Key-Rate Bound of a Semi-Quantum Protocol using an Entropic Uncertainty Relation

Walter O. Krawec

Computer Science & Engineering Department
University of Connecticut
Storrs, CT USA

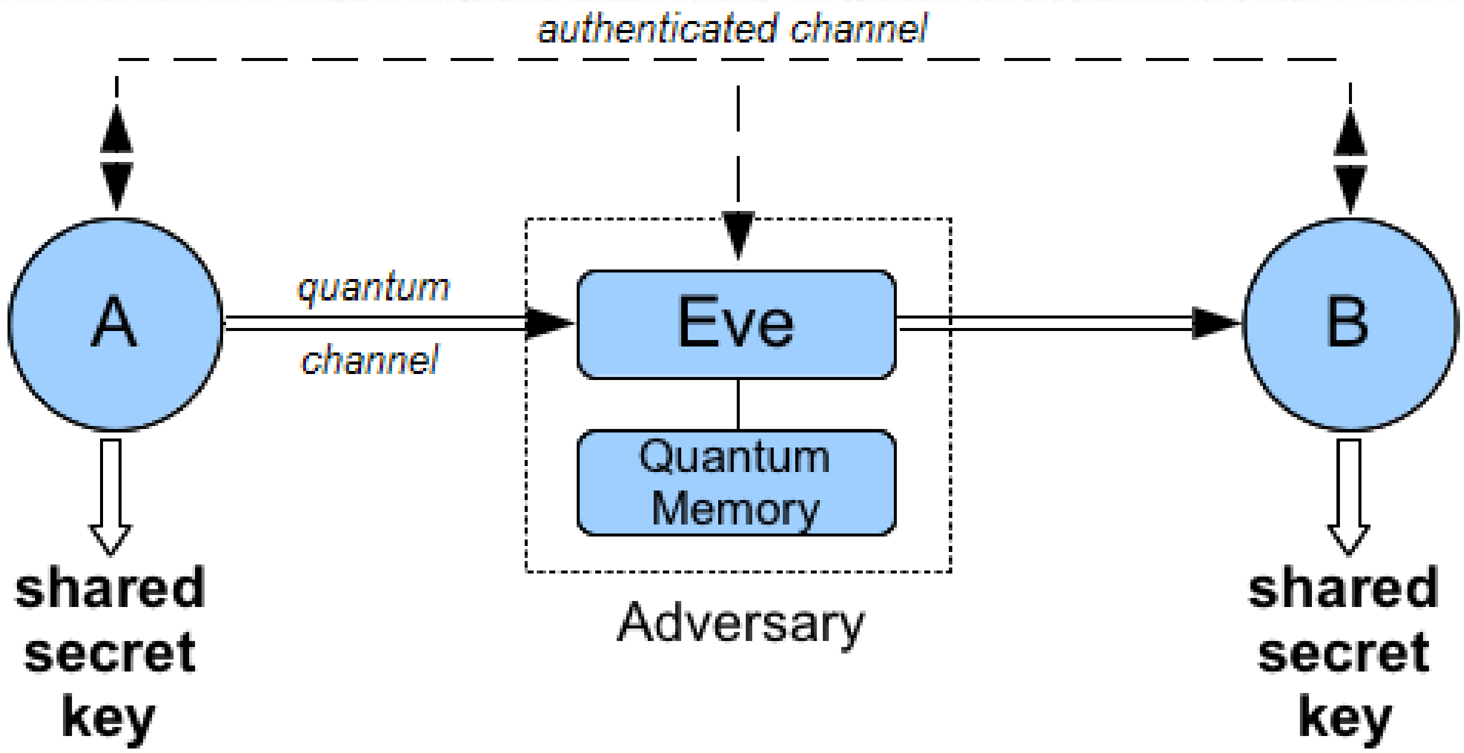
Email: walter.krawec@gmail.com

ISIT 2018

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*

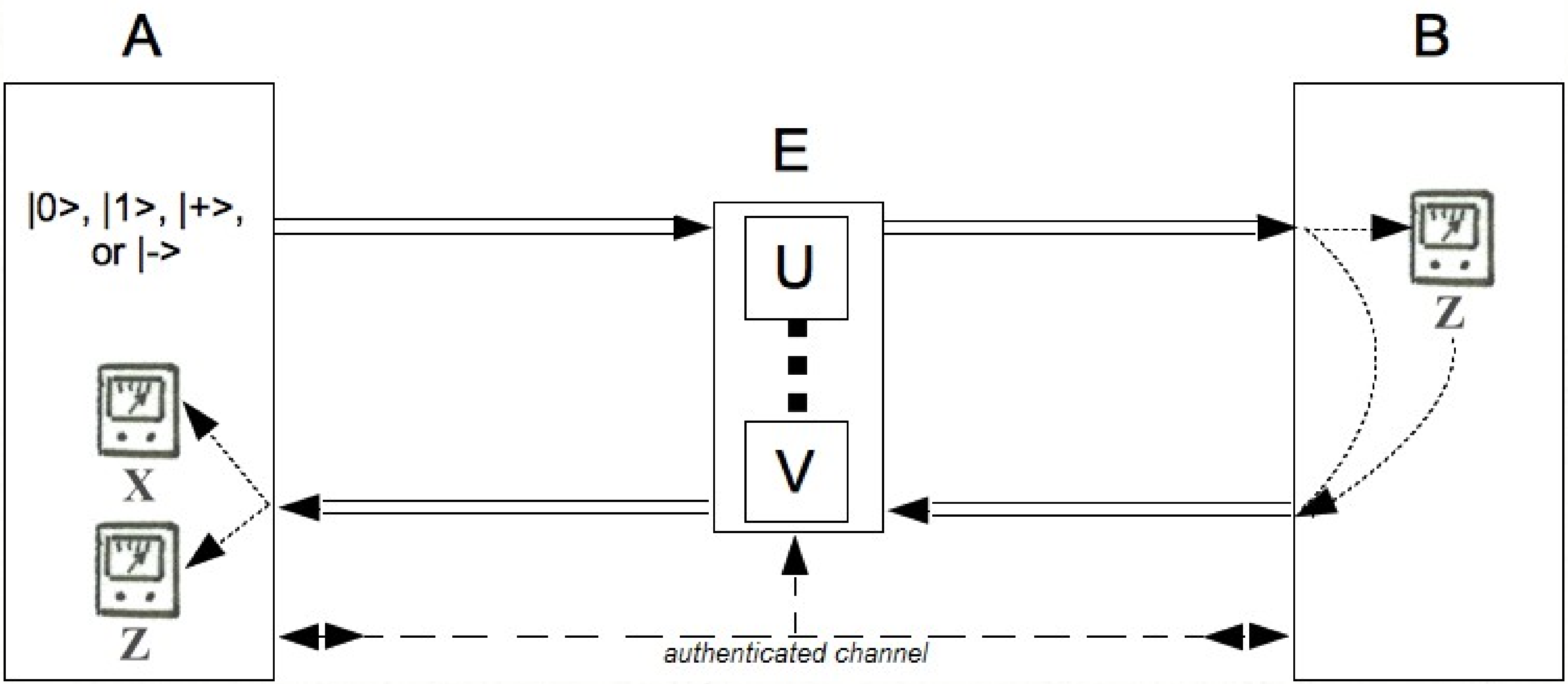
Quantum Key Distribution



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”
    - He can only directly work with the Z = {|0>, |1>} basis.
- Theoretically interesting:
    - “How quantum does a protocol need to be in order to gain an advantage over a classical one?”
- Practically interesting:
    - What if equipment breaks down or is never installed?
- **Requires a two-way quantum communication channel**

Semi-Quantum Key Distribution



SQKD Security

- Model introduced in 2007
    - With many protocols developed
    - But security proofs were in terms of "robustness"
- Not until 2015 that rigorous security proofs became available for some protocols along with noise tolerances and key-rate bounds

Original SQKD Protocol: Prior Work

- 2015: First proof - shown to tolerate 5.34%
- 2017: Adding *mismatched measurements* allows noise tolerance of 11%
  - Same as BB84!
  - But: requires the collection and use of 18 different measurement statistics

SQKD Security

- This work – new proof of security based on entropic uncertainty relation (and other tools...)
    - We show how to use this relation on semi-quantum protocols for the first time
    - Deriving a new key-rate bound without the need for mismatched measurements
        - Result is a much cleaner expression with less reliance on statistics
        - But lower noise tolerance...
- We also derive some interesting results and techniques applicable to other SQKD protocols...

