Semi-Quantum Cryptography: Security Proofs and New Directions

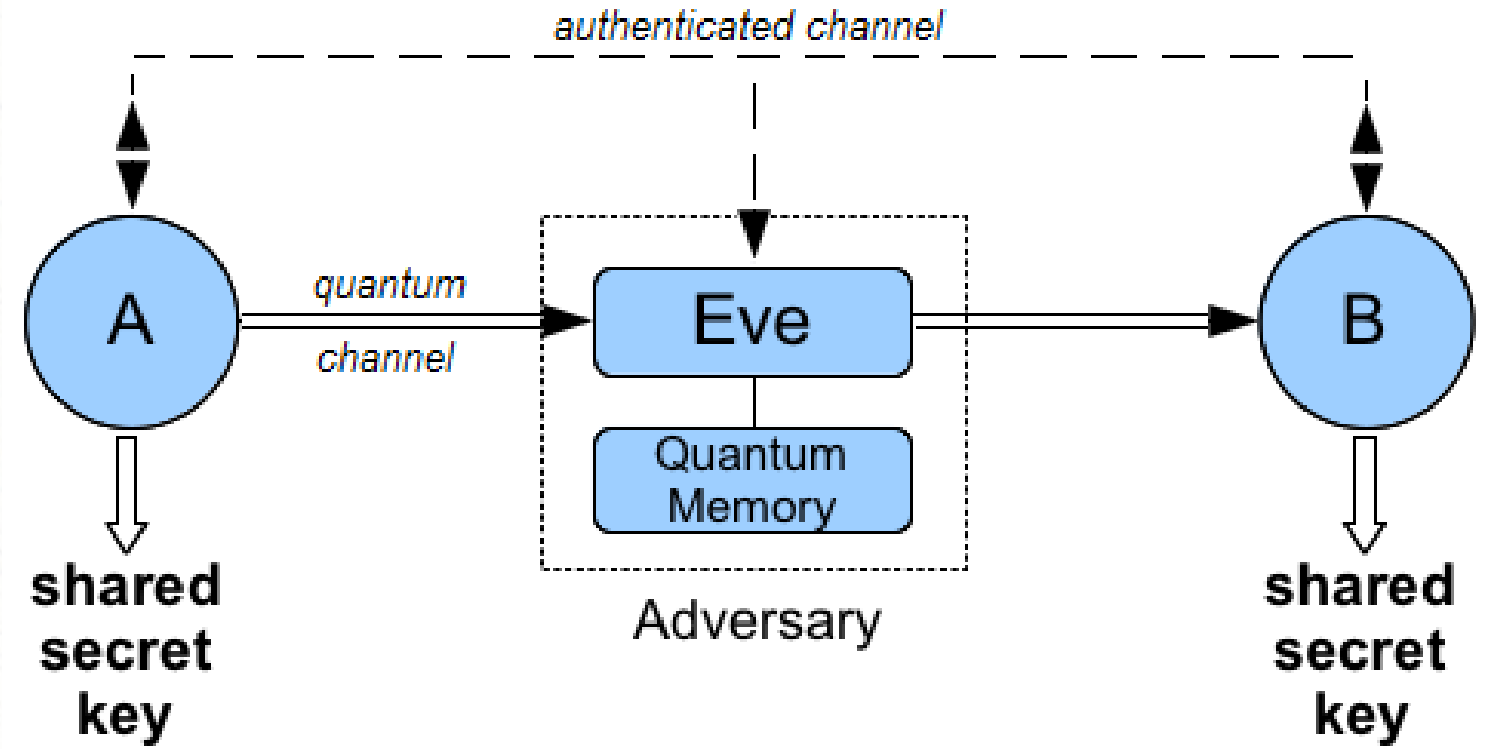
Walter O. Krawec

Iona College
CS Research Seminar
October 15, 2015

Quantum Key Distribution (QKD)

- Allows two users – Alice (A) and Bob (B) – to establish a shared secret key
- Secure against an all powerful adversary
  - Does not require any computational assumptions
  - Attacker bounded only by the laws of physics
  - Something that is not possible using classical means only
- Accomplished using a *quantum communication channel*

Quantum Key Distribution



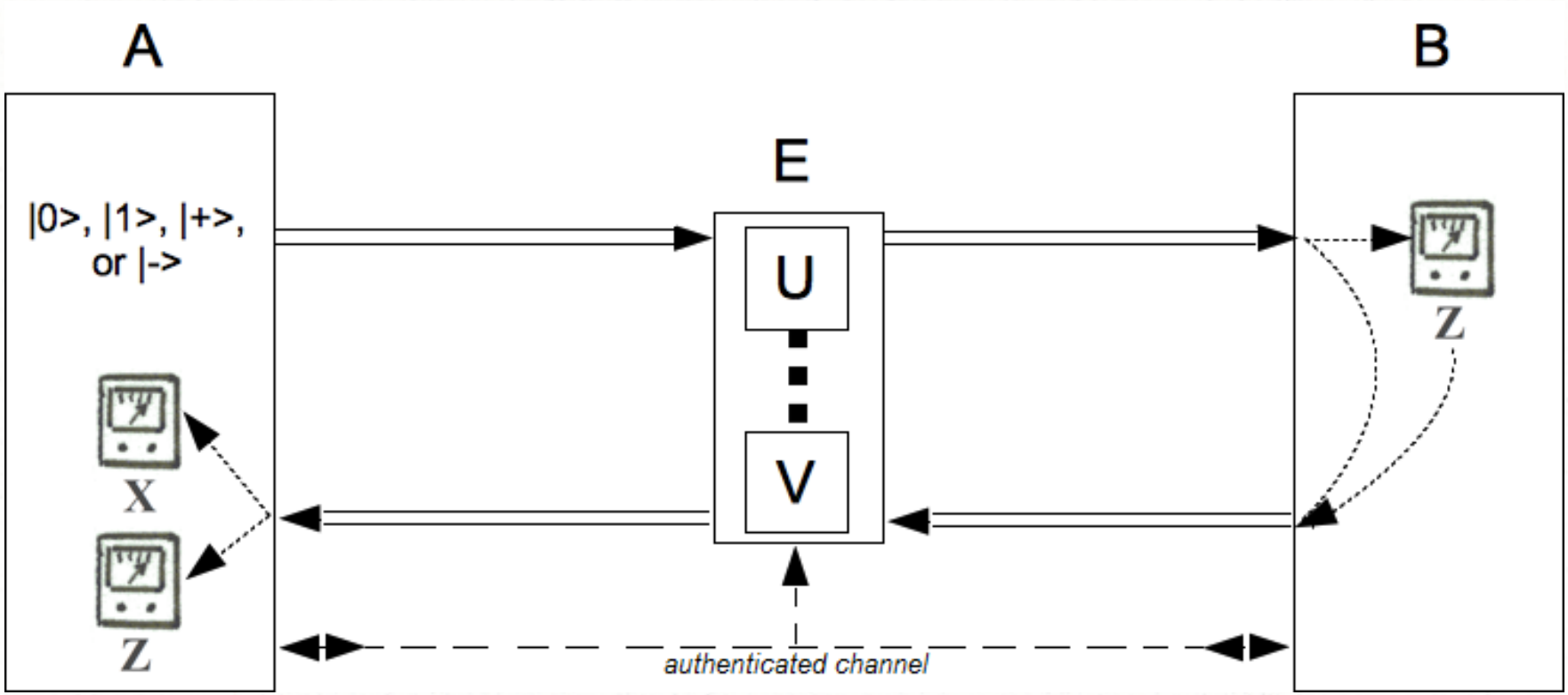
QKD in Practice

- Quantum Key Distribution is here already
- Several companies produce commercial QKD equipment
  - MagiQ Technologies in NY
  - id Quantique in Geneva
  - SeQureNet in Paris
  - Quintessence Labs in Australia
- Have also been used in various applications:
  - In 2007, QKD was used to transmit ballot results for national elections in Switzerland
  - Has also been used to carry out bank transactions

