Quamtum Key Distribution and Cryptography

Zonghai Jing

EC601 Fall 2024

Introduction

Quantum cryptography leverages the principles of quantum mechanics, such as the uncertainty principle and no-cloning theorem, to enable secure communication. Unlike classical cryptography, which relies on computational complexity, quantum cryptography provides unconditional security by ensuring that any eavesdropping attempt alters the quantum states, making it detectable. A cornerstone of quantum cryptography is Quantum Key Distribution (QKD), which allows two parties to securely exchange encryption keys. Protocols like BB84 ensure that any interception is immediately noticed. QKD is pivotal for building secure communication networks, especially in an era where quantum computers threaten the integrity of classical encryption systems like RSA and ECC.

Core Areas of Quantum Key Distribution (QKD)

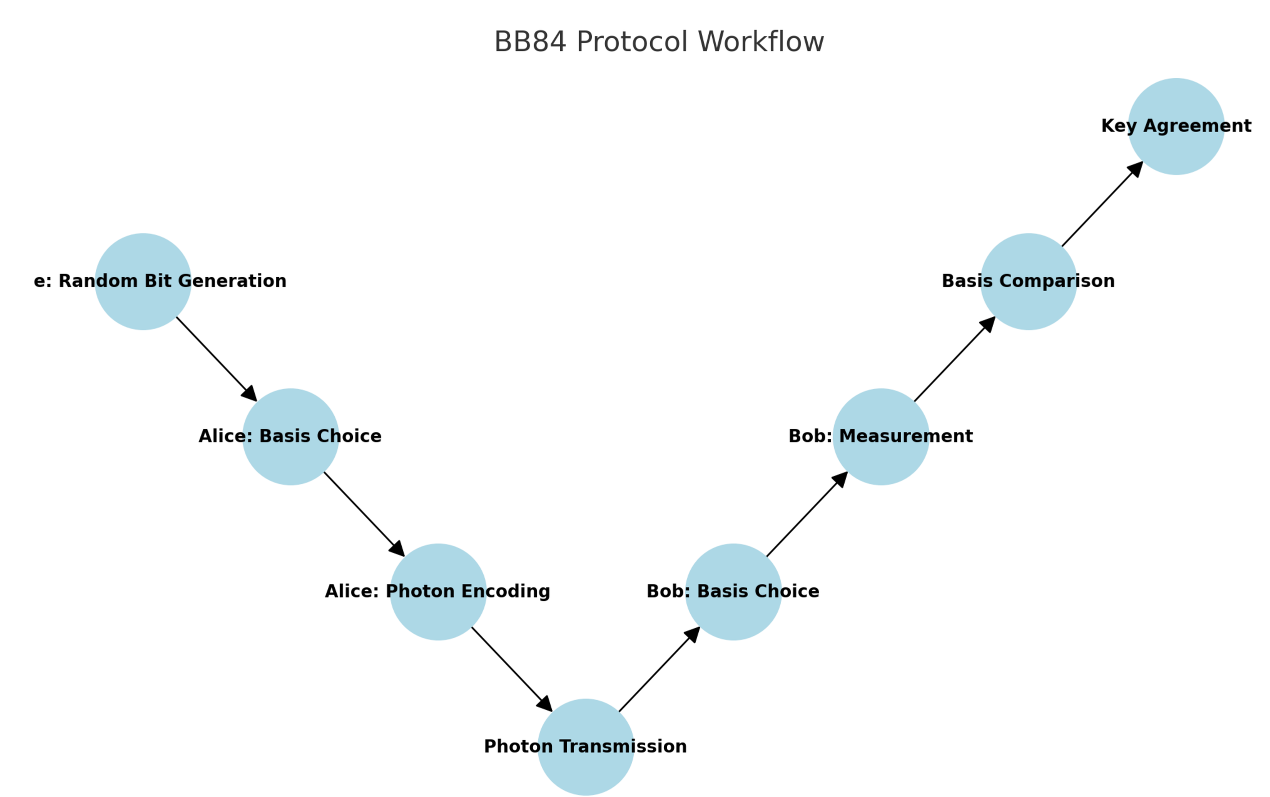

Figure1: The BB84 protocol enables Alice and Bob to securely share a cryptographic key by using quantum states and comparing their measurement bases, with security ensured by detecting any eavesdropping attempts through quantum mechanics.