SQKD Security

- Note – other work used entropic relation for two-way ***fully quantum*** protocols * but:
  - Only works for protocols that have certain "symmetry" properties
  - Semi-quantum protocols do not apply to this construction
  - We are the first to show how entropic uncertainty relations can be applied to the semi-quantum model

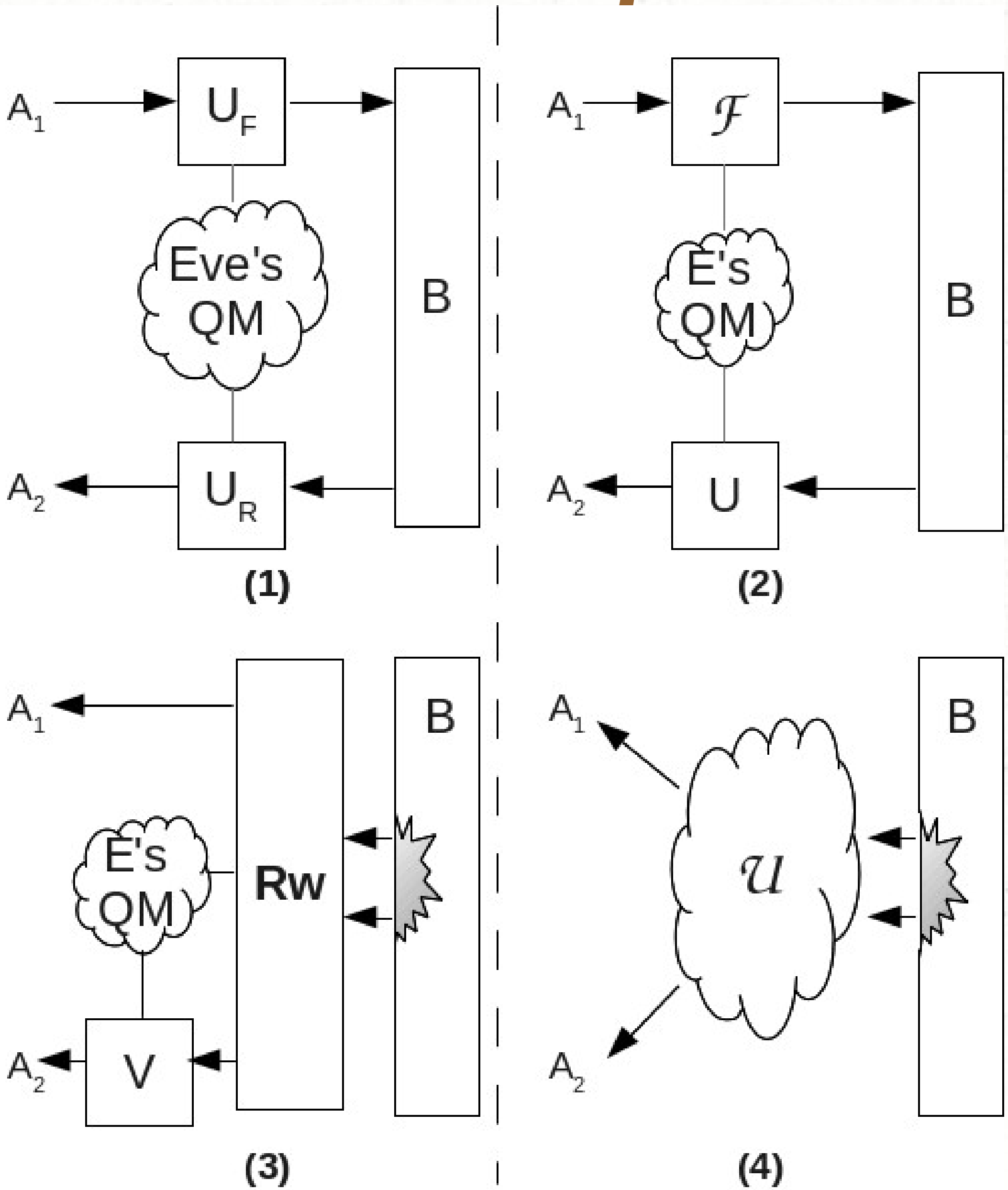
* N. Beaudry, M. Lucamarini, S. Mancini, and R. Renner. Security of two-way quantum key distribution. PRA 88(6)062302, 2013

Security Proof

Three Steps...

- First, we prove that for *any* semi-quantum protocol, it is sufficient to consider a “restricted” form of attack that is easier to analyze
- Second, we design a new “toy” protocol that is easier to analyze but implies security of the SQKD one.
- Third, we use an entropic uncertainty bound and a continuity bound on conditional von Neumann entropy to analyze the “toy” protocol.

Three Steps...



General QKD Security

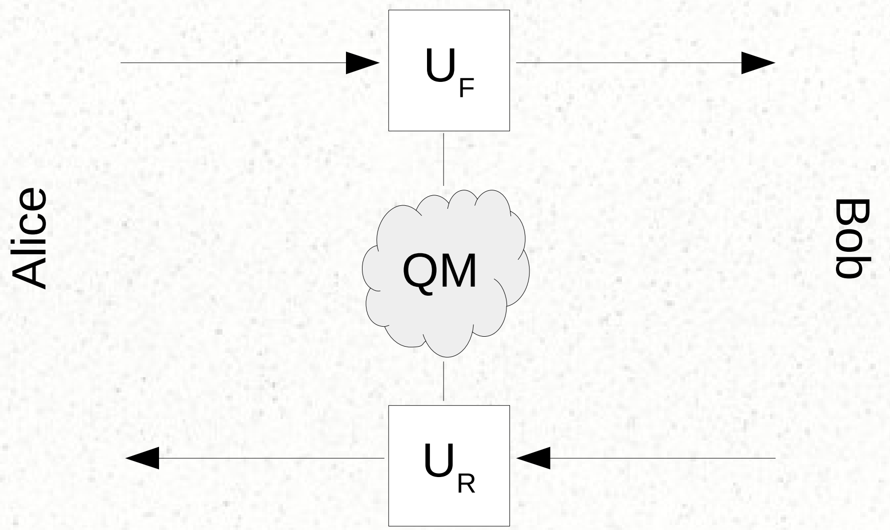
- We consider collective attacks (and comment on general attacks later)
- After the quantum communication stage and parameter estimation stage, A and B hold an N bit raw key; E has a quantum system
- They then run an error correcting protocol and privacy amplification protocol
- Result is an l(n)-bit secret key – of interest is Devetak-Winter key-rate:

$$r = \lim_{N \to \infty} \frac{l(N)}{N} = \inf \left(S(A|E) - H(A|B) \right)$$

Step 1: Restricted Attack

Restricted Attack

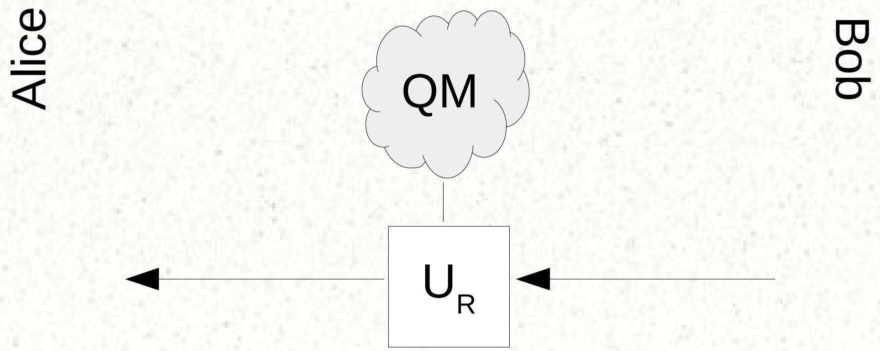
- The most general collective attack is a pair of unitary operators (U_F, U_R)



- Each U_i acts on Hilbert space H_{TE}

Restricted Attack

- For *single-state* protocols (where A only sends |+>), it was shown restricted attacks exist [5]...



