Motivations

- As our digital society becomes increasingly connected, data security and privacy have become even more critical. This is especially so for personal information that is permanent and which remains with us for life.
- Quantum key distribution (QKD), one of the most mature quantum technology, provides a practical method for secret key sharing with information-theoretic security.
- How can quantum technology be practically used to protect user privacy with provable security?

Symmetric Private Information Retrieval [1]

Database query protocol provides:
- User privacy: the server cannot learn the users selection or interest.
- Database security: the user cannot gain access to other database entries.
- Multi-database scenario requires long shared secret keys for protocol implementation.

Full security analysis [4]

- Provide a generalised SPIR definition considering QKD as the communication channel.
- Finite-key analysis of the modified SPIR protocol.

Schematic of the QKD layer

- MDI QKD system based on time-bin phase coding.
- Working frequency: 125MHz.
- Independent lasers working in gain-switching mode ensure random phases for decoy state implementation.
- HOM interference visibility: 0.48 (± 0.015)
- Intrinsic error rate in the key generation basis: 0.83 %.
- Offline implementation of Error Correction (symmetric blind LDPC [5]) and Privacy Amplification (Toeplitz FFT).

Fingerprint retrieval demonstration

- Fingerprint data following ISO 19794-2 format [6].
- User successfully retrieve the file from database with an entry size of 800.

Measurement-device-independent QKD [2,3]

- Secure against all detector-side-channel attacks.
- Star topology suitable for network expansion.
- Cost-effective for users (hold only transmitters).
- Quantum receiver can be malicious and independent from the users and databases, eliminating any distrust regarding QKD implementation.

Quantum-enhanced SPIR with provable security

Simulation and experimental result

References: