Quantum Cryptography

Walter O. Krawec

University of Connecticut, Storrs CT.

walterkrawec.org
walter.krawec@uconn.edu

Our Research

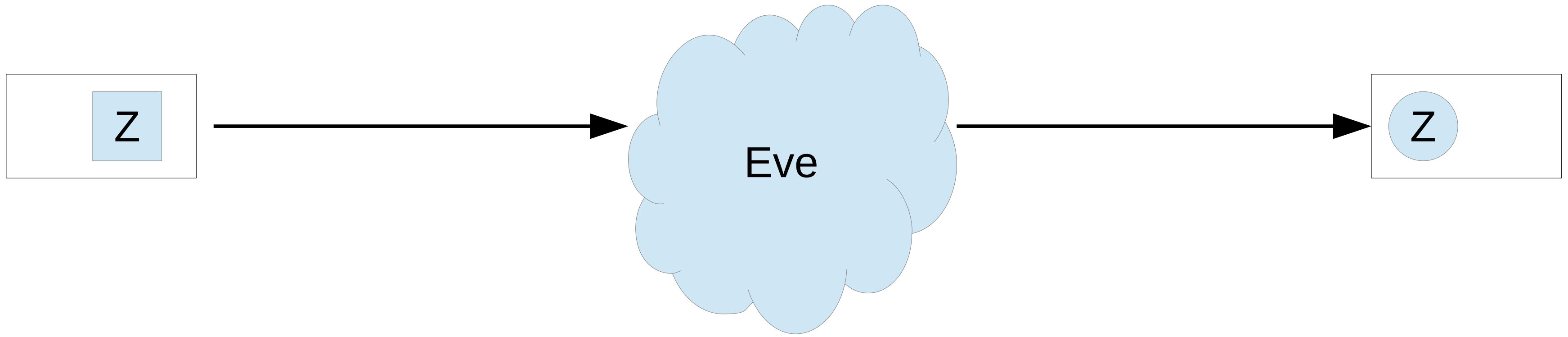
- The majority of QKD protocols require “quantum hardware”
  - Hardware capable of manipulating quantum resources in arbitrary ways
  - Can be very expensive, sensitive to noise
- Can we construct new protocols which require less quantum resources?
  - Cheaper
  - What if hardware breaks down?
  - What makes quantum communication secure?
- If so, how do we analyze their security and how do they compare?
  - Standard tools typically fail when analyzing these light-weight protocols

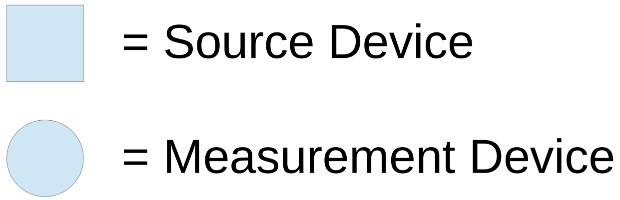
Our Research

- We construct new protocols showing only **very minimal** quantum capabilities are required
- Also, we develop **new proof methods** to bound the quantum min entropy as standard techniques often fail in these scenarios
  - New Entropic Uncertainty Relations

New Protocols

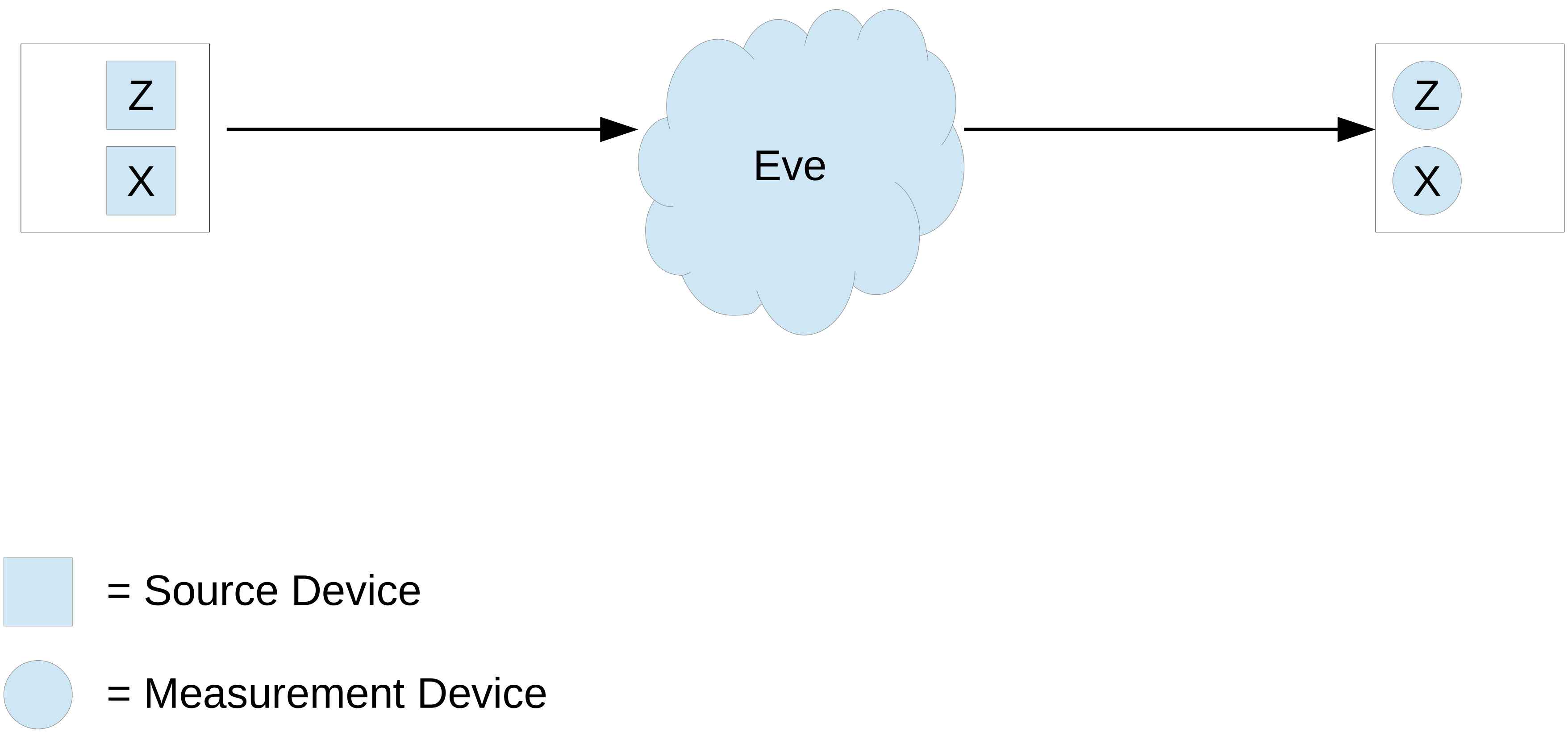
- If you only use one publicly known basis, no different than an (expensive) classical protocol:





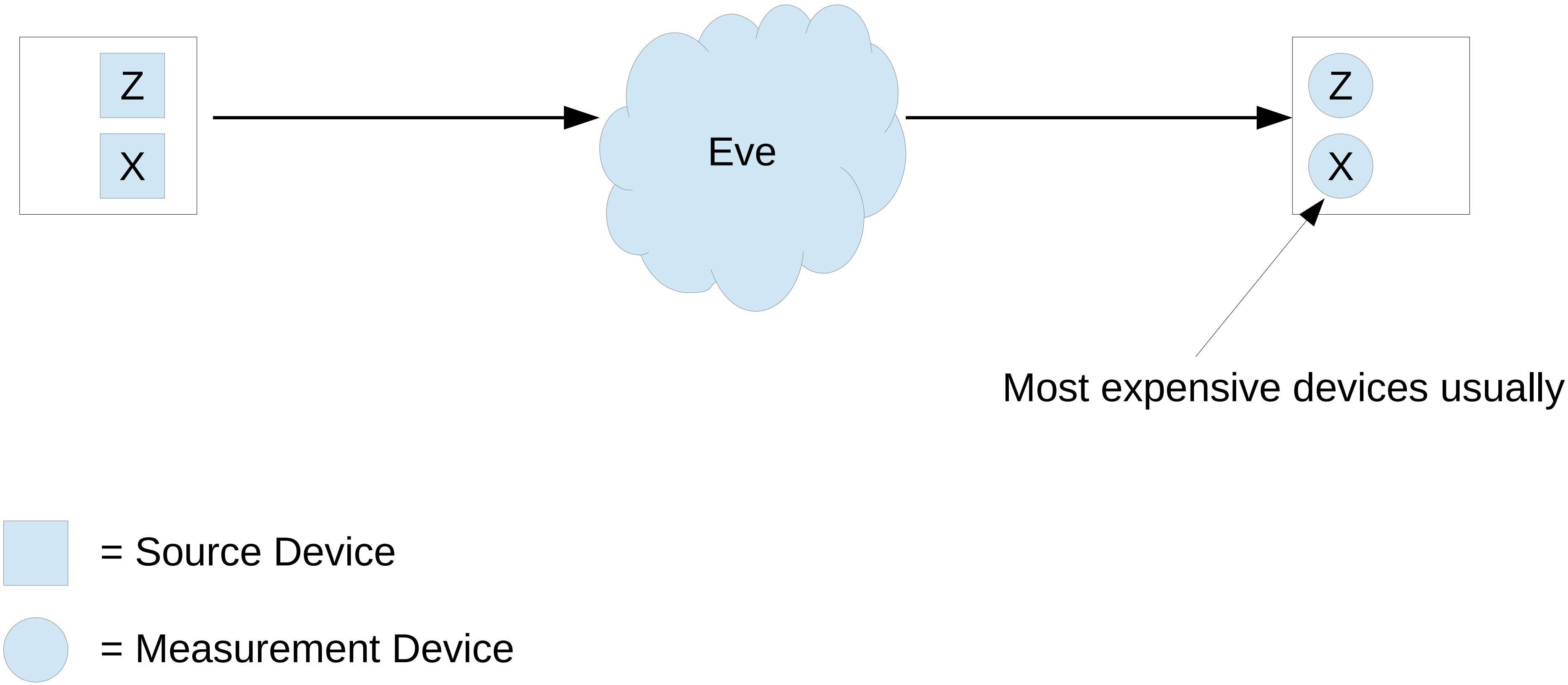
New Protocols

- Typical QKD Protocol:



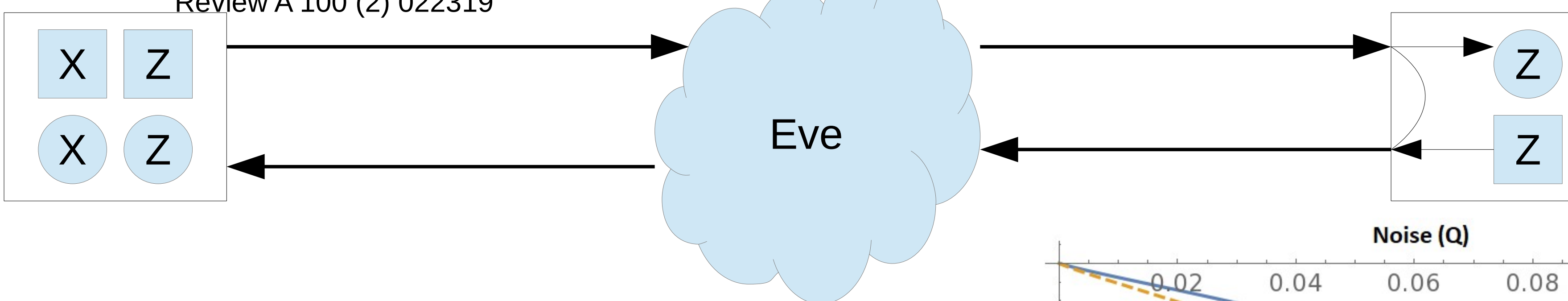
New Protocols

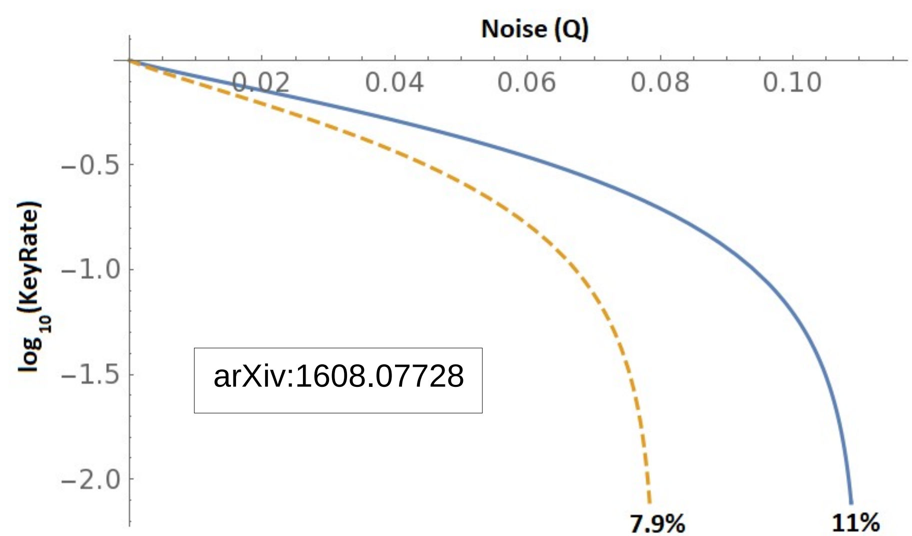
- Typical QKD Protocol:



Semi-Quantum Key Distribution

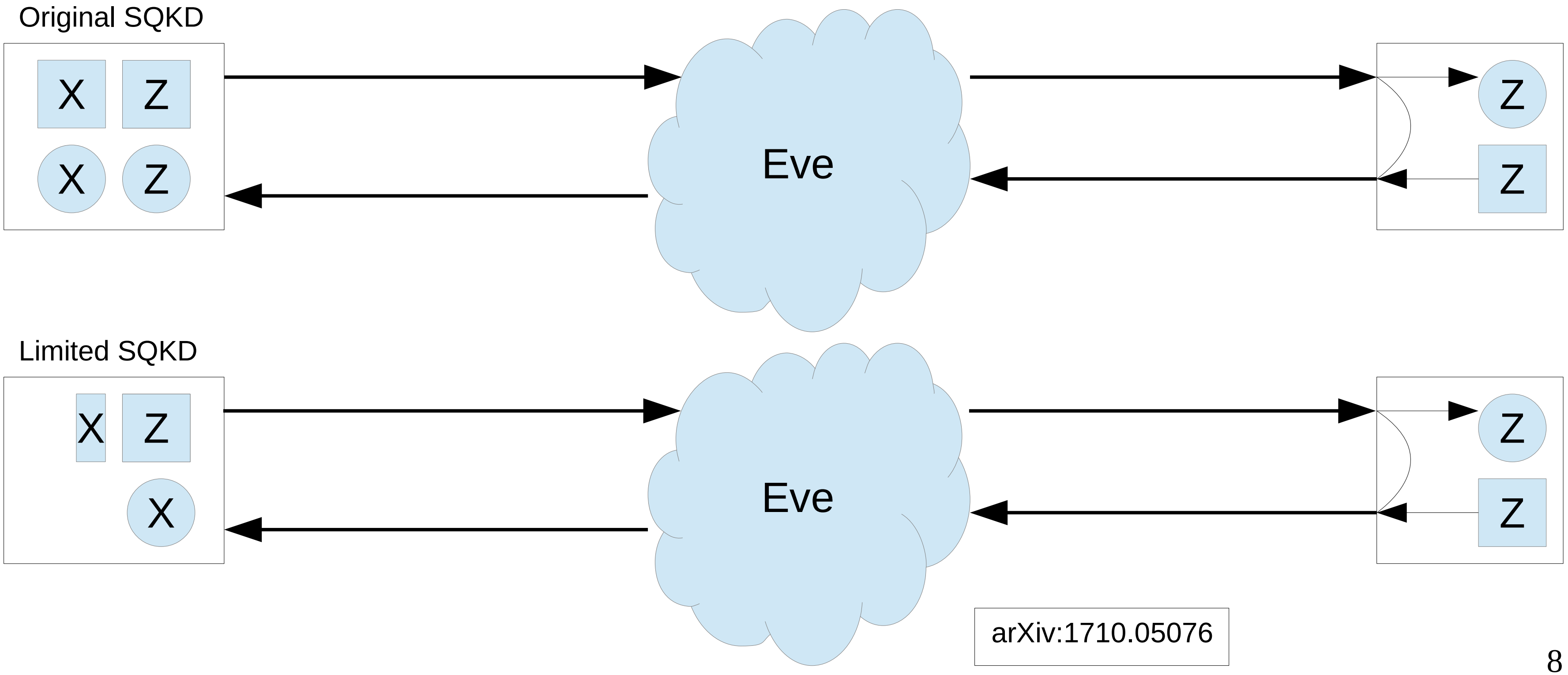
- Semi-quantum QKD
  - Introduced by Boyer et al. in 2007 PRL 99:140501
  - Survey: H. Iqbal, and W. O. Krawec. "Semi-quantum cryptography." Quantum Information Processing 19, no. 3 (2020): 1-52.
  - Analyzed in W.O. Krawec. Quantum Information & Computation 17 (3&4) pp. 209-241 arXiv:1608.07728
  - Improved in O. Amer and W.O. Krawec. Semi-Quantum Key Distribution with High Quantum Noise Tolerance. Physical Review A 100 (2) 022319





