Semi-Quantum Key Distribution: Protocols, Security Analysis, and New Models

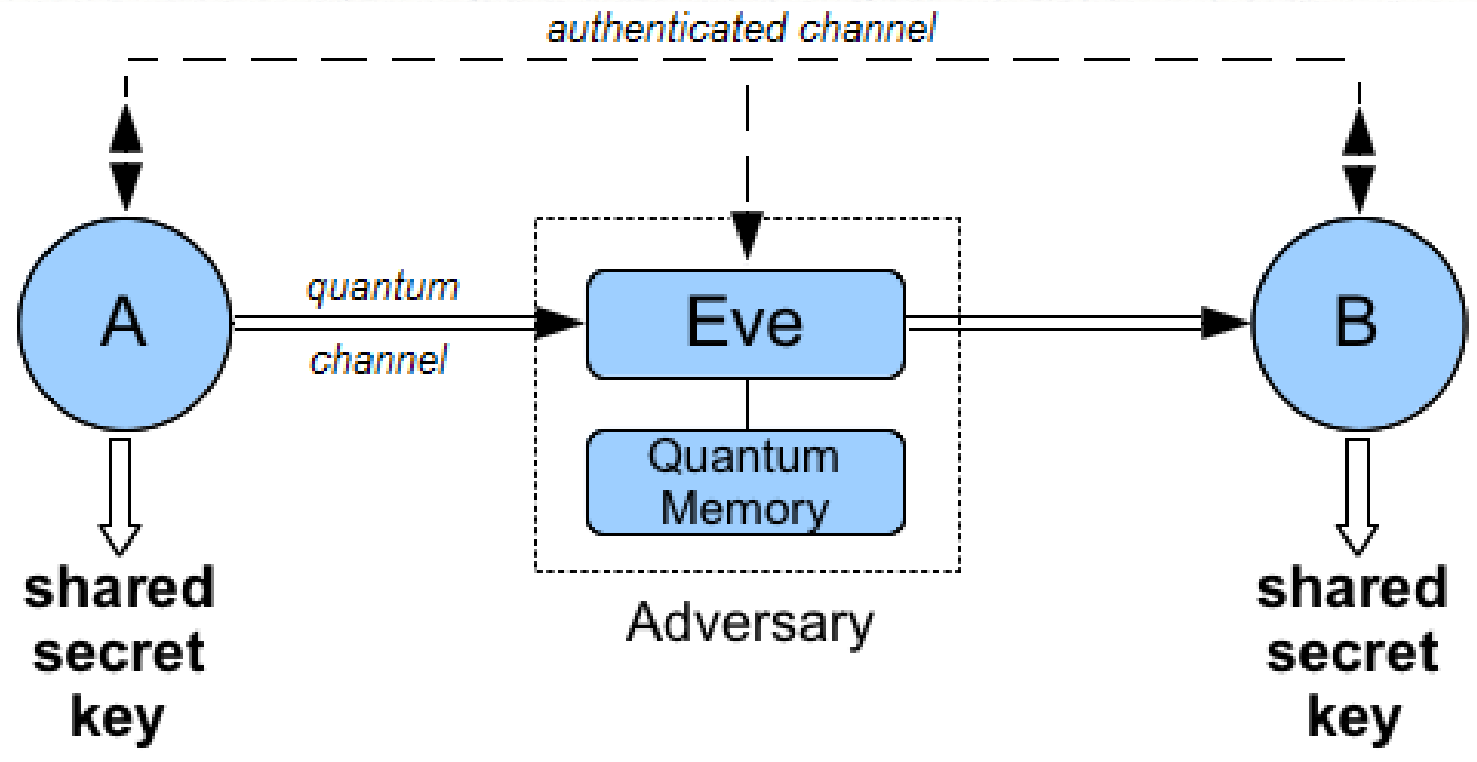
Walter O. Krawec

Ph.D. Defense
April 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

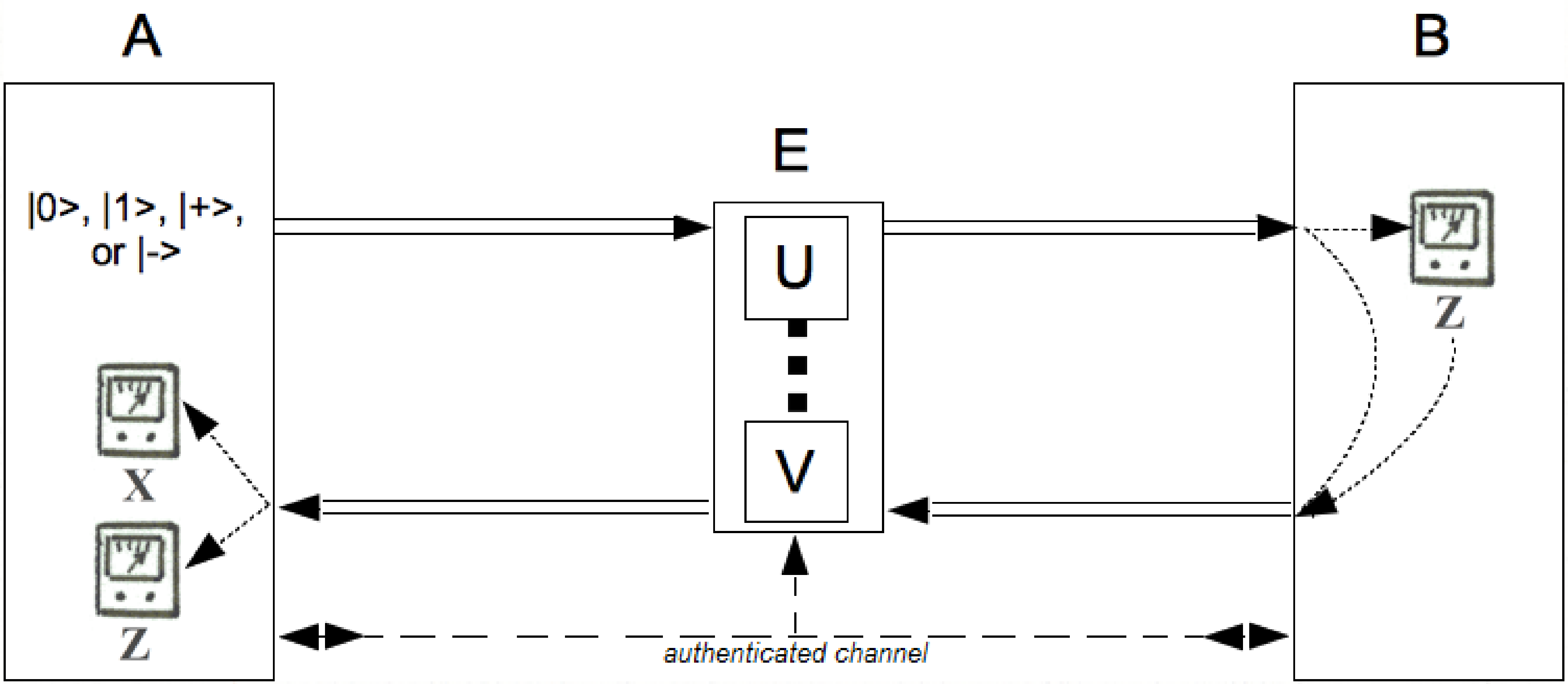
- Quantum Key Distribution is here already
- Several companies produce commercial QKD equipment
  - MagiQ Technologies in NY
  - id Quantique in Geneva
  - SeQureNet in Paris
  - Quintessence Labs in Australia
- Have also been used in various applications:
  - In 2007, QKD was used to transmit ballot 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
  - or they were proven secure assuming the attacker was limited in some way
- Our work is the first to provide full security proofs for SQKD protocols using the state of the art definitions.

Our Contributions

A) We developed a set of ***tools*** that may be used to better ***analyze the security*** of certain SQKD protocols (Krawec, 2014)

- These tools may be used to prove the unconditional security of several SQKD protocols – previously an open question

B) We developed a ***new single-state SQKD protocol***

- First semi-quantum protocol which allows X-basis qubits to contribute towards the secret key (Krawec, 2014)
- Also, our previous results can be applied to prove its unconditional security (Krawec and Nicolosi, in preparation)

C) We developed a new type of semi-quantum protocol: a ***mediated semi-quantum key distribution protocol*** (Krawec, 2015)

- Allows two **classical** users to establish a secret key with the help of an **untrusted quantum server**

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

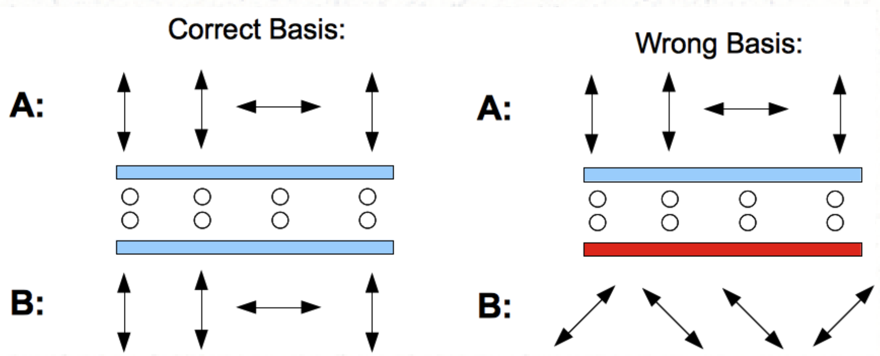
- Qubits are modeled mathematically using a two-dimensional complex vector space
- Thus, any arbitrary qubit is:

