Quantum Hacking:
Computer-Simulated Attacks against the BB84 Protocol

Leo Crowder, Inès Montaño

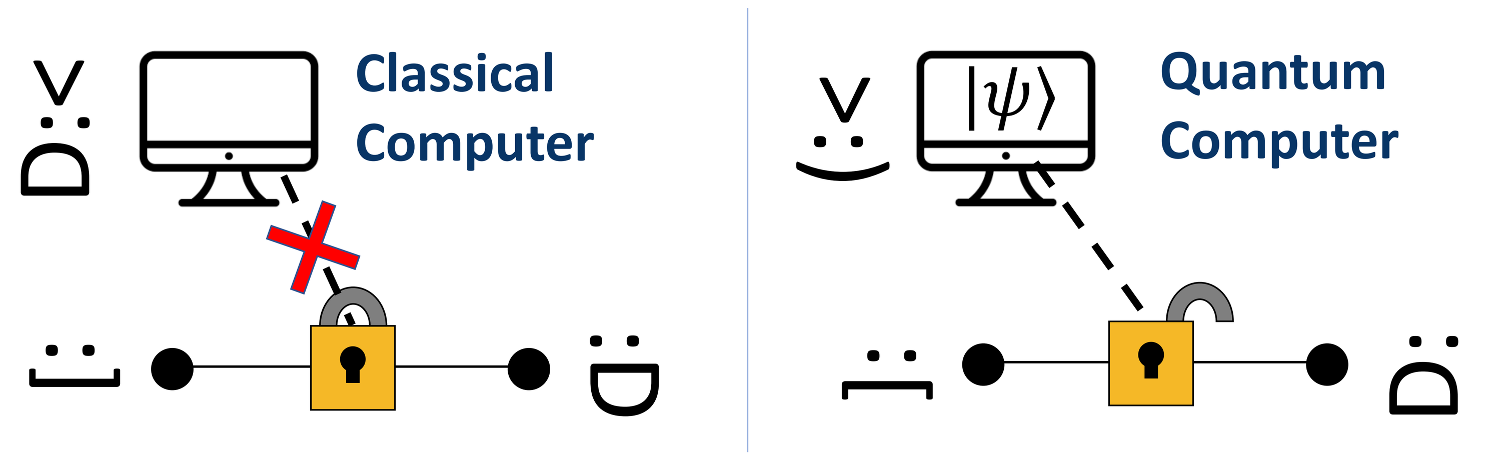
Applied Physics and Materials Science, Northern Arizona University

NAU NORTHERN ARIZONA UNIVERSITY
Office of Undergraduate Research and Creative Activity

Introduction

The Importance of Quantum Key Distribution

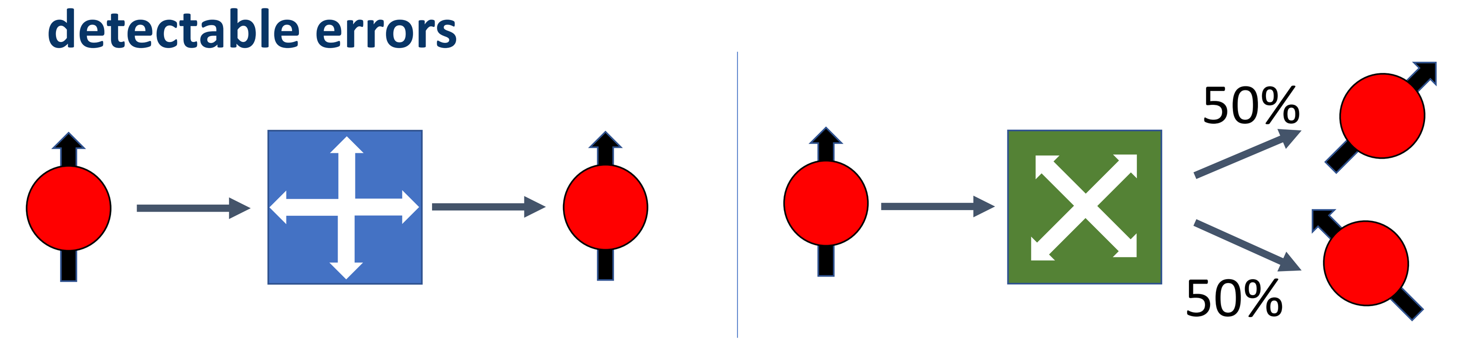
Common encryption protocols are **vulnerable** to quantum computers! (Shor's Algorithm)



Error-free BB84 and other QKD protocols are **secure** against attacks made possible by quantum computers.

