sent by Alice are used as a reference for Bob to estimate the phase

drift, this method is also called self-referenced QKD. This technique was independently introduced by groups at Oak Ridge, Sandia, and Shanghai in 2015 [45, 46, 47].

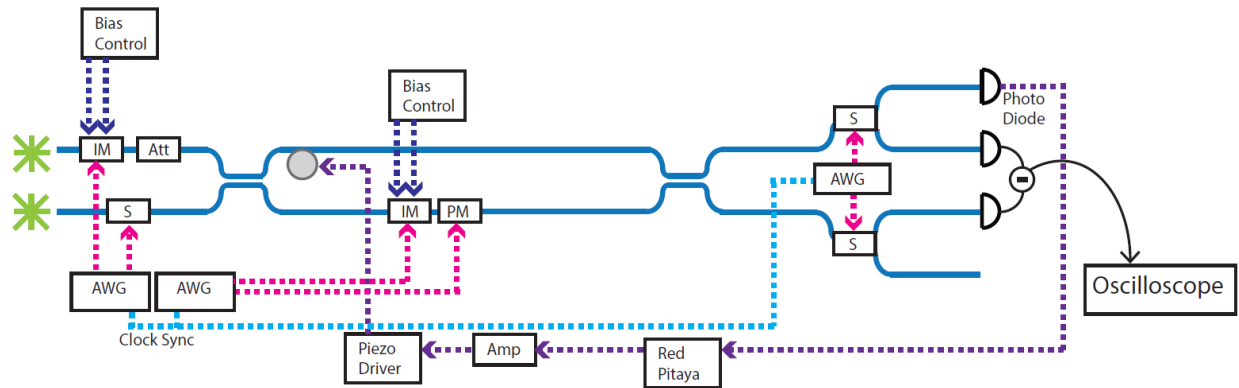
This technique does restrict Eve's ability to tamper with the LO, but it does come with its own limitations. The use of reference pulses in lieu of some signal pulses negatively impacts the key rate of the protocol. The phase drift between the two lasers must also be accurately estimated, requiring frequent measurement via reference pulses. The accuracy of this method is technically limited by the time-delay between reference pulses and signal pulses. This inaccuracy limits or prevents the generation of a secret keys if the phase noise is large.

In the self-coherent method, Alice and Bob split their laser pulses into two parts: one is used to estimate the phase reference, and the other is used as a signal. Both of these are measured coherently with Bob's LLO. Initially, Alice splits her source laser pulses into a reference pulse and a signal pulse on a delay line interferometer. Alice then modulates her signal pulse according to the QKD protocol before recombining the signal and reference pulses in a single fiber. The result of this is a temporal sequence of signal and reference pulses which are then sent to Bob. Bob possesses an identical delay-line interferometer that he uses to split the pulses of his LLO. Bob generates identical pairs of LLO pulses corresponding to the signal-reference pairs that Alice sends. Bob will use the first of each LLO pair to perform homodyne detection with the signal pulse. The second pulse of the LLO pair is measured with the reference pulse. The phase of a laser can be considered stable over the duration of a single pulse. Since Alice's reference and signal are generated from the same laser pulse and both are measured with a LLO generated from a single pulse of Bob's LLO, they inform Bob of the phase drift between his LLO and Alice's laser without a time-delay. This allows Bob to precisely measure the phase drift between Bob's LLO and Alice's laser source. The self-coherent method was first introduced by Alléaume and Marie in 2017 [48].

The primary drawback of the self-coherent method is that two distant delay-line interferometers must be precisely calibrated to the same delay, but otherwise it offers excellent phase estimation even in the presence of a fast phase drift.

In this work, a method of feedback control for phase stabilization using a field-programmable gate array (FPGA)-based microcontroller is explored. This system is designed to later be adapted into a self-referenced DGM-QKD system. A Red Pitaya microcontroller board was chosen for its specs and its ease of use. A Red Pitaya board is an FPGA with a 14-bit resolution analog-to-digital converter (ADC). It can sample at speeds up to 125 MS/s and can communicate via ethernet at speeds up to 1 Gbps. The Red Pitaya can be programmed using Matlab and Python and a software package already exists for its use in stabilizing optical cavities and interferometers [49, 50].

