# Experimental implementation of symmetric private retrieval with measurement-device-independent quantum network

Chao Wang[1], Wen Yu Kon[1], Hong Jie Ng[1], Charles Lim[1,2]

[1] *Department of Electrical & Computer Engineering, National University of Singapore*
[2] *Centre for Quantum Technologies , National University of Singapore*

## 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.

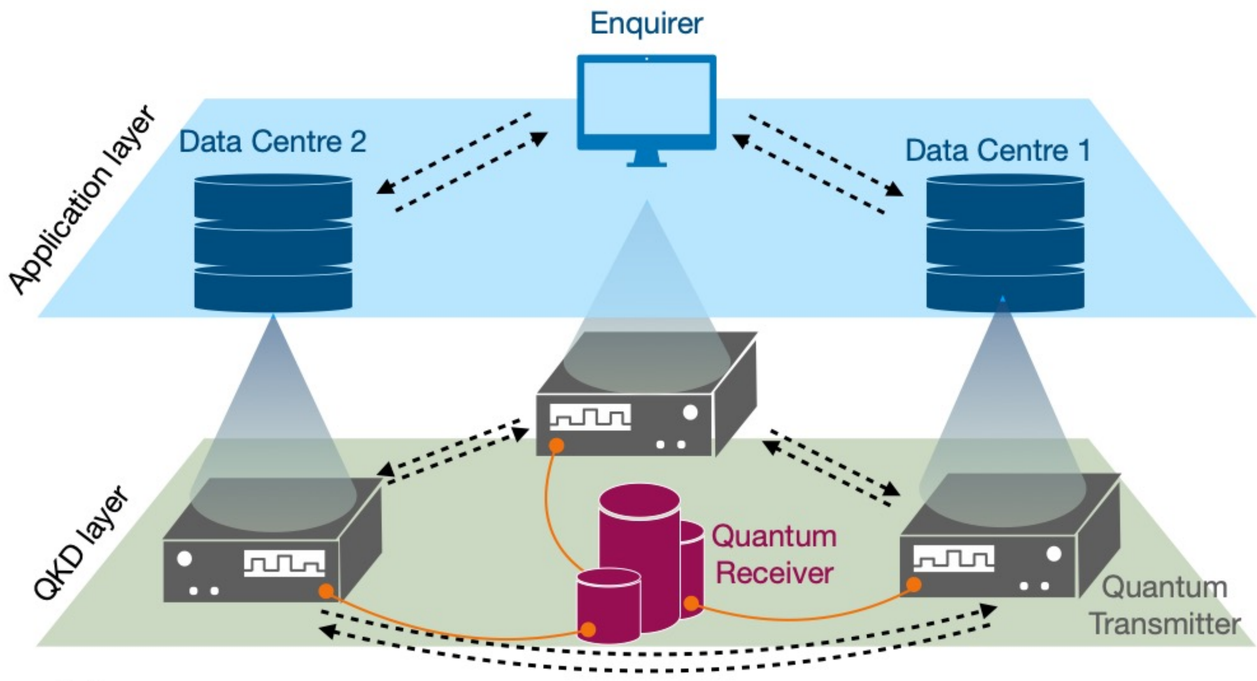
## Measurement-device-independent QKD [2,3]

- 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.

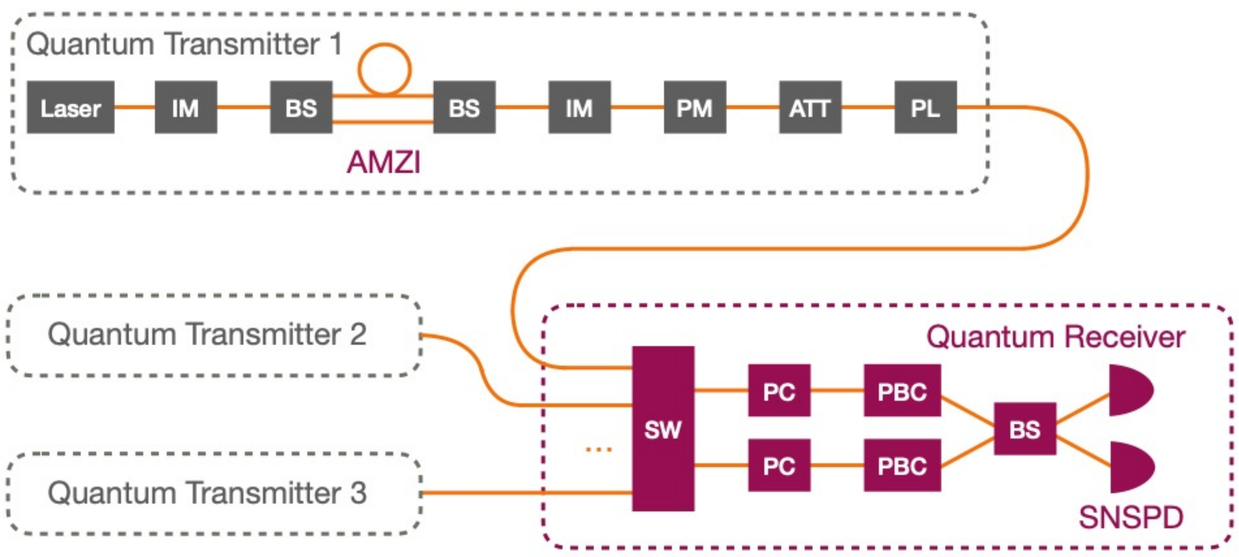
## Full security analysis [4]

