Continuous-variable Quantum Key Distribution with Gaussian-modulated Coherent States

Nam Nguyen

***Abstract*—Quantum computing and quantum information have become an emerging research topic in recent years. As the advancement of the field surges, there are new threats to the current security system. For example, Shor's and Grover's algorithms caused a devastating impact on symmetric cryptography and public-key cryptography. Hence, it is mandatory to develop and evaluate more quantum-resilient cryptography and communication to cope with quantum computers' attacks. The core of quantum-resilient communication is Quantum Key Distribution, which enables users to share random keys in the unsecured channel and preserve absolute security in principle. We can classify QKD into two sub-categories, which are fundamentally based on discrete-variable (DV-QKD) and continuous-variable (CV-QKD). Some DV-QKD paradigms can be referred to as BB84 and its variations, where the encoded information is from the polarization of single-photon states, and a single-photon detector measures the received quantum state. In contrast, CV-QKD encodes the information via amplitude and phase quadratures of the quantum state. This study will emphasize the advancements of continuous-variable quantum cryptography and communication due to its capability to be embedded in classical telecom components. Finally, we will propose several potential research directions together with implementations of discussed algorithms via IBMQ and Qskits library.**

***Index Terms*—Continuous-variable Quantum Cryptography**

I. Introduction

Continuous-variable quantum key distribution (CV-QKD) is a promising alternative for discrete-variable quantum key (DV-QKD) distribution due to its large-scale applicable potential. Being introduced fifteen years later after the first DV-QKD protocol, early CV-QKD protocols utilized squeezed states of Gaussian encoding[1], then further proliferated with usage of Gaussian-modulated coherent states[2], [3], [4], [5]. In discrete-variable protocol, single-photon counters are used as communication toolbox. On the other hand, CV-QKD used homodyne receivers, which lead to more efficient detection, in terms of higher rate and cost-effectiveness. Moreover, the improvement from early CV-QKD using squeezed states is mainly due to the usage of coherent states, which relieves the general challenge of squeezed light. While many works in the literature studying the effectiveness of CV-QKD with Gaussian-modulated coherent states GMCS, it is challenging to compare those work since the experimental results are highly sensitive to the experimental setting. As in many other field, it is worth establishing a benchmark or standard to compare different frameworks. The main appreciation of a CV-QKD study is attributed to the secure-key rate, with consideration of transmission distance. However, there are several assumptions which must be addressed from the outset. For example, we may consider the power of eavesdropper, the reconciliation efficiency, the effect of finite-key, trusted-noise classification, and so on. A promising research direction for studying CV-QKD is to investigate its resilience under various types of attack. While the security proof of DV-QKD agaist eavesdropper has been well-established in the literature, CV-QKD has less advancement of such proof. A comprehensive study related to the security of CV-QKD is given in [6], [7]. We organize our work as follow: Section II introduces quantum information via continuous-variable, including in-depth underlying quantum mechanics of continuous-variable system(II-A), squeezed states(II-B) and Gaussian-modulated coherent states(II-C); Section III illustrates the overview of CV-QKD protocols. Finally, we would like to discuss about the security of CV-QKD in Section III-B.

II. Continuous-variable Quantum Information

In the first Section II-A, we will first establish several fundamental quantum mechanics of a continuous-variable system, building a solid foundation for further discussions. Then Section II-C focuses on the core component of CV-QKD, which is Gaussian-modulated coherent state.

A. Quantum Mechanics of Continuous-variable System

To begin with, we will have a brief summary of quantum harmonic oscillator, which plays an important role to the continuous-variable quantum information. The Hamiltonian (total energy) of a particle includes kinetic energy and potential energy. In the most simple case, where we consider a particle in one-dimension with parabolic potential is given as

$$H = \frac{p^2}{2m} + \frac{1}{2}m\omega^2 x^2 \tag{1}$$

In quantum mechanics, each observable (position, momentum or velocity,... of a particle) will associate with an operator. An operator $\hat{A}$ is simply instruction to build one function to another function. For example, $\hat{1}$ is the identity operator, which acts on $f(x)$ as $\hat{1}f(x) = f(x)$, or $\hat{D}$ is the operator "instruct" us to take the partial derivative of $f(x)$ with respect to x, i.e $\hat{D}f(x) = \partial f(x)/\partial x$. There are two important operators (known as position and momentum) to the Hamiltonian, which are

