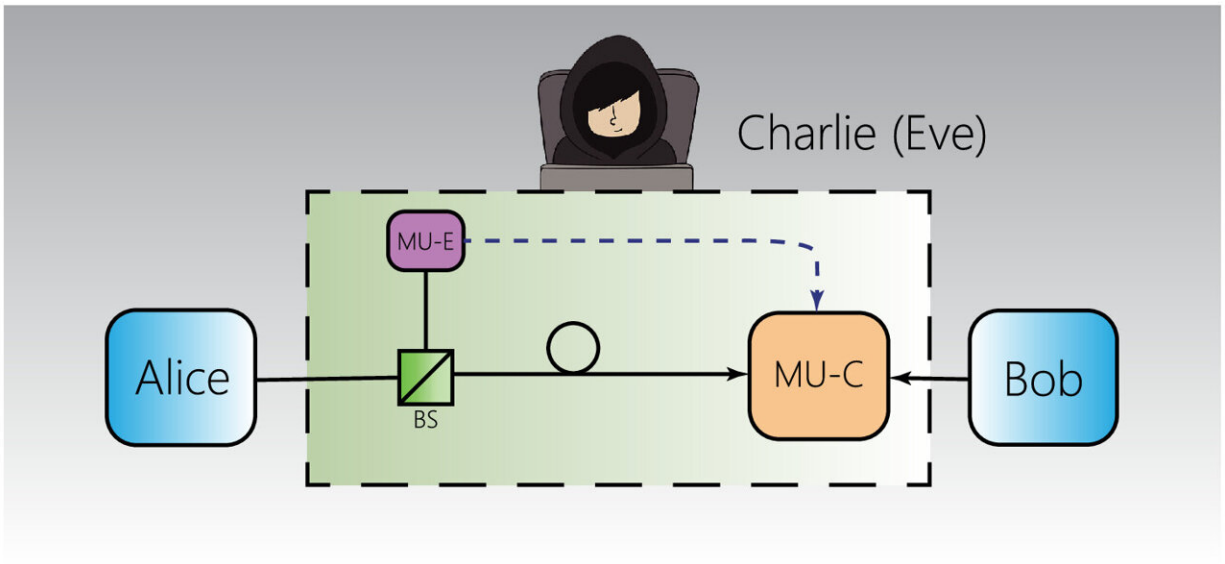
Quantum hacking alert: Critical vulnerabilities found in quantum key distribution

June 15 2023, by Liu Jia



Schematic diagram of our tagged method. MU-E, the measurement unit for projecting Alice's states on the Z basis; MU-C, the measurement unit for BSM; BS, beam splitter. Credit: *Optica* (2023). DOI: 10.1364/OPTICA.485389

A team led by academician Guo Guangcan from the University of Science and Technology of China of the Chinese Academy of Sciences made progress in the practical security of quantum key distribution (QKD).

Researchers identified a potential security vulnerability in the modulator device of the QKD transmitter and conducted quantum hacking attacks utilizing this vulnerability. The attacks demonstrated that when the vulnerability is not adequately protected, an attacker may exploit it to obtain the entire key information. The results were published in *Optica* and *Physical Review Applied*.

Although QKD theoretically enables the generation of information-theoretically secure keys between users, the non-ideal characteristics of practical devices may deviate from the theoretical assumptions, making them susceptible to eavesdropping attacks. Therefore, conducting a comprehensive and in-depth analysis of the practical security of QKD systems and subsequently designing more robust and secure practical systems are crucial for advancing the practical application of QKD.

Guo's team has made progress in analyzing the practical security of QKD systems and developing attack-defense techniques. The achievements include the discovery of a control vulnerability in the avalanche-transition region of detection devices, proposing a variable attenuation defense scheme to counter control attacks on detection devices, developing a detection-independent quantum random number generator, and designing error-correcting enhanced protocols to eliminate coding biases.

In this study, researchers proposed a novel approach to attack the QKD system by externally injecting photons to manipulate the operational state of the core device at the transmitter, compromising the security of the key. They identified and analyzed the substantial impact of photorefraction in commercial lithium niobate (LN) devices on QKD. They designed and validated attack schemes specifically targeting Bennett-Brassard 1984 protocol-based QKD systems, and revealed that the attacker could execute the attack by injecting an optimized irradiation beam with an intensity of merely 3 nW.

Additionally, the researchers developed a transmitter attack scheme tailored for measurement-device-independent QKD systems. By simultaneously measuring all quantum states transmitted by the sender and inducing photorefraction in the LN modulator through injected irradiation beam, the attacker could effectively conceal the disturbances caused by their measurement actions. A pioneering quantum hacking attack experiment on a functional measurement-device-independent QKD system demonstrated the eavesdropper's ability to surreptitiously acquire almost all the cryptographic keys.

To counteract these vulnerabilities and attacks, researchers proposed comprehensive system design strategies and technical implementation schemes that effectively mitigate the risks. The experimental validation substantiated that through meticulous system design and optimized utilization of devices, the practical security of QKD systems can be significantly bolstered.

This study not only identified and analyzed potential vulnerabilities at the transmitter and the threats they pose to practical system security, but also proposed solutions, which is of great significance for promoting the practical application and standardization of QKD.

More information: Feng-Yu Lu et al, Hacking measurement-device-independent quantum key distribution, *Optica* (2023). DOI: 10.1364/OPTICA.485389

Peng Ye et al, Induced-Photorefraction Attack against Quantum key Distribution, *Physical Review Applied* (2023). DOI: 10.1103/PhysRevApplied.19.054052

Provided by Chinese Academy of Sciences