An Introduction to Continuous-Variable Quantum Key Distribution (CV-QKD)

Panagiotis Papanastasiou

University of York

Presentation at
Department of Electrical Engineering
University of Patras

16/10/2024

Table of Contents

Introduction to QKD

Motivation for CV-QKD

Coherent States of light

CV-QKD Protocols and Gaussian Channels

Individual Attacks and Secret Key Rate

Coherent Attacks and Holevo Information

Reconciliation Efficiency and LDPC Codes

Conclusion

References

Thank You

Introduction to Quantum Key Distribution (QKD)

- QKD enables two parties (**Alice** and **Bob**) to generate a shared secret key for secure communication.
- Security is based on **quantum mechanics**, ensuring **information-theoretic security**.
- Introduced by Bennett and Brassard in 1984 (**BB84 protocol**).
- Security relies on the **no-cloning theorem** and **quantum uncertainty**.

Why is QKD Needed?

- Quantum computers (e.g., Shor's algorithm) threaten traditional cryptography (e.g., RSA).
- QKD provides **unconditional security** based on quantum principles.

Basic Principles and Steps of QKD

- Two stages: **quantum communication** and **classical post-processing**.
- During quantum communication, Alice sends quantum states to Bob. The **no-cloning theorem** states that it is impossible to create an exact copy of an unknown quantum state, which prevents Eve from perfectly copying the transmitted quantum information.
- Any attempt by Eve to intercept and measure the quantum states introduces detectable disturbances, allowing Alice and Bob to identify the presence of an eavesdropper.

Basic Principles and Steps of QKD

- Classical post-processing includes **error correction** and **privacy amplification** to ensure a secure key by reducing Eve's potential knowledge.
- **Error correction** is used to reconcile discrepancies between Alice's and Bob's measurement outcomes. Due to noise in the quantum channel, their raw keys may differ slightly. Error correction allows them to correct these differences without revealing their entire key to each other or to an eavesdropper.
- Error correction protocols typically involve exchanging syndromes over a public channel, which helps Bob adjust his key to match Alice's. This process is designed to minimize the information leaked to an eavesdropper.

One-Time Pad & QKD

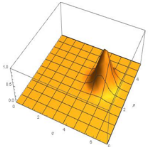
- The **One-Time Pad** requires a secret key as long as the message, used only once.
- QKD provides a secure method to generate and distribute such keys, ensuring **perfect secrecy**.

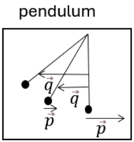
Motivation for Continuous-Variable QKD (CV-QKD)

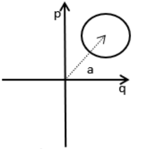
- **Continuous-Variable QKD (CV-QKD)** uses the continuous nature of quantum states, specifically the quadratures (position and momentum), to encode information.
- Unlike discrete-variable QKD, CV-QKD can leverage standard telecommunication technology, making it more practical for integration with existing fiber networks.
- CV-QKD is well-suited for applications where the use of coherent states and homodyne detection provides advantages in terms of implementation simplicity and higher key rates at short distances.
- The continuous nature of quadratures (q and p) aligns with the practical implementation of Gaussian modulation, which is more adaptable for high-speed communication.

Coherent States and Gaussian Distribution

- A **coherent state** is a quantum state of the electromagnetic field that resembles classical light.
- Coherent states are eigenstates of the annihilation operator $\hat{a}$: $\hat{a}|\alpha\rangle = \alpha|\alpha\rangle$, where α is a complex number representing the amplitude of the coherent state.
- In **phase space**, the amplitude α determines the **mean** position of the coherent state, with quadratures (q and p) representing the real and imaginary components.
- The coherent state is represented by a **Gaussian distribution** in phase space, where the **variance** represents the quantum uncertainty, giving the state its quantum nature.







coherent state

Gaussian Modulation and Measurement

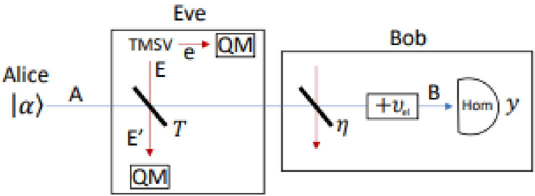
- In CV-QKD, the **amplitudes of coherent states** are modulated using a **Gaussian distribution**. This is known as **Gaussian modulation**.
- The mean values of the coherent states are varied according to Gaussian statistics, which allows for the encoding of information in the continuous quadratures.
- At the receiver's side (Bob), **homodyne** or **heterodyne detection** is used to measure the quadratures of the coherent states.
- **Homodyne detection** measures one quadrature (q and p), while **heterodyne detection** measures both quadratures simultaneously, providing complete information about the state.