$$\hat{x}f(x) = xf(x)$$

and

$$\hat{p}f(x) = -i\hbar\frac{\partial}{\partial x}f(x).$$

It is worth to mention that the Hamiltonian in Equation 1 is a number. By replacing p and x to operator, yielding

$$\hat{H} = \frac{\hat{p}}{2m} + V(\hat{x}) = \frac{-\hbar}{2m}\frac{\partial^2}{\partial x^2} + \frac{1}{2}m\omega^2 x^2 \tag{2}$$

Now, the Hamiltonian in Equation 2 becomes an operator. It is common misleading that: if we want to obtain the momentum or position of a given particle, which has the wavefunction of Ψ, we apply the corresponding on Ψ, yielding $\hat{p}\Psi$ or $\hat{x}\Psi$. **It is not correct in overall!**. In order to clarify this statement, we first need to introduce a special class of functions of an operator $\hat{A}$, which satisfies

$$\hat{A}\psi_a = a\psi_a, a \in \mathbb{C} \tag{3}$$

These functions are eigenfunctions or eigenstates of operator $\hat{A}$ (we see the similarity of eigenvalues and eigenvectors of a matrix in linear algebra). The beauty of eigenfunctions is that when we measure an observable of a particle, the associate wavefunction will collapse at one of these eigenfunctions. For example, if we measure the position of a particle at x_0, $\Psi(x)$ will be collapsed at $\delta(x - x_0) = \infty$ when $x = x_0, 0$ when $x \neq x_0$. Clearly $\delta(x - x_0)$ is the eigenfunction of $\hat{x}$, since $\hat{x}\delta(x - x_0) = x\delta(x - x_0) = x_0\delta(x - x_0)$. We can also check that e^{ikx} is the eigenfunction of $\hat{p}$.

After understanding the two operators, we now depict the most beautiful and important equality in quantum mechanics. First, the two operators are not commute. We have

$$\hat{x}\hat{p}f(x) = \hat{x}(-i\hbar\frac{\partial f(x)}{\partial x}) = -i\hbar x\frac{\partial f(x)}{\partial x}$$

and

$$\hat{p}\hat{x}f(x) = \hat{p}xf(x) = -i\hbar\frac{\partial xf(x)}{\partial x} = -i\hbar\big[f(x) + x\frac{\partial f(x)}{\partial x}\big]$$

If we define the commutator of two operators $\hat{A}$ and $\hat{B}$ as $[\hat{A}, \hat{B}] := \hat{A}\hat{B} - \hat{B}\hat{A}$, then

$$[\hat{x}, \hat{p}] = i\hbar \tag{4}$$

Again, Equation 4 is the most beautiful and important in quantum mechanics!

B. Quantum computing using Single Quantum Harmonic Oscillator

Now we will relate the introduced quantum mechanics to quantum computing and quantum information. To perform computation on harmonic oscillator quantum computer, we represent n qubits by the energy levels of a single quantum oscillator. These energy levels are the eigenstates of the introduced Hamiltonian (as mentioned before, each observable will be collapsed at one of the eigenstates after the measurement). We define $|n\rangle$ be the eigenstates of $\hat{H}$, where $n = 0, 1, 2, ...$ (these eigenstates is referred to Fock states in quantum mechanics). To decreasing or increasing the energy level, we implement the creation and annihilation operators $a^\dagger$ and a, which are given as

$$\begin{aligned}\hat{a} &= \frac{1}{\sqrt{2m\hbar\omega}}(m\omega\hat{x} + i\hat{p}) \\ \hat{a}^\dagger &= \frac{1}{\sqrt{2m\hbar\omega}}(m\omega\hat{x} - i\hat{p})\end{aligned} \tag{5}$$