Semi-Quantum Key Distribution

- In 2007, Boyer et al., introduced *semi-quantum key distribution* (SQKD)
- Now Alice (A) is quantum
- But Bob (B) is limited or "classical"
- Theoretically interesting:
  - "How quantum does a protocol need to be in order to gain an advantage over a classical one?"
- Practically interesting:
  - B's "lab" may require less complicated hardware
- Requires a two-way quantum communication channel

Semi-Quantum Key Distribution



SQKD Security

- Prior to our work, there were many different SQKD protocols developed
- However, none were proven unconditionally secure
- Instead, only weak notions of security were proven
  - e.g., no correlation established between adversary information gain and disturbance
- Our work is the first to provide full security proofs for SQKD protocols using the state of the art definitions.
  - We developed a set of mathematical tools that may be used to prove security

Background

Bits vs. Qubits

- Classical Bits:
  - May be 0 or 1
  - Can be read at any time
  - Can be copied
- Quantum Bits (*qubits*)
  - May be |0>, |1>, or a *superposition* of both
  - Reading a qubit (called measuring) can destroy it and produce random output
  - Cannot copy a qubit

Qubits

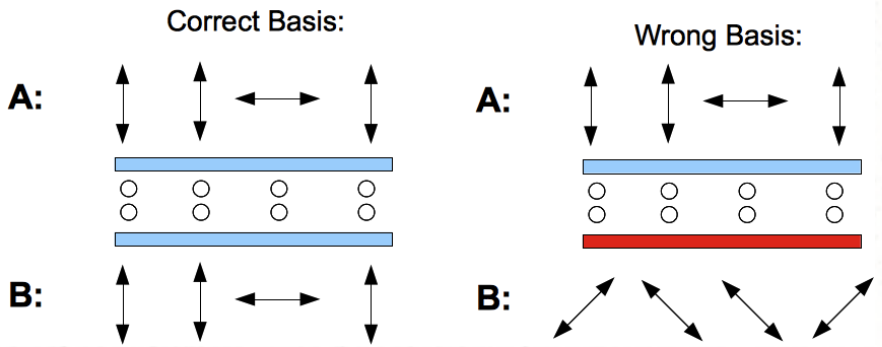
- Qubits are modeled mathematically using a two-dimensional complex vector space
- Thus, any arbitrary qubit is:

$$|q\rangle = \begin{pmatrix} a \\ b \end{pmatrix}$$

- Here, a and b are complex numbers
- Normalized: $|a|^2 + |b|^2 = 1$

Preparing and Measuring

- Many ways to send (*prepare*) a qubit
  - May prepare using any orthonormal basis of C^2
- Many ways to read (*measure*) a qubit
  - May read in any orthonormal basis of C^2
- If you prepare and measure in the same basis, result is deterministic
- Otherwise it is random and original qubit "collapses" to the observed state



Bases

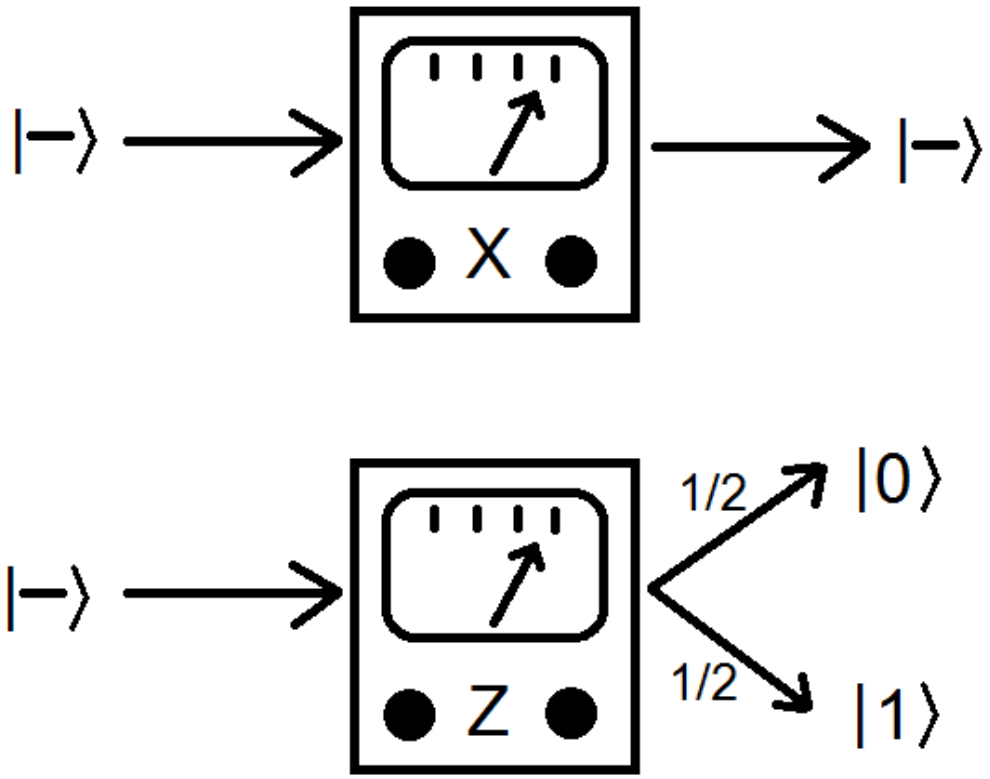
- Two important (orthonormal) bases we will use are the *computational Z basis* and the *Hadamard X basis*:
  - Z = {|0>, |1>} X = {|+>, |->}

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \qquad |1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$|+\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \qquad |-\rangle = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ -1 \end{pmatrix}$$