- We prove a similar result for *multi-state* protocols

Restricted Attack

- A Restricted Collective Attack with respect to ONB B={|v$_0$>, |v$_1$>} is a tuple (q_0, q_1, n_0, n_1, U_R) where:

$$q_{0,}\, q_1 \in [0,1]$$
$$n_{0,}\, n_1 \in \{ z \in C \text{ such that } |z| \leq 1 \}$$
$$U_R \, is\, unitary\, acting\, on\, H_{TE}$$

- Subject to:

$$q_0 n_1 \sqrt{1-q_1^2} + q_1 n_0^* \sqrt{1-q_0^2} = 0$$

Restricted Attack: (q_0, q_1, n_0, n_1, U_R)

- Eve first applies operator "F" whose action is defined as:

$$F|v_0\rangle = q_0|0,0\rangle_{TE} + \sqrt{1-q_0^2}|1,e\rangle_{TE}$$
$$F|v_1\rangle = \sqrt{1-q_1^2}|0,f\rangle_{TE} + q_1|1,0\rangle_{TE}$$

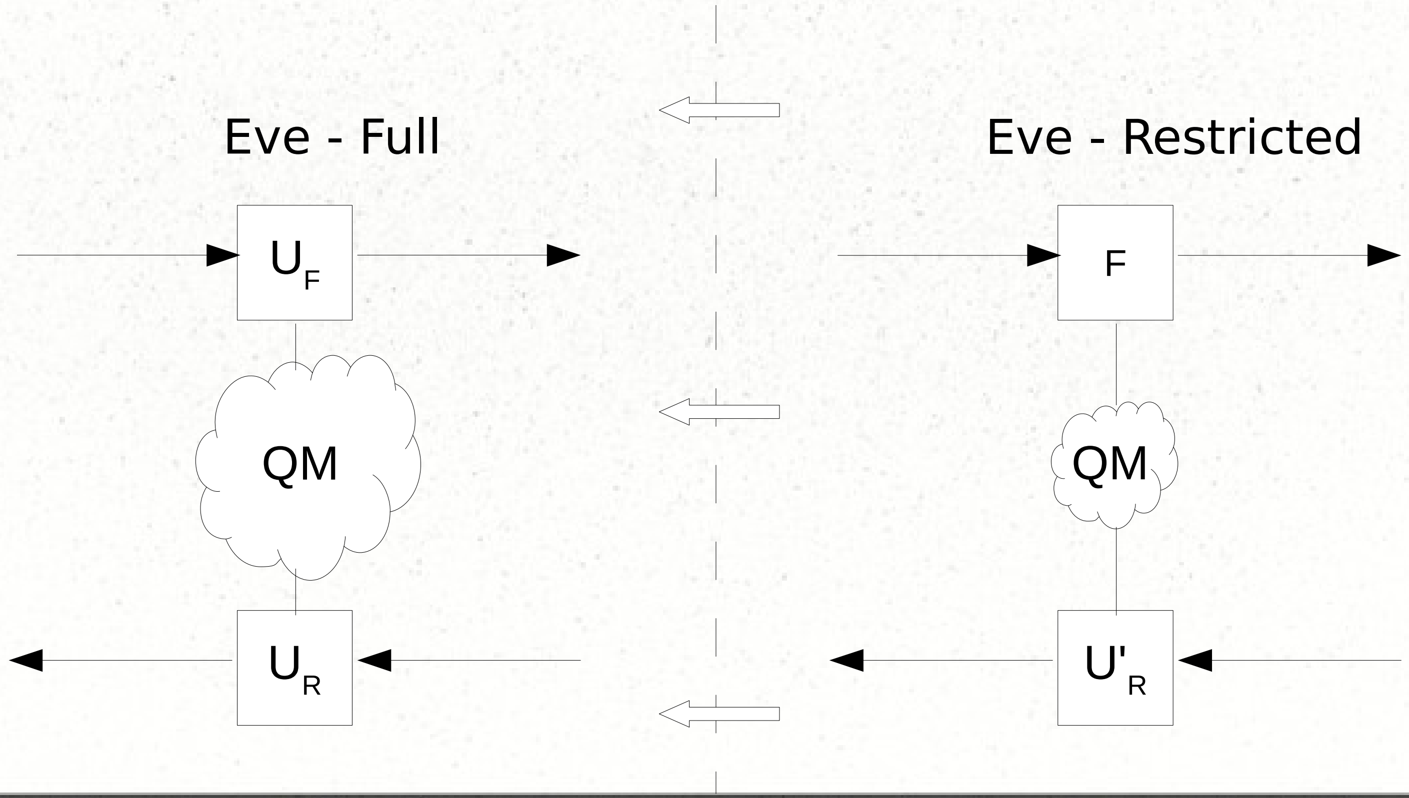
where:

$$|e\rangle = n_0|0\rangle + \sqrt{1-|n_0|^2}|1\rangle$$
$$|f\rangle = n_1|0\rangle + \sqrt{1-|n_1|^2}|1\rangle$$

- Then, on the return channel, she applies U_R
  - Acting on H_{TE}

Restricted Attack: $(q_0, q_1, n_0, n_1, U_R)$

- We prove for every collective attack, there exists an equivalent restricted attack
    - Thus, only need to consider restricted attacks for *any* SQKD protocol



Step 2: New Toy Protocol

Reduction

- Goal: Construct a new protocol that is easier to analyze
- Now, Bob *who will no longer be classical* will prepare quantum states and send them to Alice (who is still quantum)
    - Thus, it is a *one-way* protocol
- We do this using a ***"Rewind"*** operator...

New Protocol

- Now, consider the following new "toy" protocol (which is **not** semi-quantum)
  - Bob chooses randomly to "*measure*" or to "*reflect*" and prepares the state:

$$\sqrt{p_0}|0,0,0>_{A_1A_2B} + \sqrt{1-p_0}|1,1,0>_{A_1A_2B}$$ If "Reflect"

$$\sqrt{p_0}|0,0,0>_{A_1A_2B} + \sqrt{1-p_0}|1,1,1>_{A_1A_2B}$$ If "Measure"

  - Sends particle A_1 and A_2 to Alice who measures both registers in Z or X basis

New Protocol

- Now, consider the following new "toy" protocol (which is **not** semi-quantum)
    - Bob chooses randomly to "*measure*" or to "*reflect*" and prepares the state:

$$\sqrt{p_0}|0,0,0>_{A_1 A_2 B} + \sqrt{1-p_0}|1,1,0>_{A_1 A_2 B}$$ If "Reflect"

$$\sqrt{p_0}|0,0,0>_{A_1 A_2 B} + \sqrt{1-p_0}|1,1,1>_{A_1 A_2 B}$$ If "Measure"

We allow Eve to control this value

New Protocol

- Now, consider the following new "toy" protocol (which is **not** semi-quantum)
    - Bob chooses randomly to "*measure*" or to "*reflect*" and prepares the state:

$$\sqrt{p_0}|0,0,0>_{A_1A_2B}+\sqrt{1-p_0}|1,1,0>_{A_1A_2B}$$ If "Reflect"