Thermal Loss Channel and Optical Fiber Links

- The communication channel in CV-QKD is modeled as a **thermal loss channel**, which is a type of **Gaussian channel**.
- A thermal loss channel accounts for both the **loss of photons** and the **addition of thermal noise** during transmission.
- In practical implementations, this channel is often realized using **optical fiber links**, which introduce both attenuation (loss) and environmental noise.
- The **transmissivity** of the channel represents the fraction of the signal that successfully reaches Bob, while the rest may be lost or intercepted by an eavesdropper.
- Understanding the properties of the Gaussian channel is crucial for accurately estimating the **secret key rate** and ensuring the security of the protocol.

Individual Attacks in CV-QKD

- In the case of **individual attacks**, Eve interacts independently with each signal sent from Alice to Bob.
- Eve attempts to gain information by injecting a **thermal state** into the channel with variance $\omega = \frac{\tau\xi}{1-\tau} + 1$, where:
  - τ is the **transmissivity** of the channel.
  - ξ is the **excess noise** introduced by Eve.
- This model allows Eve to gather information while maintaining a minimal impact on the channel's overall behavior.



Secret Key Rate for the Asymptotic Regime

- The **secret key rate** K is defined as the difference between the mutual information shared by Alice and Bob (I_{AB}) and the information Eve has about Alice's data (I_{AE}):

$$K = I_{AB} - I_{AE} \tag{1}$$

- The mutual information between Alice and Bob, I_{AB}, is given by:

$$I_{AB} = \frac{1}{2}\log_2\left(1 + \frac{\tau V}{1 + \tau\xi}\right) \tag{2}$$

- The mutual information between Eve and Alice, I_{AE}, is given by:

$$I_{AE} = \frac{1}{2}\log_2\left(1 + \frac{(1-\tau)V}{\tau\omega + 1 - \tau}\right) \tag{3}$$

Intuition Behind the Secret Key Rate

- The secret key rate K is derived as the difference between the information shared by Alice and Bob and the information Eve could potentially acquire.
- The rationale behind this equation is that the security of the key relies on Alice and Bob having more information than Eve.
- If Eve's information (I_{AE}) approaches Alice and Bob's information (I_{AB}), the secret key rate decreases, reducing the security of the protocol.
- The goal of CV-QKD is to maximize I_{AB} and minimize I_{AE}, ensuring a positive secret key rate that guarantees secure communication.

Coherent Attacks in CV-QKD

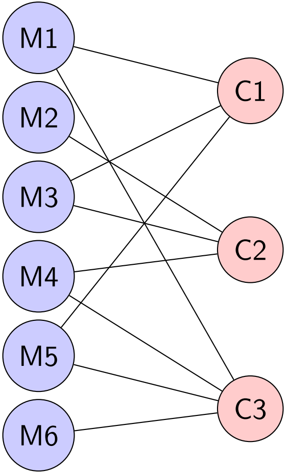
- In **coherent attacks**, Eve is more powerful and uses **quantum memory** to store intercepted quantum states for later measurement.
- Eve interacts collectively with the transmitted signals and can correlate her measurements to maximize her information gain.
- The security analysis in the presence of coherent attacks involves the **Holevo information** (χ), which is the quantum counterpart of mutual information.
- The Holevo information provides an upper bound on the information that Eve can obtain about the key after interacting with the quantum system.

Reconciliation Efficiency in Error Correction Protocols

- The **reconciliation efficiency** β is a key factor in finite-size effects of QKD and is related to the efficiency of error correction (EC) protocols.
- The relationship is given by $\beta I_{AB} = H(X) - \text{leak}_{\text{ec}}$, where:
  - When $\text{leak}_{\text{ec}} = H(X|Y)$, $\beta = 1$, representing the ideal asymptotic case, as stated by the **Slepian-Wolf theorem**.
  - In reality, $\text{leak}_{\text{ec}} > H(X|Y)$ due to imperfections in practical EC protocols, for example, protocols that utilize low-density parity-check (LDPC) codes.