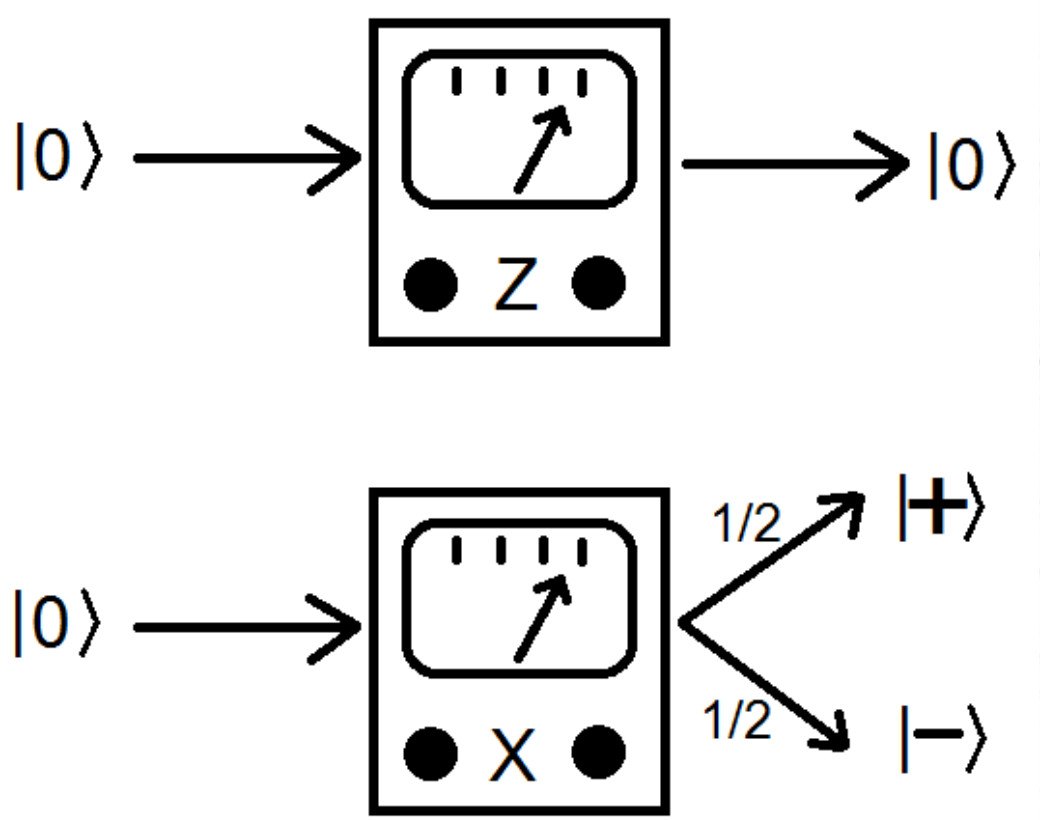
Measuring a Qubit

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



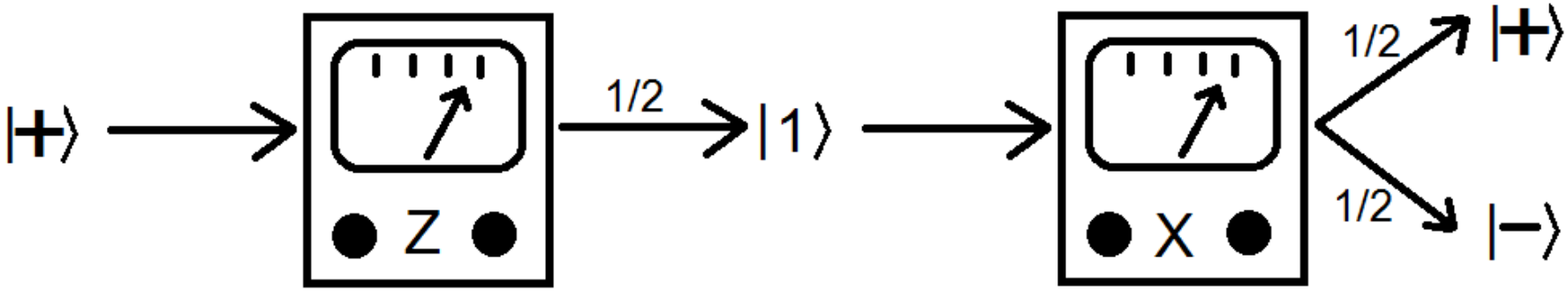
Measuring a Qubit

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



Measuring a Qubit

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



Quantum and Semi-Quantum Key Distribution

BB84 (Bennett and Brassard, 1984)

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

Alice

Key:	0	1	1	0
X or Z	Z	X	Z	Z
Qubit	|0>	|->	|1>	|0>

Bob

X or Z	Z	X	X	Z
Result	|0>	|->	|+>	|0>
Key	0	1	0	0

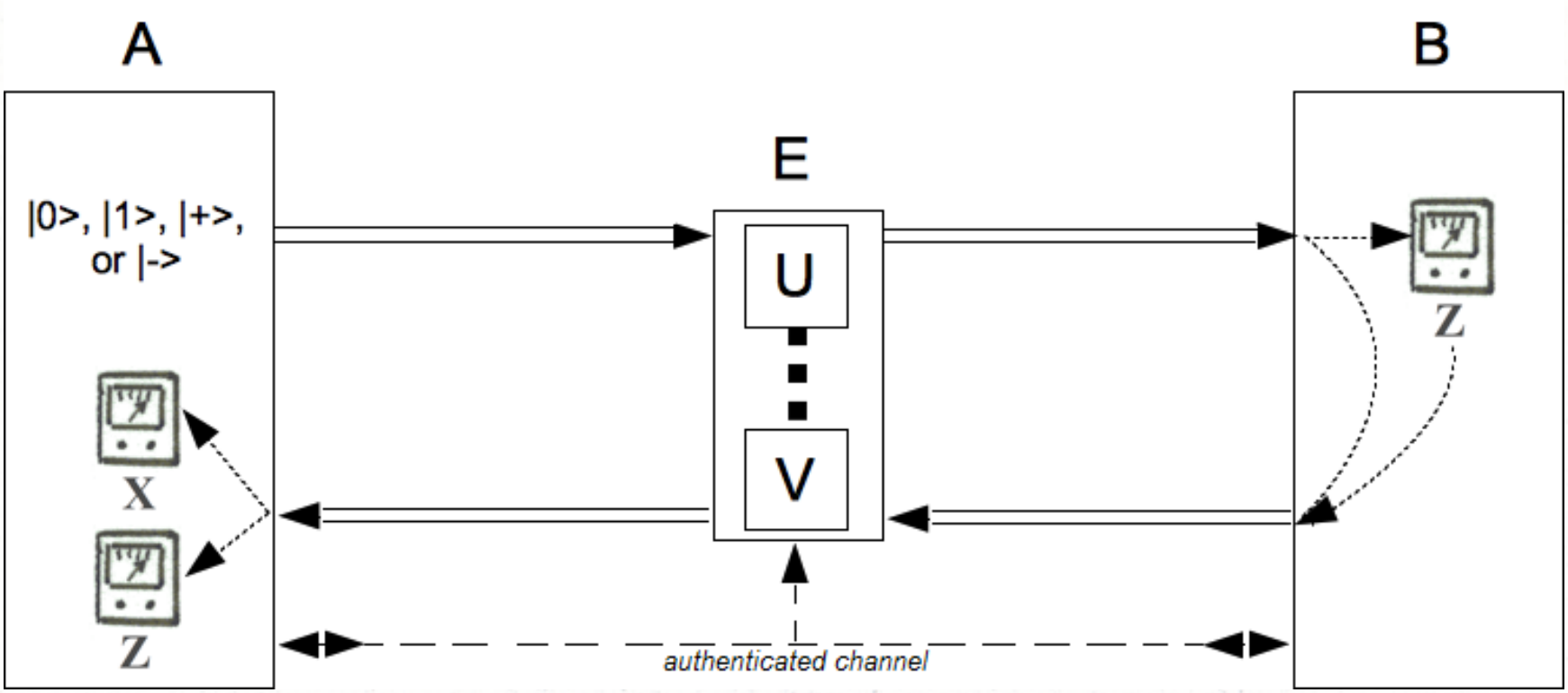
Use?	Y	Y	N	Y

- A picks a random key bit and basis; based on her choice she sends one of |0>, |1>, |+>, or |->.
- B picks a random basis Z or X and measures
- Using an *authenticated classical channel*, A and B inform each other of their basis choice
- If they use the same basis, they use this iteration to contribute towards their *raw key*
- A and B the run an *Error Correcting* protocol and a *Privacy Amplification* protocol