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

- 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

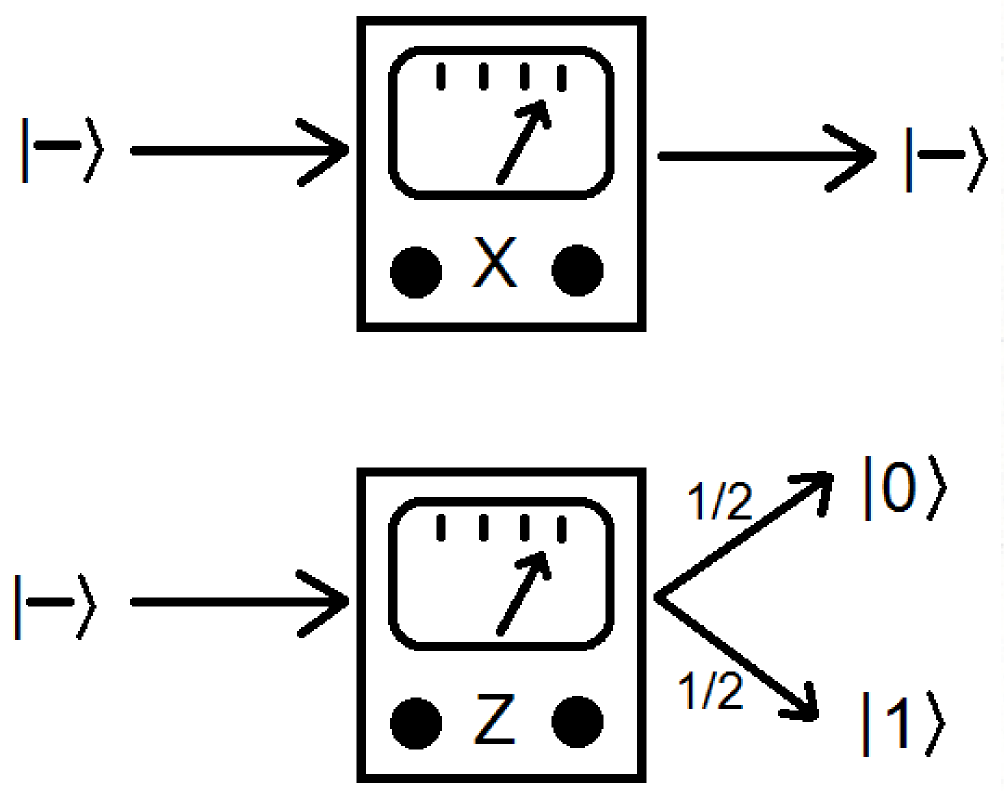
- Two important (orthonormal) bases we will use are the *computational Z basis* and the *Hadamard X basis*:
  - Z = {|0>, |1>}   X = {|+>, |->}

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

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

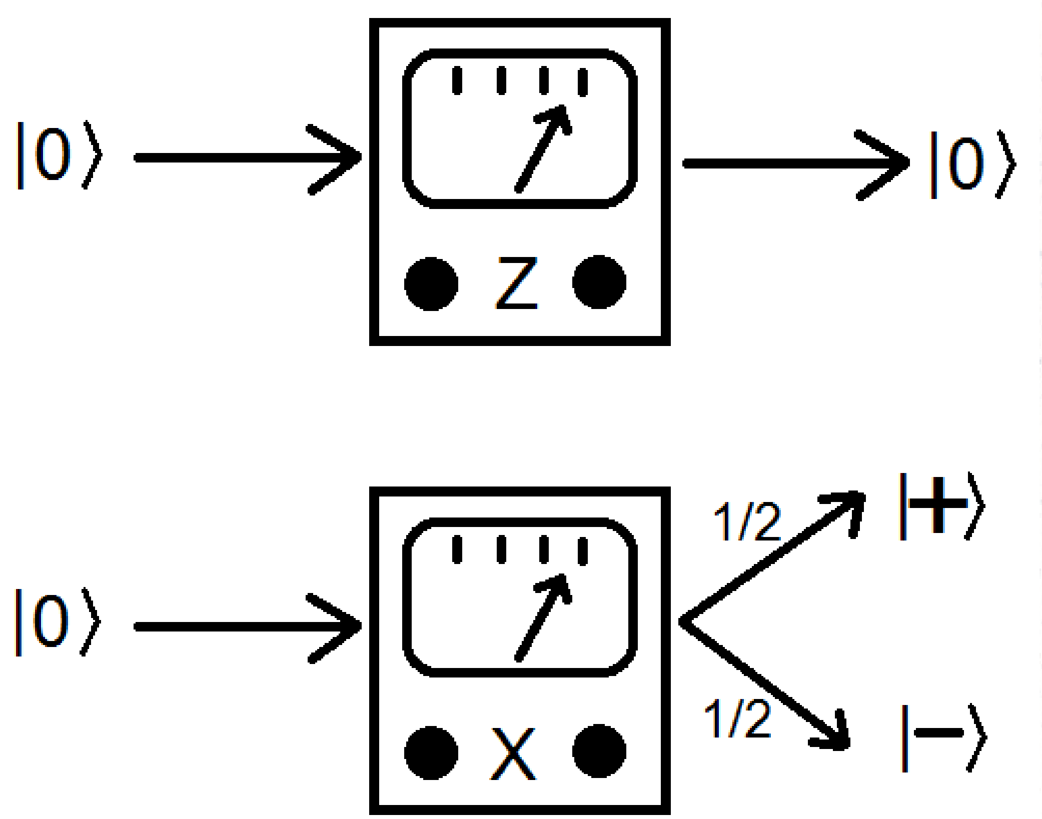
Measuring a Qubit

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



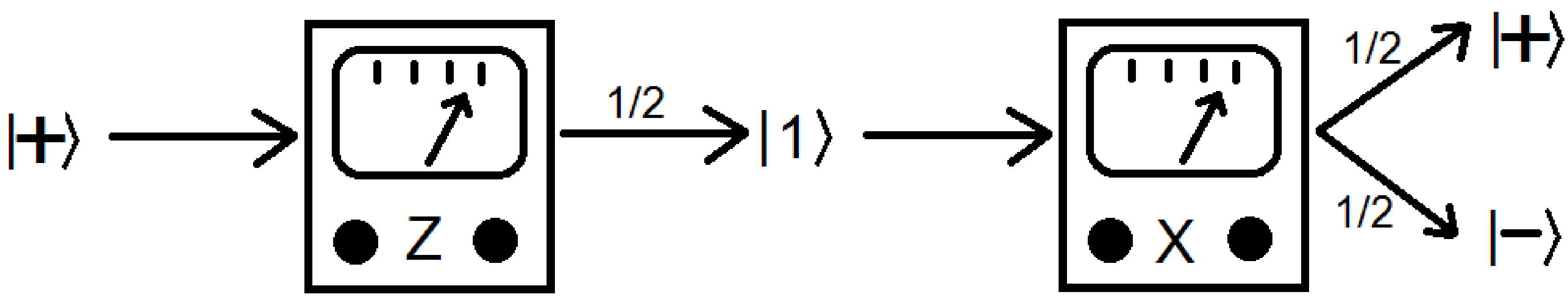
Measuring a Qubit

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

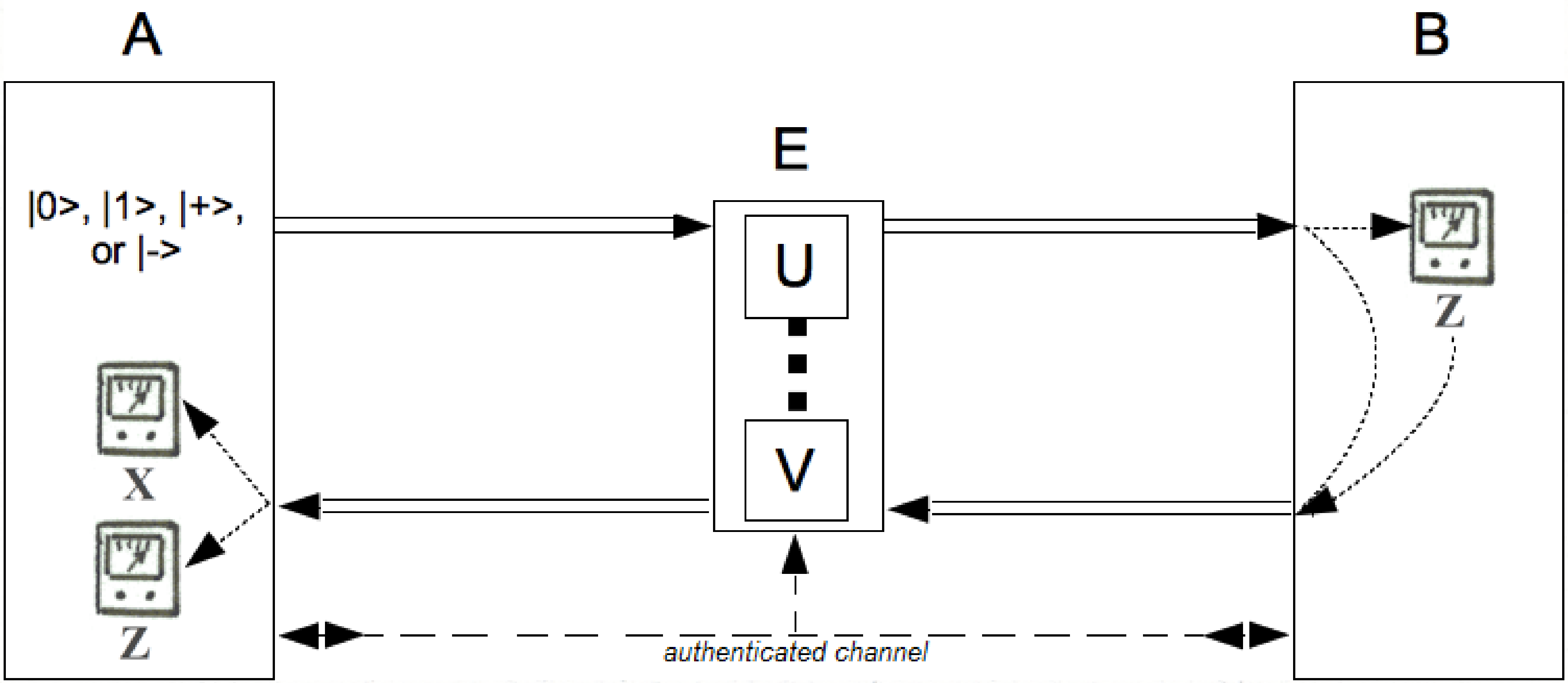
X or Z	Z	X	X	Z
Result	|0>	|->	|+>	|0>
Key	0	1	0	0
Use?	Y	Y	N	Y