Tanner Graph for LDPC Codes

- LDPC codes can be represented using a **Tanner graph**, which consists of message nodes and parity-check nodes.
- Below is an example Tanner graph with 6 message nodes and 3 check nodes.



Parity-Check Matrix and Syndrome Calculation

- The **parity-check matrix** H corresponding to the previous Tanner graph is:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \end{bmatrix}$$

- The **syndrome s** for a message vector **m** is calculated as:

$$\mathbf{s} = H \cdot \mathbf{m}^T \mod 2$$

Code Rate Calculation and Practical Challenges

- The length of the **syndrome** determines the number of parity checks, which in turn defines the code rate R_{code} of the LDPC scheme.
- For our example, with 6 message nodes and 3 check nodes, the **code rate** R_{code} is:

$$R_{\text{code}} = 1 - \frac{N_{\text{check}}}{N_{\text{message}}} = 1 - \frac{3}{6} = 0.5$$

- In practice, it is very challenging to approach the **Slepian-Wolf limit** for all **SNR** regimes, where SNR describes the conditional entropy

$$H(X|Y) \leq \text{leak}_{\text{ec}} := q(1 - R_{\text{code}}) = q\frac{N_{\text{check}}}{N_{\text{message}}}.$$

Where q is the descretization.

Conclusion

- Quantum Key Distribution (QKD) provides a fundamental method for secure communication, leveraging quantum principles to ensure **unconditional security**.
- Continuous-Variable QKD (CV-QKD) utilizes coherent states and Gaussian modulation, offering practical advantages for integration with existing telecommunication infrastructure.
- Efficient **Error Correction (EC)** methods are crucial for achieving secure key rates in CV-QKD. These methods must adapt to different **SNR** regimes to optimize performance.
- Practical implementations require overcoming constraints such as **memory usage**, **speed**, **computational power**, and achieving a high **successful probability** of error correction.

References

- Bennett, C. H., Brassard, G. (1984). Quantum Cryptography: Public Key Distribution and Coin Tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*.
- Pirandola, S., Andersen, U. L., Banchi, L., Berta, M., Bunandar, D., Colbeck, R., Englund, D., Gehring, T., Lupo, C., Ottaviani, C., Pereira, J., Razavi, M., Shaari, J. S., Tomamichel, M., Usenko, V. C., Vallone, G., Villoresi, P., Wallden, P. (2019). Advances in Quantum Cryptography. arXiv preprint arXiv:1906.01645v1.
- Weedbrook, C., Pirandola, S., García-Patrón, R., Cerf, N. J., Ralph, T. C., Shapiro, J. H., Lloyd, S. (2011). Gaussian Quantum Information. arXiv preprint arXiv:1110.3234v1.
- Grosshans, F., Grangier, P. (2002). Continuous Variable Quantum Cryptography Using Coherent States. *Physical Review Letters*, 88(5), 057902.
- van Assche, G., Cardinal, J., Cerf, N. J. (2004). Reconciliation of a Quantum-Distributed Gaussian Key. *IEEE Transactions on Information Theory*, 50(2), 394-400.
- Pacher, C., Martinez-Mateo, J., Duhme, J., Gehring, T., Furrer, F. (2018). Information Reconciliation for Continuous-Variable Quantum Key Distribution using Non-Binary Low-Density Parity-Check Codes. arXiv preprint arXiv:1602.09140v1.
- Slepian, D., Wolf, J. K. (1973). Noiseless Coding of Correlated Information Sources. *IEEE Transactions on Information Theory*, 19(4), 471-480.
- Gallager, R. G. (1962). Low-Density Parity-Check Codes. *IRE Transactions on Information Theory*, 8(1), 21-28.
- Mountogiannakis, A. G., Papanastasiou, P., Braverman, B., Pirandola, S. (2021). Composably Secure Data Processing for Gaussian-Modulated Continuous Variable Quantum Key Distribution. arXiv preprint arXiv:2103.16589v3.

Thank You

Thank You!

Questions and Discussions Welcome

Panagiotis Papanastasiou
University of York
Presentation at Department of Electrical Engineering, University of Patras