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

## Quantum-enhanced SPIR with provable security

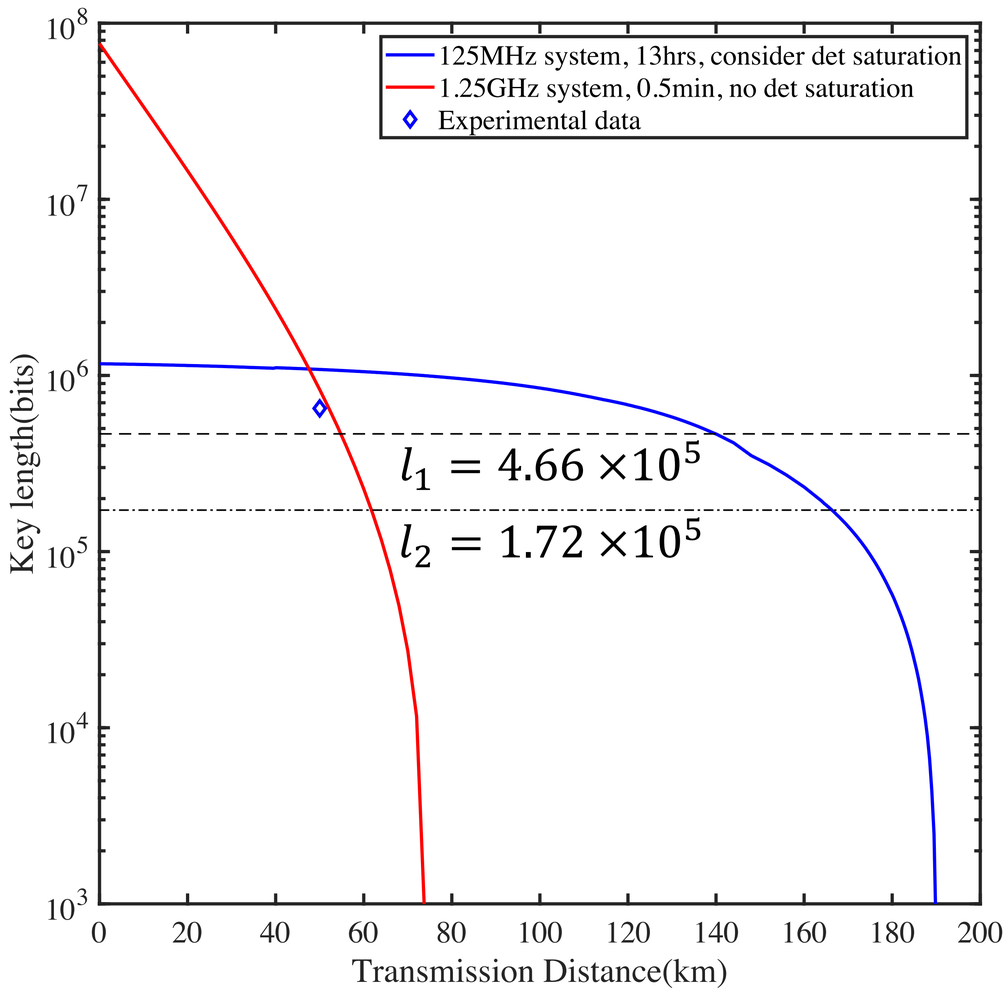



## Schematic of the QKD layer




- 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 ($\pm$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).

## Simulation and experimental result




## Fingerprint retrieval demonstration

*Databases*

464D5200 20323000 00000150 00000 184 0176 00C5 00C5 …

*Enquirer*

464D5200 20323000 00000150 00000 184 0176 00C5 00C5 …

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

**References:**

[1] *J. Comput. Syst. Sci. 2000, 60, 592–629.*
[2] *Phys. Rev. Lett. 108, 130502 (2012).*
[3] *Phys. Rev. Lett. 108, 130503 (2012).*
[4] *Entropy 23, 1 (2021).* [5] *Phys. Rev. Applied 8, 044017 (2017).*
[6] *ISO/IEC 19794-2:2011.*