- 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

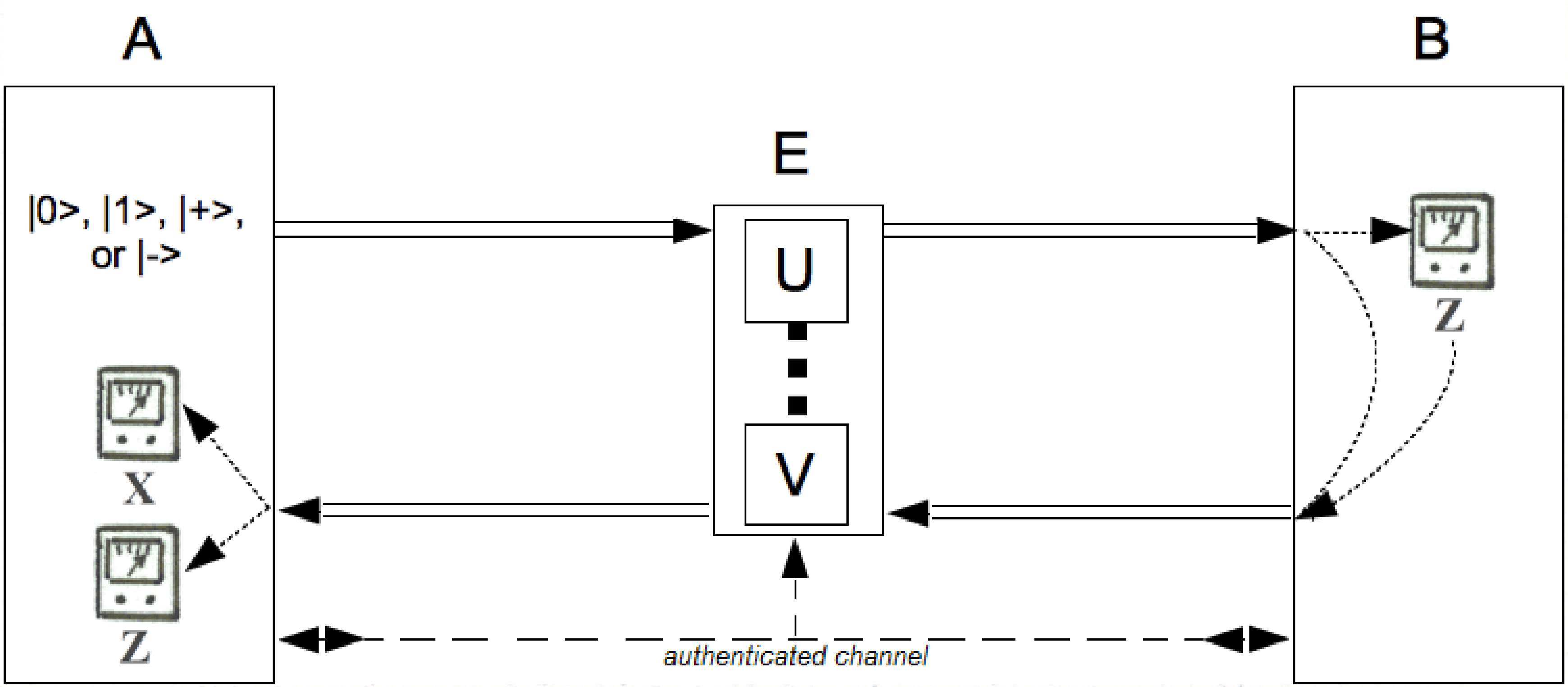
Semi-Quantum Key Distribution



Semi-Quantum Key Distribution: Classical Bob

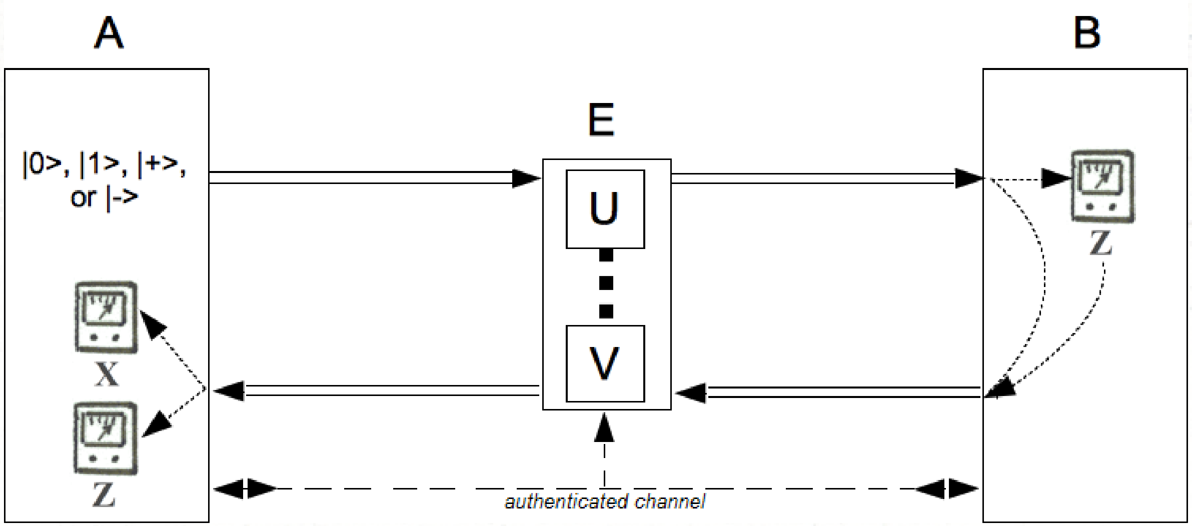
- Semi-Quantum Key Distribution (SQKD), introduced in (Boyer et al., 2007) requires one of the users (typically Bob) to be *classical* or *semi-quantum*:
- B may **Measure and Resend**
  - The incoming qubit is measured in the Z basis
  - B then resends a qubit based on this result
  - e.g., if he measures |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



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?

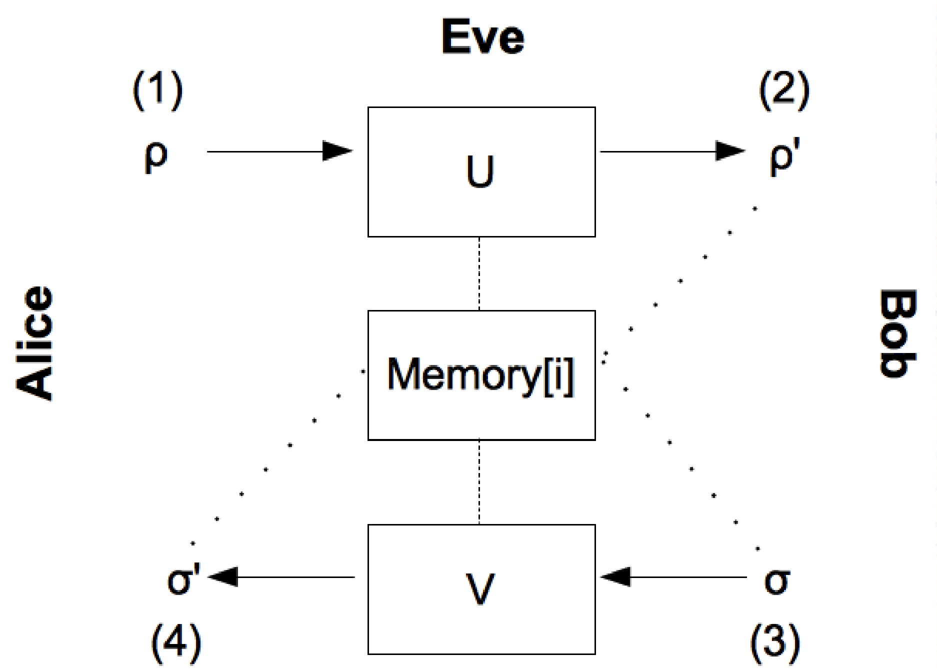
Robustness

- 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 in this dissertation, 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...

