CONTINUOUS-VARIABLE QUANTUM KEY DISTRIBUTION AND CRYPTOGRAPHY

Nam Nguyen
Department of Electrical Engineering
University of South Florida
Tampa, FL 33620, USA
{namnguyen2}@usf.edu

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. We will first introduce the background and advancements of CV-QKD in Section 1. Then, Section 2 will focus on the core components of CV-QKD, which are Gaussian state and Qumode-based quantum computing. This section aims to establish a solid mathematical foundation of CV-QKD, offering us more insights into further discussion. Section 3 will have a detailed survey on recent state-of-the-art CV-QKD research, which includes (Grosshans & Grangier, 2002; Zhou et al., 2019; Madsen et al., 2012; Pirandola et al., 2008; Zhang et al., 2020; Tang et al., 2020; Grosshans et al., 2003; Bennett & Brassard, 2020; Huang et al., 2018). Finally, we will propose several potential research directions in Section 4. Moreover, we will provide implementations of discussed algorithms via IBMQ and Qskits library.

REFERENCES

Charles H Bennett and Gilles Brassard. Quantum cryptography: Public key distribution and coin tossing. *arXiv preprint arXiv:2003.06557*, 2020.

Frédéric Grosshans and Philippe Grangier. Continuous variable quantum cryptography using coherent states. *Physical review letters*, 88(5):057902, 2002.

Frédéric Grosshans, Gilles Van Assche, Jérôme Wenger, Rosa Brouri, Nicolas J Cerf, and Philippe Grangier. Quantum key distribution using gaussian-modulated coherent states. *Nature*, 421 (6920):238–241, 2003.

Peng Huang, Jingzheng Huang, Zheshen Zhang, and Guihua Zeng. Quantum key distribution using basis encoding of gaussian-modulated coherent states. *Physical Review A*, 97(4):042311, 2018.

Lars S Madsen, Vladyslav C Usenko, Mikael Lassen, Radim Filip, and Ulrik L Andersen. Continuous variable quantum key distribution with modulated entangled states. *Nature communications*, 3(1):1–6, 2012.

Stefano Pirandola, Stefano Mancini, Seth Lloyd, and Samuel L Braunstein. Continuous-variable quantum cryptography using two-way quantum communication. *Nature Physics*, 4(9):726–730, 2008.

Xinke Tang, Rupesh Kumar, Shengjun Ren, Adrian Wonfor, Rihard V Penty, and Ian H White. Performance of continuous variable quantum key distribution system at different detector bandwidth. *Optics Communications*, 471:126034, 2020.

Yichen Zhang, Ziyang Chen, Christian Weedbrook, Song Yu, and Hong Guo. Continuous-variable source-device-independent quantum key distribution against general attacks. *Scientific reports*, 10(1):1–10, 2020.

Chao Zhou, Xiangyu Wang, Yichen Zhang, Zhiguo Zhang, Song Yu, and Hong Guo. Continuous-variable quantum key distribution with rateless reconciliation protocol. *Physical Review Applied*, 12(5):054013, 2019.