Other QKD Protocols

- Several other QKD protocols have been developed including:
  - Six-state BB84 (Bennett et al., 1984)
  - Three-state BB84 (Fung and Lo, 2006)
  - SARG04 (Scarani, et al., 2004)
  - B92 (Bennett, 1992)
  - …
- These protocols have been analyzed extensively and we have good bounds on their security

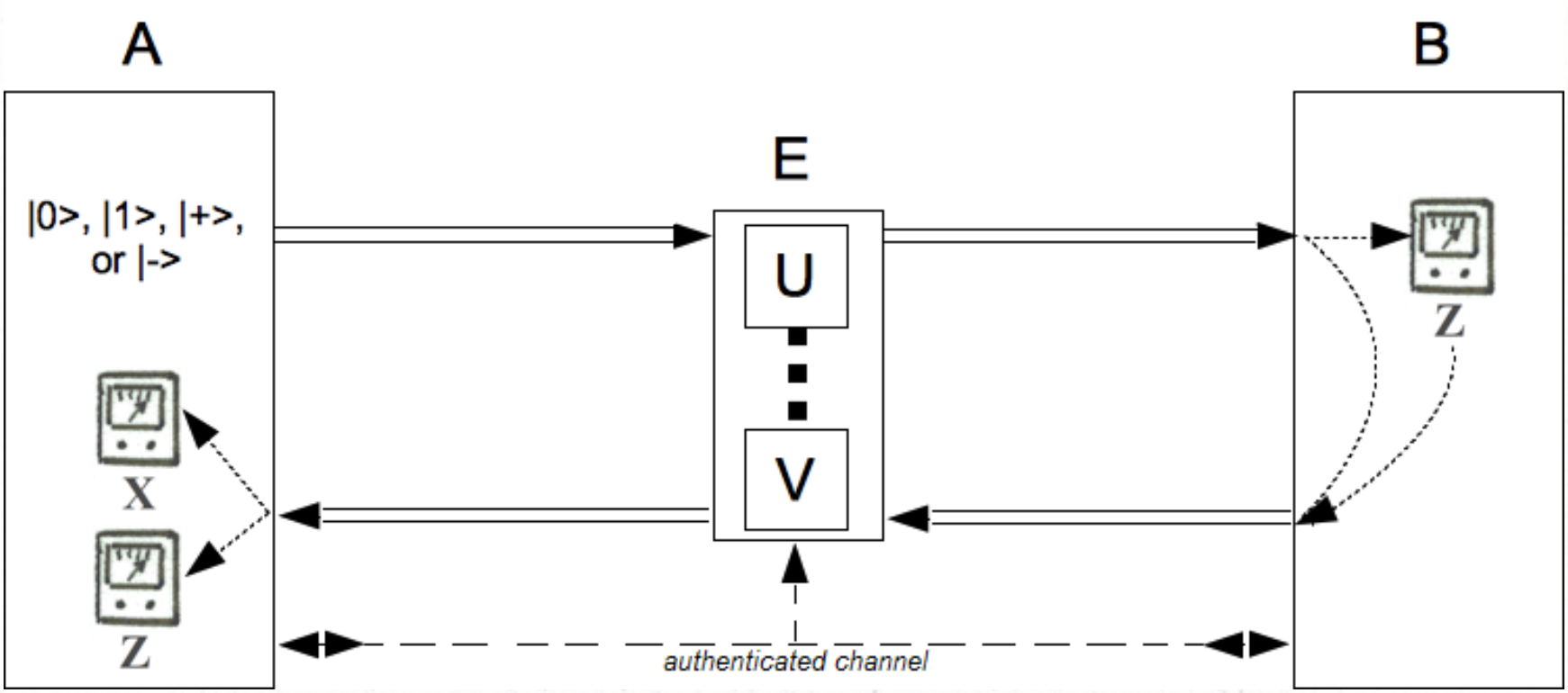
Semi-Quantum Key Distribution



Semi-Quantum Key Distribution: Classical Bob

- Semi-Quantum Key Distribution (SQKD), introduced in (Boyer et al., 2007) requires one of the users (typically Bob) to be *classical* or *semi-quantum*:
- B may **Measure and Resend**
  - The incoming qubit is measured in the Z basis
  - B then resends a qubit based on this result
  - e.g., if he measures |1>, he sends |1> back to A
- B may **Reflect**
  - The incoming qubit is ignored, and "bounced" back to A (B learns nothing about the qubit's state)
  - The qubit leaves B's lab undisturbed

Semi-Quantum Key Distribution



Example: (Zou et al. 2009)'s protocol

Alice

Qubit	|+>	|+>	|+>	|+>

Bob

M or R	M	R	R	M
Result	|0>	N/A	N/A	|1>
Output	|0>	|+>	|+>	|1>

Alice

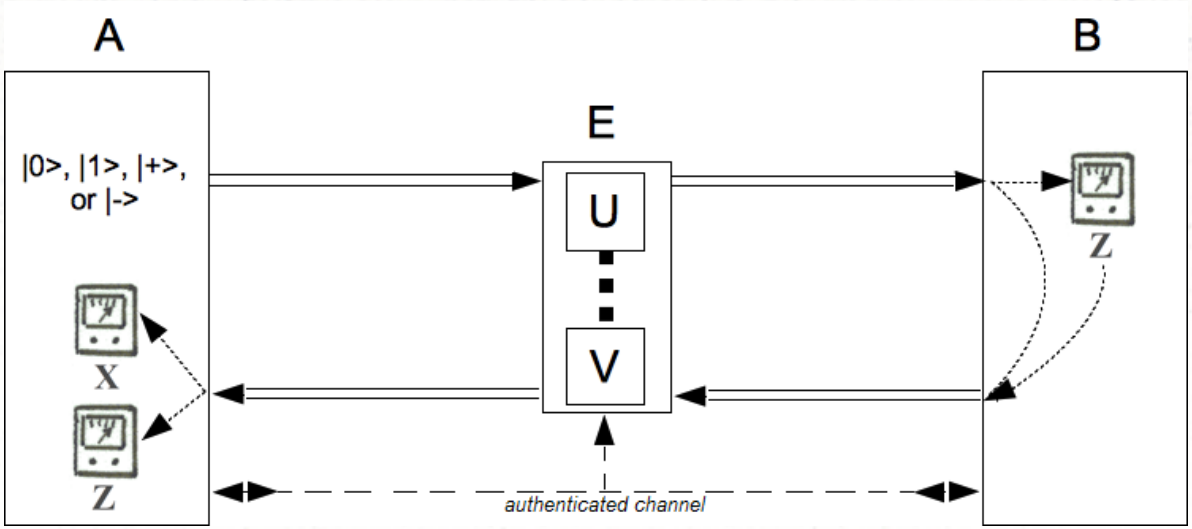
X or Z	Z	X	Z	X
Result	|0>	|+>	|1>	|->

Use?	Y	N	N	N

- A sends a qubit of the form |+>
- B chooses randomly to reflect the qubit, or measure and resend
- A measures in a random basis (Z or X)
- If A chose to measure in the Z basis and B measured, they share a random bit
- If B reflected, and A chose X, A should measure |+>

SQKD Security

- The all-powerful attacker Eve will capture and attack every qubit sent (in both directions)
- This attack will *entangle* the qubit with E's private quantum memory
  - This memory is modeled mathematically as an n-dimensional C vector space.



