ARIA
APPLIED RESEARCH IN ACTION

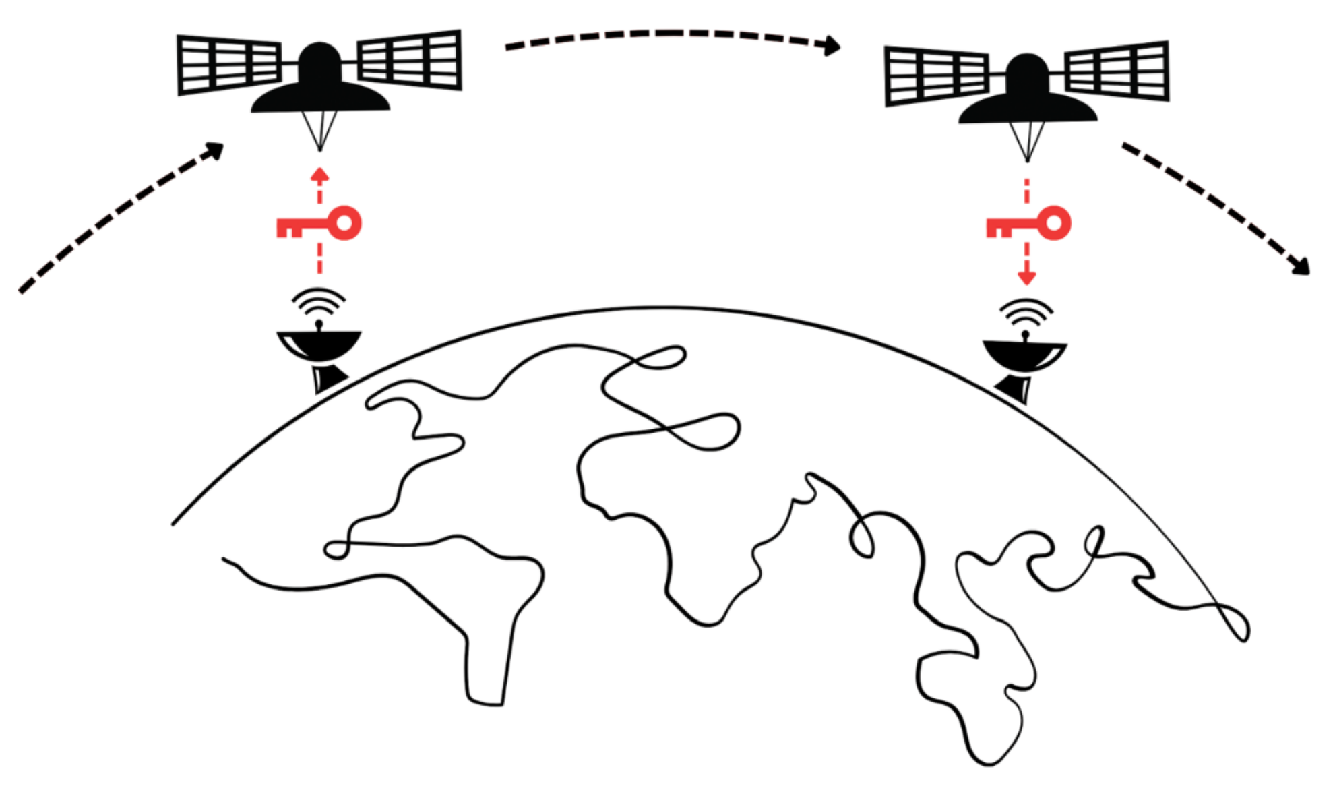
Advancing the Security of Commercial Quantum-Key-Distribution Systems