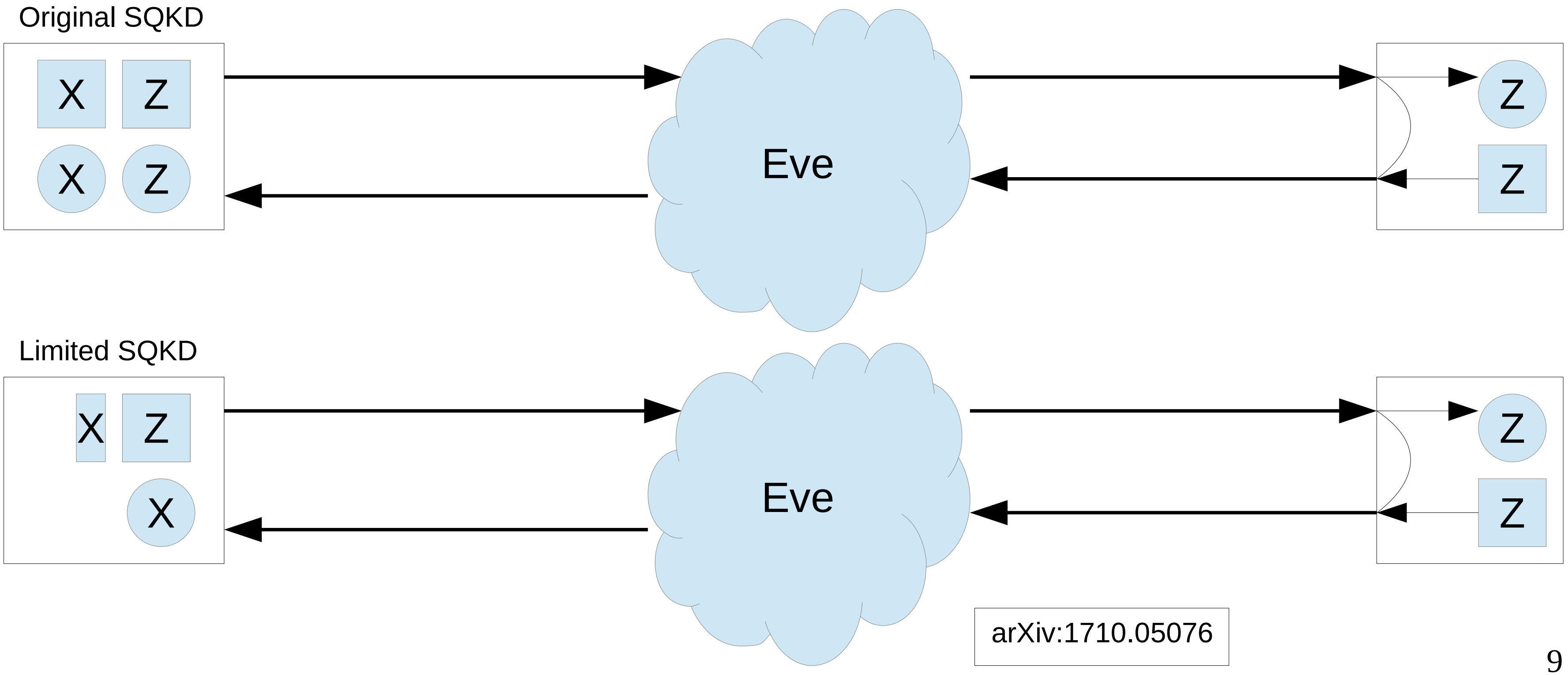
Semi-Quantum Key Distribution

- Semi-quantum QKD
  - It is possible to perform even fewer measurements+states
    (W.O. Krawec and E. Geiss. Semi-Quantum Key Distribution with Limited Measurement Capabilities Proc. International Symposium on Information Theory and Its Applications (ISITA), Singapore, 2018)



