Quantum-Secured Data Centre Interconnect in a Field Environment

KaiWei Qiu[1], Jing Yan Haw[2*], Hao Qin[2*], Nelly H. Y. Ng[1],
Michael Kasper[3], Alexander Ling[2,4]

[1] School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore
[2] Centre for Quantum Technologies, National University of Singapore
[3]Fraunhofer Singapore Research Centre@NTU, Nanyang Technological University
[4]Department of Physics, National University of Singapore
[*]Email: jy.haw@nus.edu.sg; hao.qin@nus.edu.sg

NATIONAL QUANTUM-SAFE NETWORK SINGAPORE

Introduction

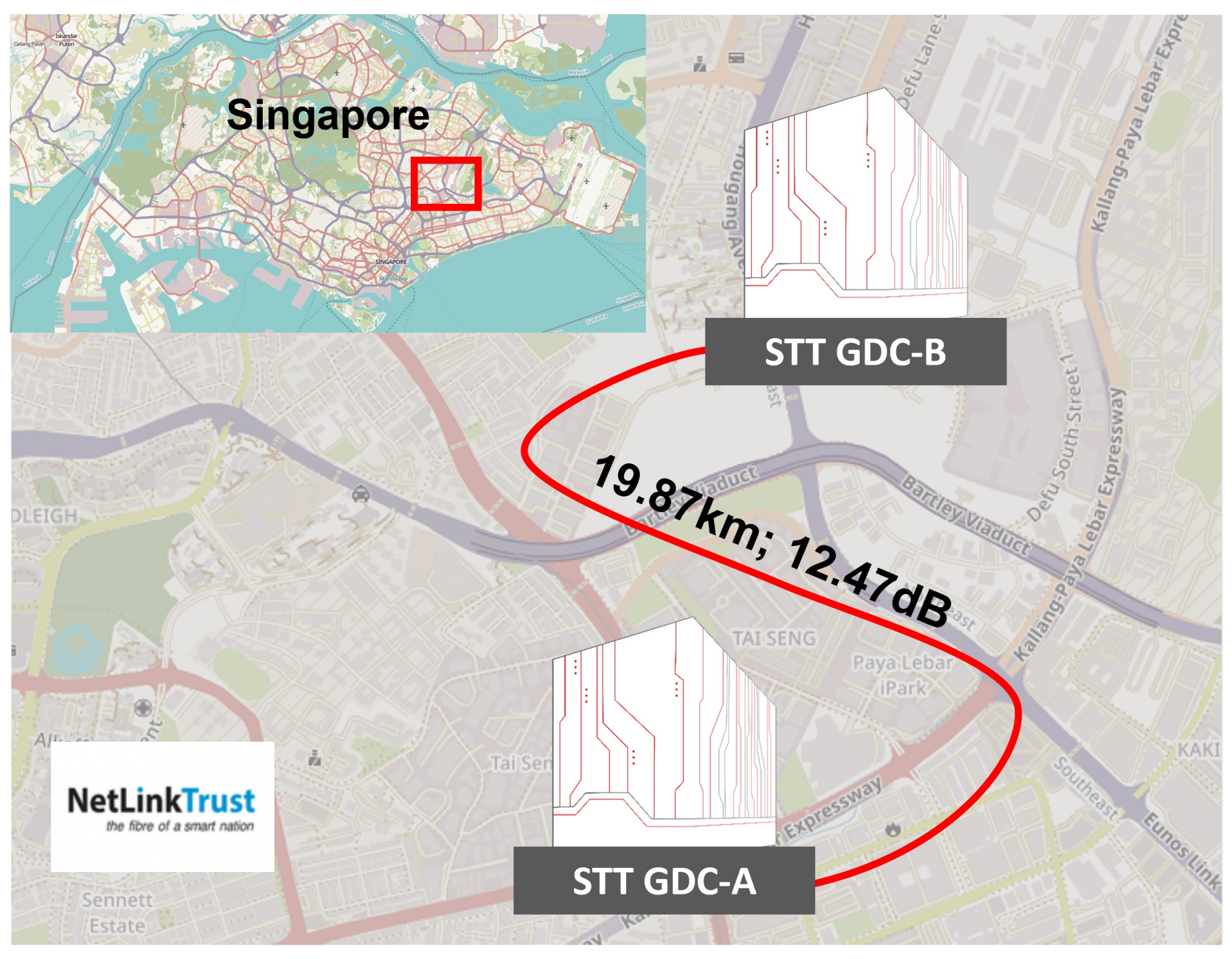
- With the advancement of quantum computers, the current asymmetric encryption methods are endangered.
- Long term security requires evaluating quantum-safe technologies.
- **Quantum Key Distribution (QKD)** provides a mature and commercially ready method to generate secure symmetric secret keys between two parties, where they are secure from potential eavesdropper
- **Field test** of the feasibility of operating QKD devices in commercial environment with existing fiber infrastructure is required.