What is BB84?

- Generate a cryptographic key using polarized quantum particles of light (photons).
- Eavesdropper's (Eve) attempts to learn the key will **induce detectable errors**



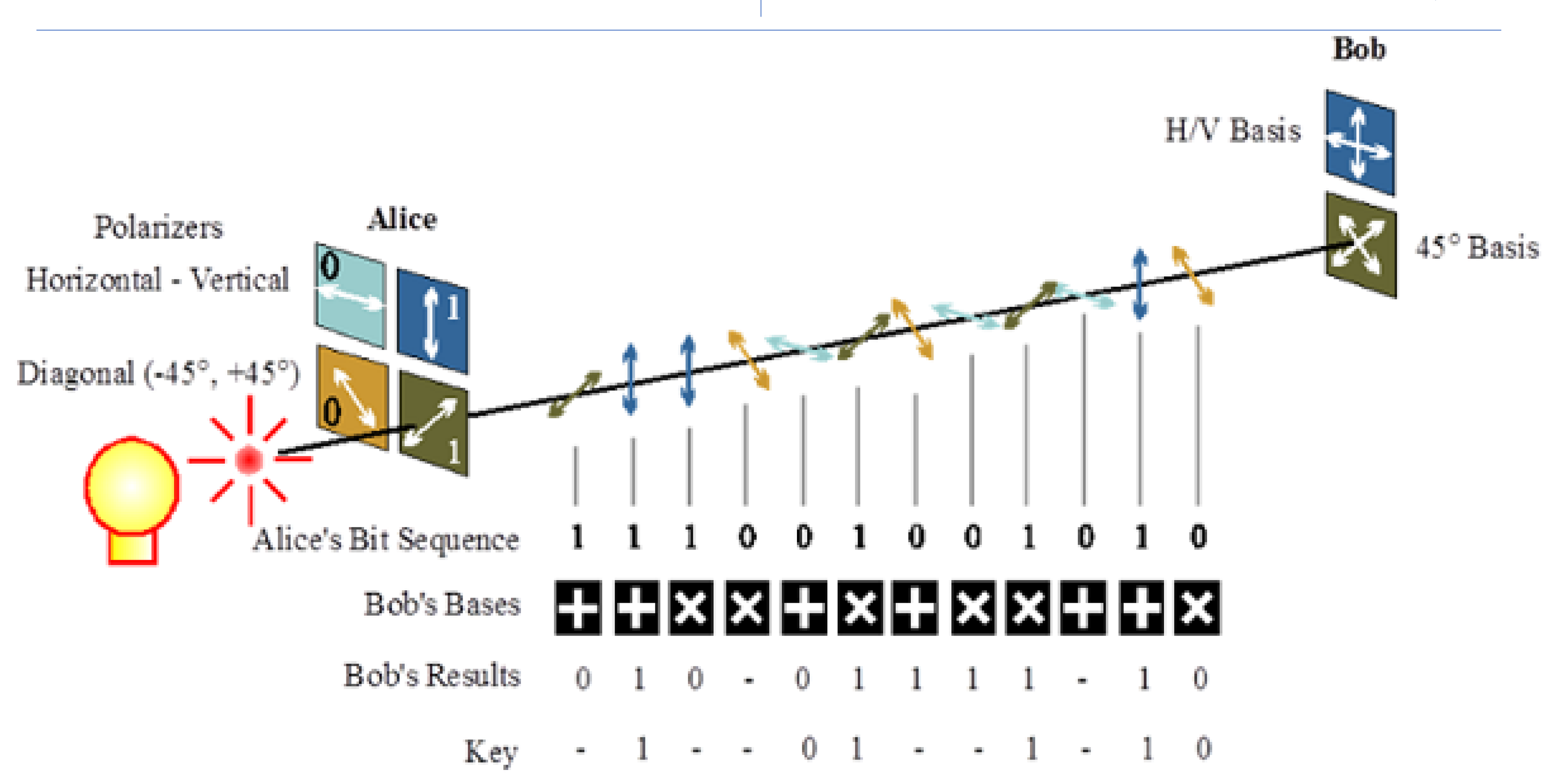
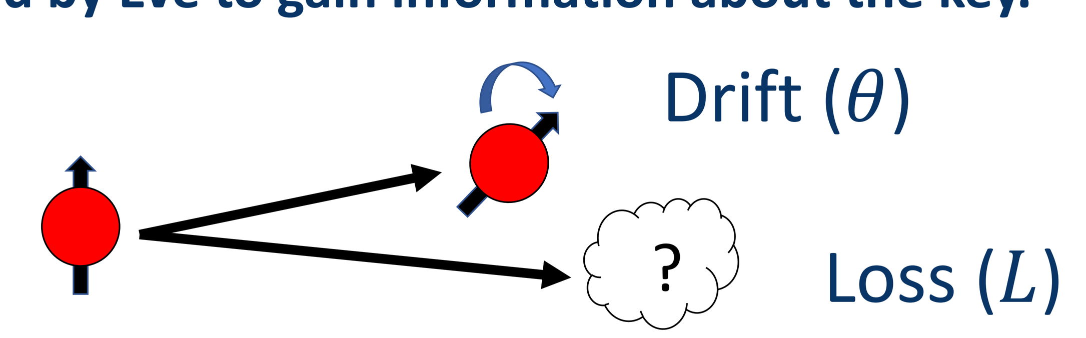


