Measuring Quantum Key Distribution (QKD) Dependability via Wide Area Network Fault Injection

Audrey Feng and Dr. Phuong Cao | National Center for Supercomputing Applications, University of Illinois Urbana-Champaign

BACKGROUND

- Hybrid HPC-QC systems integrate quantum computers with classical supercomputing infrastructure; quantum networks are the principal element for secure communication in them
- White House mandating transition to post-quantum cryptography (PQC) by 2035 [1]
- BB84 QKD [2] enables Alice and Bob to create a shared encrypted key, with eavesdropping detectable via quantum mechanics
- Experiments conducted on QFabric [3], built on the NSF FABRIC testbed [4] (Figure 1), which goes over a real WAN link

QFabric is uniquely suited for studying simultaneous classical and quantum fault interactions

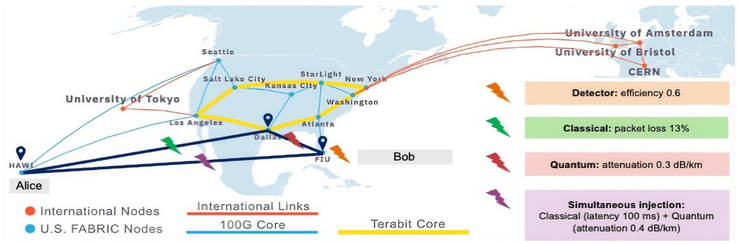


Figure 1. Fault injection points on the FABRIC testbed infrastructure. Adapted from Baldin et al [4]

PROBLEM STATEMENT

- Systematic studies of quantum networks remain limited despite their increasing importance
- Existing simulators assume ideal conditions, ignoring real-world faults (latency, jitter, packet loss) that affect protocol behavior
- In real deployments, classical channel faults may compromise the authentication of the sifting channel, an additional security risk not captured by single-layer fault injection
- Documented failures like the 2021 AWS congestion event [8] and 2026 Cloudflare BGP route leak [9] show classical infrastructure faults are a real deployment risk
- Existing fault injection studies only inject faults at a single layer, failing to capture compounding effects of simultaneous multi-layer faults

RELEVANCE TO CRYPTOGRAPHICALLY RELEVANT QUANTUM COMPUTERS (CRQC)

- A cryptographically relevant quantum computer (CRQC) [12] could break RSA/ECC within roughly a decade
- "Harvest now, decrypt later" [1] incentivizes moving to quantum-safe cryptography now, not later
- QKD and PQC are often deployed together in hybrid systems; faults in QKD's classical sifting channel can be exploited if not understood
- This work provides a framework for stress-testing QKD dependability before large-scale deployment

METHOD

- We conduct experiments on QFabric, deployed on the NSF FABRIC testbed

Layer	Parameter	Range
Classical Network	Delay	10–200 ms
	Jitter	±20 ms
	Packet Loss	1–15%
Quantum Channel	Attenuation (α)	0.1–0.5 dB/km
	Distance (L)	1–100 km
	Polarization Fidelity (p_f)	0.8–1.0
Detector	Dark Count Rate	100–10,000 cps
	Efficiency	0.5–1.0

Table 1. Fault Injection Parameters Applied in Experiment.

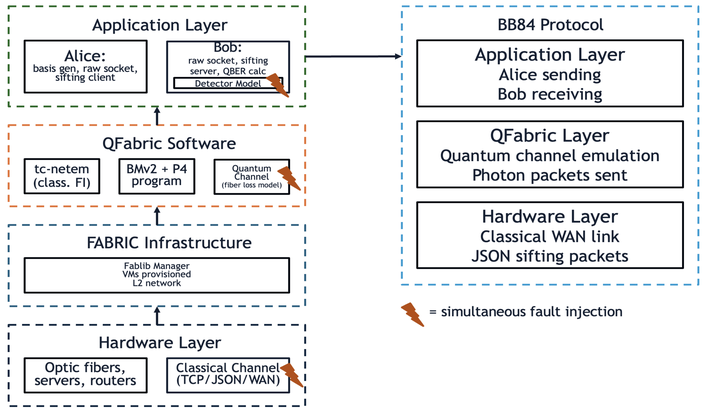


Figure 2. QFabric system architecture with fault injection design.