A) 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

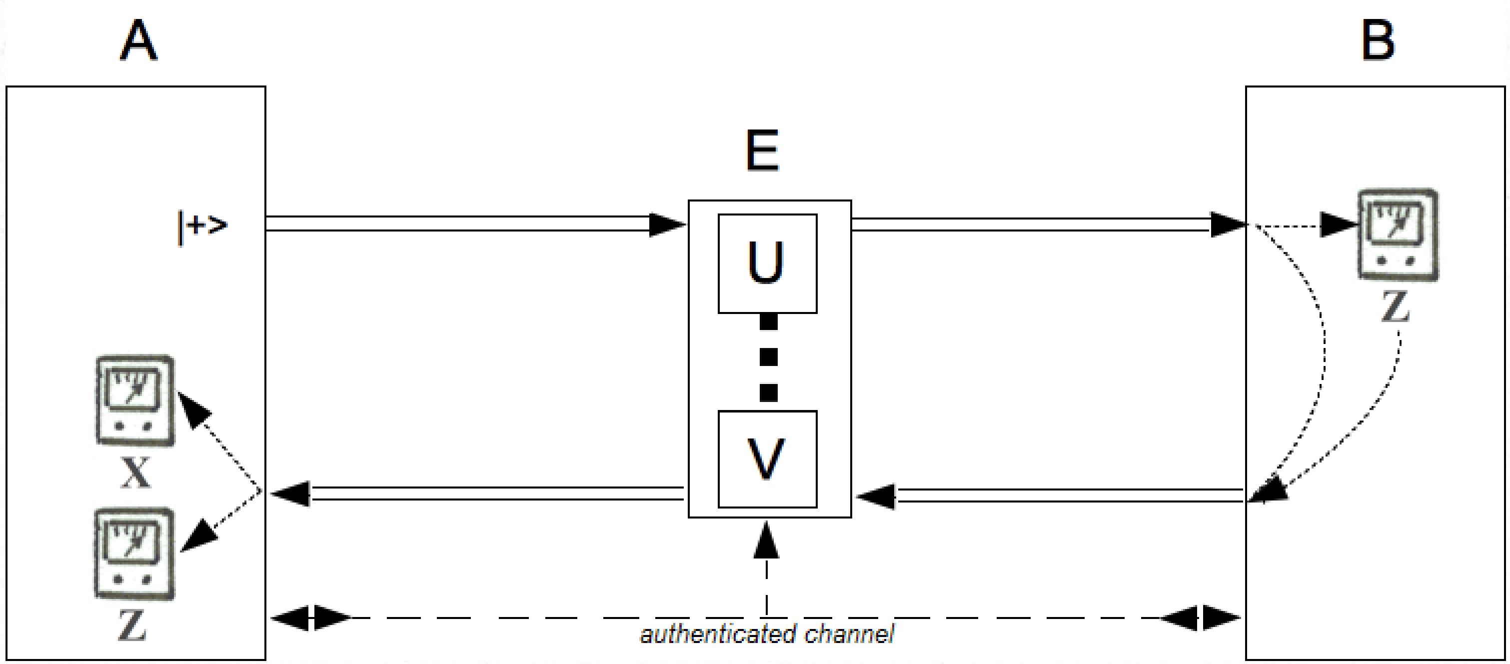


Attack Models

- 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!

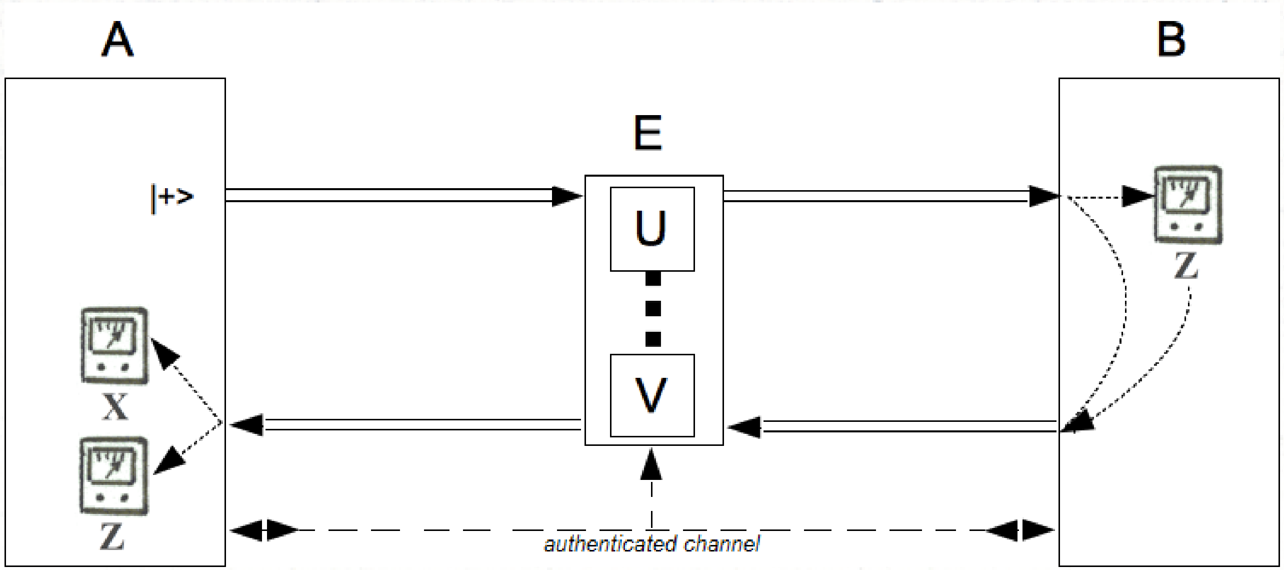
Single-State SQKD Protocols

- A single-state SQKD protocol, first introduced in (Zou et al., 2009) is one where B is classical and A can only prepare one type of qubit each iteration - typically |+>
  - A, however, can still measure in either Z or X basis



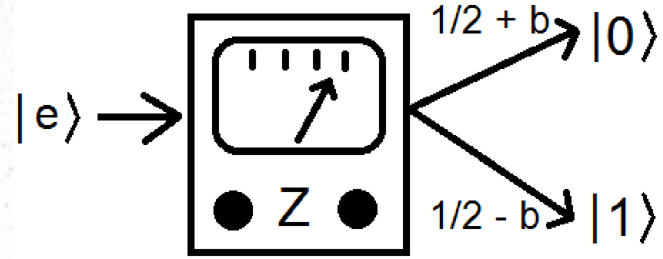
Single-State SQKD Protocols

- 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)

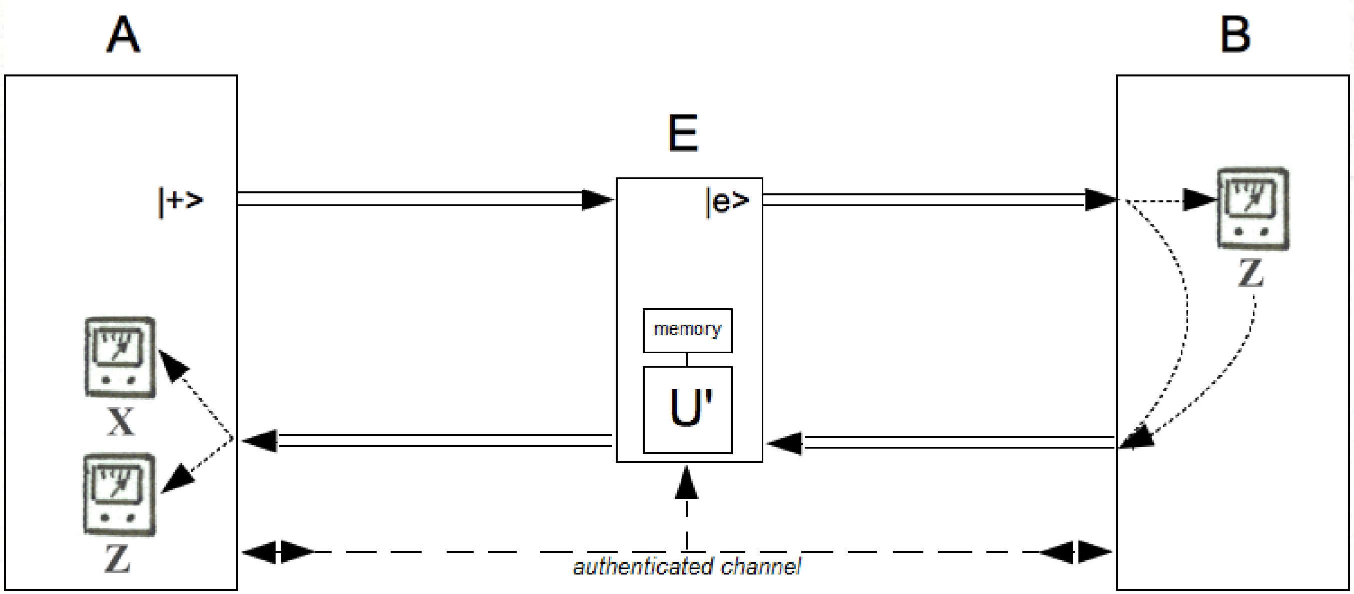


Restricted Collective Attacks

- We define a *restricted collective attack* to be a pair (b, U')
  - b is a "bias" parameter in the range [-½, ½], used by E to bias B's measurement results



  - U' is a unitary attack operator used in the reverse direction (B → A)



First 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.

First Theorem

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

(Krawec, 2014) (Renner, 2007)

$$\underbrace{\text{Restricted Collective}}_{\text{Easier to Analyze Mathematically}} \Rightarrow \underbrace{\text{Collective Attacks} \Rightarrow \text{General Attacks}}_{\text{Harder to Analyze Mathematically}}$$

B) A New Single-State SQKD Protocol

New Single-State SQKD Protocol

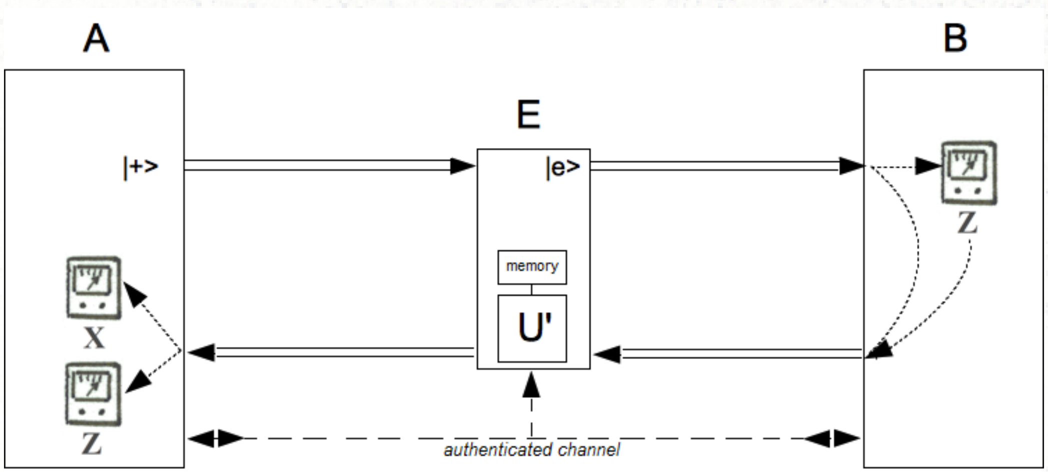
- We designed a new single-state SQKD protocol
- This is the first semi-quantum protocol which allows X-basis states (|+> and |->) to contribute to the raw key
  - In all prior protocols, they were used only to verify the security of the quantum channel.
- Since it is a single-state protocol, our previous results apply, allowing us to preform a more rigorous proof of security