Figure 1: BB84 implementation using polarized photons

The Problem

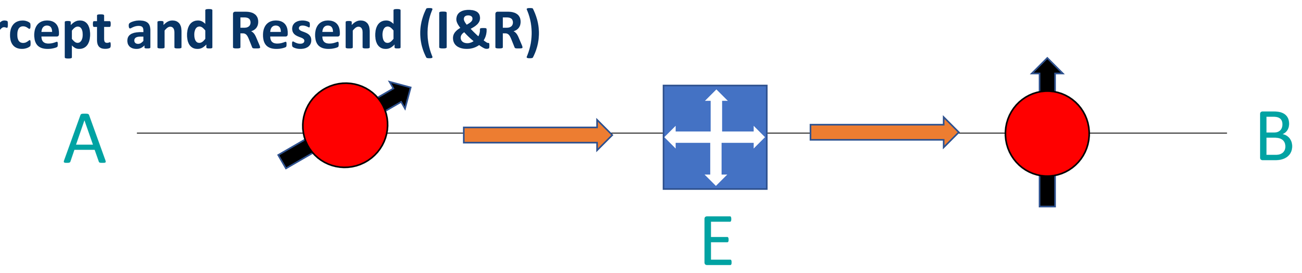
Practical implementation is prone to natural errors which can be **exploited by Eve to gain information about the key.**