## 5.2 Using a Red Pitaya for Phase Compensation



**Fig. 10: Complete experimental setup for DGM-QKD with phase compensation. Att: optical attenuator, S: switch, AWG: arbitrary waveform generator, IM: intensity modulator, PM: phase modulator, Amp: voltage amplifier**

A complete optical setup for a DGM protocol using phase compensation is shown in Fig. 10.

This setup alternates in operation between two modes: signal and reference mode. In signal mode, the continuous-wave output of the top laser (Clarity NLL-1550-LP) is carved by an intensity modulator and attenuator into a series of pulses which are sent into an interferometer. The top arm of this interferometer serves as a LO while the bottom arm is modulated into a series of signal pulses using an intensity and phase modulator. Alice chooses the modulation for each coherent state signal according to the probability distribution  $r(x)$  of the DGM-protocol and the additional random phase  $\varphi_j$  that she selects. The LO and signal are then recombined on an interferometer and sent to Bob's homodyne detector where he performs coherent detection. In the reference mode, the continuous-wave output of the bottom laser (also Clarity NLL-1550-LP) is carved into a series of pulses and sent into the interferometer. However, no modulation from Alice is applied to the signal arm, resulting in equal powers in the signal arm and in the LO arm.

Both arms are recombined and sent to Bob for measurement. Bob splits the signal on a 50/50 beam splitter but opts instead to divert one half to a separate photodiode (New Port 1811-FC Fiber-Optic Receiver) using a switch. The other half may be used for a duplicate measurement or discarded. Using his measurement from the photodiode, Bob can determine the relative phase between the signal and LO pulses. This information can be used to correct for the phase drift between the two arms of the interferometer using a piezoelectric ring located in the LO arm. Several loops of fiber are wound around the piezoelectric ring so that expansion of the ring will apply a small phase shift in the path length of the LO arm. A feedback loop is implemented using a Red Pitaya board to monitor the output of the photodiode and adjust the piezoelectric ring, resulting in a constant phase relationship between the signal and LO of the reference pulses. The reason a separate photodiode is used is because our homodyne detector is a single module. It is not possible to access the output of the individual homodyne photodiode. A monitor output which taps off a small portion of the output from the individual homodyne photodiodes does exist, but this output is too noisy to use in stabilizing the interferometer.

By alternating between signal and reference modes, this configuration can correct for drift that occurs between the path lengths of the signal and LO arm of the interferometer. In principle, every time the system is operated in reference mode, optical path length difference between the signal and LO should return to the same default value. The only other major source of drift is the laser source itself. However, since both the signal and LO pulses are created from the same laser pulse, any drift in the laser should not impact Bob's measurement.

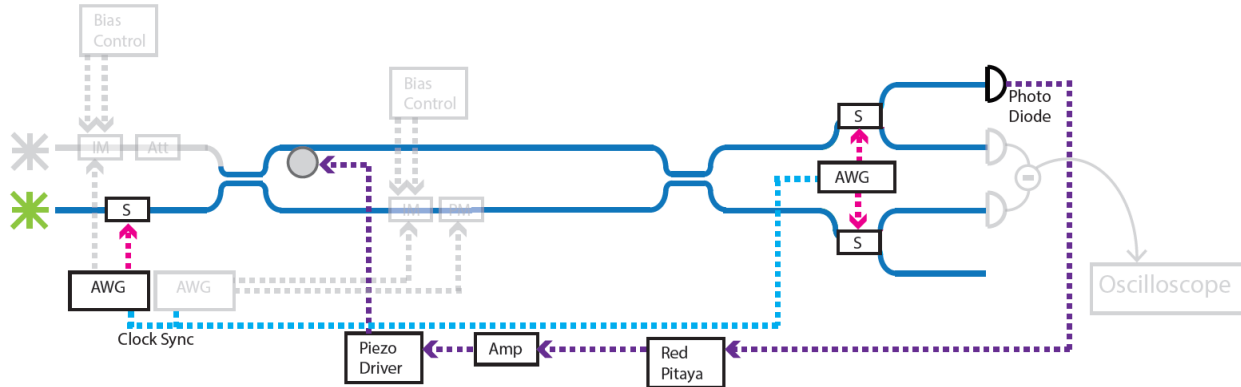
To prevent light from the reference from leaking into the signal, we employ a switch after the reference laser to attenuate the laser source when operating in signal mode. Likewise, when operating in reference mode the signal pulses are turned off by an intensity modulator. We

alternate between signal and reference modes at a rate of 2 MHz. This results in a series of reference pulses 500 ns wide with a rep rate 1 MHz. Between these reference pulses, signal pulses can be interwoven at 25 MHz for example.