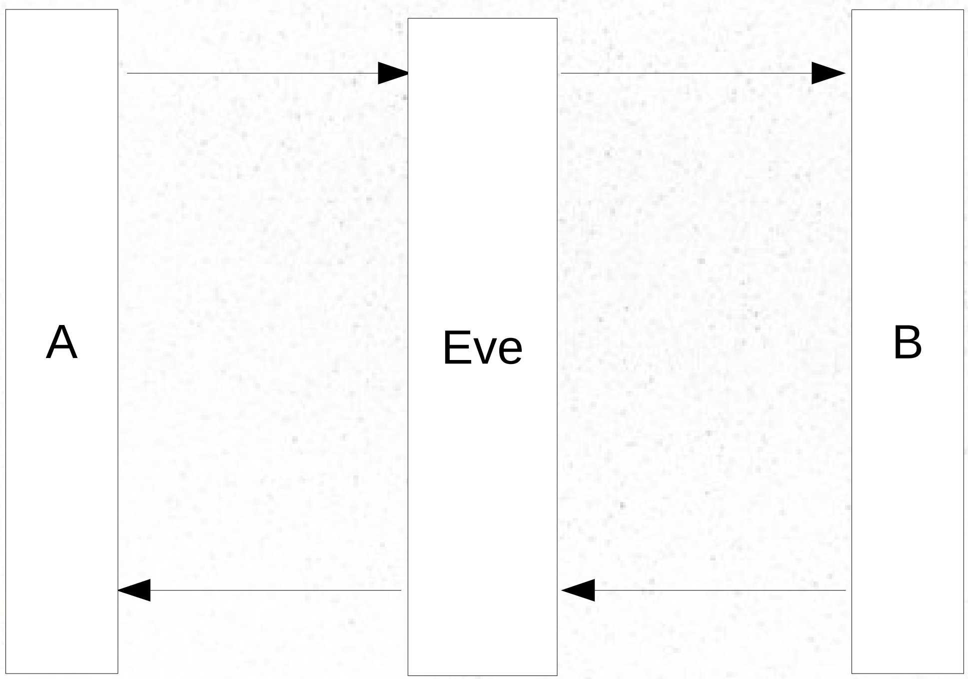
$$\sqrt{p_0}|0,0,0>_{A_1A_2B}+\sqrt{1-p_0}|1,1,1>_{A_1A_2B}$$ If "Measure"

We allow Eve to control this value

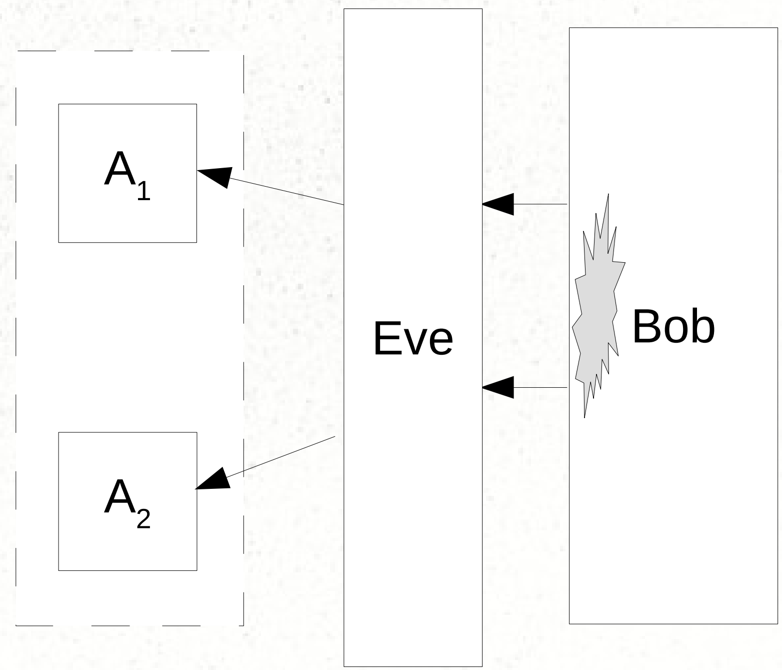
Furthermore, she gets to attack *both* registers simultaneously