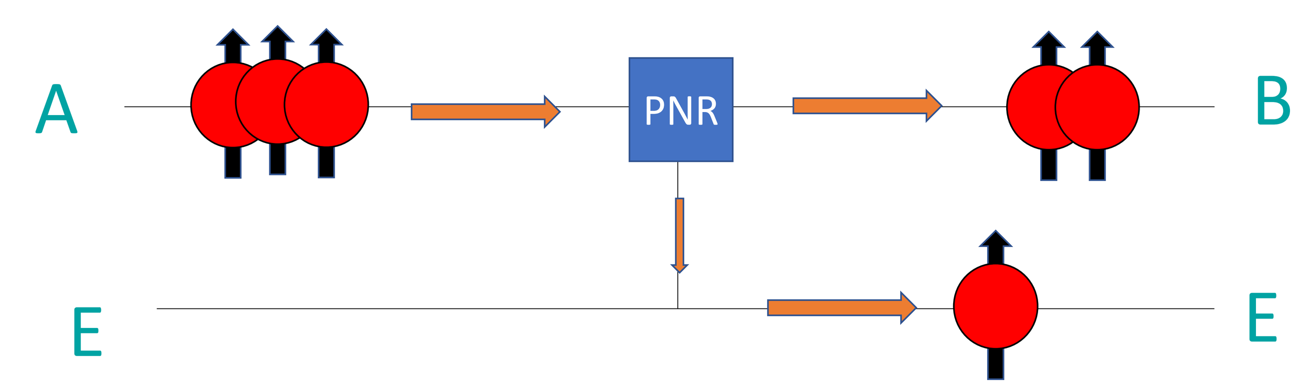
Methods

Attacks

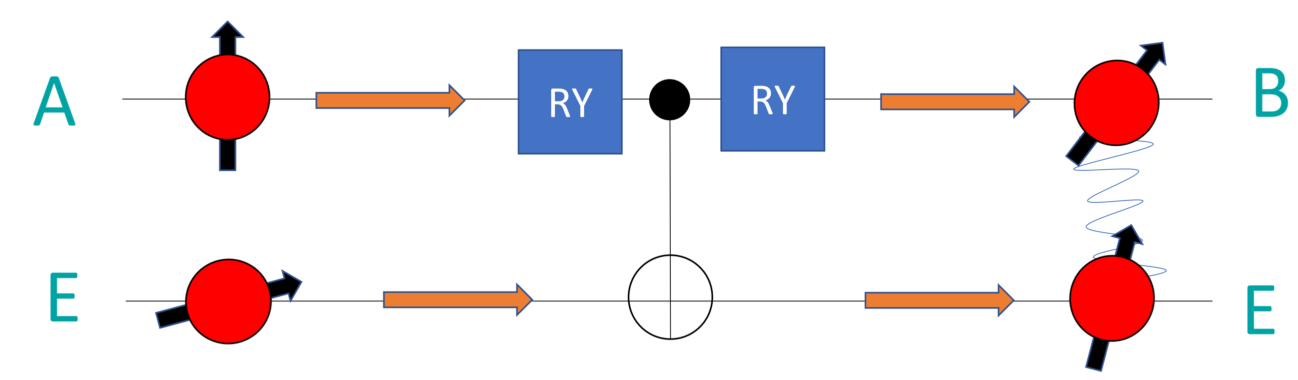
Intercept and Resend (I&R)



Photon-Number Splitting (PNS)



Slutsky-Brandt (SB)

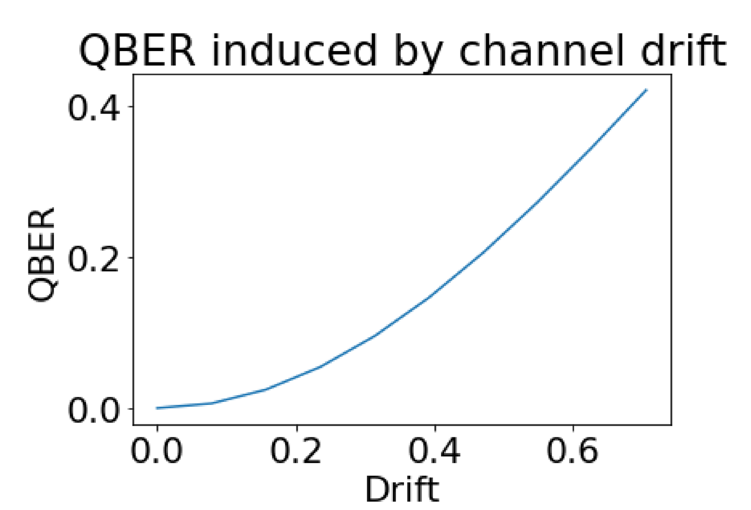


Strategy

Eve tries to gain as much information as possible while inducing **exactly** the expected $QBER$ and L to go undetected.