The Protocol

- A sends |+>
- B chooses to **measure and resend** or **reflect** – his key bit is based on his *action*, not on his measurement result
  - If he measures and resends, his key bit is 0
    - (If he measures |1>, the iteration is discarded)
  - If he reflects, his key bit is 1
- A measures in the Z or X basis to determine which action B chose
  - If she measures in the Z basis, her key bit is 1
    - (If she measures |0> the iteration is discarded)
  - If she measures in the X basis, her key bit is 0
    - (If she measures |+> the iteration is discarded)

New Protocol: The Idea

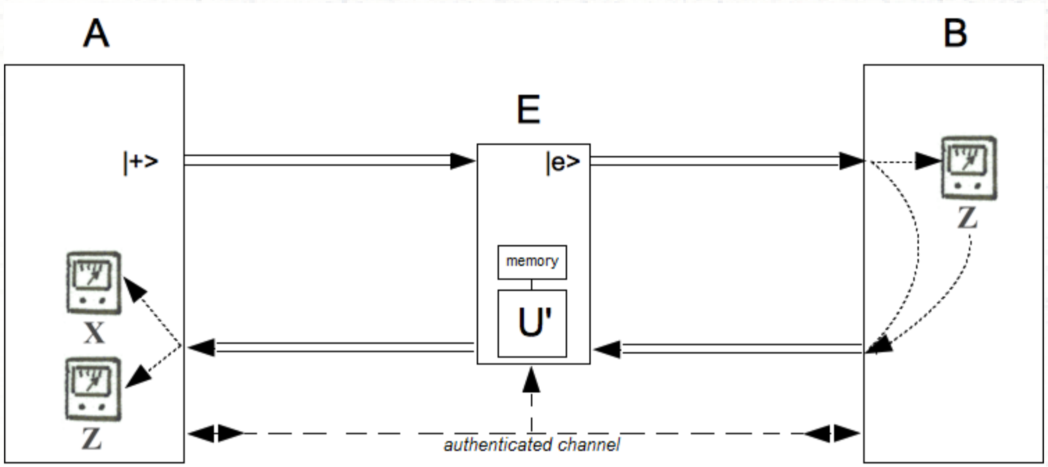
- Alice always sends |+> to Bob.
- Bob chooses to **measure and resend** or **reflect**
  - His key bit is based on his *action* not his measurement result
- Alice must determine what B did:



	Measure |0> (key=0)	Reflect (key=1)
Z (key=1)	|0>	|0> or |1>
X (key=0)	|+> or |->	|+>

New Protocol: The Idea

- Alice always sends |+> to Bob.
- Bob chooses to **measure and resend** or **reflect**
  - His key bit is based on his *action* not his measurement result
- Alice must determine what B did:



	Measure |0> (key=0)	Reflect (key=1)
Z (key=1)	|0>	|0> or |1>
X (key=0)	|+> or |->	|+>

New Single-State SQKD Protocol

Alice				
Qubit	|+>	|+>	|+>	|+>
Bob				
M or R	M:|0>	R	M:|1>	R
Key	0	1	n/a	1
Output	|0>	|+>	n/a	|+>
Alice				
X or Z	X	Z	n/a	X
Key	0	1	n/a	0
Result	|->	|1>	n/a	|+>
Use?	Y	Y	N	N

- A sends |+>
- B chooses to measure (key_B=0) or reflect (key_B=1)
  - If he measures |1> this iteration is discarded
- Alice measures in the Z (key_A=1) or X (key_A=0) basis
  - If she measures |+> or |0> this iteration is discarded

Security

- Since this is a single-state SQKD protocol, our previous results apply
  - In particular, we only need to consider restricted collective attacks (b,U)
- We can now use this previous result to prove our new protocol's unconditional 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:

$\Gamma_\nu = \{$ all attacks (b, U') which conform to the observed statistics $\nu \}$

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

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

$$r(\nu) = inf_{(b,U') \in \Gamma_\nu}\left(S(A|E_{(b,U')}) - H(A|B)\right) \leq 1$$

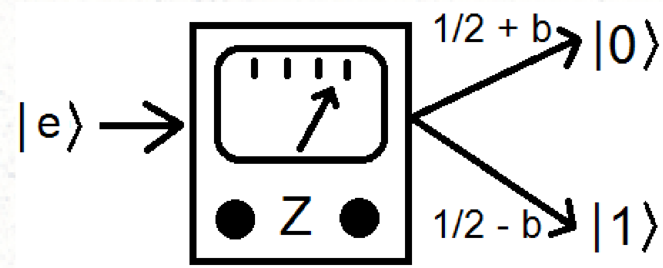
S: von-Neumann Entropy , H: Shannon Entropy

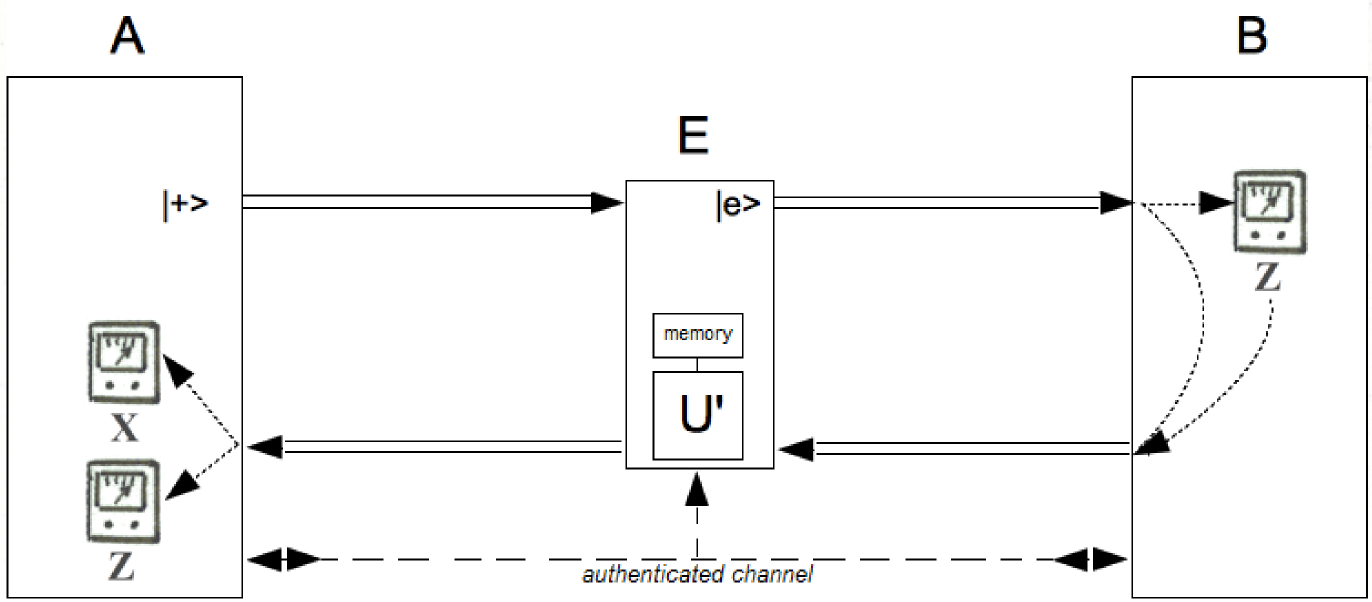
- Thus, r() is a function of certain observed parameters – in particular the error rate
- Our goal now is to lower-bound the key rate...

Proof of Security: First Step

- First, we fix an attack operator U' and determine a bound on how much the bias parameter “b” alters the key rate. That is, we find f(b) so that:

$$|r(0,U')-r(b,U')|\leq f(b)$$





Proof of Security: Second Step

- Let Q be the probability that |i> flips to |1-i>
- Let Q_X be the probability that |+> flips to a |->
- Now, we find a lower-bound for $r(0, Q, Q_X) = \inf r(0,U)$
  - That is, what is the key rate if E does not attack the first channel ($A \rightarrow B$)?
  - Now, the protocol becomes a uni-directional one
- In this case, we prove $r(0,Q,Q_X)$ is lower-bounded by the key-rate of the B92 protocol (Bennett, 1992).
- That is, we can find a function $g(Q, Q_X)$ such that:

$$r(0, Q, Q_X) \geq g(Q, Q_X)$$

Proof of Security: Third Step

- Finally, we combine everything to derive:

$$l(N) \approx N \cdot r(b, Q, Q_X)$$

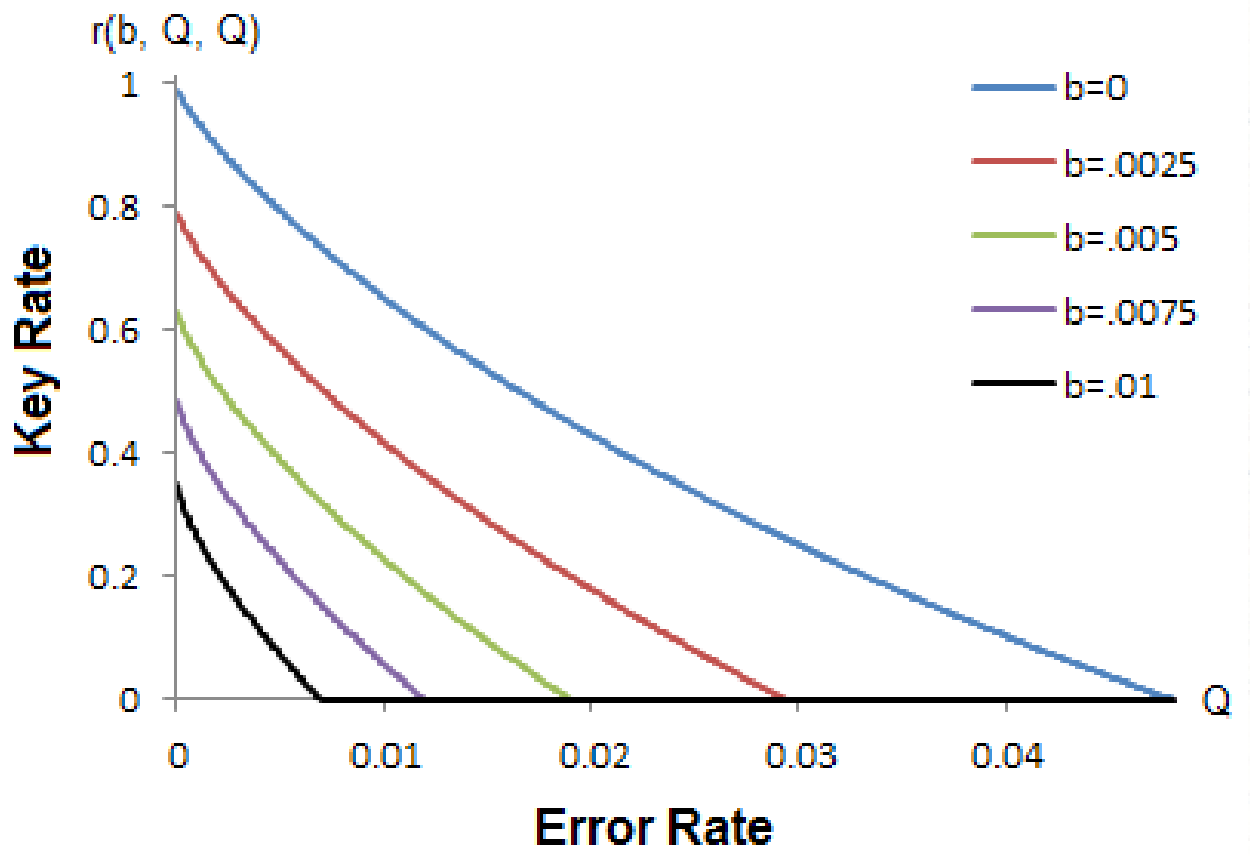
$$r(b, Q, Q_X) \geq g(Q, Q_X + 2|b|) - f(b),$$

$$\textit{where}:$$

$f(b)$ was found in step 1

$g(Q, Q_X)$ is the key rate of B92 (step 2)

A Lower-Bound on the Key Rate

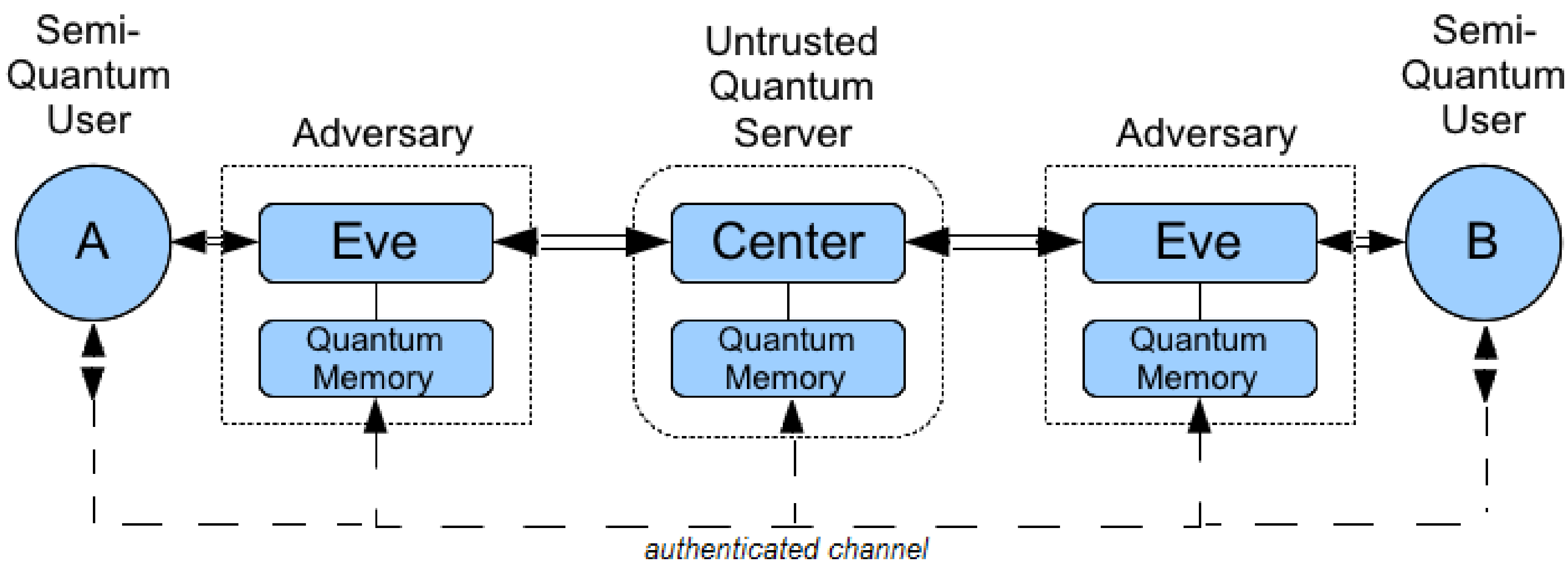


Q is the probability that a |i> flips to a |1-i>
Q_X is the probability that a |+> flips to a |->
Above, we consider the case when $Q = Q_X$

C) Mediated Semi-Quantum Key Distribution

Mediated SQKD: The Setting

- With SQKD protocols, one user, Bob, is classical while the other is fully quantum.
- What if both A and B are classical?



Related Work: Fully Quantum

- There have been several *multi-user* QKD protocols developed
- Protocols where both A and B are fully quantum, but rely on an untrusted quantum server
- Not all have complete security proofs

Related Work: Semi-Quantum

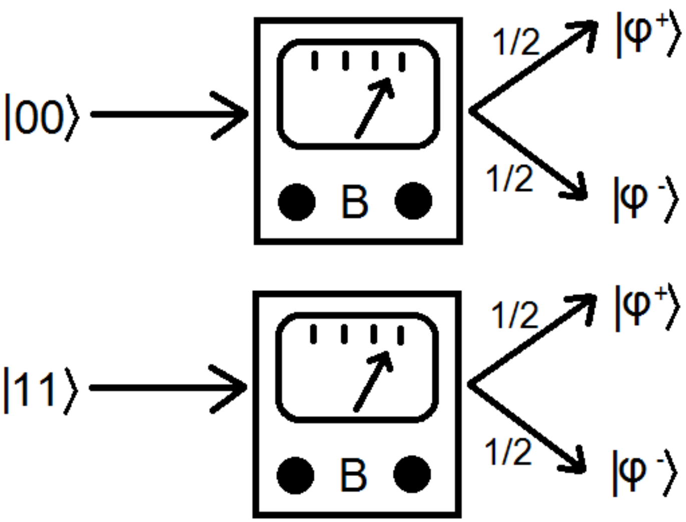
- (Zhou et al., 2009) developed a protocol where a fully quantum, and ***fully trusted***, A established a key with multiple classical users
- (Lu and Cai, 2008) developed a protocol where two classical users could establish a key using the help of a quantum server
  - However, this protocol required a ***private quantum channel*** connecting A and B, outside the view of the server
  - Also assumed the server performed the protocol correctly – that is, the server is assumed to be ***semi-honest***

Two-Qubit Systems

- Two qubits are modeled mathematically using a 2^2=4-dimensional C vector space
- Two important bases we consider:

Computational:

$|00>,|01>,|10>,|11>$



Bell:

$$|\phi^{+}>=\frac{1}{\sqrt{2}}|00>+\frac{1}{\sqrt{2}}|11>,$$

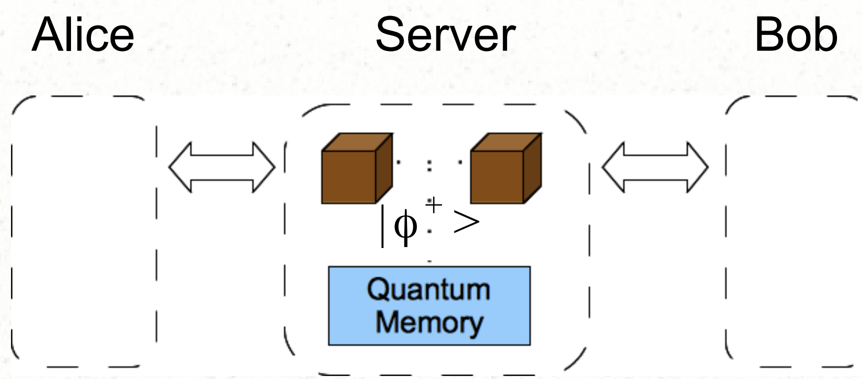
$$|\phi^{-}>=\frac{1}{\sqrt{2}}|00>-\frac{1}{\sqrt{2}}|11>,$$