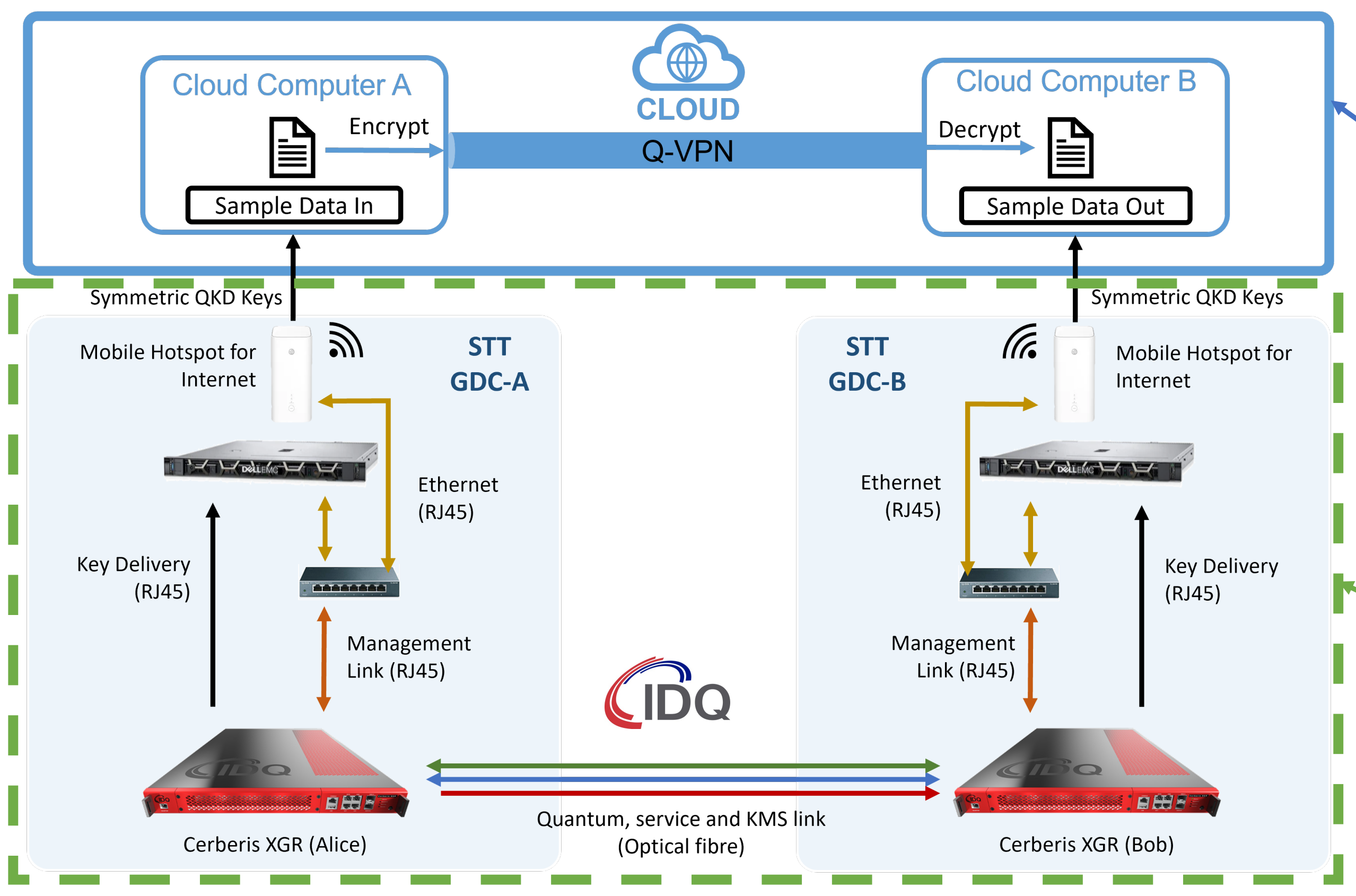
- In collaboration with 2 data centers from the Singapore Technologies Telemedia Global Data Centers (STT-GDC), we successfully [1]