Alternatively, the reference can be rotated in polarization by  $90^\circ$  and the switches before the homodyne detector can be replaced by a polarizing beam splitters which serve to filter out reference light. However, care must be taken to avoid measuring leakage from the reference on the homodyne detectors as the polarization of the reference laser may drift. As the reference is intended to be stronger than the combined LO and signal states at the homodyne detector, a very high extinction ratio is needed for each polarizing beam splitter.

The output of Bob's photodiode is read by a Red Pitaya microcontroller and processed using the PyRPL controller algorithm to generate a correction voltage. The Red Pitaya maximum output voltage of 1V is too low to directly tune the piezoelectric ring in this experiment. To compensate, the 1V output is first amplified up to a maximum of 5V before being sent into a high voltage amplifier inside the piezo driver.

PyRPL, or Python Red Pitaya Lockbox, is an open-source software package developed by Leonard Neuhaus and Samuel Deleglise. This experiment implements a feedback loop using a modified version of PyRPL. The standard PyRPL software package uses an input module to track a continuous input signal and provide feedback to a lockbox module directly from the measurements. However, our system uses a pulsed reference signal. To accommodate for this, the input module was modified to identify and measure pulse peaks. The modified input module then outputs these peak measurements to the lockbox and only updates this output when a threshold number of peak points have been sampled. In this way, we have adapted PyRPL to provide feedback based on a pulsed reference signal.