New Protocol

Actual SQKD Protocol



Our new "toy" Protocol

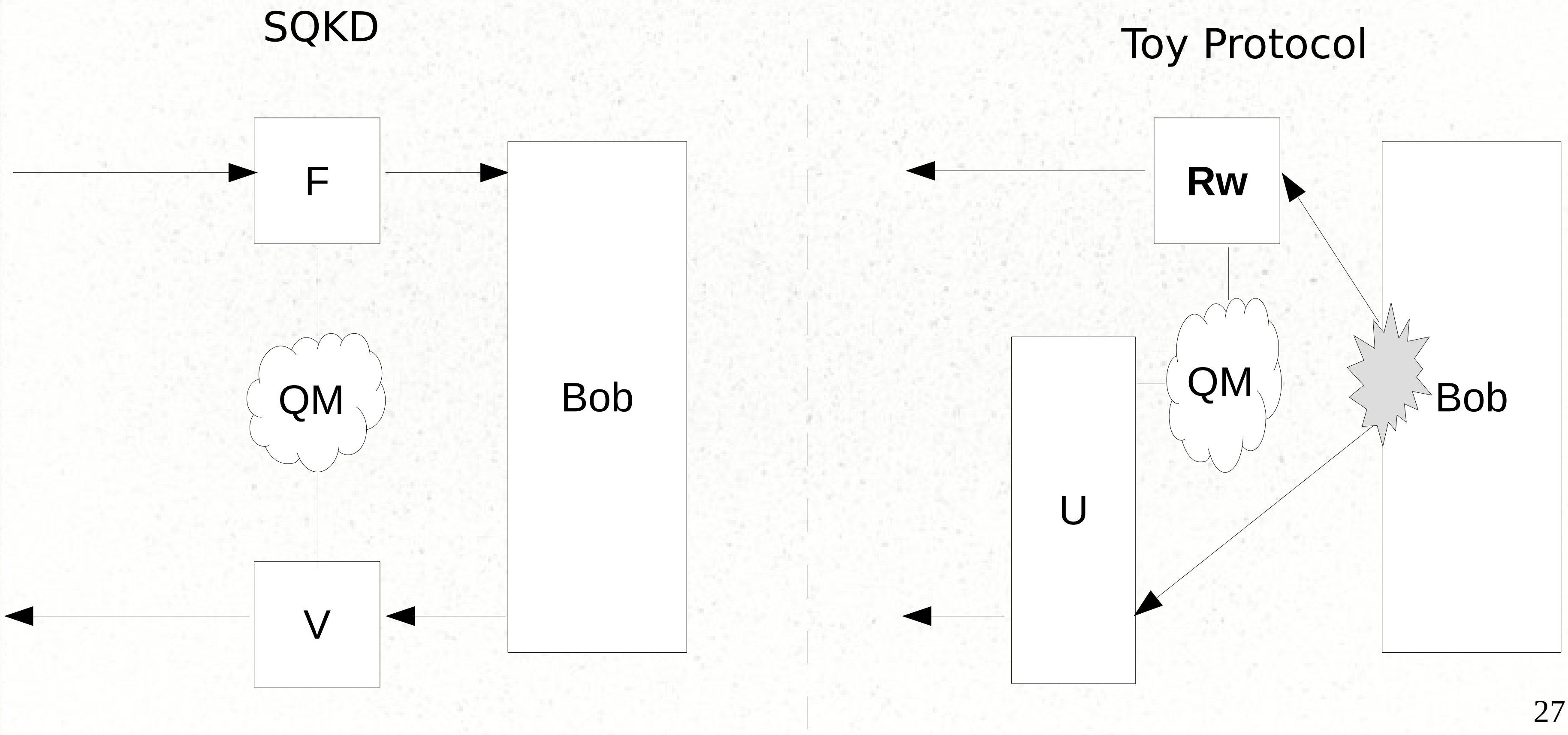


Security of new protocol ==> SQKD

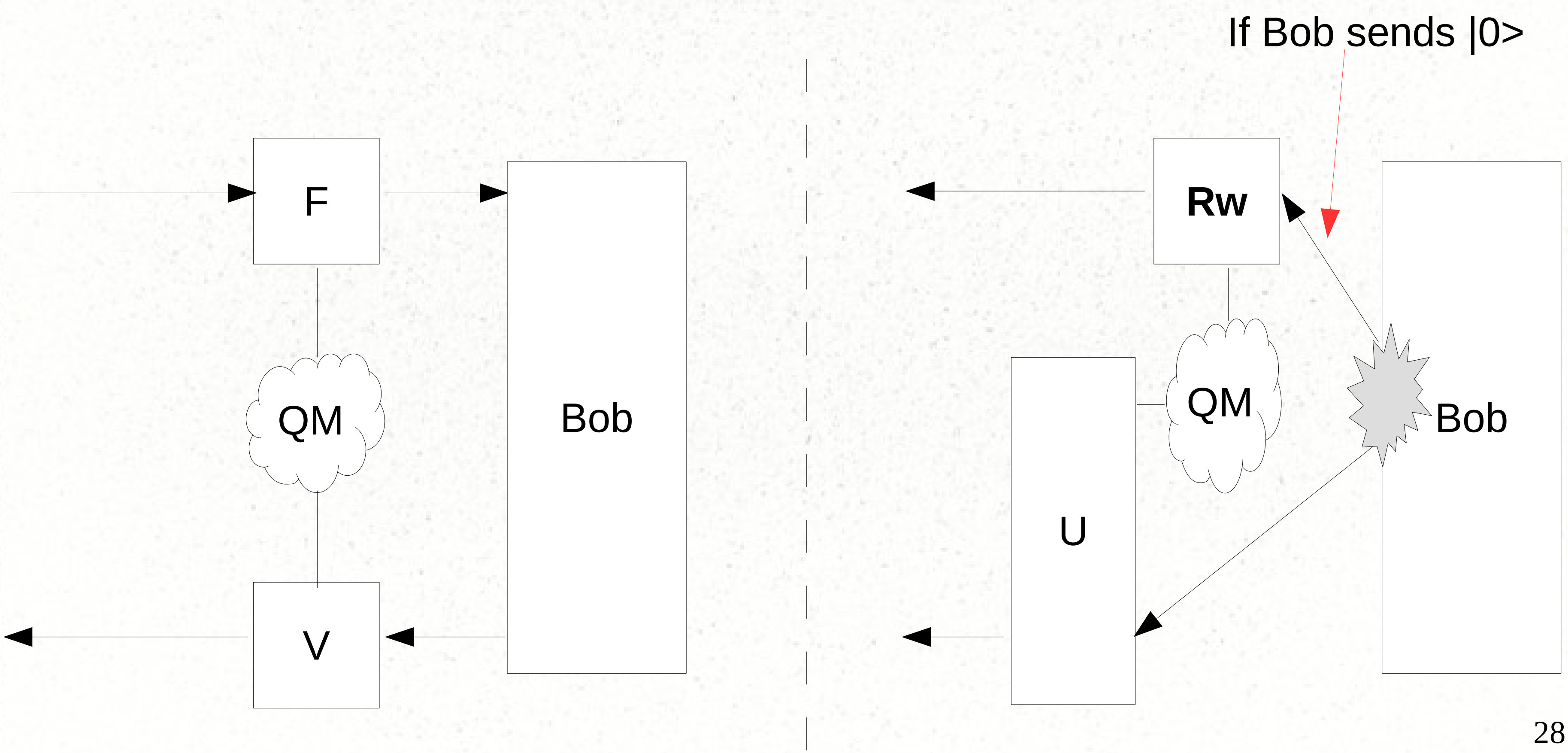
Theorem 2: Let (U_F, U_R) be a collective attack against the original SQKD protocol and ρ_{ABE} be the density operator describing the protocol under this attack. Then there exists an attack (p_0, U) against the new protocol such that:

- If σ_{ABE} is the density operator modeling new protocol under attack (p_0,U), then $\sigma_{ABE}=\rho_{ABE}$

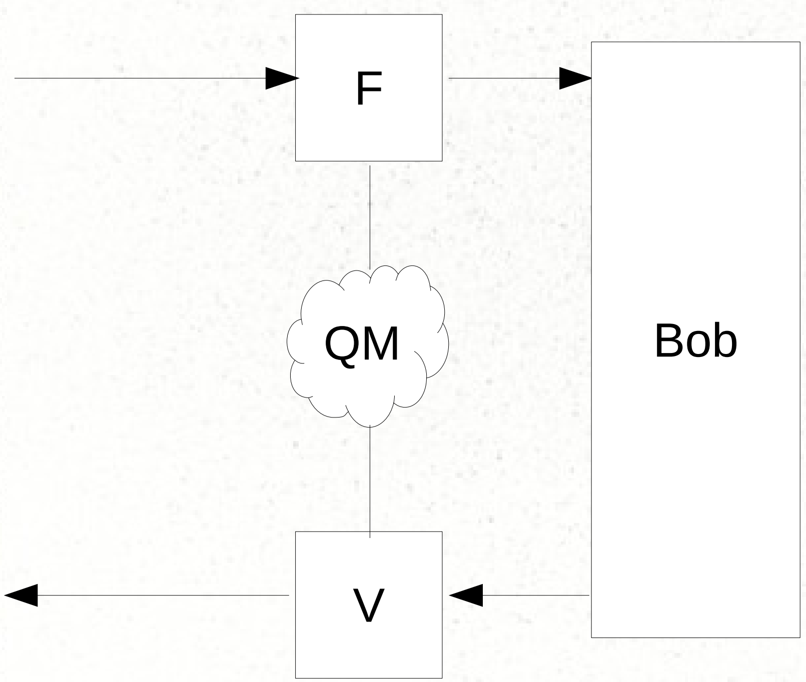
Proof "idea"

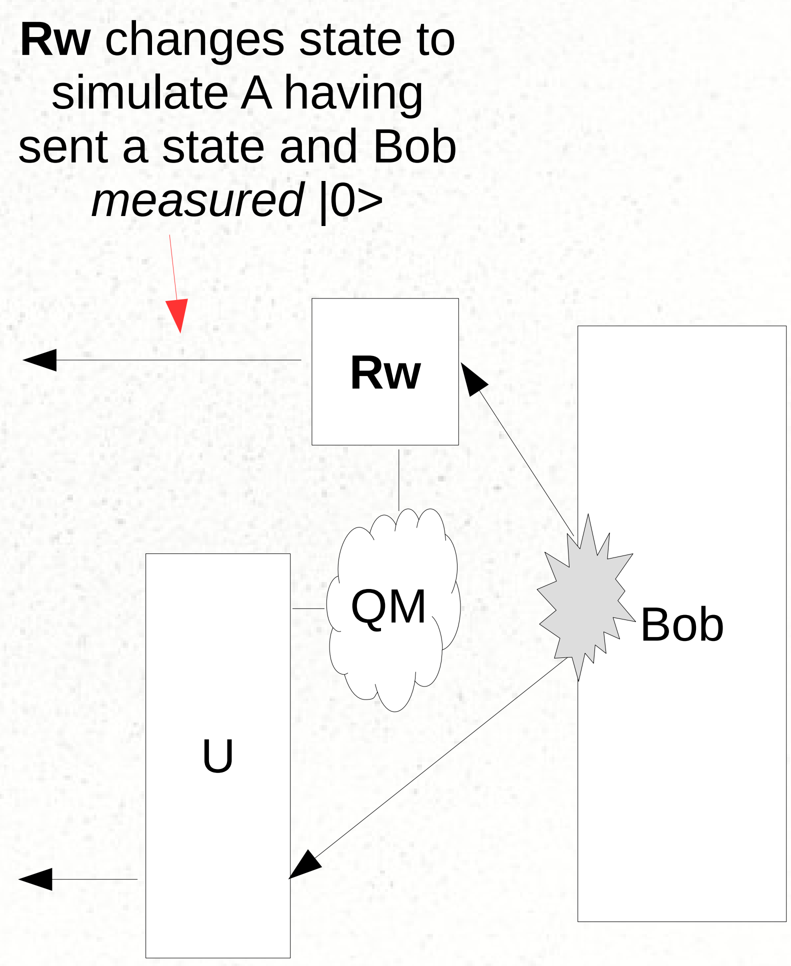


Proof "idea"