1. Demonstrated continuous key rate generation, 24x7 operations over data center fiber.
2. Simulated extra fiber loss to study quantum bit error rate (QBER) and key rate correlation
3. Implemented ETSI GS QKD 014 REST-based API with QKD devices to build a quantum-secured virtual private network (Q-VPN) for data transmission between two data centers.

Fiber Network Infrastructure and QKD Application

Fiber information and QKD locations





Q-VPN

- Cloud-based key management for sample data encryption using AES-256.
- Extract symmetric QKD keys via ETSI GS QKD 014 and establish a secure Q-VPN tunnel for file transfer.

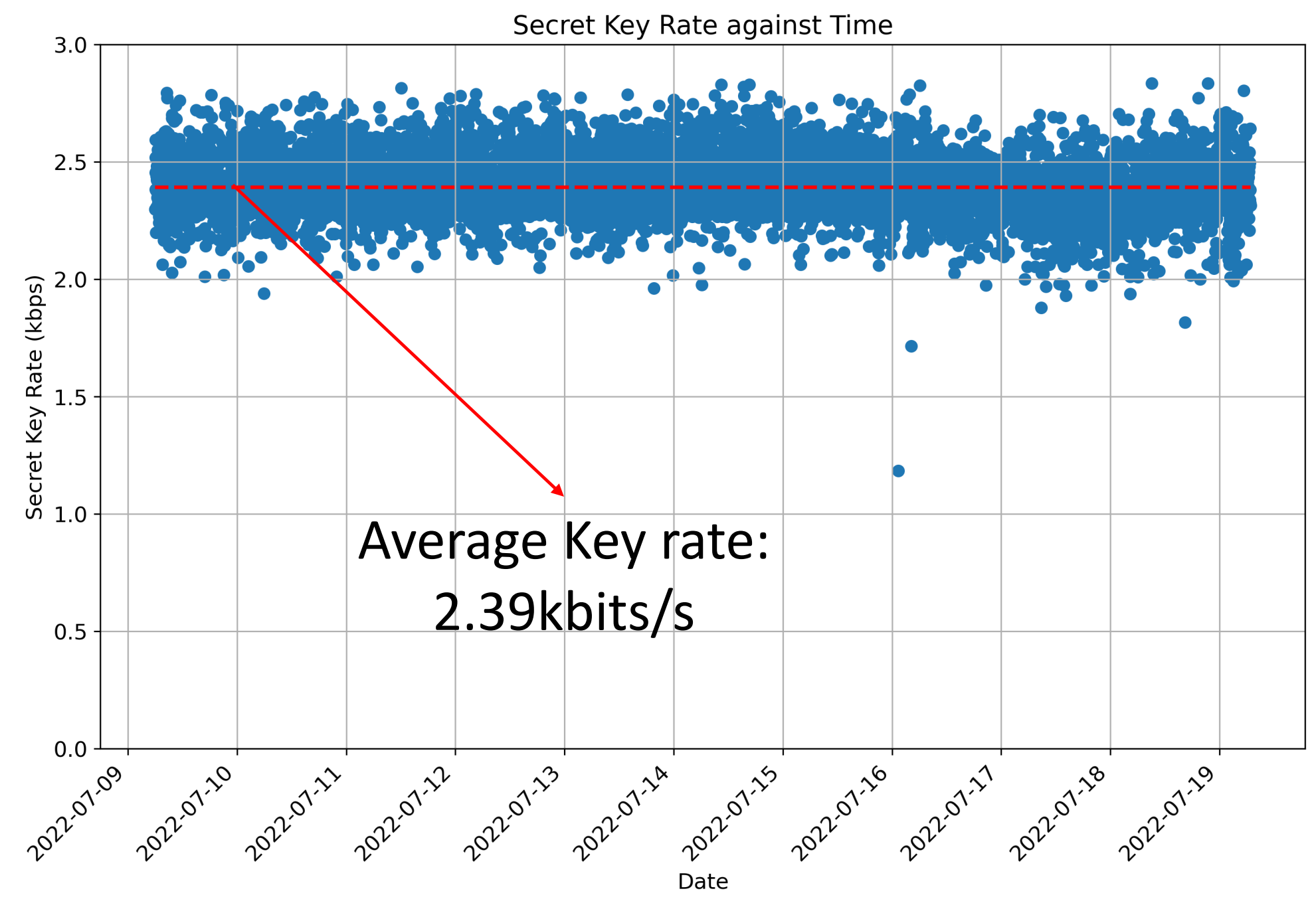
QKD Architecture

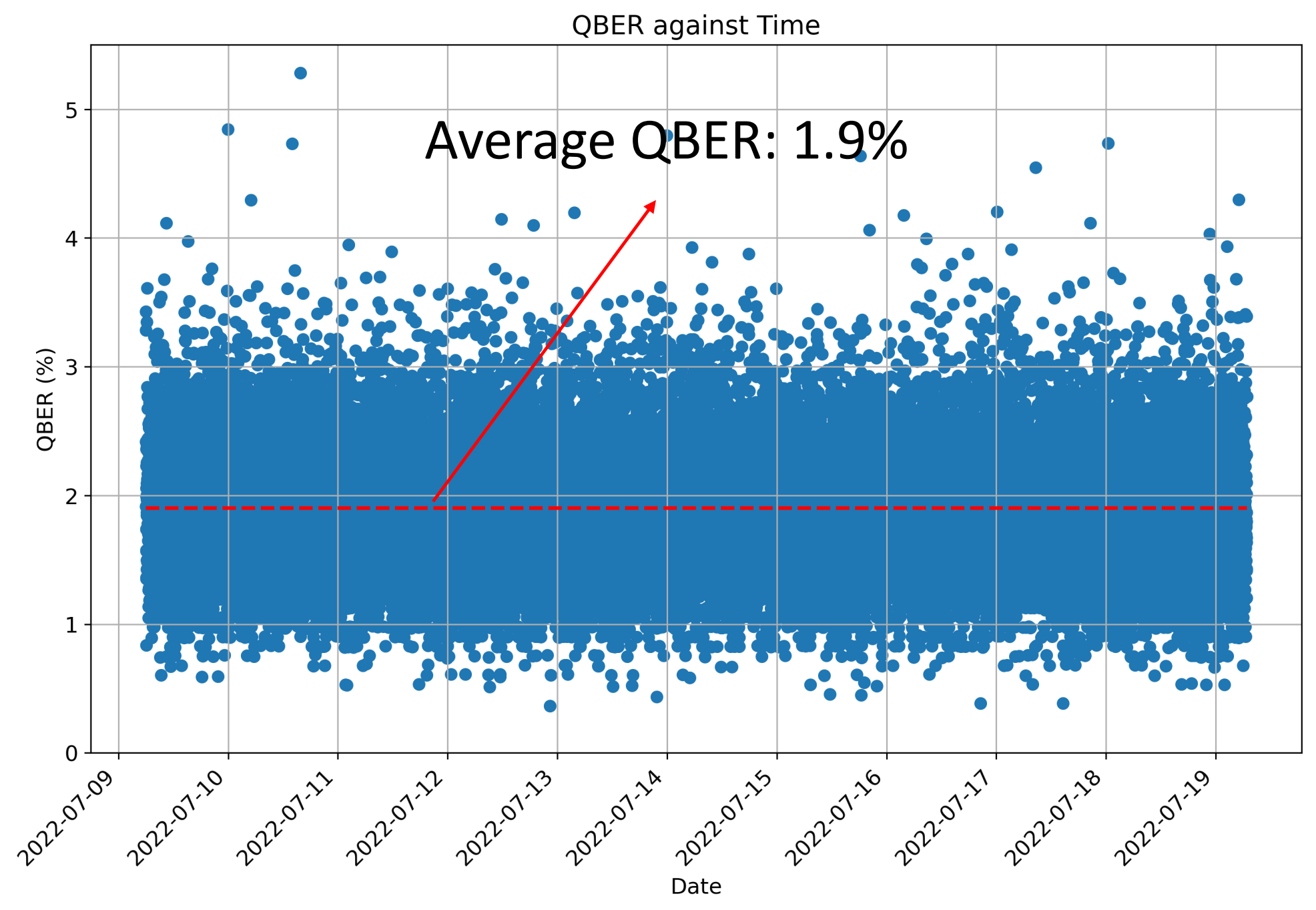
- Two IDQ QKD units (Alice & Bob) running the Coherent One Way (COW) protocol [2] connected by fiber with quantum (red), service (blue), and key management (green) channels