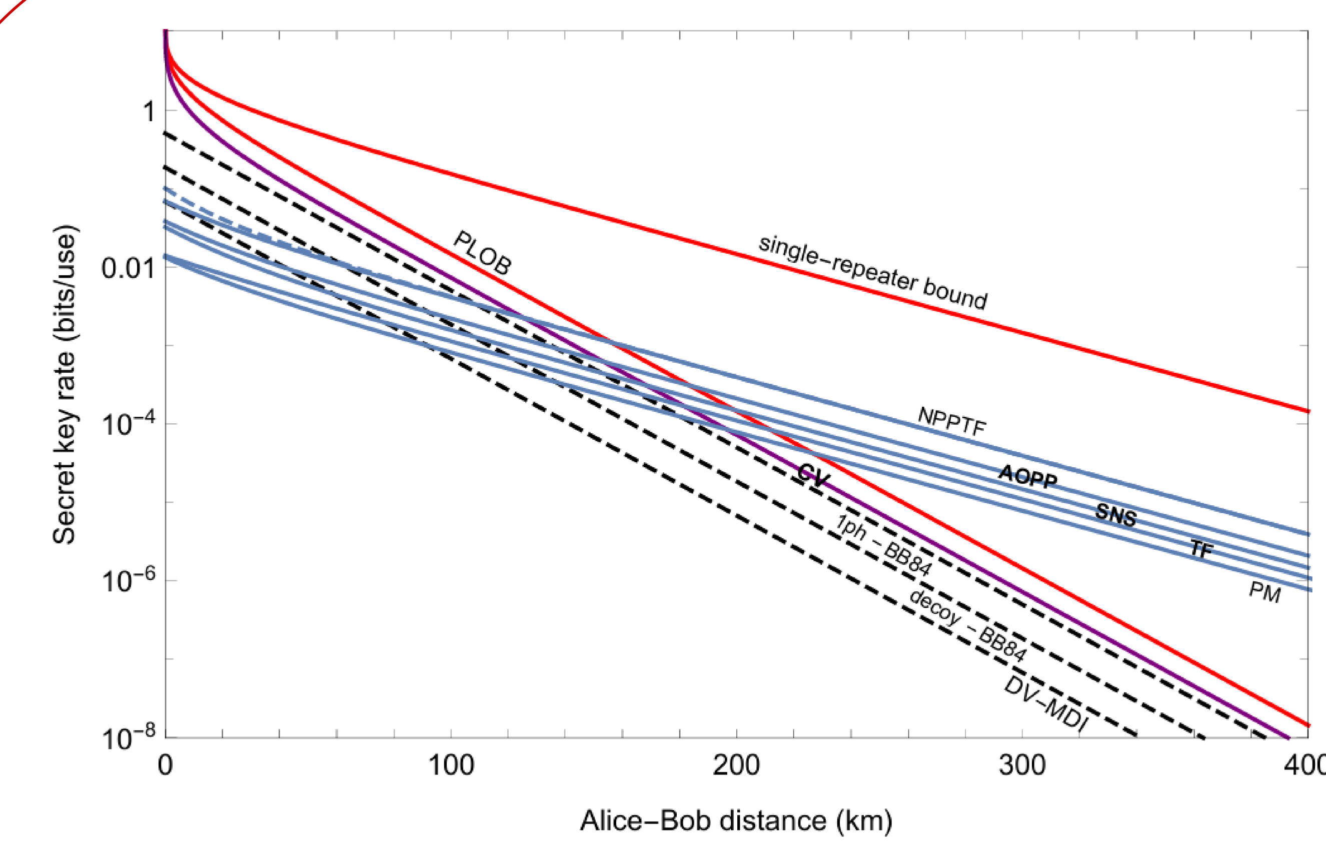

Figure2: State of the art in high-rate QKD.