Channel-induced Errors = **Attack-induced Errors**

$$QBER = \sin^2\theta$$

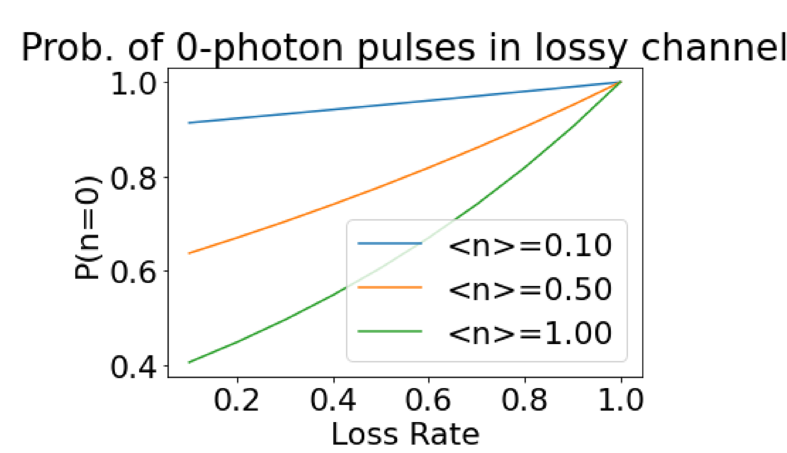


$$QBER_{I\&R} = 0.25$$

$$QBER_{SB} = \frac{S^2}{2}$$

*$|T_{in}\rangle = \frac{\sqrt{1-S^2}+S}{\sqrt{2}}|0\rangle + \frac{\sqrt{1-S^2}-S}{\sqrt{2}}|1\rangle$ is the input state of Eve's entangling probe

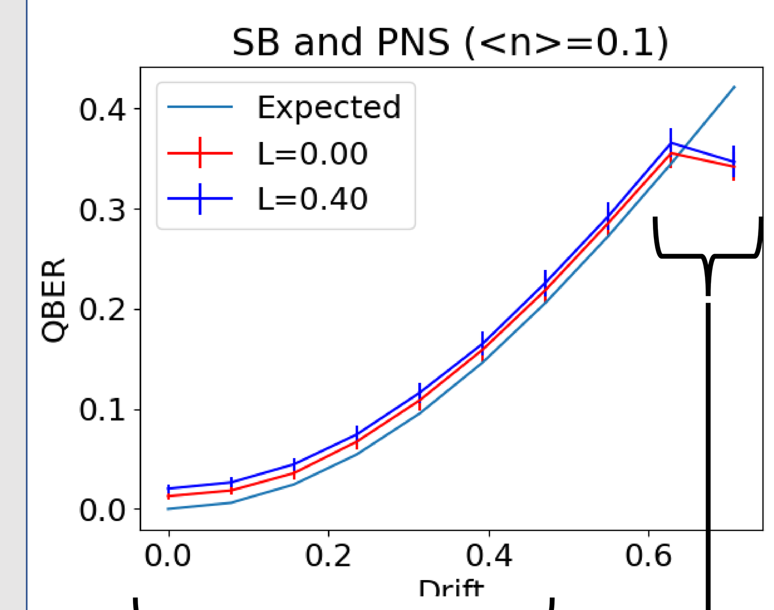
$$P(n=k) = \frac{(1-L)^k e^{-\langle n\rangle(1-L)}\langle n\rangle^k}{k!}$$