Results

1. Performance & stability

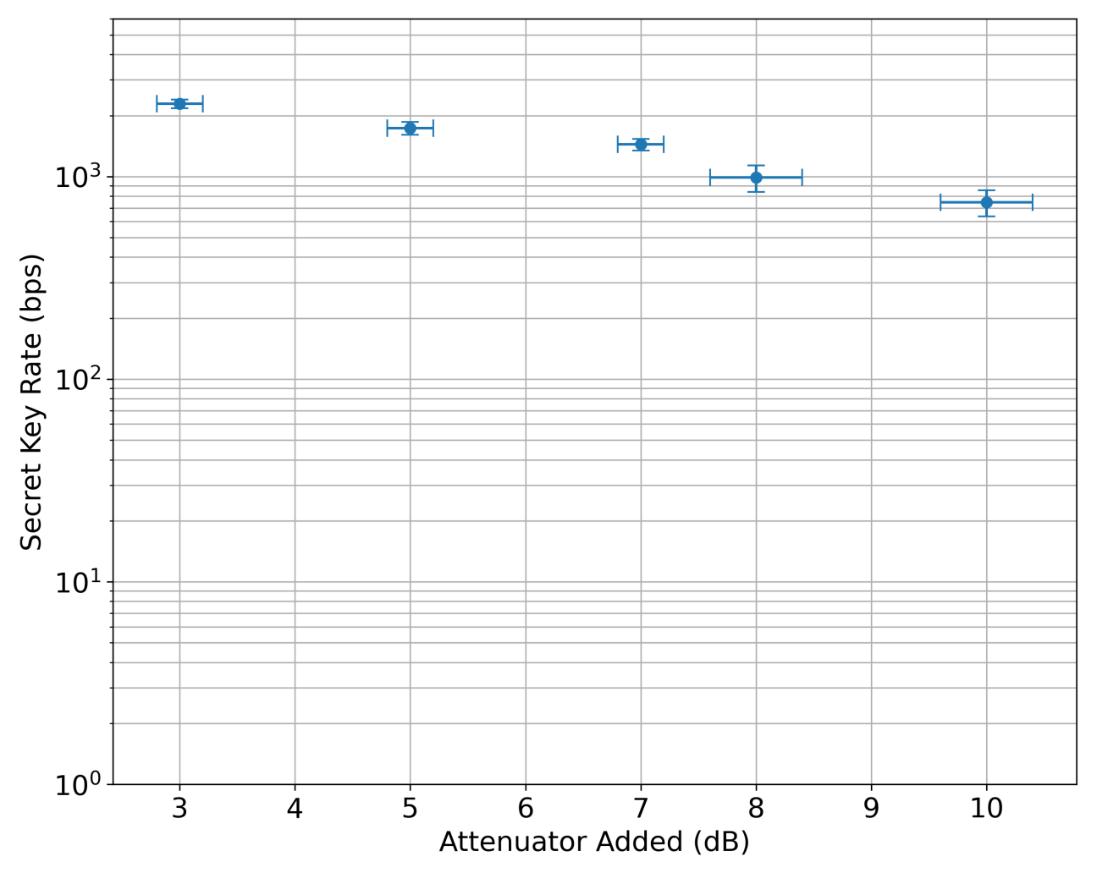
- A total of 2 Gbits of keys (or equivalently more than 8 million AES-256 keys) generated