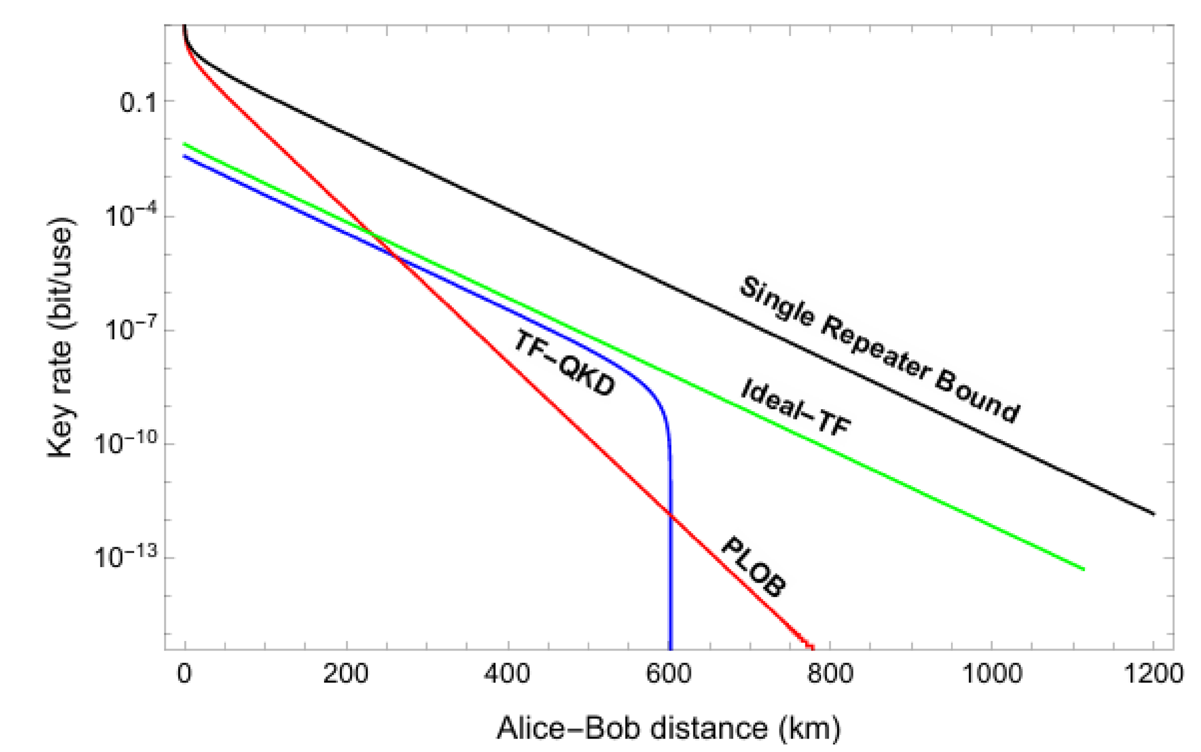

Figure3: Key rate of the TF-QKD protocol versus Alice Bob total distance in standard optical fiber (0.2 dB/km), assuming ideal (green line) and realistic (blue line) conditions.