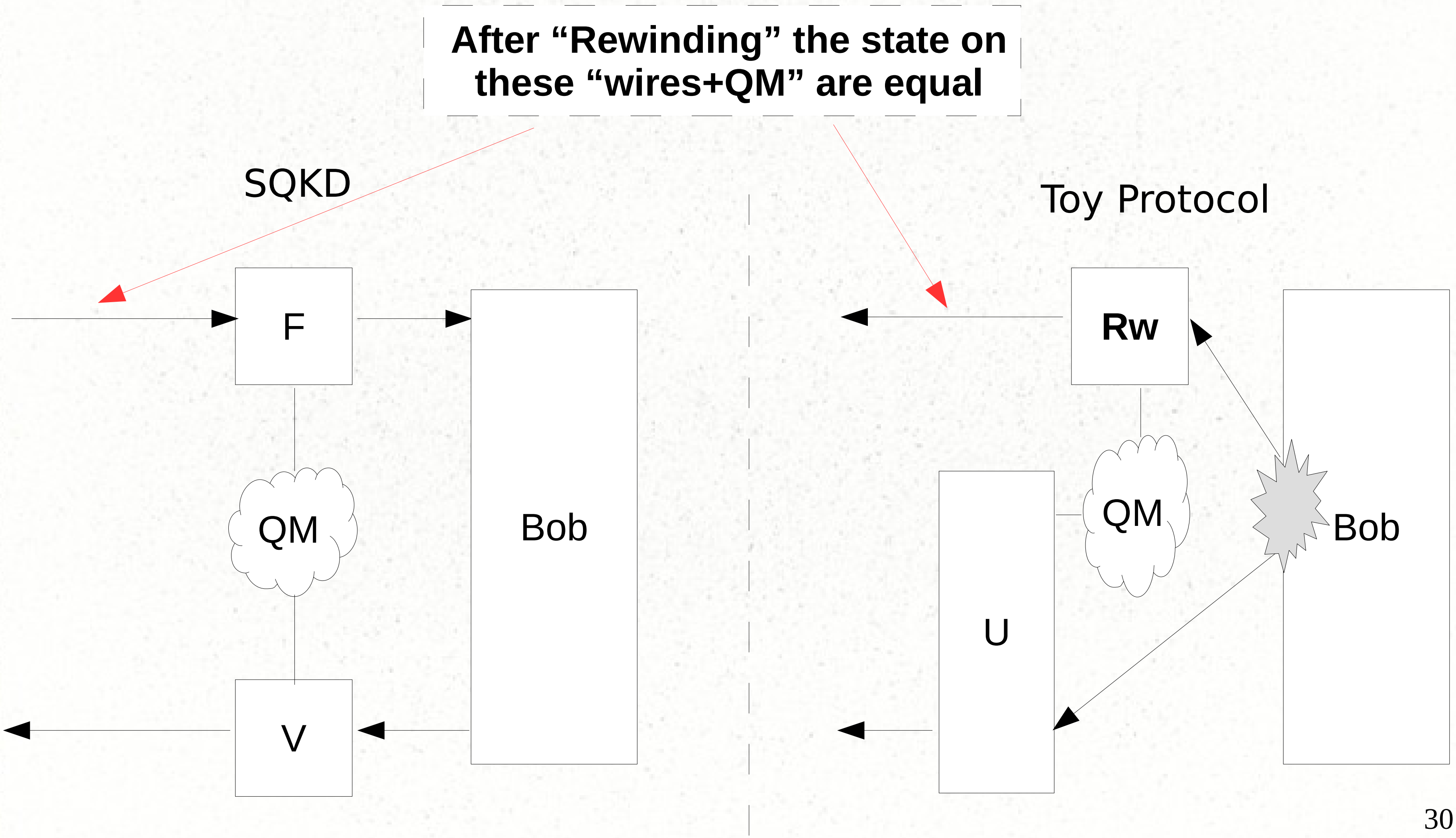


Proof "idea"


F
QM
Bob
V

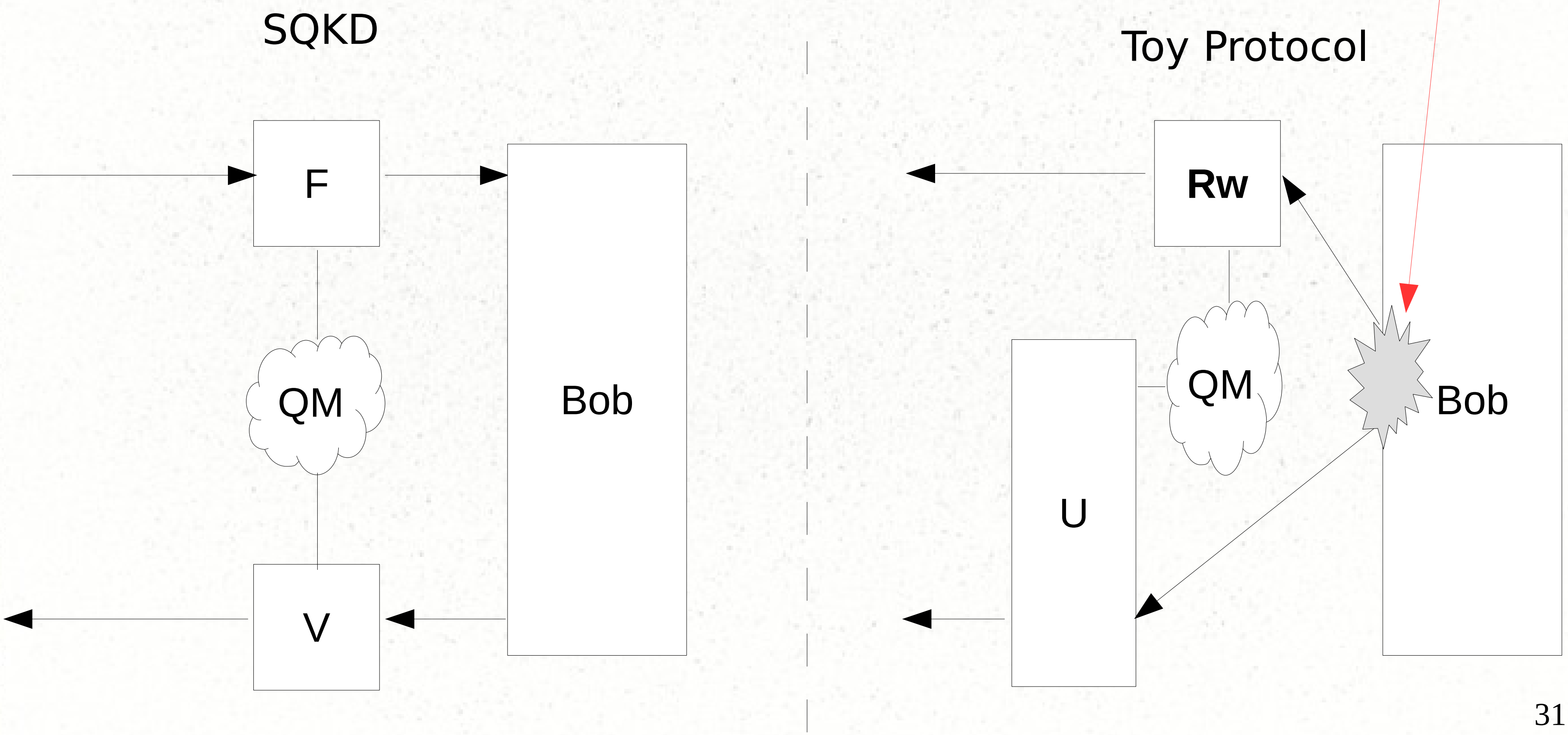

Rw changes state to simulate A having sent a state and Bob *measured* |0>
Rw
QM
U
Bob

Proof "idea"


After "Rewinding" the state on these "wires+QM" are equal
SQKD
Toy Protocol
F
QM
V
Bob
Rw
QM
U
Bob