$$|\psi^{+}>=\frac{1}{\sqrt{2}}|01>+\frac{1}{\sqrt{2}}|10>,$$

$$|\psi^{-}>=\frac{1}{\sqrt{2}}|01>-\frac{1}{\sqrt{2}}|10>,$$

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

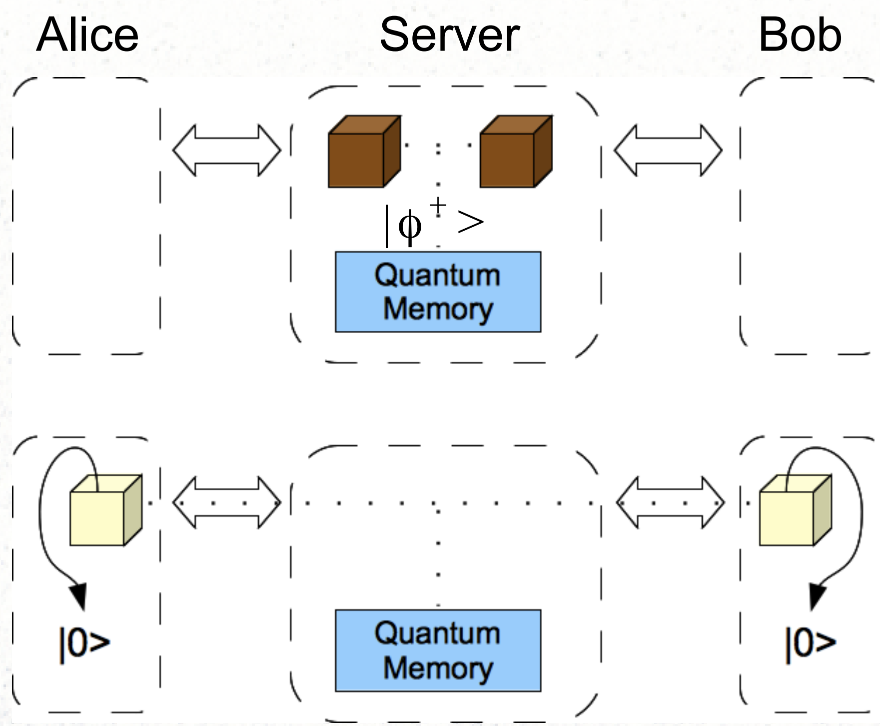
Step 1:



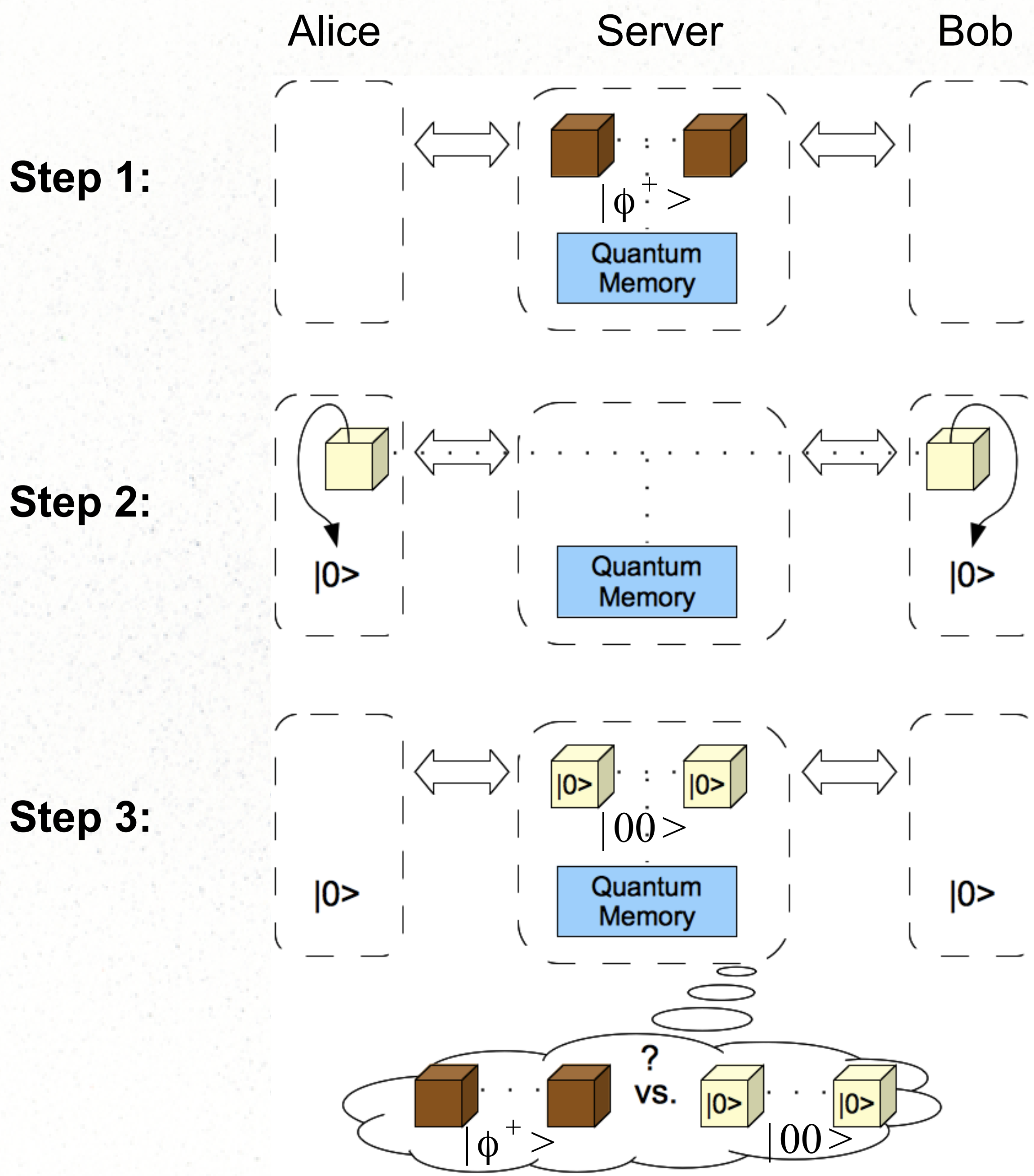
$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

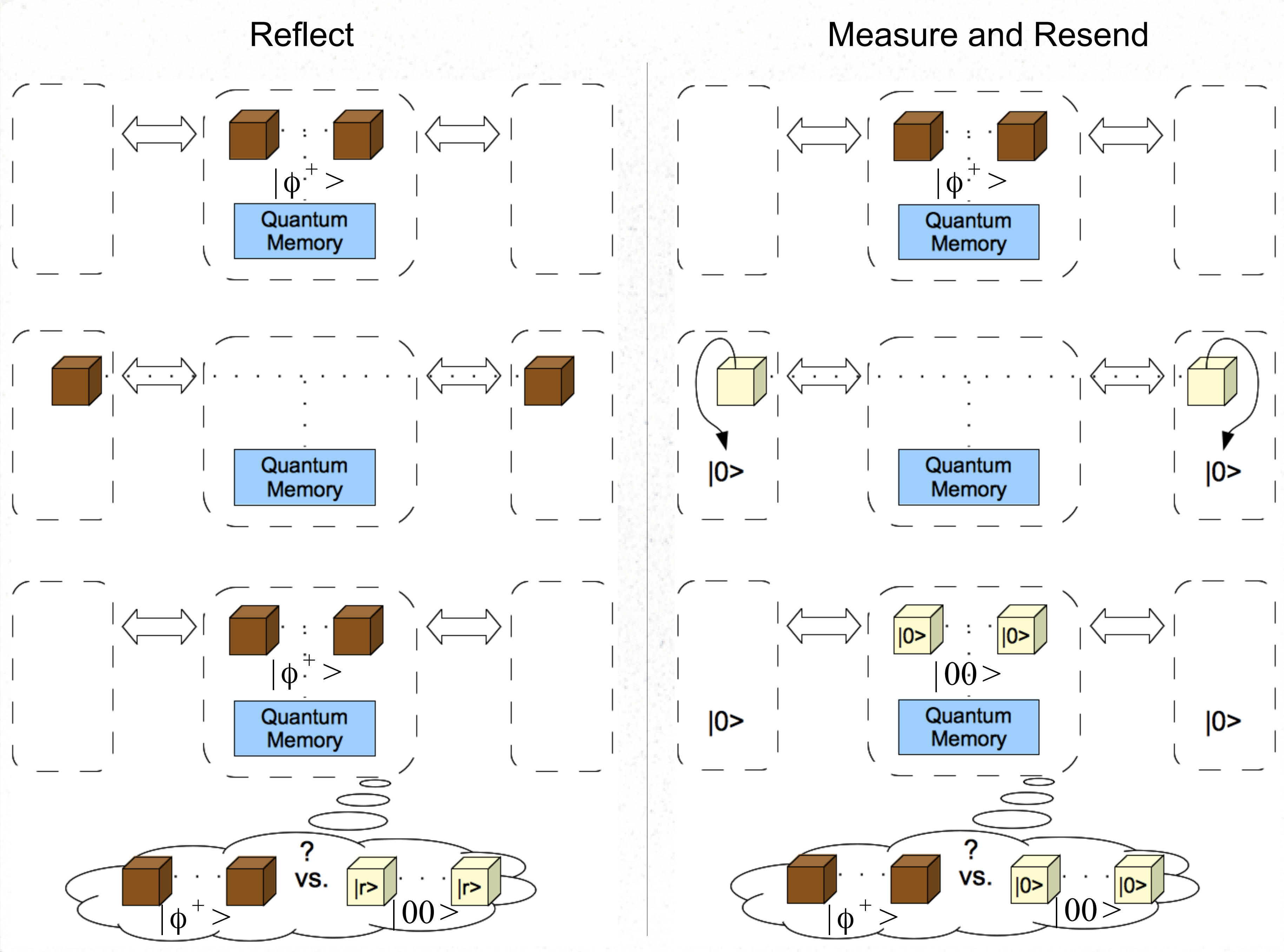
Step 1:

Step 2:



$$|\phi^+\rangle = \frac{1}{\sqrt{2}}|00\rangle + \frac{1}{\sqrt{2}}|11\rangle$$

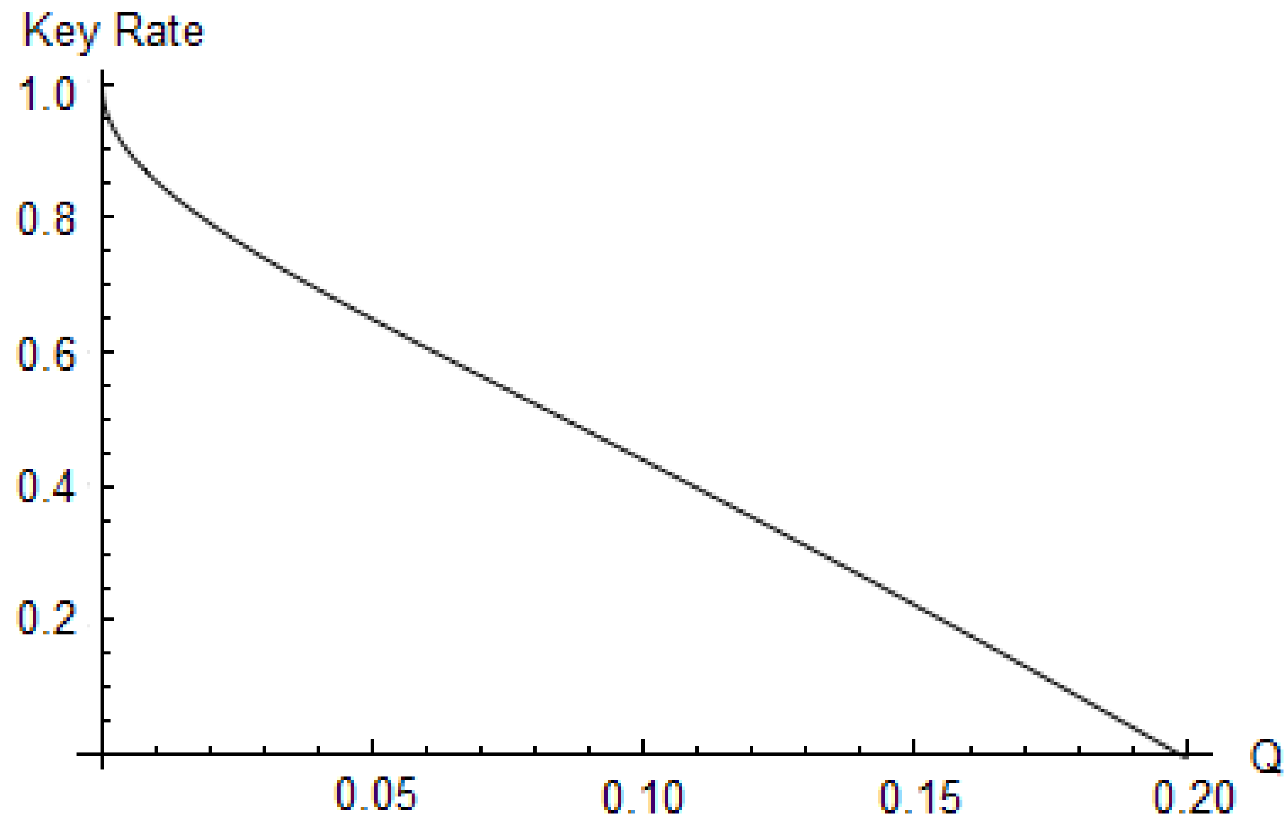



Reflect
Measure and Resend
|φ+>
Quantum Memory
Quantum Memory
|φ+>
Quantum Memory
?
vs.
|r>
|r>
|φ+>
|00>
|φ+>
Quantum Memory
|0>
Quantum Memory
|0>
|0>
|0>
|00>
Quantum Memory
|0>
|0>
?
vs.
|0>
|0>
|φ+>
|00>

Our Protocol: Security

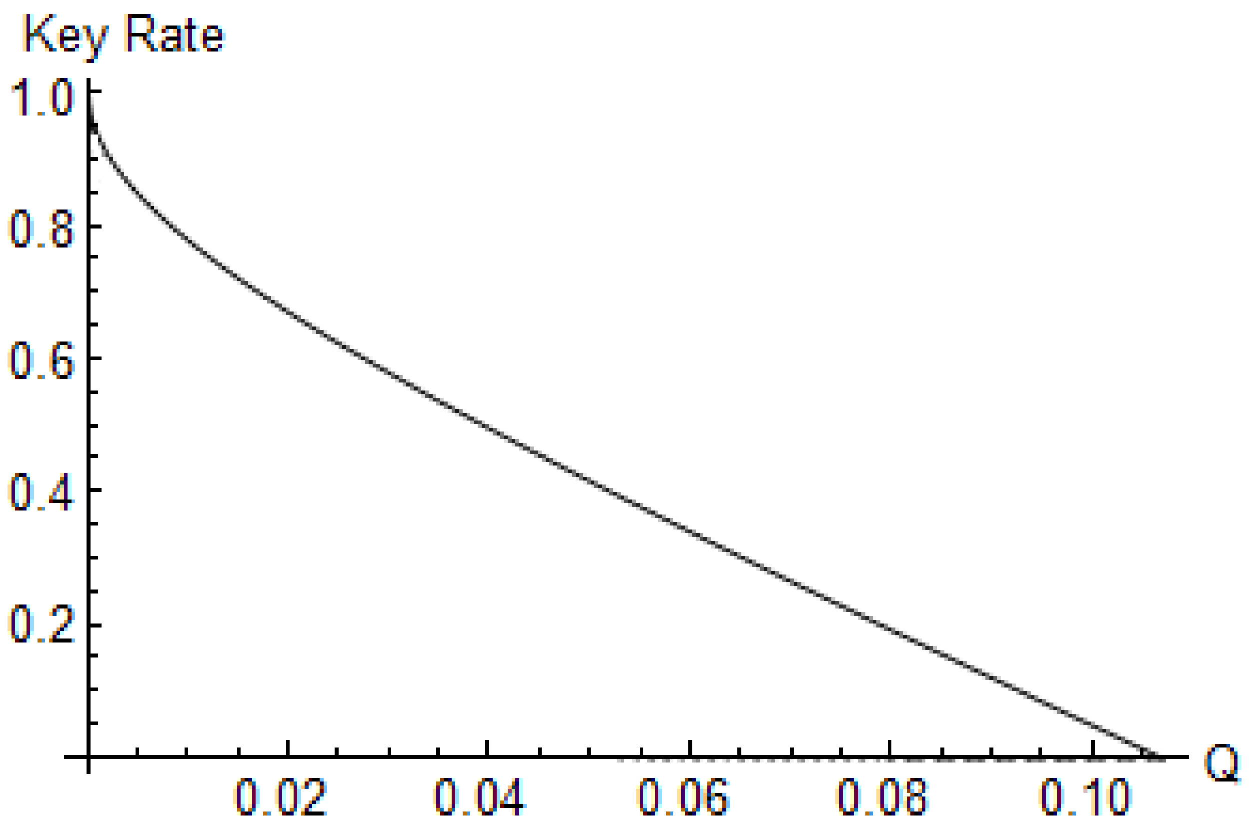
- We consider two scenarios:
  - First, the Server is semi-honest. In this case, we prove that our protocol can withstand up to a 19.9% error rate.
  - Second (worst case), the Server is adversarial. In this case, we prove our protocol can withstand up to 10.65% noise.
- Proof requires different techniques – though we do use a result similar to our first Theorem along the way...

Security: Honest Server



$$r \geq 1 - h\left(Q^2\right) - Q^2 - 2(1-Q)\sqrt{\frac{1}{2}Q - \frac{3}{4}Q^2}$$

Security: Adversarial Server



$$r \geq 1 - h\left(2Q^2\right) - 2\left(\sqrt{1-Q}\left(Q + \sqrt{p_W}\right) + Q^2\right)$$

Summary

Summary

A) We have developed new analytical and proof techniques which can be applied to future SQKD protocols

- We have also applied these techniques to the security proofs of two different SQKD protocols
- This is the first time a proof of unconditional security has been achieved for a semi-quantum protocol.
- All prior SQKD protocol papers simply stated "A and B must abort if the error rate is greater than some user-defined amount"

Summary

B) We have developed new semi-quantum protocols with unique features

- We also leveraged our previous security results to prove their unconditional security

C) We have shown it is possible for two limited classical users to establish a secret key with the help of an untrusted quantum server

We have proven that even with limited, classical users, protocols exist with security comparable to fully quantum ones.

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.

Publications while at Stevens

- Security proof of a semi-quantum key distribution protocol. *To appear, proc. IEEE ISIT 2015 (Hong Kong)*.
- Mediated semi-quantum key distribution. Phys. Rev. A. 91 032323, 2015.
- History Dependent Quantum Walk on the Cycle with an Unbalanced Coin. To appear Physica A; pre-print available online: arXiv:1411.6298
- Security in the Semi-Quantum Setting. Abstract presented at the AMS/MAA Joint Math Meetings, San Antonio TX. January 2015
- Restricted Attacks on Semi-Quantum Key Distribution Protocols. Quantum Information Processing: 13(11), pages 2417-2436 (2014)
- An Algorithm for Evolving Multiple Quantum Operators for Arbitrary Quantum Computational Problems. Proc. GECCO Comp. 2014 (Vancouver, BC, Canada)
- Using Evolutionary Techniques to Analyze the Security of Quantum Key Distribution Protocols. Proc. GECCO Comp. 2014 (Vancouver, BC, Canada)
- n-Player Impartial Combinatorial Games with Random Players. to appear Theoretical Computer Science
- Regarding Modular Multiplicative Graphs. Graph Theory Notes of NY LXIV, pages 45-48, May 2013
- On the Emergent Behaviors of a Robot Controlled by a Real-Time Evolving Neural Network. Proc. of Artificial Life 13, pages 364-371, 2012. (East Lansing, MI)

Thank you! Questions?