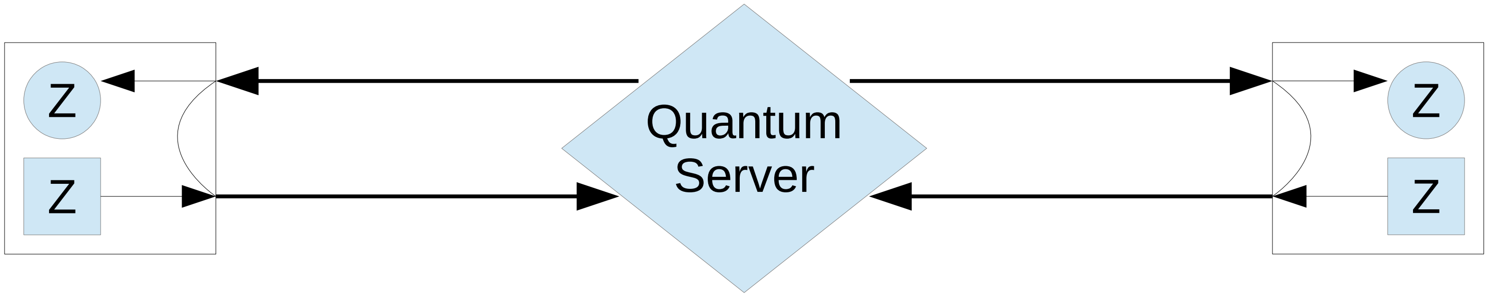
Semi-Quantum Key Distribution

- Semi-quantum QKD
  - It is possible to perform even fewer measurements+states
    (W.O. Krawec and E. Geiss. Semi-Quantum Key Distribution with Limited Measurement Capabilities Proc. International Symposium on Information Theory and Its Applications (ISITA), Singapore, 2018)
  - As secure as the original **only if you compensate with classical communication!**



SQKD

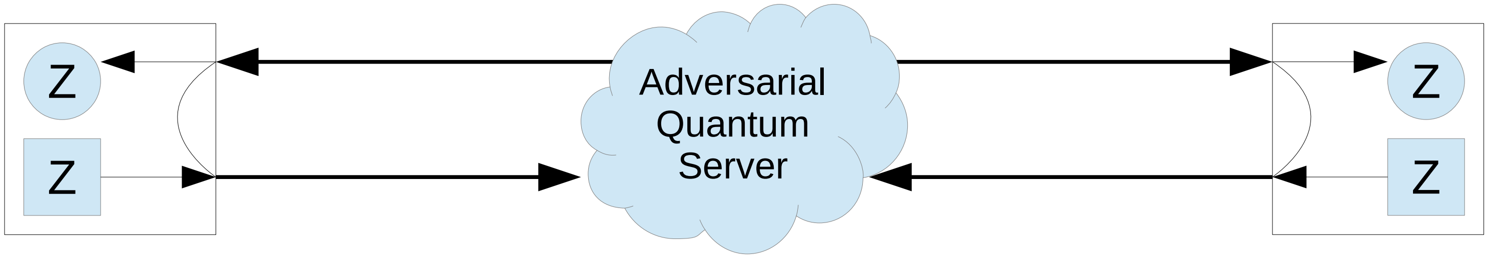
- But can both parties be restricted?
- Yes!
- **Mediated Semi-Quantum Key Distribution**



Krawec, W. O. (2015). Mediated semiquantum key distribution. Physical Review A, 91(3), 032323.

SQKD

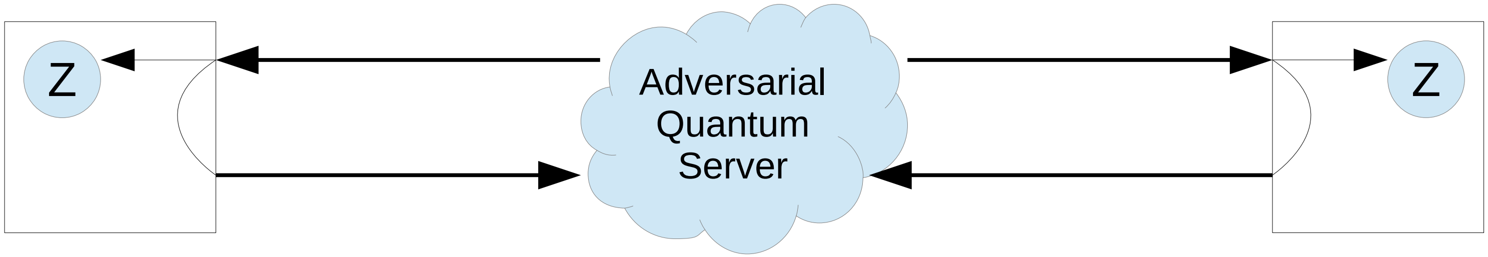
- But can both parties be restricted?
- Yes!
- **Mediated Semi-Quantum Key Distribution**
- Assumes the server is adversarial



Krawec, W. O. (2015). Mediated semiquantum key distribution. Physical Review A, 91(3), 032323.