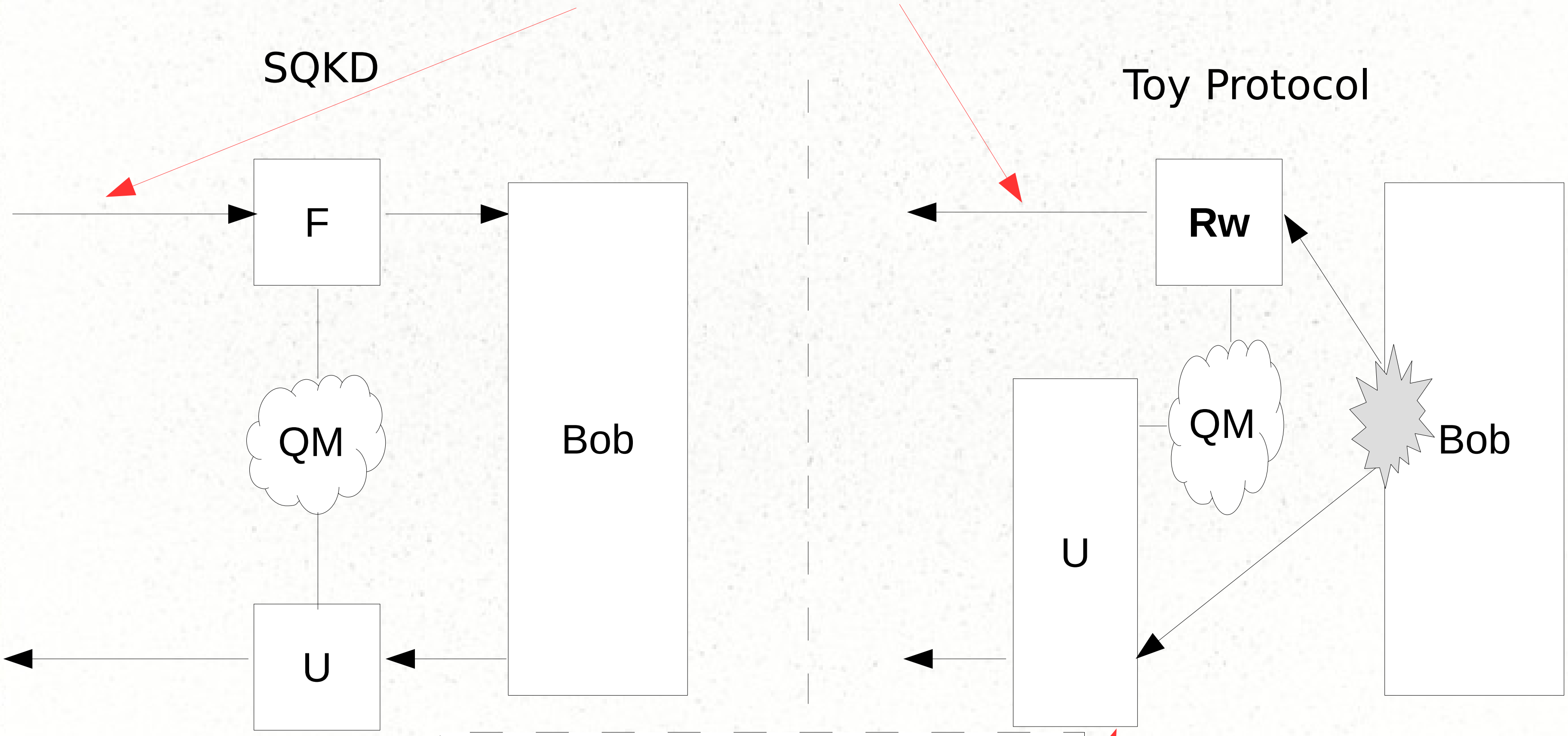
Proof "idea"

Only thing E can't "rewind" is the probability of observation



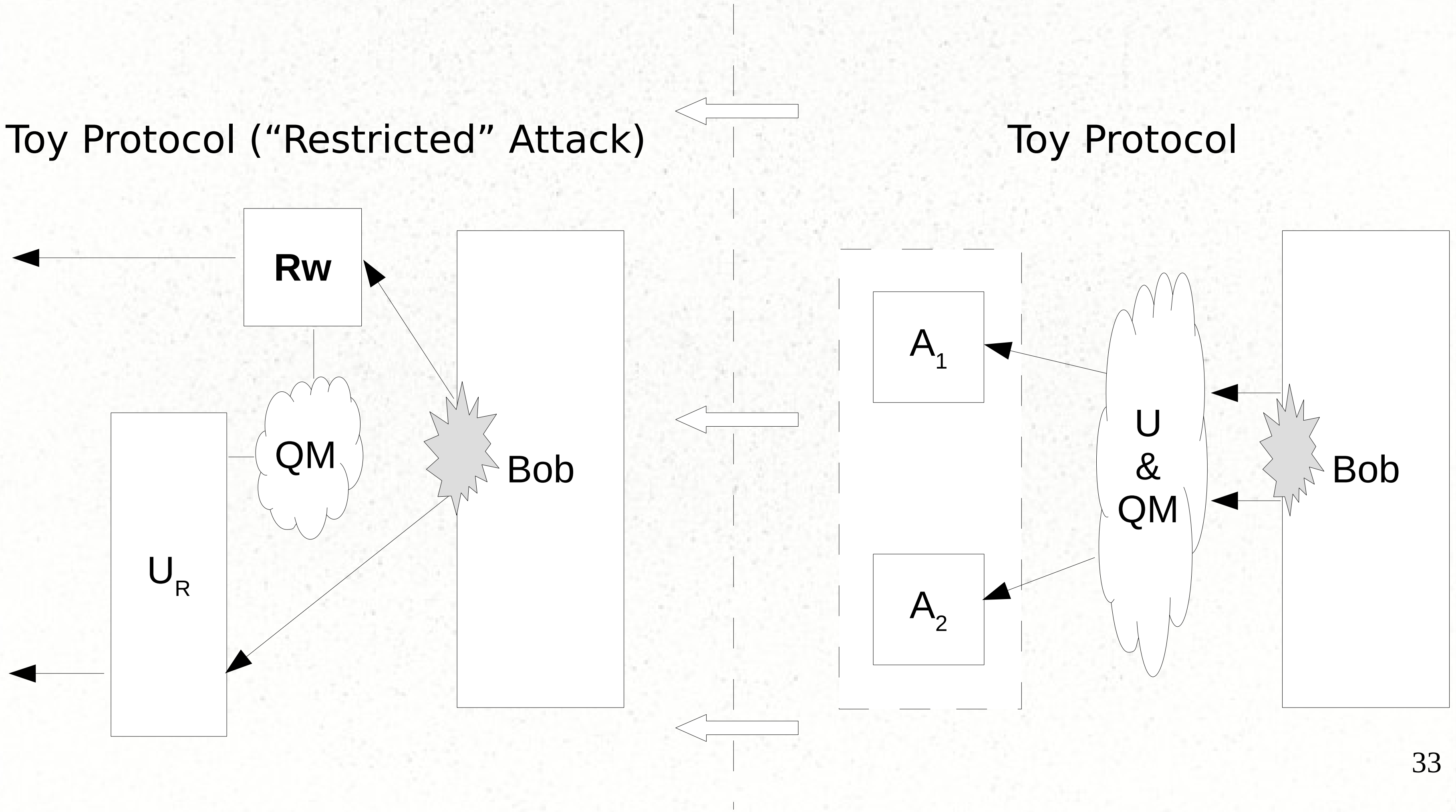
Proof “idea”

After “Rewinding” the state on these “wires+QM” are equal



These two operators are the same then

Of course, giving Eve more power doesn't hurt...