Thus, the Hamiltonian operator becomes

$$\hat{H} = \hbar\omega(\hat{a}^\dagger\hat{a} + 1/2) \tag{6}$$

Important properties of these operators are

$$\begin{aligned}a^\dagger a\,|n\rangle &= n\,|n\rangle \\ a^\dagger\,|n\rangle &= \sqrt{n+1}\,|n+1\rangle \\ a\,|n\rangle &= \sqrt{n}\,|n-1\rangle\end{aligned} \tag{7}$$

Besides, it is impossible to measure a negative value of energy, so we define the lowest energy of $\hat{H}$ is $|0\rangle$, such that $\hat{a}^n\,|0\rangle = 0$. Intuitively, due to the fact that $|0\rangle$ is the lowest energy value, applying multiple times of lowering operator $\hat{a}$ always yield 0. The state $|0\rangle$ is called the vacuum state of the Hamiltonian, since any higher energy states $|n\rangle$ can be written as

$$|n\rangle = \frac{(\hat{a}^\dagger)^n}{\sqrt{n!}}\,|0\rangle \tag{8}$$

We illustrate a quantum operation over 2-qubit system; for example C-NOT gate

$$\begin{aligned}|00\rangle &\to |00\rangle \\ |01\rangle &\to |01\rangle \\ |10\rangle &\to |11\rangle \\ |11\rangle &\to |10\rangle\end{aligned} \tag{9}$$

We distinguish the quantum qubits to the introduced eigenstates $|n\rangle$ by a subscription, say $|n\rangle_H$. Hence, we can implement the C-NOT gate by the mapping

$$\begin{aligned}|00\rangle &= |0\rangle_H \\ |01\rangle &= |2\rangle_H \\ |10\rangle &= (|4\rangle_H + |1\rangle_H)/\sqrt{2} \\ |11\rangle &= (|4\rangle_H - |1\rangle_H)/\sqrt{2}\end{aligned}$$

Starting at $t = 0$, we evolve the system to time $t = \pi/\hbar\omega$, so the current eigenstates $|n\rangle_H \to \exp(-i\pi\hat{a}^\dagger\hat{a})\,|n\rangle_H = (-1)^n\,|n\rangle_H$ (since $\hat{a}^\dagger\hat{a} = n$ and $\exp(i\pi) = -1$). As a result, $|0\rangle_H, |2\rangle_H$ and $|4\rangle_H$ remains unchanged while $|1\rangle_H \to -|1\rangle_H$.

Comments: Quantum computing using harmonic oscillator is not an idea approach, due to the fact that we cannot fully observe the eigenvalues spectrum of the unitary for some certain quantum operation. However, it lays a solid foundation for further improvements. As along as we can model each mode of the electromagnetic field as a quantum harmonic oscillator and its creation and annihilation operator, we can define the canonical conjugate variables (or quadratures) $\hat{x}$ and $\hat{p}$ and perform quantum computation on energy level of the Hamiltonian.

C. The Gaussian-modulated Coherent State

In this section, we will discuss about the Gaussian-modulated coherent state (GMCS). To begin with, we will summarize several main points from the previous section. Firstly, from Equation 5, we can derive the position and momentum operators as

$$\begin{aligned}\hat{x} &= \sqrt{\frac{\hbar}{2\omega}}\left(\hat{a}+\hat{a}^\dagger\right)\\ \hat{p} &= -i\sqrt{\frac{\hbar\omega}{2}}\left(\hat{a}-\hat{a}^\dagger\right)\end{aligned} \tag{10}$$

One important inequality rooted by the Heisenberg uncertainty relation is

$$\langle(\Delta\hat{x})^2\rangle\langle(\Delta\hat{p})^2\rangle \geq \frac{1}{4}|\langle[\hat{x},\hat{p}]\rangle|^2 = \frac{1}{16}, \tag{11}$$

where $\langle(\Delta\hat{A})^2\rangle \equiv \langle(\hat{A}-\langle\hat{A}\rangle)^2\rangle$ - the variance of arbitrary observable $\hat{A}$. We define the quantum state satisfies the minimum uncertainty relation as *coherent state*. In the quantum optics's jargon, the conjugate variables $\hat{x}$ and $\hat{p}$ is known as *amplitude* Q and *phase* P quadrature operators associated with a quantum variable. From now, we can simplify the representation of a quantum variable by

$$\begin{aligned}X &= \frac{1}{\sqrt{2}}(\hat{a}+\hat{a}^\dagger)\\ P &= \frac{-i}{\sqrt{2}}(\hat{a}-\hat{a}^\dagger)\end{aligned} \tag{12}$$