Figures 2 & 3 source: 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. (2020). *Advances in Quantum Cryptography*. Advances in Optics and Photonics, 12(4), 1012–1097. https://doi.org/10.1364/AOP.361502

Simulation

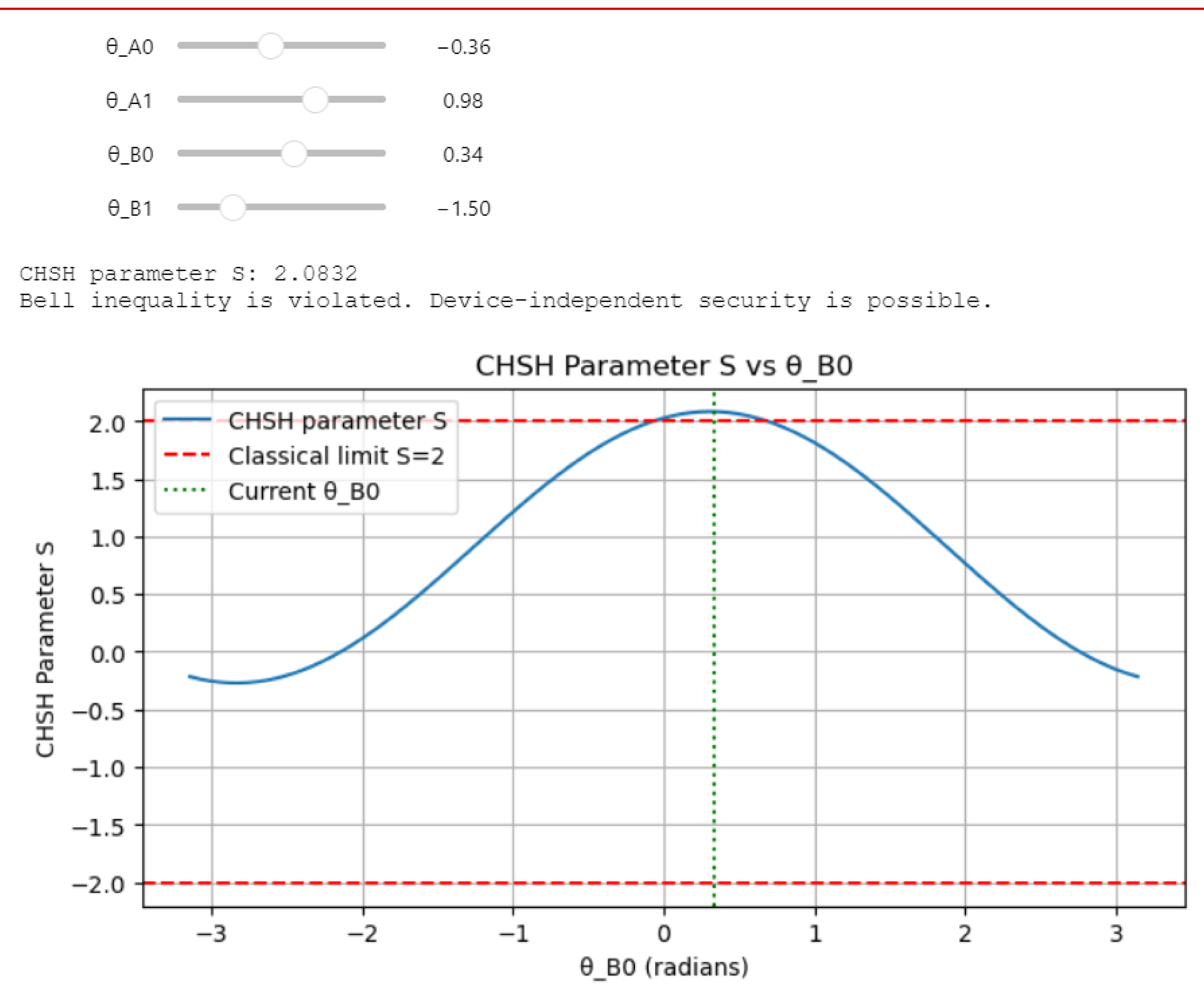

Figure4 shows how the CHSH parameter (*S*) exceeds the classical limit (*S*>2), proving quantum entanglement and ensuring secure, device-independent key distribution.