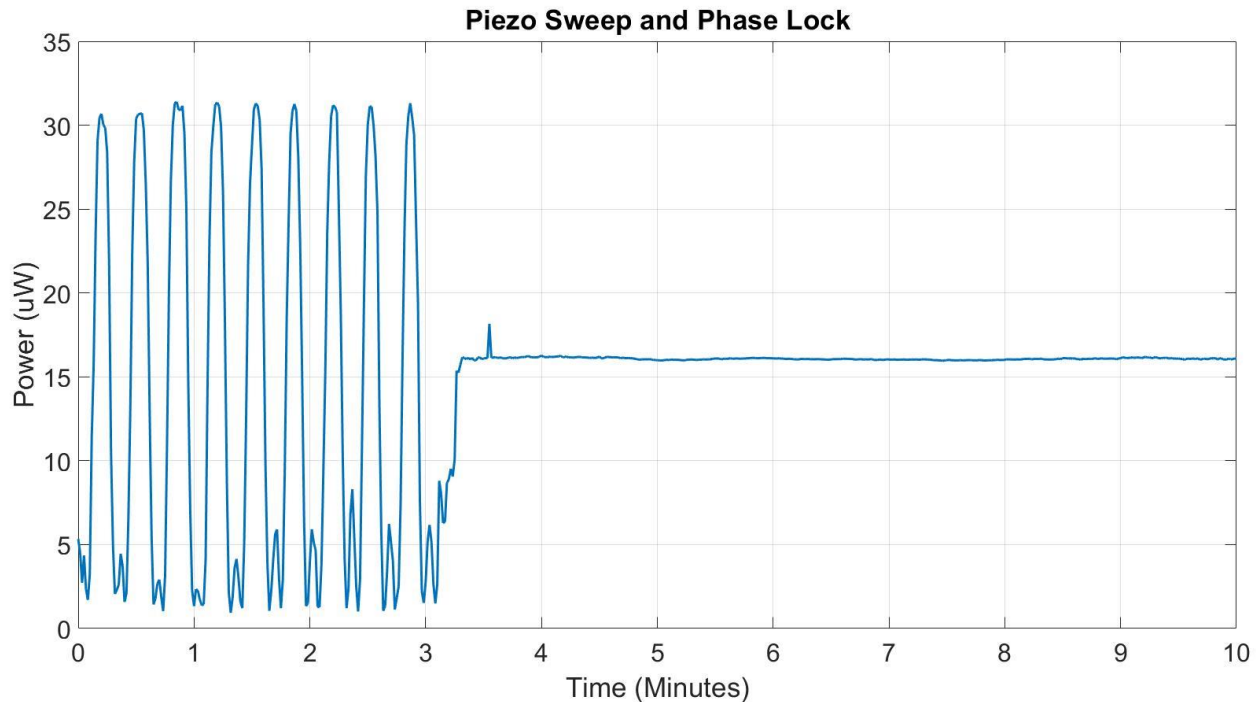


**Fig. 11: Simplified experimental setup for testing phase compensation performance.**

A simplified setup of the one from Fig 10. is presented in Fig. 11. In this setup, we only include components necessary for phase compensation system. We use this setup in lieu of the complete setup solely to test the performance of the phase stabilization system. In this system, 500 ns reference pulses are repeated at a speed of 1 MHz as in the previous example. The only difference is that no light travels through the system when operating in signal mode.

To test this system, the Red Pitaya is first used to perform a phase scan of the interferometer by outputting a ramp function. This phase scan is tuned to cover slightly more than a full phase period. This is necessary to ensure that at least one peak and one trough is obtained with each scan. Several full phase scans are performed over several minutes and used as a reference for the next step. The Red Pitaya is then instructed to lock at the midrange of the phase scan, halfway between the minimum and maximum values. Using the initial phase scans, the variance observed while the lock is active can be translated into a phase variance as a measure of the system performance.

For data collection, several periods of the phase are scanned followed by a 6-minute phase lock. The normalized results of this test are presented in Fig. 12. The maximum and minimum powers measured on the photodiode were 31.40  $\mu\text{W}$  and 933.8 nW, respectively. These extrema



**Fig. 12: Power measured for a set of piezo-induced phase scans followed by a phase lock performed by the Red Pitaya. Data collected after 4 minutes is used to characterize the performance of the phase lock.**

correspond to a visibility of 94.2%. While locked to the midrange of 16.17 uW, we measured a variance in power of  $0.0034 \text{ uW}^2$ . By assuming a linear relationship between the measured power and the phase near the lock point, the power variance can be converted to a phase variance of  $1.446 \times 10^{-4} \text{ rad}^2$  or  $0.4746 \text{ deg}^2$ .

The impact of the phase variance is small when operating at low mean photon numbers. However as  $N_S$  increases, perhaps to accommodate experimental limitations, we modify the variance of each coherent state in the constellation. This modification smears the distribution of each point in the constellation along a small arc of a circle of radius  $|\alpha_x|$ . This modified distribution well matches the unmodified distribution, but only if  $N_S$  is small. This accentuates the need to operate at a low mean photon number.

Our phase noise result of  $1.446 \times 10^{-4}$  is comparable with previous GMCS experiments which have demonstrated phase noises on the order of  $10^{-3}$ ,  $10^{-4}$ , and  $10^{-6}$  [52, 19, 53]. However, the duty cycle of 50% that we employ comes at a larger cost terms of the SKR. A system employing a duty cycle of 90% instead could achieve a SKR up to 80% higher.

Optimization of the duty cycle may be possible, but performance is limited by a combination of two factors. The Red Pitaya can sample at a rate of 125 MS/s, so out of every 1000 ns window only 125 points can be obtained. The current setup using 500 ns pulses allows 62.5 points on average to be obtained from each ideal reference pulse. However, in reality each pulse has a rise and fall time. Points lying inside the rise and fall times are not an accurate representation of the pulse peak and so must be filtered out. Even if the pulse duration is decreased, the rise and fall times will remain the same. The rise and fall times are determined by the smallest electrical bandwidth between our modulator, homodyne receiver, and arbitrary function generator. Amongst these components, our homodyne receiver is the limiting factor with an electrical bandwidth of 75 MHz. This bandwidth corresponds to a rise time of about 4.7 ns. Since the Red Pitaya samples with a period of 8 ns, this does not significantly impact our performance, but this rise time should be considered for future optimization when sampling at higher speeds. How many points are necessary to maintain the current performance is an open question and future work may explore this optimization.

## Chapter 6: Summary and Outlook

In theory, quantum key distribution offers the potential for unconditional security when properly implemented alongside a one-time pad encryption. However, physical implementations of QKD systems are far from the ideal, and security loopholes arising from the transmission of a local oscillator, from a non-ideal Gaussian modulation, or even from flaws not yet thought of are still being worked through. Exploring adaptation of the current GMCS protocol into a secure, discrete one as in this work will bring us one step closer towards the ultimate goal of unconditional security.