It is worth to note that X and P are operators, hence we can start to form a computational basis by eigenstates of X, which are $\{|x\rangle\}_{x\in\mathbb{R}}$. In contrast to Qubit-based quantum computing, which is formed by digital computational basis $\{|0\rangle, |1\rangle\}$, the computational basis of x is analog. We also refer this approach to Qumode-based quantum computing.

We now have adequate building blocks for defining the Gaussian-modulation coherent state. Mathematically, the a coherent state $|\alpha\rangle$ is the (unique) eigenstate of the annihilation operator $\hat{a}$, i.e

$$\hat{a}\,|\alpha\rangle = \alpha\,|\alpha\rangle\,. \tag{13}$$

Noted that $\hat{a}$ is not Hermitian, i.e $\hat{a} \neq \hat{a}^\dagger$ (See Equation 5), then α is a complex number in general. Thus, we can writing any coherent state as $|\alpha\rangle = |\alpha|\exp(i\phi)$. Let $x = \langle\alpha|\,x\,|\alpha\rangle = |\alpha|\cos\phi$ and $p = \langle\alpha|\,p\,|\alpha\rangle = |\alpha|\sin\phi$, we can restate a coherent state as

$$|\alpha\rangle = |x+ip\rangle\,, \tag{14}$$

where x and p are quadratures of the field (position and momentum, amplitude and phase). We form a Gaussian-modulated coherent state by treating x and p as realizations of two independent and identically distributed (i.i.d) random variables $\mathcal{X}$ and $\mathcal{P}$, where X and P follow Gaussian distribution $\mathcal{N}(0,\sigma^2)$. In a plain language, we prepare a GMCS by drawing two different samples x and p from the same Gaussian distribution $\mathcal{N}(0,\sigma^2)$, obtaining $|\alpha\rangle = |x+ip\rangle$. The variance of Gaussian distribution σ^2 is called *modulation variance* of the quadrature components x and p, while $4\sigma^2$ is the modulation variance of the quadrature operators $\hat{x}$ and $\hat{p}$. It is noted that even when $\sigma^2 = 0$, the quadrature operators always carry the *shot noise* $\sigma_0^2 = 1$ due to the uncertainty relation.

III. Quantum Key Distribution via Gaussian-modulated Coherent States

A. General Framework

The protocol of CV-QKD includes two phases, which are

1) Quantum pre-processing information
   a) Quantum state preparation.
   b) Transmission (via insecure quantum channel).
   c) Measurement of non-orthogonal states to distribute raw key.
2) Classical post-processing information
   a) Reconciling the measurement bases if required.
   b) Error correction
   c) Privacy amplification.

The idea of CV-QKD using GMCH is very similar to BB84 protocol, which leverages the computational bases $\{|0\rangle, |1\rangle\}$ and $\{|+\rangle, |-\rangle\}$.

1) Pre-processing information: Suppose Alice wants to send Bod a message of sequences $\alpha_1, ..., \alpha_N$, she prepares a sequence of GMCH

$$|\alpha_k\rangle = |x_k^A + ip_k^A\rangle\,,$$

where x_k and p_k are realizations of two i.i.d random variables $\mathcal{X}$ and $\mathcal{P}$ following Gaussian $\mathcal{N}(0,\sigma^2)$. Then Alice transmits the prepared states $\{|\alpha_k\rangle\}$ to Bob using Gaussian quantum channel (may be insecure). Bob then measures the eigenvalue of either on or both of quadrature operators using homodyne or heterodyne detection. The measurement results of Bob are

$$|\beta_k\rangle = |x_k^B + ip_k^B\rangle\,,$$

where x_k^B and p_k^B is corresponding to x_k^A and p_k^A.