Security

- E's attack creates noise in the channel
- The more “invasive” her attack, the more knowledge she gains
- But, the more noise she creates
- **Goal**: Bound the maximal amount of information the attacker can gain given a certain noise level
- **Question**: How much noise is too much?

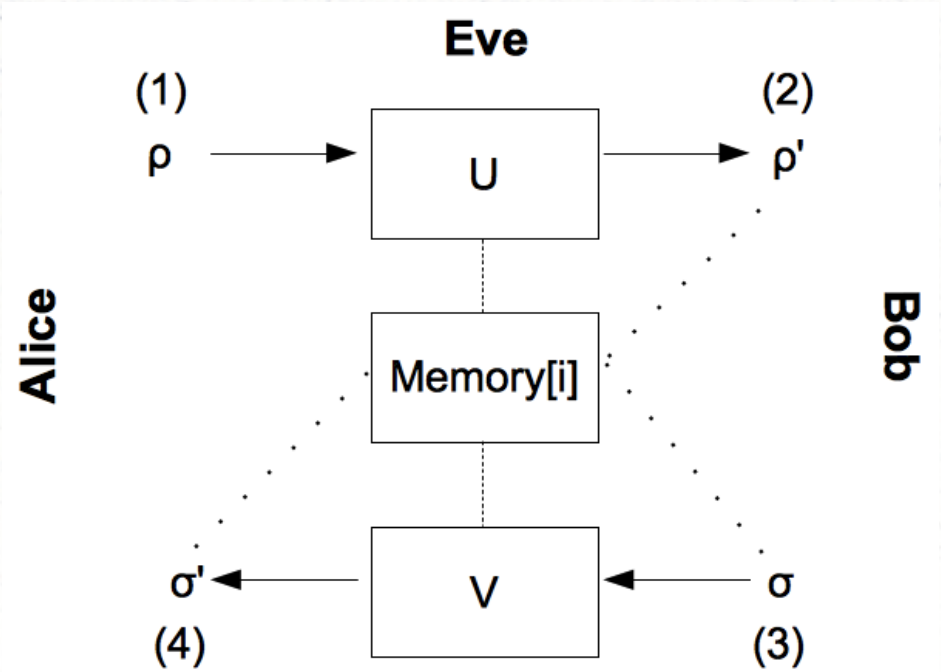
Robustness

- Due to the two-way quantum channel, past security analyses of semi-quantum protocols have been limited
- Most protocols are only proven to be *robust*
  - Any attack can be detected with non-zero probability
- Says nothing about how much noise is too much
- Until our work, all SQKD protocols stated "A and B abort if the error rate is higher than some threshold," but no one knew what this threshold was...

Analyzing the Security of SQKD Protocols

Attack Models

- Collective Attacks
  - E performs the same attack each iteration, applying a *unitary operator* acting on the qubit and E's private *quantum memory* (an n-dimensional complex vector space)
  - E is allowed to measure at any time of her choosing

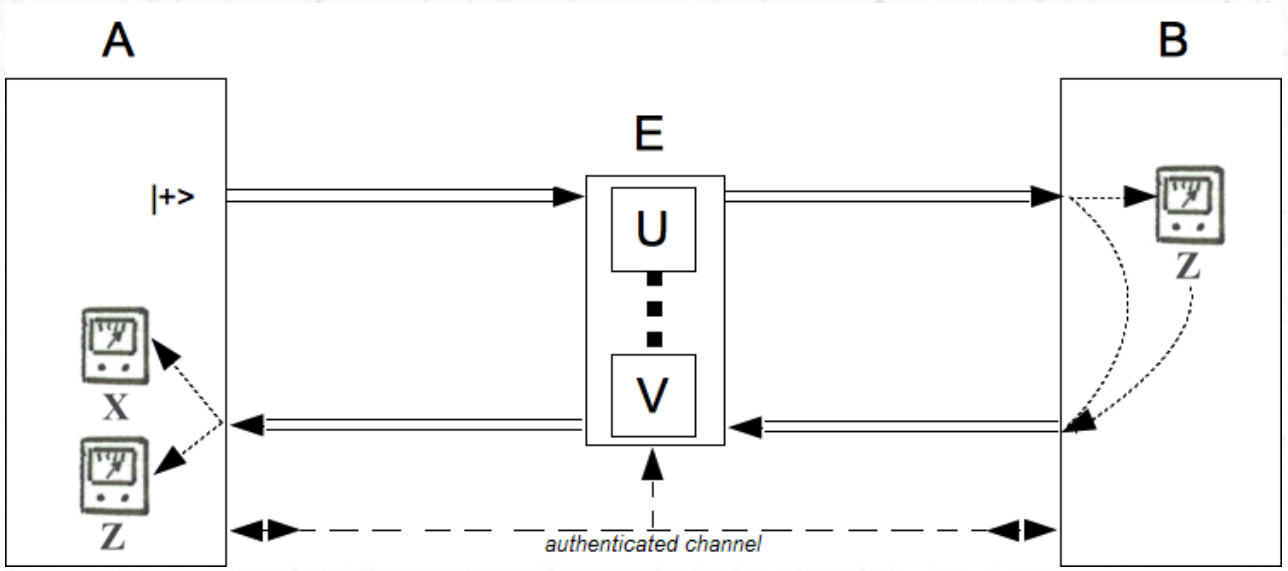


Attack Models

- General Attacks
  - Eve is allowed to perform different attacks each iterations (perhaps based on the result of an attack on a previous iteration)
- Ultimate goal: prove a QKD protocol is secure against general attacks
- However, (Renner, 2007) proved that security against collective attacks implies security against general attacks
- Thus, it is sufficient to prove security against collective attacks
  - Still difficult in the SQKD setting due to E's ability to attack a qubit twice!

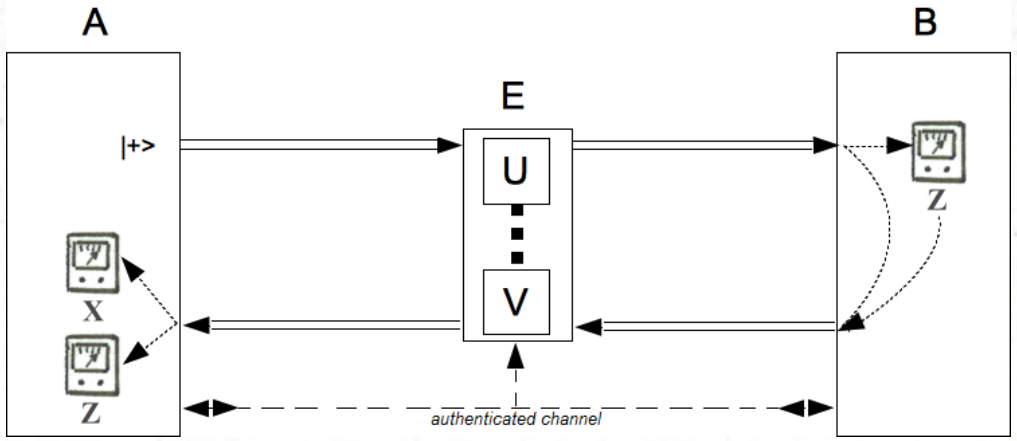
SQKD Protocols: Attacks

- A *collective attack* is a pair (U, V) of unitary attack operators (both of which act on the qubit and E's private n-dimensional quantum memory) which Eve will use on each iteration
  - U is used in the forward direction (A → B)
  - V is used in the reverse direction (B → A)



SQKD Protocols

- Given an attack (**U**,**V**) sometimes, we can consider an equivalent "restricted" attack:
  - (b,**U**) : for single-state protocols
    - b is a "bias" term (b in [-1/2, 1/2])
  - (Q, z, **U**) : for all other SQKD protocols
    - Q is the "noise" in the forward channel
    - z is an (annoying) complex number



Theorem

Theorem: For any single-state SQKD protocol, let (U,V) be a collective attack. Then, there exists an equivalent restricted collective attack (b,U') where:

- E will bias Bob's measurement results using bias parameter “b”
  - B will measure |0> with probability ½ + b
  - B will measure |1> with probability ½ – b

- E will then use unitary attack operator U' on the returning qubit.