This work outlines methods for characterizing the performance of a QKD system implementing the DGM protocol presented in [39]. Two optical fiber-based experimental setups, one for a proof-of-principle experiment and another for a full implementation of the DGM protocol, were presented. The first setup was constructed and aimed at estimating the SKR of the DGM protocol based on a set of coherent state measurements obtained from a set of temperature phase sweeps performed at different signal powers. The reason for doing it this way is that the phase stabilization software was not fully ready. The second showed how the full DGM protocol could be demonstrated in a laboratory. This setup was partially constructed, including only elements necessary for the phase compensation system. A phase compensation based on the Red Pitaya microcontroller with the PyRPL software package was implemented. This setup was tested

to measure the performance of the phase compensation system and demonstrated performance similar to previous experiments implementing the GMCS protocol.

Further development of these experiments is expected to continue. Estimation of the key rate of the DGM protocol is currently limited by the capability to generate and measure coherent states of low mean photon number (approx. 1-10 photons). Developments include expanding the capabilities of the proof-of-principle experiment to generate and measure weaker coherent states. The limitations on increasing the thermal state mean photon number  $N_s$  while maintaining a positive key rate will be explored as a means of relaxing the low mean photon number requirements of the DGM protocol for the proof-of-principle demonstration.

Once an estimation of the key rate is obtained, we will work towards adapting the proof-of-principle experiment into the complete demonstration shown in Fig. 10. This requires getting the phase stabilization system to operate in conjunction with the signal and local oscillator pulses required for QKD. It also requires replacing the current attenuator and temperature sweeping scheme with an intensity and phase modulator alongside integrating these modulators with the existing electronics. Once the complete setup has been constructed, characterization of the contributions to the excess noise will need to be verified in addition to the remaining total excess noise. These characterizations include the CMRR, detector electronic noise, and the phase noise.

For the phase compensation system, a custom phase controller is under development for the Red Pitaya. With the custom controller, we have more control over the feedback system and can easily modify or adapt it as needed. We are currently working on characterizing and optimizing this loop to reduce its overhead on the SKR when implemented in a QKD system. If necessary, the current modulator may be replaced by one with a faster rise and fall time and a better extinction ratio. As a next step, this phase compensation system will be replaced with a self-referenced

version utilizing an LLO on Bob's end to close up any security loopholes resulting from the transmitted LO and to make the system suitable for use over deployed fiber.

This investigation has aimed to test one of the first DGM protocols implemented by design. The GMCS protocols that have so far been implemented have used a discrete modulation but have not taken into account the effects of their discretization [19, 32, 44, 45, 46, 52, 53]. This thesis provides an in-depth understanding of how discretization alters the performance of the standard GMCS protocol. While we do not yet have a key rate to characterize the performance of the system, we hope that our future results will demonstrate that the DGM protocol can achieve performance comparable to that of the GMCS protocol.

# References

- [1] R. L. Rivest, A. Shamir, L. Adleman. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems." *Communications of the ACM*, 21(2), pp. 120–126.(1978).
- [2] H. Bennett, G. Brassard and J.-M. Robert. "Privacy amplification by public discussion." *SIAM Journal on Computing* 17(2), pp. 210 – 229 (1988).
- [3] D. Kahn. "Codebreakers." New York. Macmillan (1967).
- [4] D. Luciano, G. Prichett. "Cryptology: From Caesar Ciphers to Public-Key Cryptosystems". *The College Mathematics Journal*. 18(1) (1987).
- [5] Cornell Department of Mathematics. <http://pi.math.cornell.edu/~mec/2003-2004/cryptography/subs/frequencies.html> (2021).
- [6] B. Schneier. "Applied Cryptography - Second Edition." John Wiley & Sons, New York NY (1996).
- [7] C. Shannon. "A Mathematical Theory of Communication," *The Bell System Technical Journal* 27, 379 (1948).
- [8] National Institute for Standards and Technology. "Data Encryption Standard." *Federal Information Processing Standards Publication* 46, 1 (1977).
- [9] W. Diffie, M. Hellmann. "New Directions in Cryptography." *IEEE Transactions on Information Theory* 6, 664 (1976).
- [10] Electronic Foundation. "Cracking DES - Secrets of Encryption Research." *Wiretap Politics & Chip Design*. O'Reilly Media, Sebastopol, CA, (1998).