2) Classical post-processing information: Once Alice transmitted a sequence of states and Bod have measured all of these states, they will pick a random subset of data to compare the state was sent and their corresponding measurements. By this parameter estimation process, they can estimate the total transmission and excess noise of the channel by their mutual information I_{AB}. Moreover, they also notice the appearance of an eavesdropper Eve throughout the communication. Let I_E be the information of Eve, the protocol is insecure when $I_E \geq \gamma I_{AB}$ (we will discuss the detail in the next section), and hence Alice and Bod will abort the communication. Otherwise, if $I_E < \gamma I_{AB}$, Alice and Bod will continue the communication by information reconciliation (or error correction). We can categorize the information reconciliation into two approaches: (1) direct reconciliation and (2) reverse reconciliation. In the former approach, Bob corrects his measured bits according to Alice's revealed data. [4] shows that a total transmittance of $T < 0.5 \approx -3bD$, Eve may possess more information than Bob on the same Alice's prepared information. Thus, the communication is harmed by the fact that no secret key can be distributed. On the other hand, the reserve reconciliation (Alice corrects her bits by Bob's data), can overcome the loss limit

and ensure that Alice's information and Bob's measurement result is always greater than Eve's information. In case of CV-QKD, there are two alternatives for information reconciliation, which are slice reconciliation and multidimensional reconciliation. Both frameworks leverage the low-density parity-check (LDPC) codes for the error correction. This is a promising research direction for information reconciliation of CV-QKD. After information reconciliation, Alice and Bobs confirm the communication protocol. Alice and Bob choose one particular hash function from a pre-defined family and then encode their key by the hash function. They exchange and compare their hash values over classical public channel. The difference in hash values implies the difference in their keys, so that they will cancel the protocol. Otherwise, they continue the communication if the hash values are equal. The successful confirmation ensures a very high probability that Alice and Bob shared the same bit of string. At this point, Eve has been possessed a certain amount of information on the key. Thus, Eve can correctly guess a part of key to a certain level. To reduce Eve's guessing chance, Alice and Bod will perform a privacy amplification, which simply applies a seeded randomness algorithm on their strings of bits. The last step of the protocol may involve authentication using strongly hash function, which prevent the attacks by non-ITS authentication.

B. Security of CV-QKD with GMCS

Secure-key rate: In the communication between Alice and Bob, we assume the eavesdropped; Eve, fully accesses tho the quantum channel (insecure and public). Eve can control and manipulate information over the public channel, but she cannot intervene in the communication between Alice and Bob, which is established in an authenticated channel (classical). The attack of Eve can be performed by an arbitrary ancillary states, which she uses to interact with the transmitted signal states and its measurement. An important case of attack involving a quantum memory, which enables Eve to store her states for later measurement, when she has already observed and learnt from the classical post-processing. Theoretically, the security of a QKD protocol depends on the power of potential eavesdropper, which can be categorized into three types:

1) Individual Attack: Eve prepares separable ancilla states for attack individually each of signal pulse in the quantum channel. She then stores the states in a quantum memory until the end of sifting procedure and before the post-processing step. Each state will be measured independently.
2) Collective Attack: Similar to individual attack but except the measurement step. Now, Eve will perform a optimal collective measurement on all quantum states.
3) Coherent Attack: In this type of attack, we ignore the assumption of i.i.d ancilla state. In specific, Eve prepares an optimal global ancilla state whit modes interact with the signal pulses in the channel. Then the storing and measuring is performed as in collective attack.

Security proofs: Asymptotic limit is used to offer the security proof of CV-QKD. We use an infinite or finite number of symbols in the transmission. In general, the asymptotic limit is not directly applicable in any realistic system. In stead, the asymptotic limit offers an upper bound for corresponding non-asymptotic attack with easier derivation. Early works had successfully proved the security for individual and collective attack[4], [8]. Along with the growth of the literature, recent study attempts to provide the security proof for the strongest attack - coherence attack. The underlying idea for such proof can be delivered though two main approach:

1) "Simplify" coherent attack to collective attacks using Finetti representation theorem for infinite dimension [9].
2) Usage of the optimality of Gaussian attack, in which has proved that the state minimizes the key rate is Gaussian with a given covariance matrix[9].