SQKD

- But can both parties be restricted?
- Yes!
- **Mediated Semi-Quantum Key Distribution**
- Assumes the server is adversarial
- Recent work improves this:

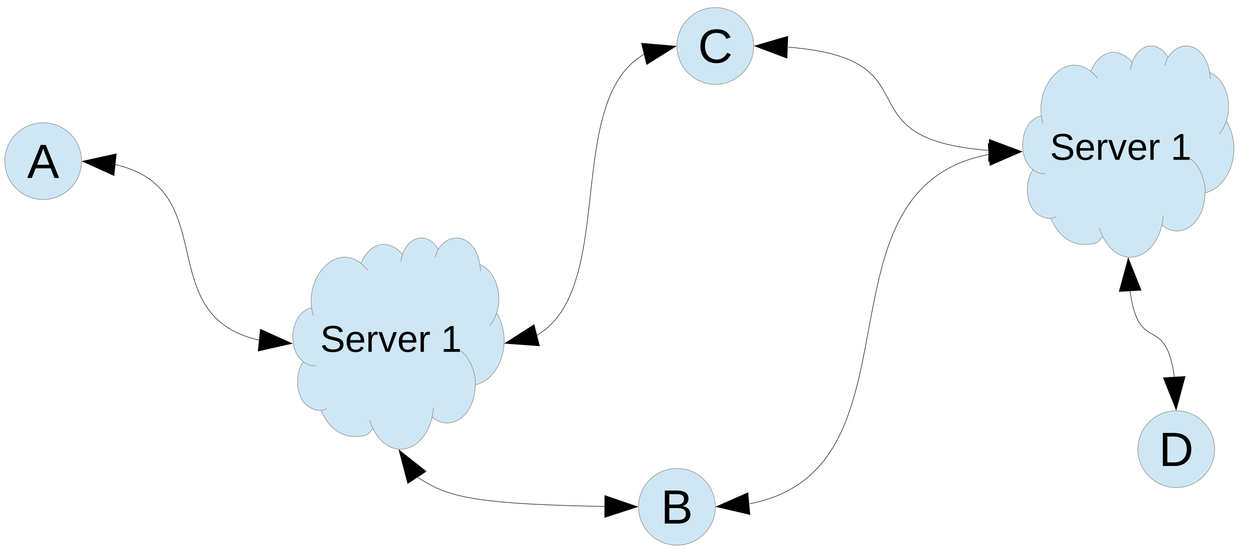


F. Massa, P. Yadav, A. Moqanaki, W. O. Krawec, P. Mateus, N. Paunkovic, A. Souto, and P. Walther.
Experimental Quantum Cryptography With Classical Users. pre-print available online: arXiv:1908.01780

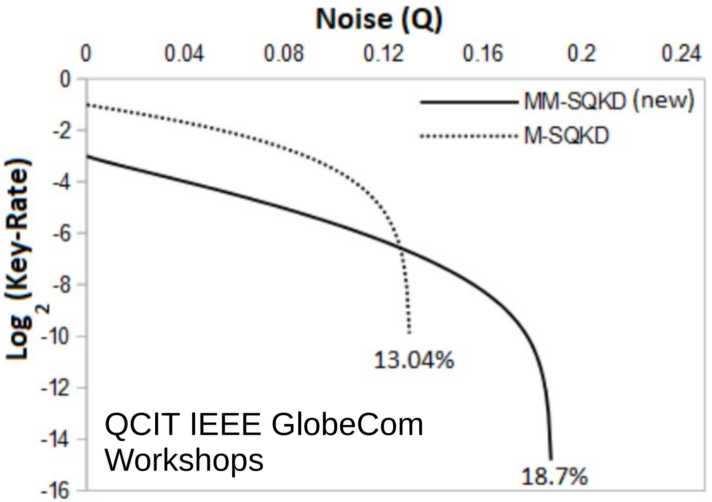
Our Protocol

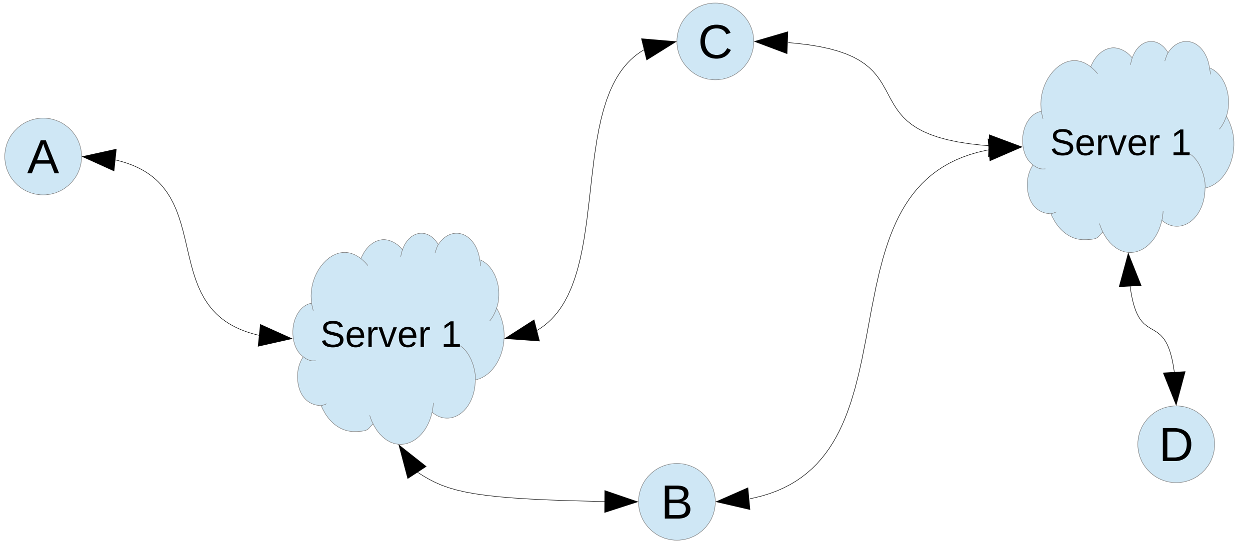
- We've shown that it is possible to experimentally implement these “limited resource” protocols
- We can show that the most important item is the **Server's Equipment (Detector and Source)**
- A and B can use much cheaper, poorly performing devices