Thus, there is no advantage for E in using a more complicated collective attack.

Theorem

- Thus, for any single state SQKD protocol, it is sufficient to consider only restricted collective attacks

(Renner, 2007)

$$\text{Restricted Collective} \Rightarrow \text{Collective Attacks} \Rightarrow \text{General Attacks}$$

Easier to Analyze Mathematically

Harder to Analyze Mathematically

Theorem

Theorem: For any SQKD protocol, let (U,V) be a collective attack. Then, there exists an equivalent restricted collective attack (Q, z,U') where:

- E will induce an (Z basis) error rate of “Q” in the forward channel
- E will also entangle the qubit with her ***two dimensional*** quantum memory based on “z”

- E will then use unitary attack operator U' on the returning qubit.

Thus, there is no advantage for E in using a more complicated collective attack.

Theorem

- Thus, for *any* SQKD protocol, it is sufficient to consider only restricted collective attacks

(Renner, 2007)

$$\text{Restricted Collective} \Rightarrow \text{Collective Attacks} \Rightarrow \text{General Attacks}$$

Easier to Analyze Mathematically

Harder to Analyze Mathematically

Proof of Security

QKD Security: Key Rate

- After communicating with qubits, A and B have a *raw key* of size N bits
- Next, they run an error correcting protocol and a privacy amplification protocol
- This results in a secure key of size $l_v(N) < N$ bits
  - $l_v(N)$ may be zero
- Question: Given the error rate of the raw key, what is $l_v(N)$?
- Question: When is $l_v(N) = 0$?

Key Rate

- Let:

  $\Gamma_\nu = \{\text{all attacks which conform to the observed statistics } \nu\}$

- It was shown in (Renner et al., 2005) that:

$$l_\nu(N) \approx Nr(\nu)$$

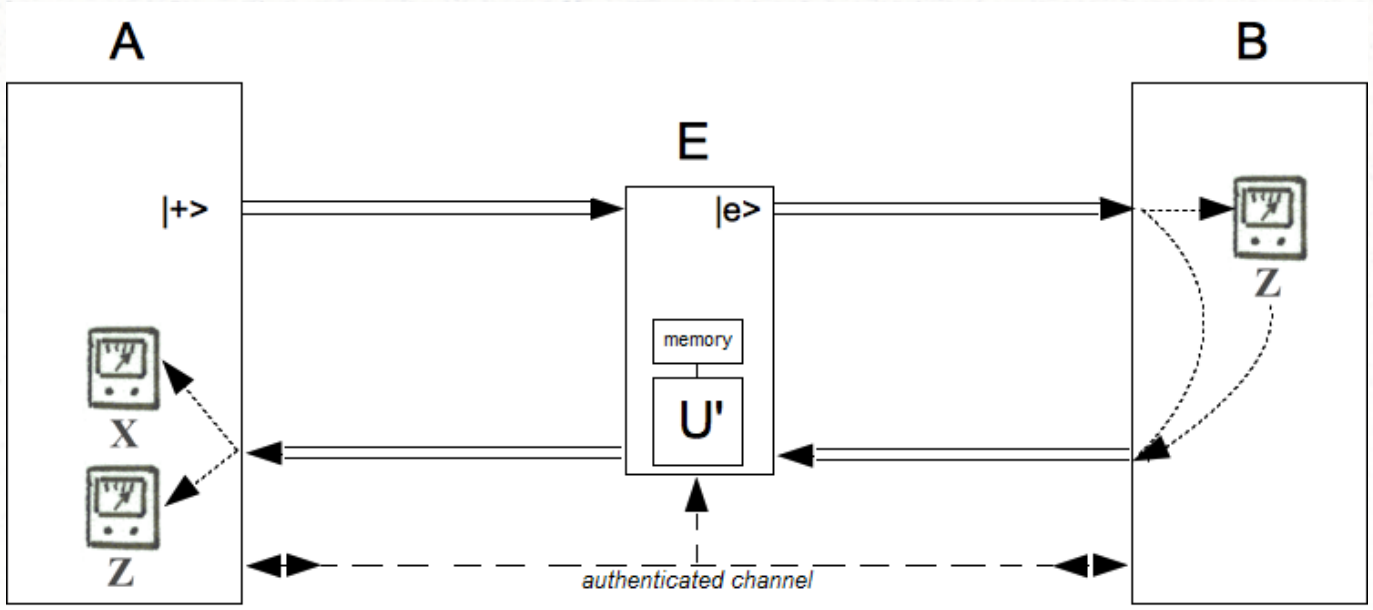
$$r(\nu) = inf_{\Gamma_\nu}(S(B|E) - H(B|A)) \leq 1$$

S: von-Neumann Entropy , H: Shannon Entropy

- Thus, r() is a function of certain observed parameters – in particular the error rate
- Our goal now is to lower-bound the key rate...

Proof of Security: First Step

- First, consider a restricted attack (Q, z, **U**) and break the protocol into two cases:
  - E flips the qubit (an error)
  - E does not flip the qubit (no error)



Proof of Security: First Step

- Describe the protocol in both cases:
  - With probability "Q" there was an error (in the forward channel)
  - With probability "1-Q" there was no error (in the forward channel)
- It can be written as a density operator (matrix):