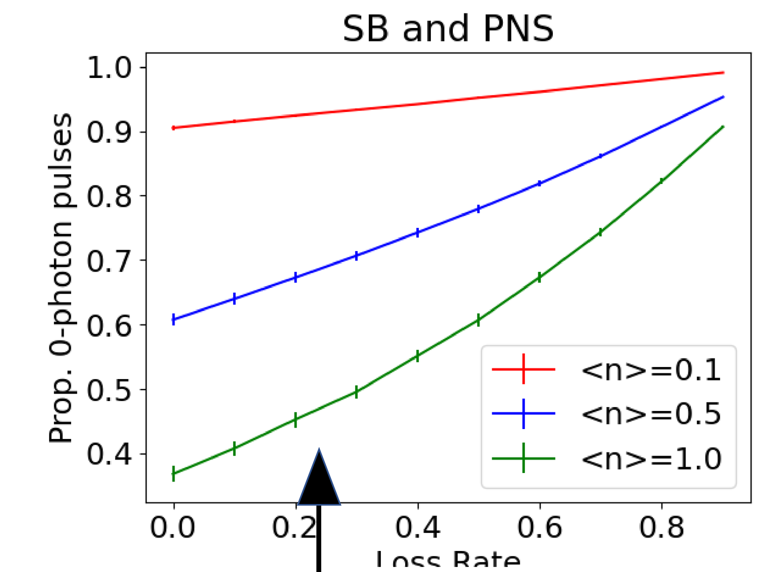


$$L_{PNS} = e^{-\langle n\rangle} + \sum_i P_i \frac{\langle n\rangle^i}{i!} e^{-\langle n\rangle}$$

*P_i =probability that Eve "blocks" a qubit with photon number i.

Results



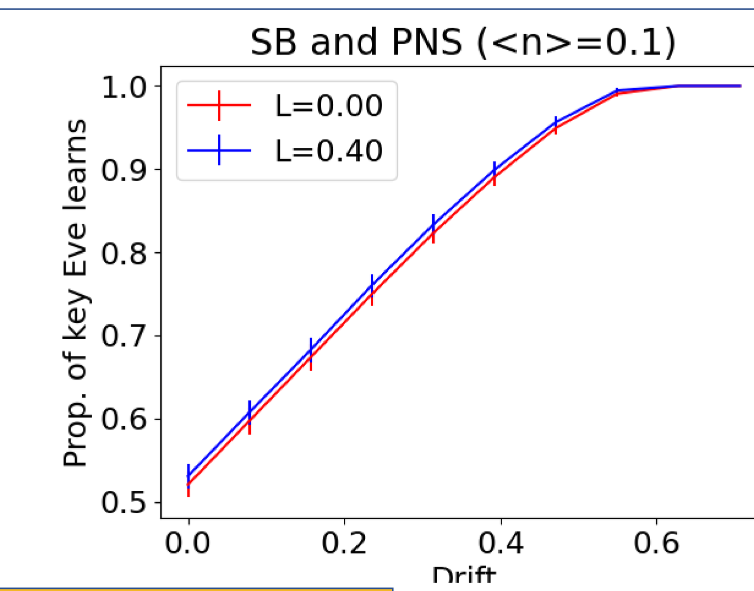


Attack-induced errors **closely match** expected channel errors

Curves match expected loss

Attack-induced errors begin to **deviate** from expected channel errors

Higher drift, loss, and mean photon number ⇒ Eve learns a larger portion of the key.



Conclusion

- Greater errors generally allow Eve to acquire more information.
- Eve's strategy **needs refinement:**
  - Her induced error closely (but not exactly) matches expected error.
  - Quickly diverges beyond $\theta \approx 0.6$
- The security of BB84 is **highly dependent** on the technology used to implement the protocol.
- Imperfect implementation of BB84 must be supplemented with procedures to prevent or detect potential eavesdropping.

References

–[1]Vasileios Mavroeidis, Kamer Vishi, Mateusz D. Zych and Audun Jøsang, "The Impact of Quantum Computing on Present Cryptography" International Journal of Advanced Computer Science and Applications(ijacsa), 9(3), 2018. http://dx.doi.org/10.14569/IJACSA.2018.090354
–[2]C.H. Bennett, G. Brassard: Quantum Cryptography, Public key distribution and coin tossing, Proc. Int. Conf. Computer Systems and Signal Processing, 175, Bangalore 1984
–[3]M Dušek, O Haderka, M Hendrych 1999 Optics Communications 169 103-108
–[4]Boris A. Slutsky, Ramesh Rao, Pang-Chen Sun, and Y. Fainman. Phys. Rev. A **57**, 2383 – Published 1 April 1998

Acknowledgements

This project would not be possible without funding and support through the Hooper Undergraduate Research Award.