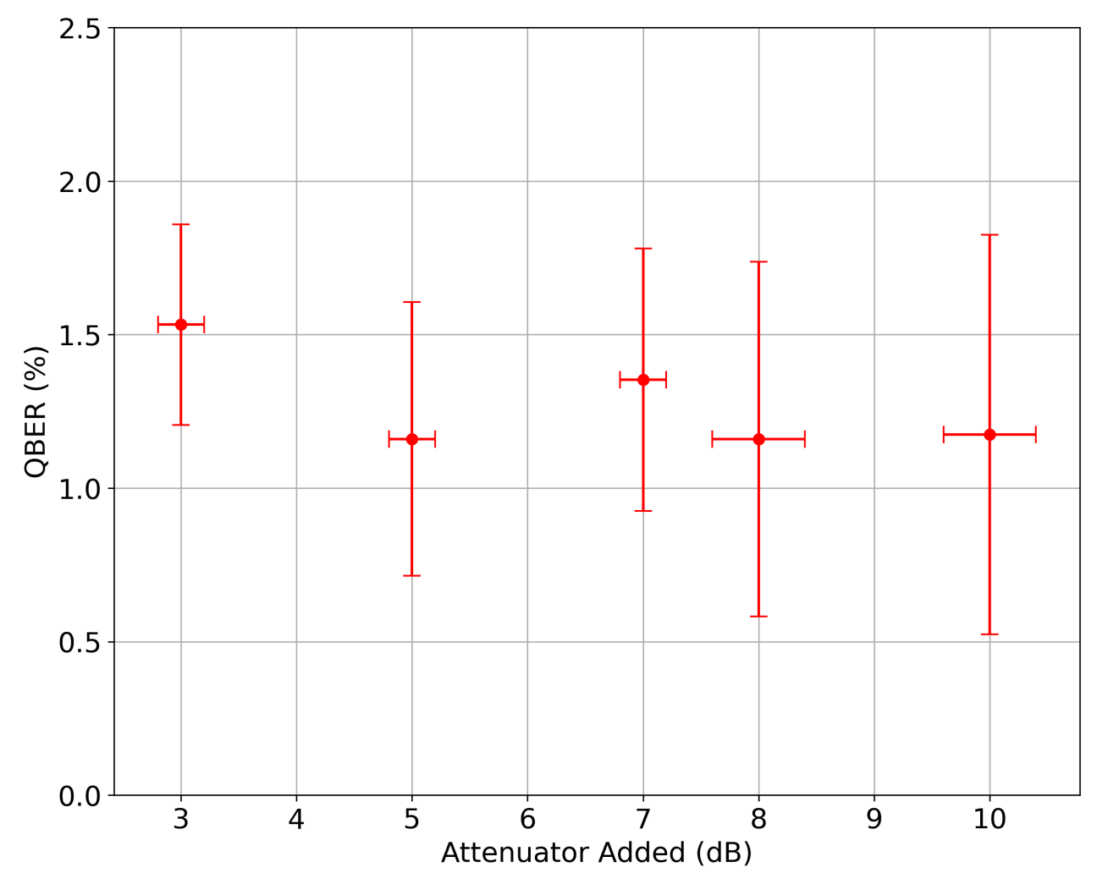




2. Attenuation test for key rate and QBER

- Key rate drops as expected with attenuation added





3. QKD Application Integration

- Q-VPN (AES-256) achieved 2.39kbit/s, enabling 11 key refreshes per second.
- Since Q-VPN renews every 10 second, QKD in commercial environment can generate sufficient keys to support the application.