- [11] C. Bennett, , and G. Brassard. "Quantum cryptography: Public key distribution and coin tossing." Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, pp. 175-179. (1984).
- [12] S. Wiesner. "Conjugate coding." Sigact News 15(1). pp. 78 – 88 (1983).
- [13] G. Brassard. "Brief history of quantum cryptography: A personal perspective." In IEEE Information Theory Workshop on Theory and Practice in Information-Theoretic Security, pp. 19-23 (October 2005).
- [14] G. Brassard and L. Salvail "Notes in Computer Science 765, pp. 410-423 (1994).
- [15] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson. "Fast, efficient error reconciliation for quantum cryptography." Phys. Rev. A 67, 052303 (2003).
- [16] M. Bloch, A. Thangaraj, S. W. McLaughlin and J. Merolla, "LDPC-based Gaussian key reconciliation." 2006 IEEE Information Theory Workshop - ITW '06 Punta del Este, pp. 116-120 (2006).
- [17] F. Grosshans, and P. Grangier. "Reverse reconciliation protocols for quantum cryptography with continuous variables." arXiv quant-ph/0204127 (2002).
- [18] C. H. Bennett, G. Brassard, C. Crepeau and U. M. Maurer. "Generalized privacy amplification." IEEE Transactions on Information Theory 41(6), pp. 1915-1923 (1995).
- [19] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N.J Cerf, R. Tualle-Brouri, S.W. McLaughlin, P. Grangier "Quantum key distribution over 25 km with an all-fiber continuous-variable system." Physical Review A 76, 4 (2007).

- [20] R. Renner. "Security of quantum key distribution." *International Journal of Quantum Information*, 6(01), 1-127 (2008).
- [21] A. Holevo. "The capacity of the quantum channel with general signal states." *IEEE Transactions on Information Theory* 44.1 269-273 (1998).
- [22] A. Rubenok. "Quantum Key Distribution with Temporal Mode Encoding." MS thesis, University of Calgary (2011).
- [23] M. Caloz, M. Perrenoud, C. Autebert, B. Korzh, M. Weiss, C. Schnenberger, R. J. Warburton, H. Zbinden, and F. Bussières. "High-detection efficiency and low-timing jitter with amorphous superconducting nanowire single-photon detectors." *Applied Physics Letters*, vol. 112, no. 6, p. 061103 (2018).
- [24] B. Korzh, T. Lunghi, K. Kuzmenko, G. Boso, and H. Zbinden. "Afterpulsing studies of low-noise InGaAs/InP single-photon negative-feedback avalanche diodes." *Journal of Modern Optics*. vol. 62, no. 14, pp. 1151–1157 (2015).
- [25] L. Comandar, B. Fröhlich, M Lucamarini, K. Patel, A. Sharpe, J. Dynes, Z. Yuan, R. Penty, A. Shields. "Room temperature single photon detectors for high bit rate quantum key distribution." *Appl. Phys. Lett.* 104, 021101 (2014).
- [26] B Fröhlich, M. Lucamarini, J. Dynes, L. Comandar, W. Tam, A. Plews, A. Sharpe, Z. Yuan, A. Shields. "Long-distance quantum key distribution secure against coherent attacks." *Optica* 4, 163-167 (2017).
- [27] 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, J.-W. Pan. "Measurement-device-independent quantum key distribution over a 404 km optical fiber." *Physical review letters* 117.19 (2016).