- So, you can imagine the complex, expensive, devices being pushed to the servers while users only need really cheap poorly performing detectors



- Ability to use two servers also provides unique opportunities



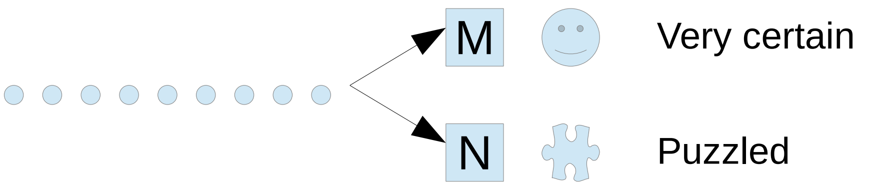


Security

Entropic Uncertainty

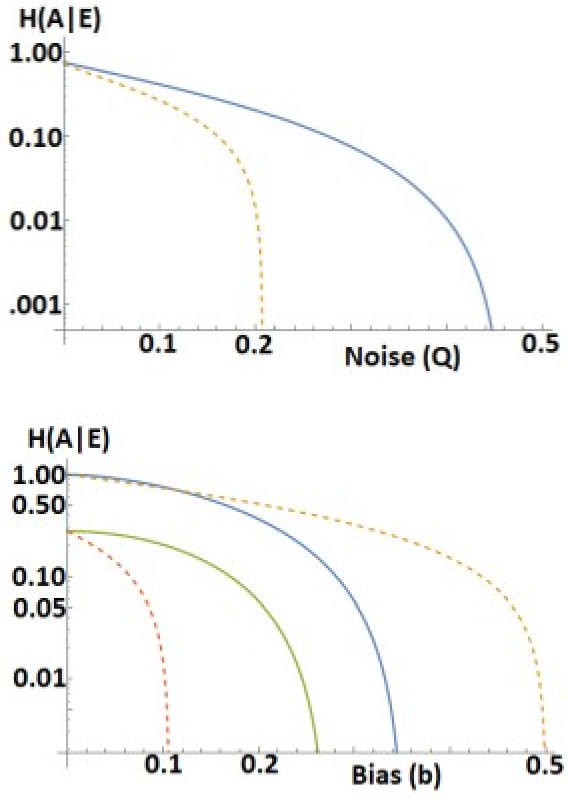
- Entropic Uncertainty Relations, informally, characterize our uncertainty of a quantum system undergoing different measurements

$$H(M)_\rho + H(N)_\rho \geq \gamma$$

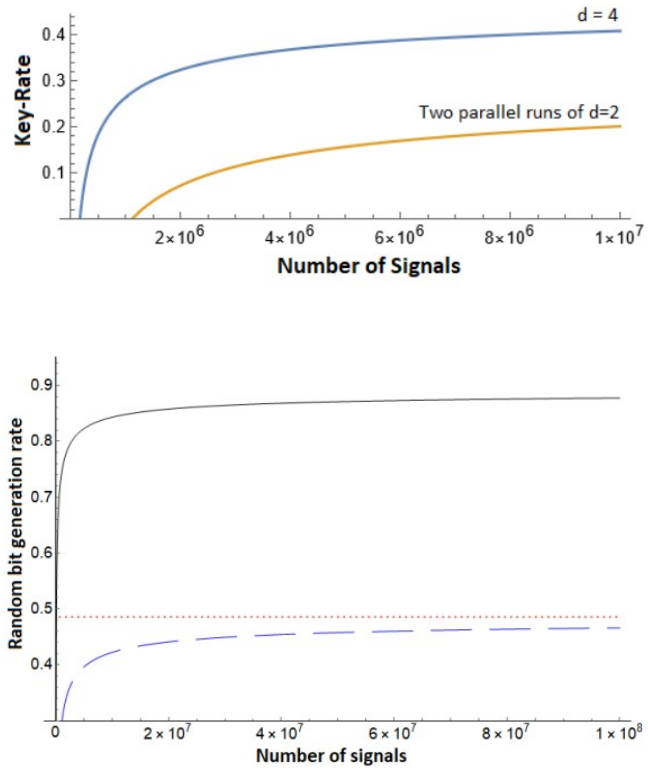


- Quantum Sampling: a framework introduced by Bouman and Fehr to translate classical sampling strategies to quantum sampling
- We recently showed how this framework can be used to discover novel entropic uncertainty relations
  - Our relations are easier to use in applications and often lead to better security results for limited-resource protocols