PQC vs QKD

Comparison of Post-Quantum Cryptography (PQC) and QKD for the post-quantum era

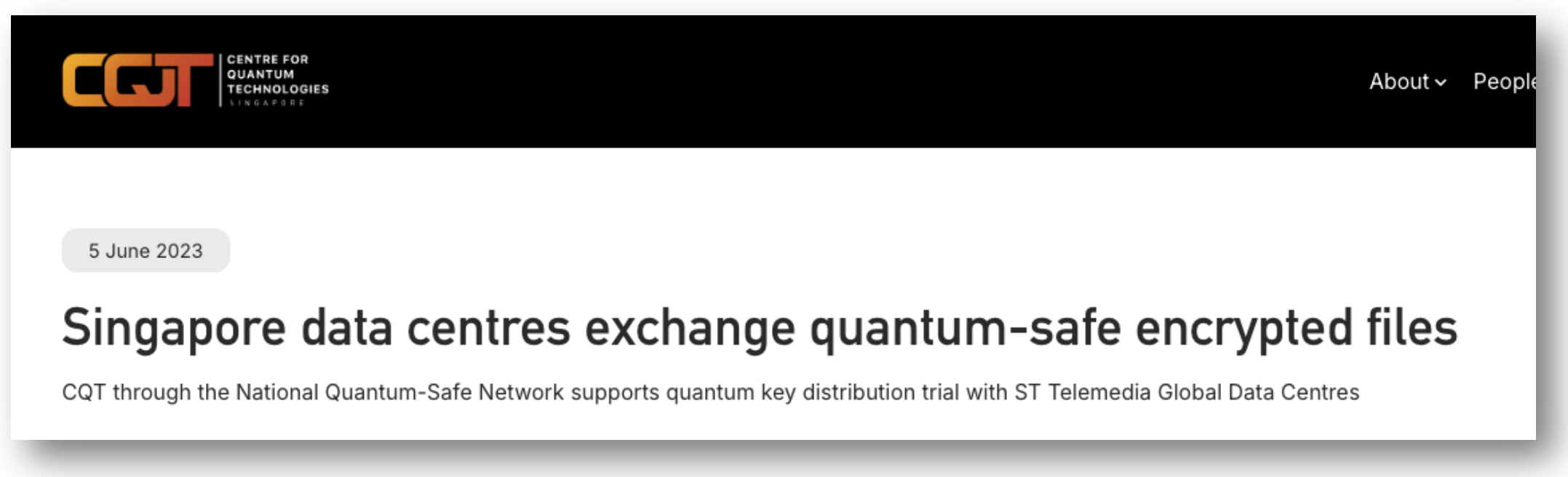
	PQC	QKD
Implementation	Software and hardware	Hardware
Protocol security	Computational Complexity	Information-theoretic security
Implementation loopholes	Exist	Exist
Application and usage	Public-key encryption and key establishment, Digital signature	Key establishment
Migration	Software and hardware upgrade	Infrastructure and hardware upgrade
Standardisation and certification	Required	Required

Outlook

- Extend point-to-point QKD link to QKD network topology
- Explore other QKD protocols and vendors
- Security requirements & standard compliance

References and Acknowledgements

[1] Qiu, K., Haw, J. Y., Qin, H., Ng, N. H., Kasper, M., & Ling, A. (2024). Quantum-Secured Data Centre Interconnect in a field environment. Journal of Surveillance, Security and Safety, 5(3), 184-197
[2] Damien Stucki et al., "Continuous high speed coherent one-way quantum key distribution," Opt. Express 17, 13326-13334 (2009)



5 June 2023

Singapore data centres exchange quantum-safe encrypted files

CQT through the National Quantum-Safe Network supports quantum key distribution trial with ST Telemedia Global Data Centres

QUANTUM ENGINEERING PROGRAMME SINGAPORE · NUS National University of Singapore · CQT Centre for Quantum Technologies · NANYANG TECHNOLOGICAL UNIVERSITY SINGAPORE · Fraunhofer SINGAPORE · STTelemedia Global Data Centres · NetLinkTrust the fibre of a smart nation