Although security of CV-QKD with GMCS has been proved by computational approach under asymptotic limit[10], [11], [12], on going research for the security of CV-QKD considers finite block sizes [13], [14], [15], [16], [17], which is crucial for further improvement.

IV. Research Direction and Discussion

As we go through study in the related field, although the literature proliferates throughout decades, it lacks of a comprehensive survey on the security of continuous-variable quantum key distribution. In the literature, there are two comprehensive tutorial on the field, which are [7], [6]. However, these works rather gave an overview of CV-QKD using GMCH rather than focus on its security aspect. Second, it is worth further studying other approach for CV-QKD. For example, recent study considers rateless reconciliation protocol for CV-QKD[18], or [19] utilized two-mode squeezed states

References

[1] N. J. Cerf, M. Levy, and G. Van Assche, "Quantum distribution of gaussian keys using squeezed states," *Physical Review A*, vol. 63, no. 5, p. 052311, 2001.

[2] F. Grosshans and P. Grangier, "Continuous variable quantum cryptography using coherent states," *Physical review letters*, vol. 88, no. 5, p. 057902, 2002.

[3] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, "Quantum key distribution using gaussian-modulated coherent states," *Nature*, vol. 421, no. 6920, pp. 238–241, 2003.

[4] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, "Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables," *arXiv preprint quant-ph/0306141*, 2003.

[5] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, "Quantum cryptography without switching," *Physical review letters*, vol. 93, no. 17, p. 170504, 2004.

[6] E. Diamanti and A. Leverrier, "Distributing secret keys with quantum continuous variables: principle, security and implementations," *Entropy*, vol. 17, no. 9, pp. 6072–6092, 2015.

[7] 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," *Advanced Quantum Technologies*, vol. 1, no. 1, p. 1800011, 2018.

[8] F. Grosshans and N. J. Cerf, "Continuous-variable quantum cryptography is secure against non-gaussian attacks," *Physical review letters*, vol. 92, no. 4, p. 047905, 2004.

[9] R. Renner and J. I. Cirac, "de finetti representation theorem for infinite-dimensional quantum systems and applications to quantum cryptography," *Physical review letters*, vol. 102, no. 11, p. 110504, 2009.

[10] M. M. Wolf, G. Giedke, and J. I. Cirac, "Extremality of gaussian quantum states," *Physical review letters*, vol. 96, no. 8, p. 080502, 2006.

[11] R. Garcia-Patron and N. J. Cerf, "Unconditional optimality of gaussian attacks against continuous-variable quantum key distribution," *Physical review letters*, vol. 97, no. 19, p. 190503, 2006.
[12] M. Navascués, F. Grosshans, and A. Acin, "Optimality of gaussian attacks in continuous-variable quantum cryptography," *Physical review letters*, vol. 97, no. 19, p. 190502, 2006.
[13] A. Leverrier, F. Grosshans, and P. Grangier, "Finite-size analysis of a continuous-variable quantum key distribution," *Physical Review A*, vol. 81, no. 6, p. 062343, 2010.
[14] A. Leverrier, R. García-Patrón, R. Renner, and N. J. Cerf, "Security of continuous-variable quantum key distribution against general attacks," *Physical review letters*, vol. 110, no. 3, p. 030502, 2013.
[15] A. Leverrier, "Composable security proof for continuous-variable quantum key distribution with coherent states," *Physical review letters*, vol. 114, no. 7, p. 070501, 2015.
[16] L. Ruppert, V. C. Usenko, and R. Filip, "Long-distance continuous-variable quantum key distribution with efficient channel estimation," *Physical Review A*, vol. 90, no. 6, p. 062310, 2014.
[17] O. Thearle, S. M. Assad, and T. Symul, "Estimation of output-channel noise for continuous-variable quantum key distribution," *Physical Review A*, vol. 93, no. 4, p. 042343, 2016.
[18] C. Zhou, X. Wang, Y. Zhang, Z. Zhang, S. Yu, and H. Guo, "Continuous-variable quantum key distribution with rateless reconciliation protocol," *Physical Review Applied*, vol. 12, no. 5, p. 054013, 2019.
[19] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, "Continuous variable quantum key distribution with two-mode squeezed states," *arXiv preprint arXiv:1110.5522*, 2011.