The state of the protocol if there is a forward attack

$$\chi_{BEC} = (1-Q)|C><C| \times \rho_{BEC} + Q|W><W| \times \sigma_{BEC}$$

The state of the protocol if there is no forward channel attack

Proof of Security: First Step

- Recall:

$$\text{key rate} = S(B|E) - H(B|A)$$

- If the protocol state can be written:

$$\chi_{BEC} = (1-Q)|C><C| \times \rho_{BEC} + Q|W><W| \times \sigma_{BEC}$$

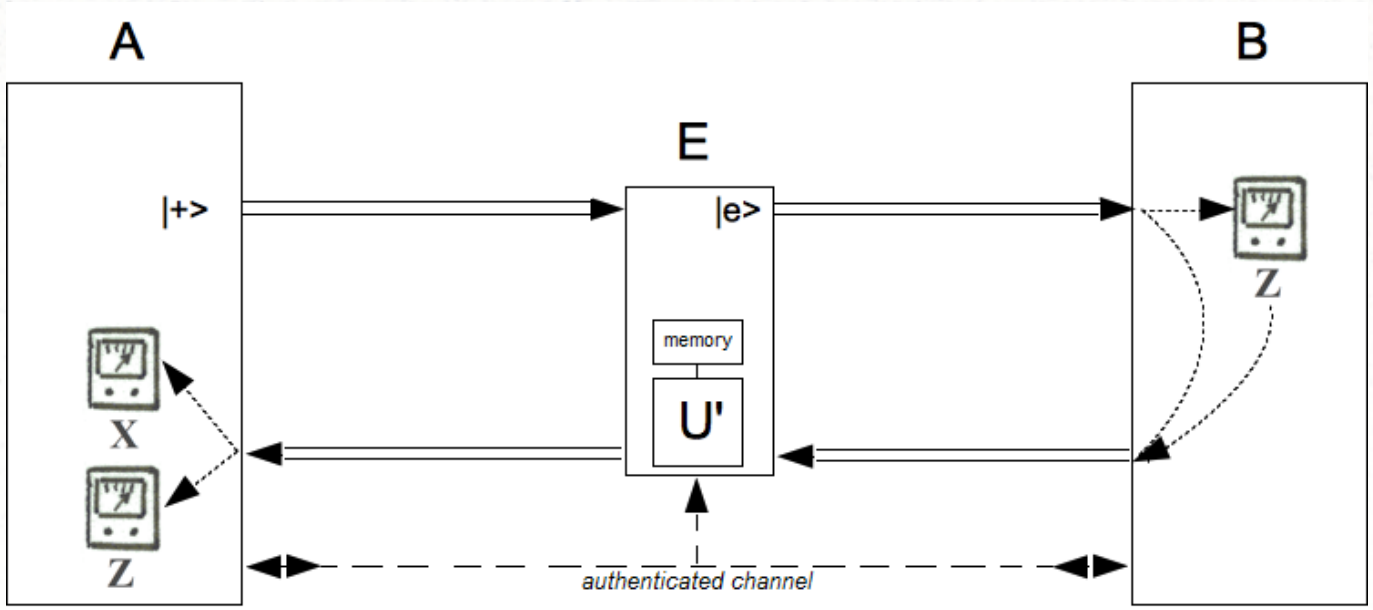
- We can prove:

$$S(B|E)_{\chi} \geq S(B|E)_{\rho} - Q \cdot \log dim\, E$$

Usually 2...

Proof of Security: Second Step

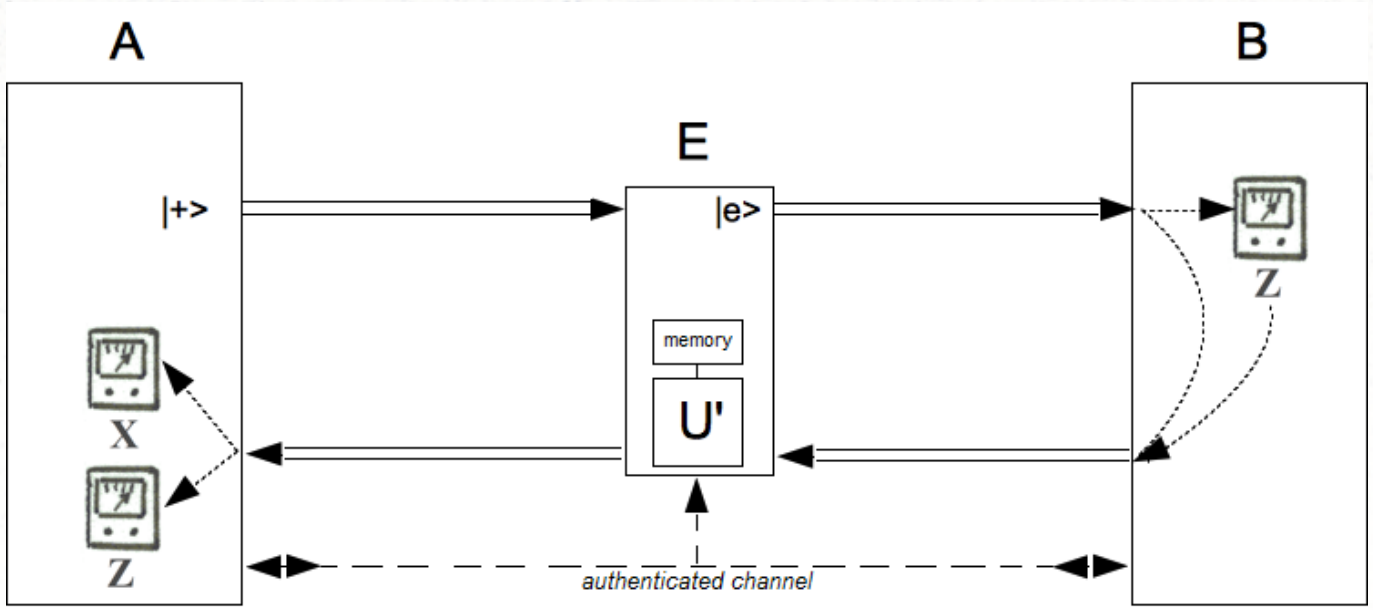
- Now, we just need to determine S(B|E) for the "no forward channel attack" case
- This usually boils down to finding an equivalent (fully) quantum protocol
  - For these, many bounds already exist!