Future work

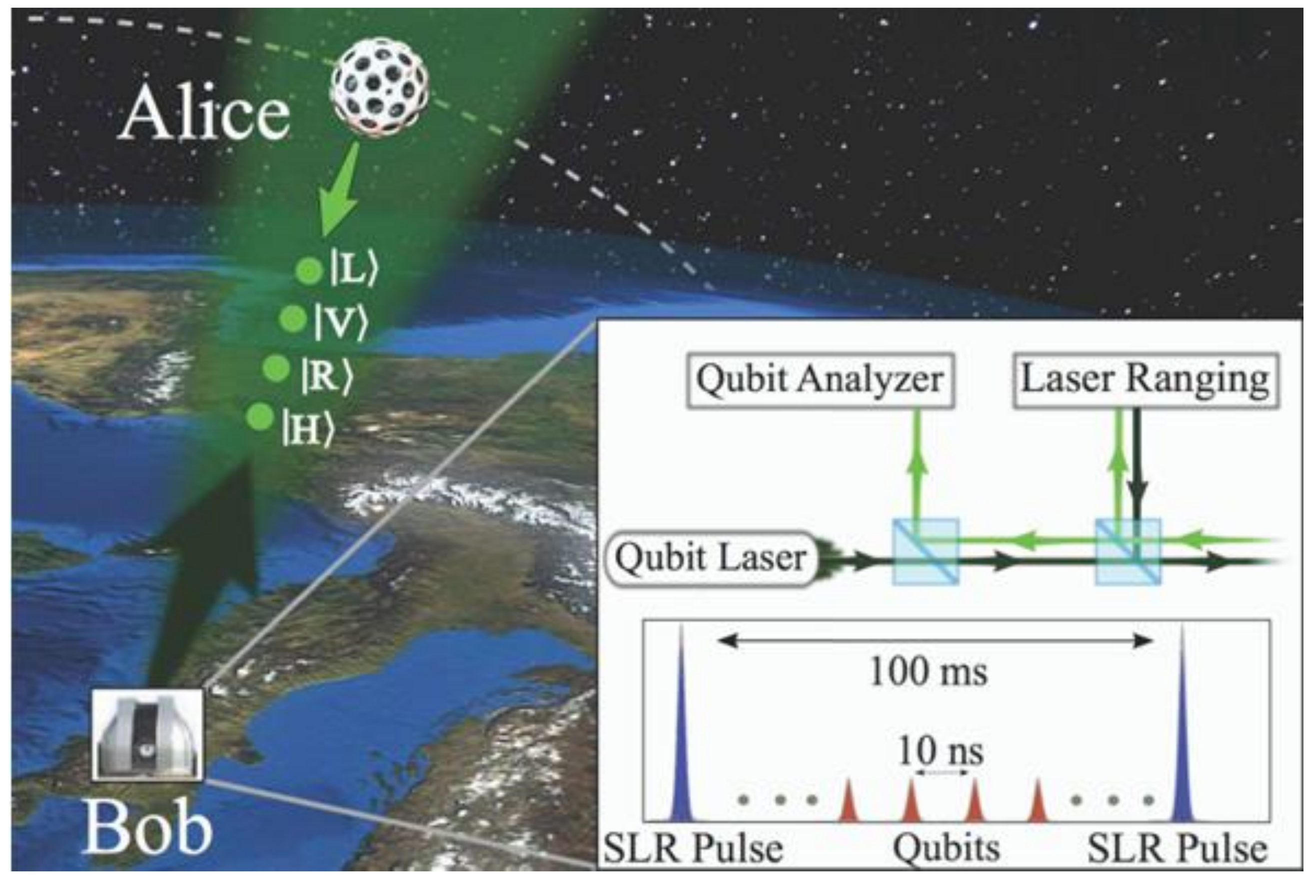

Figure5: Satellite QKD demonstration: possible direction of future.

Figure5 source: G. Vallone, D. Bacco, D. Dequal, S. Gaiarin, V. Luceri, G. Bianco, and P. Villoresi, "Experimental Satellite Quantum Communications," *Phys. Rev. Lett.* **115**, 040502 (2015).