Entropic Uncertainty



Biased Measurements



High Dimensional Systems

Future Work

Closing Remarks

- We've shown, through this and other projects, that you really don't need a lot of “quantum” to get an advantage over classical.
- Fundamental questions of “how quantum” should a protocol be?
- New security techniques applicable to other (fully) quantum protocols
- Interesting connections showing how classical resources can overcome quantum limitations

Future Work

- Improving key-rates for biased measurements
  - Our current proof requires an assumption on the source, can this be removed?
- Looking at network scenarios with multiple servers and clients
  - What new protocols can be developed?
  - How can multi-servers be used effectively?
- Designing new (S)QKD protocols
  - What are the theoretical limits of weakly-quantum devices for cryptography?
  - Can new proof techniques be developed?
- Alternative cryptographic protocols beyond QKD
  - Certified deletion
  - Quantum Public Keys

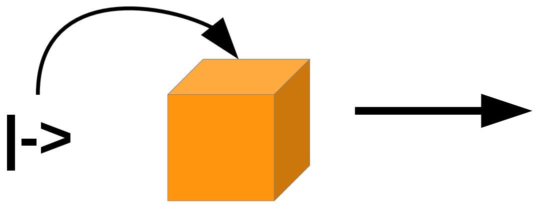
Thank you! Questions?

BB84: the idea

0 == { |0>, |+> }
1 == { |1>, |-> }

Alice **Eve** **Bob**

```
Key-bit = 1
Basis   = X
```



0 == { |0>, |+> }
1 == { |1>, |-> }

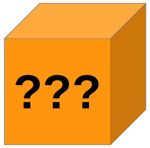
0 == { |0>, |+> }
1 == { |1>, |-> }

Alice

Key-bit = 1
Basis   = X

Eve

Key-guess = ?
Basis = ???
Basis-Guess = Z



Bob

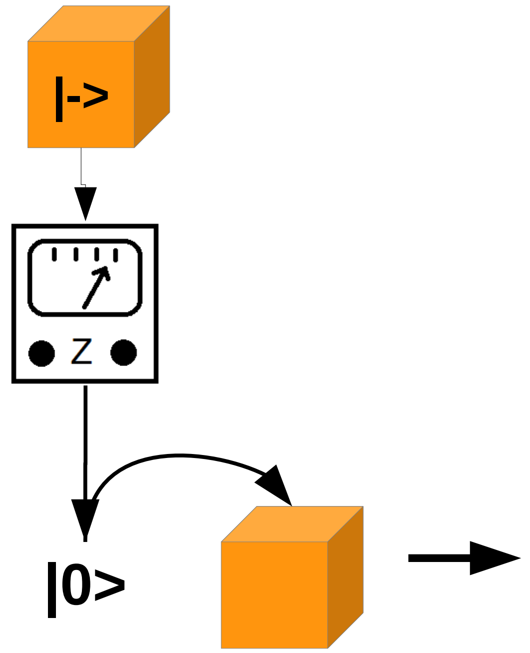
0 == { |0>, |+> }
1 == { |1>, |-> }

0 == { |0>, |+> }
1 == { |1>, |-> }

Alice **Eve** **Bob**

```
Key-bit = 1
Basis   = X
```

```
Key-guess = 0
Basis = ???
Basis-Guess = Z
```



0 == { |0>, |+> }
1 == { |1>, |-> }

0 == { |0>, |+> }
1 == { |1>, |-> }

Alice

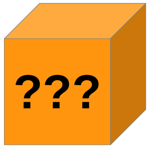
Key-bit = 1
Basis   = X

Eve

Key-guess = 0
Basis = ???
Basis-Guess = Z

Bob

Key-bit = ?
Basis   = ?



0 == { |0>, |+> }
1 == { |1>, |-> }

0 == { |0>, |+> }
1 == { |1>, |-> }

Alice

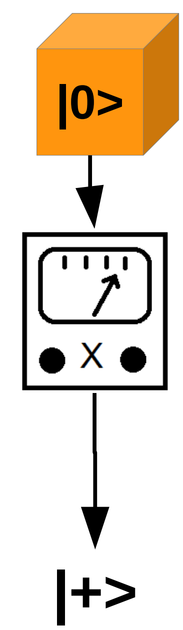
```
Key-bit = 1
Basis   = X
```

Eve

```
Key-guess = 0
Basis = X!
Basis-Guess = Z
```

Bob

```
Key-bit = 0
Basis   = X
```



0 == { |0>, |+> }
1 == { |1>, |-> }

0 == { |0>, |+> }
1 == { |1>, |-> }

Alice

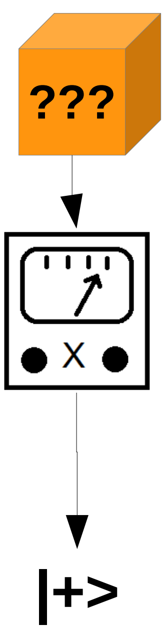
```
Key-bit = 1
Basis   = X
```

Eve

```
Key-guess = 0
Basis = X!
Basis-Guess = Z
```

Bob

```
Key-bit = 0
Basis   = X
```



Any attack induces errors in the quantum channel which A and B may detect!

Goal: Bound E's information gain as a function of this error rate.

0 == { |0>, |+> }
1 == { |1>, |-> }