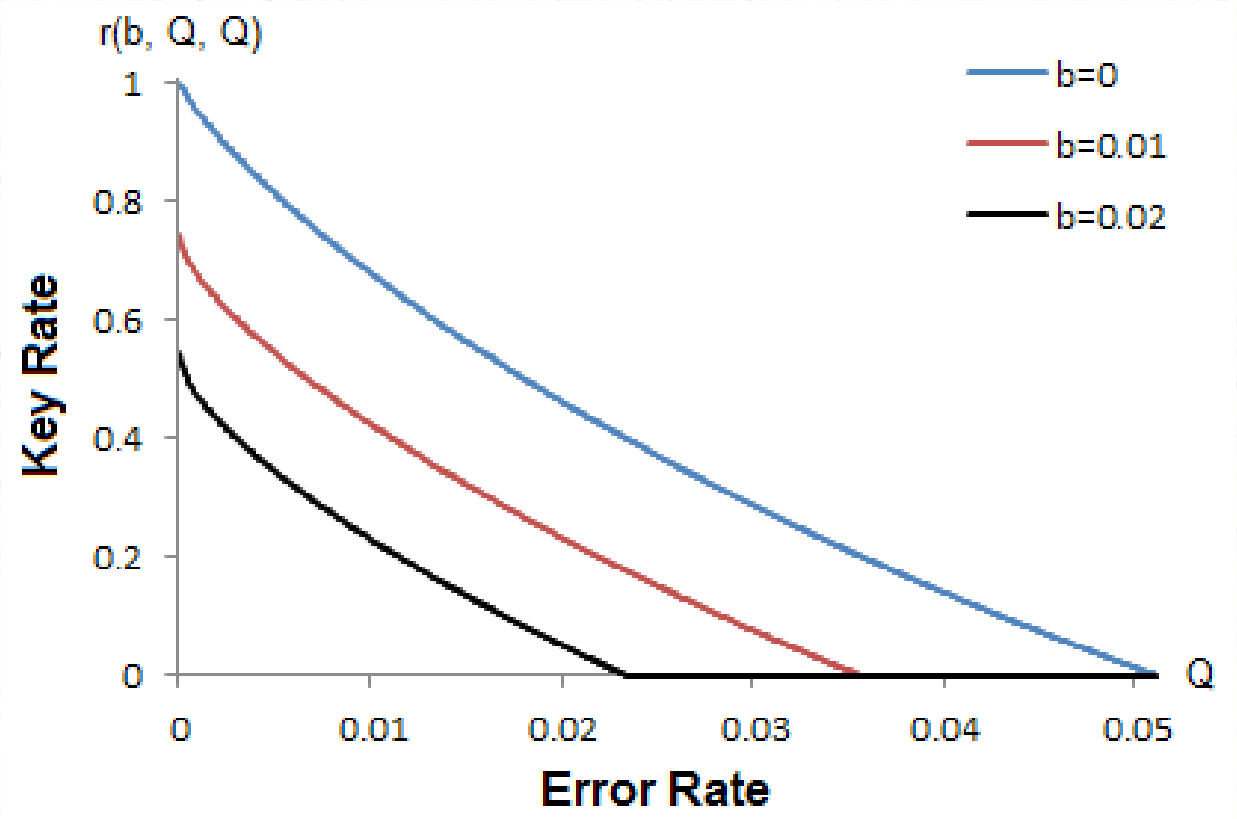
Proof of Security: Third Step

- Finally, combine everything; though care must be taken about the noise in alternative bases

$$S(B|E)_{\chi} \geq S(B|E)_{\rho} - Q \cdot \log dim\, E = r(\text{some protocol}) - c \cdot Q$$



Example:


r(b, Q, Q)
1
0.8
0.6
0.4
0.2
0
Key Rate
0
0.01
0.02
0.03
0.04
0.05
Error Rate
Q
b=0
b=0.01
b=0.02

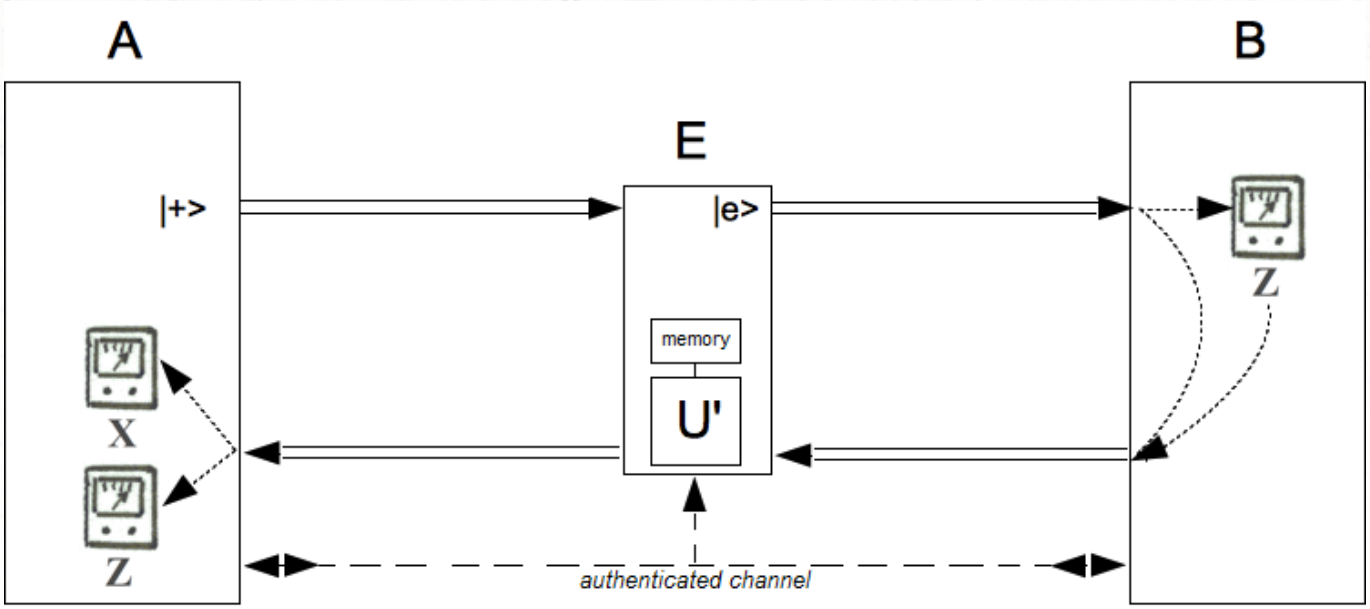
Future Work

Extending this Technique

- It may be possible to extend this proof technique to other fully quantum protocols which rely on a two-way quantum channel
  - There are several; only a few have proofs and they are complicated
- Use our bound to understand other problems in QKD research
  - e.g., the effects of preprocessing or multi-photon sources

Multi-Photon Sources

- What happens if E spams Bob's lab with photons
  - She's allowed to count photons without disturbing them



Numerical Techniques

- We have developed an algorithm to find upper-bounds on the key rate
  - Program could be improved; also new features: multi photon sources
- An interesting project is to design new algorithms to analyze optimal attack strategies against arbitrary protocols
  - Programming required
- Also to understand the security of these protocols for more "practical" attacks
  - Math and Programming

Finding Optimal Protocols

- A new project is to find optimal protocols given certain attacks
  - Usually we look for optimal attacks given a protocol
  - Some preliminary results...
  - Program needs a lot of work
  - Also need a way to better define “certain attacks”

Thank you! Questions?

References

- C.H. Bennett and G. Brassard, 1984, Quantum cryptography: Public key distribution and coin tossing. in Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing. Vol 175, NY.
- C.H. Bennett, 1992, Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett., 68:3121-3124.
- M. Boyer, D. Kenigsberg, and T. Mor, 2007, Quantum Key Distribution with classical bob, in ICQNM.
- C.H.F. Fung and H.K. Lo, 2006, Security proof of a three-state quantum key distribution protocol without rotational symmetry. Phys. Rev. A, 74:042342.
- W.O. Krawec, 2014, Restricted attacks on semi-quantum key distribution protocols. Quantum Information Processing, 13(11):2417-2436.
- W.O. Krawec, 2015, Mediated semi-quantum key distribution. Phys. Rev. A. 91 032323.
- W.O. Krawec, and A.R. Nicolosi, in preparation, Effects of bias on the key-rate of certain single-state semi-quantum key distribution protocols.

References (cont.)

- H. Lu and Q.-Y. Cai, 2008, Quantum key distribution with classical Alice, Int. J. Quantum Information 6, 1195.
- R. Renner, N. Gisin, and B. Kraus, 2005, Information-theoretic security proof for QKD protocols. Phys. Rev. A, 72:012332.
- R. Renner, 2007, Symmetry of large physical systems implies independence of subsystems, Nat. Phys. 3, 645.
- V. Scarani, A. Acin, G. Ribordy, and N. Gisin, 2004, Phys. Rev. Lett. 92, 057901.
- Z. Xian-Zhou, G. Wei-Gui, T. Yong-Gang, R. Zhen-Zhong, and G. Xiao-Tian, 2009, Quantum key distribution series network protocol with m-classical bobs, Chin. Phys. B 18, 2143.
- Xiangfu Zou, Daowen Qiu, Lvzhou Li, Lihua Wu, and Lvjun Li, 2009, Semiquantum key distribution using less than four quantum states. Phys. Rev. A, 79:052312.