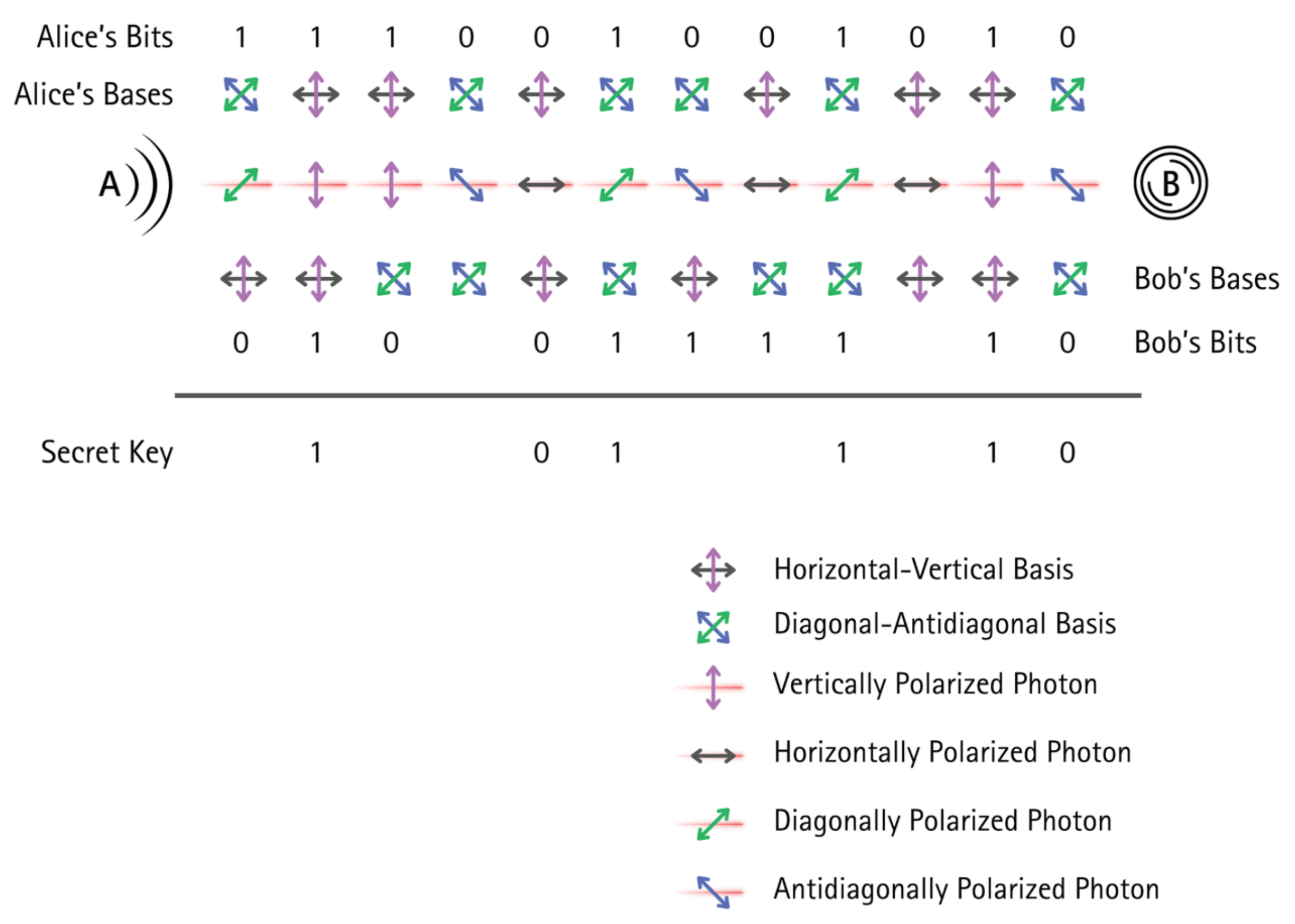
A Proactive Approach to Vulnerability Assessment and Resolution

Michael Luciuk

Dr. Li Qian
ACADEMIC SUPERVISOR

Cordell Grant, Dr. Jean-Philippe Bourgoin
INDUSTRY SUPERVISORS




Alice's Bits 1 1 1 0 0 1 0 0 1 0 1 0
Alice's Bases
A
B
Bob's Bases
Bob's Bits 0 1 0 0 1 1 1 1 1 0
Secret Key 1 0 1 1 1 0
Horizontal-Vertical Basis
Diagonal-Antidiagonal Basis
Vertically Polarized Photon
Horizontally Polarized Photon
Diagonally Polarized Photon
Antidiagonally Polarized Photon

PROJECT SUMMARY

Encryption is crucial for ensuring data privacy and data integrity. However, quantum computers threaten the traditional key distribution technologies underpinning modern encryption [1]. One solution is quantum-key-distribution (QKD), which is based on the laws of quantum mechanics [2]. Although QKD is theoretically secure [3], real-world implementations suffer numerous security vulnerabilities.

In this project, we proactively sought out and addressed vulnerabilities in QEYnet's commercial QKD transmitter. Potential vulnerabilities were identified from QKD literature, classical cryptography literature, and internal system design and test reports. Each of the identified vulnerabilities were then risk assessed for impact and exploitation feasibility and categorized accordingly.

Over the course of the project, we identified and risk assessed 19 security vulnerabilities. To date, comprehensive designs have been developed addressing 9 of the highest-risk vulnerabilities by means of opto-mechanical device modifications and increased privacy amplification. Preliminary paths to resolution have been identified for the remaining 10 vulnerabilities.

Our work builds upon a prior receiver-side security assessment conducted at QEYnet [4]. Together, these efforts represent the most comprehensive QKD security assessment to date and provide increased confidence in practical QKD technology and in QEYnet's capacity to deliver unbreakable security.

REFERENCES

[1] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," in Proceedings 35th Annual Symposium on Foundations of Computer Science, 1994, pp. 124–134. doi: 10.1109/SFCS.1994.365700.

[2] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," Theoretical computer science, vol. 560, no. 1, pp. 7–11, 2020, doi: 10.1016/j.tcs.2014.05.025.

[3] P. W. Shor and J. Preskill, "Simple proof of security of the BB84 quantum key distribution protocol," Physical review letters, vol. 85, no. 2, pp. 441–444, 2000, doi: 10.1103/PhysRevLett.85.441.

[4] J.-P. Bourgoin, private communication, 2021.

QEYnet

Computer Science
UNIVERSITY OF TORONTO

Master of Science in
Applied Computing