Thermodynamic Limits of Quantum Search and their implications for quantum-classical cryptography

Ralf Riedinger
Donika Imeri, Pius Gerisch, Daniel Tippel, Henning Mollenhauer

Institut für Laserphysik und Zentrum für Optische Quantentechnologien, Universität Hamburg, 22761 Hamburg, Germany
The Hamburg Centre for Ultrafast Imaging, 22761 Hamburg, Germany

Ralf.riedinger@uni-hamburg.de

Quantum computers fundamentally require thermodynamic work to perform meaningful operations [1]. In this talk I will discuss the resulting work-time trade-off for Grover's search algorithm, and use it to determine the size a cryptographic key needs to have, to be considered quantum-resistant: Even an all-powerful quantum adversary has a negligible chance to recover such a key within a given time.

We apply this limit to devise a hybrid quantum-classical cryptography protocol to encrypt long distance, high bandwidth data channels. In the limit of high loss, the capacity of classical data channels fundamentally exceeds that of an equivalent quantum channel [2]. Hence, the data stream cannot be fully encrypted by one-time-pad, but (symmetric) ciphers are required. Our novel hybrid protocol relies on the same assumptions as conventional quantum key distribution (QKD) and the existence of a secure cipher. It yields comparable security to QKD-based encryption of the data link at substantially reduced technical complexity, offering a route towards quantum-based security for consumer-level electronic devices.

References

[1] Margolus, Levitin, Physica D, 120 (1998) 188
[2] Pirandola et al., Nature Communications, 8 (2017) 15043