- [28] N. Lütkenhaus and M. Jahma. "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack." *New Journal of Physics* vol. 4, no. 1 p. 44 (2002).
- [29] F. Laudenbach, C. Pacher, C.-H.F. Fung, A. Poppe, M. Peev, B. Schrenk, M. Hentschel, P. Walther, and H. Hübel. "Continuous-Variable Quantum Key Distribution with Gaussian Modulation—The Theory of Practical Implementations." *Adv. Quantum Technol.*, 1: 1800011 (2018).
- [30] G. Van Assche, J. Cardinal, and N. J. Cerf. "Reconciliation of a quantum-distributed gaussian key." *IEEE Transactions on Information Theory*, vol. 50, no. 2, pp. 394–400 (2004).
- [31] P. Jouguet and S. Kunz-Jacques. "High performance error correction for quantum key distribution using polar codes." *Quantum Information & Computation*. vol. 14, no. 3-4 (2012).
- [32] P. Jouguet, S. Kunz-Jacques, and A. Leverrier. "Long-distance continuous-variable quantum key distribution with a Gaussian modulation." *Phys. Rev. A*, 84, 062317 (2011).
- [33] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier. "Analysis of imperfections in practical continuous-variable quantum key distribution." *Physical Review A* 86, no. 3: 032309 (2012).
- [34] T. Ralph. "Continuous variable quantum cryptography." *Physical Review A* 61, 010303 (1999).
- [35] M. Reid. "Quantum cryptography with a predetermined key, using continuous-variable Einstein-Podolsky-Rosen correlations." *Physical Review A* 62, 062308 (2000).

- [36] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki. “Quantum cryptography using pulsed homodyne detection.” *Physical Review A* 68, 042331 (2003).
- [37] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus. “Asymptotic security of binary modulated continuous-variable quantum key distribution under collective attacks.” *Physical Review A* 79, 012307 (2009).
- [38] K. Brádler and C. Weedbrook. “Security proof of continuous-variable quantum key distribution using three coherent states.” *Physical Review A* 97, 022310 (2018).
- [39] E. Kaur, S. Guha, & M. Wilde. “Asymptotic security of discrete-modulation protocols for continuous-variable quantum key distribution.” *Physical Review A*, 103(1), 012412 (2021).
- [40] S. Ghorai, P. Grangier, E. Diamanti, and A. Leverrier. “Asymptotic security of continuous variable quantum key distribution with a discrete modulation.” *Physical Review X* 9, 021059 (2019).
- [41] J. Lin, T. Upadhyaya, and N. Lütkenhaus. “Asymptotic security analysis of discrete-modulated continuous-variable quantum key distribution.” *Physical Review X* 9, 041064 (2019).
- [42] E. Ip and J. Kahn. “Feedforward Carrier Recovery for Coherent Optical Communications.” *Journal of Lightwave Technology*. 25, 2675 (2007).
- [43] H.-C. Park, M. Lu, E. Bloch, T. Reed, Z. Griffith, L. Johansson, L. Coldren, and M. Rodwell. “40Gbit/s coherent optical receiver using a Costas loop.” *Opt. Exp.* 20, B197 (2012).

- [44] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier. “Quantum key distribution using Gaussian-modulated coherent states.” *Nature*, 421, 238 (2003).
- [45] D. Huang, P. Huang, D. Lin, C. Wang, and G. Zeng. “High-speed continuous-variable quantum key distribution without sending a local oscillator.” *Opt. Lett.* 40, 3695 (2015).
- [46] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek. “Generating the local oscillator ‘locally’ in continuous-variable quantum key distribution based on coherent detection.” *Phys. Rev. X*, 5, 041009 (2015).
- [47] D. B. Soh, C. Brif, P. J. Coles, N. Lutkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar. “Self-referenced continuous-variable quantum key distribution protocol.” *Phys. Rev. X*, 5, 041010 (2015).
- [48] A. Marie and R. Alleaume. “Self-coherent phase reference sharing for continuous-variable quantum key distribution.” *Phys. Rev. A*, 95, 012316 (2017).
- [49] StemLabs. <<https://www.redpitaya.com/>> (2021).
- [50] Leonhard Neuhaus, Samuel Deléglise. <<https://pyrpl.readthedocs.io/en/latest/index.html>> (2021).
- [51] A. Leverrier, R. Alleaume, J. Boutros, G. Zemor, and P. Grangier. “Multidimensional reconciliation for a continuous-variable quantum key distribution.” *Phys. Rev. A*, 77, 042325 (2008).
- [52] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo. “Experimental study on the Gaussian-modulated coherent state quantum key distribution over standard telecommunication fibers.” *Phys. Rev. A*, 76, 052323 (2007).

- [53] D. Huang, P. Huang, D. Lin, and G. Zeng. “Long-distance continuous-variable quantum key distribution by controlling excess noise.” *Sci. Rep.* 6, 19201 (2016).