RESULTS

- Polarization fidelity determines QBER; packet loss doesn't interact with it ($F=699.6$, $p<10^{-58}$; interaction $p=0.35$)
- 25.8% of individual runs at marginal fidelity (pf=0.8) exceeded the 11% failure threshold from ordinary variance alone with no crossings at higher fidelity
- Detector efficiency shows no interaction with packet loss either, confirming the pattern is about fault mechanism (state-corrupting vs. photon-loss), not specific to one fault type

Even without interaction, operating near a fidelity boundary carries hidden per-run risk

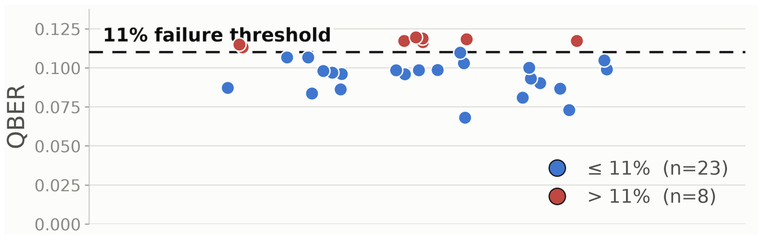


Figure 3. Individual-run QBER at marginal fidelity (pf=0.8, n=31), relative to the 11% BB84 failure threshold.

RESULTS

Cross-layer interaction in BB84 depends on the underlying physical mechanism, not a universal rule

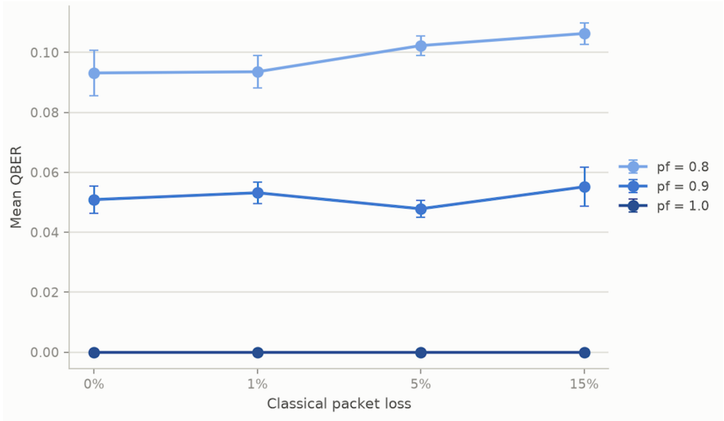


Figure 3. Mean QBER vs. classical packet loss

REFERENCES & ACKNOWLEDGEMENTS

[1] The White House, "National Security Memorandum on Promoting United States Leadership in Quantum Computing While Mitigating Risks to Vulnerable Cryptographic Systems," NSM-10, 2022.
[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *Theoretical Computer Science*, vol. 560, pp. 7–11, Dec. 2014.
[3] K. Thareja, "QFabric: Quantum network emulation on FABRIC (BB84 QKD over P4)," FABRIC Artifact Manager, 2026.
[4] I. Baldin et al., "FABRIC: A national-scale programmable experimental network infrastructure," *IEEE Internet Computing*, vol. 23, no. 6, pp. 38–47, 2019.
[5] X. Wu, A. Kolar, J. Chung, D. Jin, T. Zhong, R. Kettimuthu, and M. Suchara, "SeQUeNCe: a customizable discrete-event simulator of quantum networks," *Quantum Science and Technology*, vol. 6, no. 4, 2021.
[6] T. Coopmans, R. Knegjens, A. Dahlberg, et al., "NetSquid, a network simulator for quantum information using discrete events," *Communications Physics*, vol. 4, no. 1, 2021.
[7] L. Garms, T. K. Paraïso, N. Hanley, et al., "Experimental integration of quantum key distribution and post-quantum cryptography in a hybrid quantum-safe cryptosystem," *Advanced Quantum Technologies*, vol. 7, no. 4, 2024.
[8] Amazon Web Services, "Summary of the AWS service event in the US-East-1 region," 2021. [Online]. Available: https://aws.amazon.com/message/12721/
[9] Cloudflare, "Route leak incident on January 22, 2026," 2026. [Online]. Available: https://blog.cloudflare.com/route-leak-incident-january-22-2026/
[10] S. Hemminger, "Network emulation with NetEm," Linux.conf.au, 2005.
[11] M.-C. Hsueh, T. K. Tsai, and R. K. Iyer, "Fault injection techniques and tools," *Computer*, vol. 30, no. 4, pp. 75–82, 1997.
[12] National Institute of Standards and Technology, "Transition to post-quantum cryptography standards," NIST IR 8547, 2024.

This material is based upon work supported by the National Science Foundation under Grant No. 2430244, 2447843, 2530738, 2620473. Dr. Phuong Cao was partially supported by the NSF Grant No. 2537355. Audrey Feng was partially supported by the CRA-WP Distributed Research Experiences for Undergraduates (DREU) program. We thank the NCSA Computing Infrastructure directorate for supporting this work and the QFabric for their open source platform. We thank Dr. R. Srikant, Professor R.K. Iyer, Dr. Anita Nikolich, and Komal Thareja for this advising. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the funder.