Step 3: Security of New Protocol

(which then implies security of SQKD)

Security of New Protocol

- There are two modes to the new protocol:
  - "Reflect" $\sqrt{p_0}|0,0,0>_{A_1 A_2 B} + \sqrt{1-p_0}|1,1,0>_{A_1 A_2 B}$
  - "Measure" $\sqrt{p_0}|0,0,0>_{A_1 A_2 B} + \sqrt{1-p_0}|1,1,1>_{A_1 A_2 B}$

- After attacking, but before A_1 and A_2 measure, the state of the system can be written:

$$\tau_{A_1 A_2 BE} = P_M \mu_{A_1 A_2 BE} + P_R \rho_{A_1 A_2 BE}$$

Security of New Protocol

- There are two modes to the new protocol:
  - "Reflect" $\sqrt{p_0}|0,0,0>_{A_1A_2B}+\sqrt{1-p_0}|1,1,0>_{A_1A_2B}$
  - "Measure" $\sqrt{p_0}|0,0,0>_{A_1A_2B}+\sqrt{1-p_0}|1,1,1>_{A_1A_2B}$
- After attacking, but before A_1 and A_2 measure, the state of the system can be written:

$$\tau_{A_1A_2BE}=\underbrace{P_M\mu_{A_1A_2BE}}_{\text{Measure}}+\underbrace{P_R\rho_{A_1A_2BE}}_{\text{Reflect}}$$

Security of New Protocol

- There are two modes to the new protocol:
  - "Reflect" $\sqrt{p_0}|0,0,0>_{A_1 A_2 B} + \sqrt{1-p_0}|1,1,0>_{A_1 A_2 B}$
  - "Measure" $\sqrt{p_0}|0,0,0>_{A_1 A_2 B} + \sqrt{1-p_0}|1,1,1>_{A_1 A_2 B}$

- After attacking, but before A_1 and A_2 measure, the state of the system can be written:

$$\tau_{A_1 A_2 BE} = P_M \mu_{A_1 A_2 BE} + P_R \rho_{A_1 A_2 BE}$$

Measure
Only these are used for key distillation

Reflect

Security of New Protocol

$$\tau_{A_1 A_2 BE} = P_M \mu_{A_1 A_2 BE} + P_R \rho_{A_1 A_2 BE}$$

Measure

Only these are used for key distillation

Reflect

- Thus, we must compute: $S(A_1^Z | E)_\mu$
- Instead, we will first compute: $S(A_1^Z | E)_\rho$

Security of New Protocol

Lemma 1: Let $\rho_{A_1 A_2 BE}$ be the state of the system if B chooses "Reflect" in our toy protocol. Let QX be the error rate in the X basis (e.g., probability that A_1 measures |+> and A_2 measures |->). Then:

$$S\left(A_1^Z | E\right)_\rho \geq 1 - h\left(Q_X\right)$$

Security of New Protocol

Proof (sketch):
B is completely independent of A_1A_2E.

Thus, we may trace out his system and: $\rho_{A_1A_2BE} = \rho_{A_1A_2E}$
We may now consider A_1 and A_2 as two separate parties and invoke a quantum entropic uncertainty relation* along with some properties of entropy** to show:

$$S(A_1^Z|E)_\rho + S(A_1^X|A_2)_\rho \geq 1$$

Thus:

$$S(A_1^Z|E)_\rho \geq 1 - S(A_1^X|A_2)_\rho$$
$$\geq 1 - H(A_1^X|A_2^X)_\rho = 1 - h(Q_X)$$

*: M. Berta, M. Christandl, R. Colbeck, J. Renes, and R. Renner. The uncertainty principle in the presence of quantum memory. Nature Physics 6(9):659-662, 2010.
** N. Beaudry, M. Lucamarini, S. Mancini, and R. Renner. Security of two-way quantum key distribution. PRA 88(6)062302, 2013

Security of New Protocol

$$\tau_{A_1 A_2 BE} = P_M \mu_{A_1 A_2 BE} + P_R \rho_{A_1 A_2 BE}$$

Measure

Only these are used for key distillation

Reflect

- We must compute: $S(A_1^Z | E)_\mu$
- We have computed: $S(A_1^Z | E)_\rho \geq 1 - h(Q_X)$

Security of New Protocol

$$\tau_{A_1 A_2 BE} = P_M \mu_{A_1 A_2 BE} + P_R \rho_{A_1 A_2 BE}$$

Theorem 3: Given the above density operator, let Q be the Z basis error rate in a single channel (B->A_1 and B->A_2) and let Eve's attack be "symmetric" (i.e., p_0 = ½). Let:

$$\delta = 2Q(1-Q) + \left(\frac{1}{2} + 2Q(1-Q)\right) \cdot h\left(\frac{4Q(1-Q)}{1+4Q(1-Q)}\right)$$

Then, it holds that: $S(A_1^Z|E)_\mu \geq f(Q)$, where

$$f(Q) = \begin{cases} S(A_1^Z|E)_\rho - \delta & \text{if } S(A_2^Z|E)_\rho \geq 2\delta \\ \frac{1}{2} S(A_1^Z|E)_\rho & \text{otherwise} \end{cases}$$

Security of New Protocol

$$\tau_{A_1 A_2 BE} = P_M \mu_{A_1 A_2 BE} + P_R \rho_{A_1 A_2 BE}$$

Proof – takes advantage of the concavity of von Neumann entropy and also the use of a continuity bound on conditional entropy by Winter* to bound the difference in conditional entropy between states based on the “Reflect” case and the “Measure” case:

$$|S(A_1^Z|E)_\sigma - S(A_1^Z|E)_\nu| \leq \epsilon + (1+\epsilon) \cdot h\left(\frac{\epsilon}{1+\epsilon}\right)$$

$$\text{where: } \frac{1}{2}\|\sigma_{AE} - \nu_{AE}\| \leq \epsilon \leq 1$$

*: A. Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. *Communications in Mathematical Physics*, 347(1):291-313, 2016

Summing it all up...

Final Key-Rate Expression

- In summary, we prove the key-rate of the SQKD protocol is bounded by: $\text{key-rate} \geq g(Q, Q_X) - h(Q)$

$$g(Q, Q_X) = \begin{cases} 1 - h(Q_X) - \delta & \text{if } 1 - h(Q_X) \geq 2\delta \\ \frac{1}{2}\left(1 - h(Q_X)\right) & \text{otherwise} \end{cases}$$

where:

$$\delta = 2Q(1-Q) + \left(\frac{1}{2} + 2Q(1-Q)\right) \cdot h\left(\frac{4Q(1-Q)}{1+4Q(1-Q)}\right)$$

Final Key-Rate Expression

- In summary, we prove the key-rate of the SQKD protocol is bounded by: $\text{key-rate} \geq g(Q, Q_X) - h(Q)$

$$g(Q, Q_X) = \begin{cases} 1 - h(Q_X) - \delta & \text{if } 1 - h(Q_X) \geq 2\delta \\ \frac{1}{2}(1 - h(Q_X)) & \text{otherwise} \end{cases}$$

where:

$$\delta = 2Q(1-Q) + \left(\frac{1}{2} + 2Q(1-Q)\right) \cdot h\left(\frac{4Q(1-Q)}{1+4Q(1-Q)}\right)$$

Old proof of security required multiple pages to fit equation....

Noise Tolerance Results

	Old Proof [14]	New Proof	With MM [17]
$Q_X = Q$	5.34%	**6.14%**	11%
$Q_X=2Q(1-Q)$	4.57%	**4.82%**	7.9%
$Q_X = ½ Q$	5.92%	**7.5%**	15.12%

Our new key-rate bound provides a better noise tolerance than prior work **without** mismatched measurements (MM).

However, it is not as high as results **with** MM.

This is not surprising – with MM requires the collection of 18 different measurement statistics to bound the key-rate.

Here we use only 4: Q (forwards and backwards); Q_X; and p_0

Future Work

- Can the bound be improved?
- We only considered collective attacks – does the usual techniques of applying de Finetti work here?
    - We suspect so, but do not have a formal proof
    - Difficulty is in the fact that we took advantage of the “restricted collective attack”
- Can this technique be extended to other SQKD protocols?
    - Or other two-way protocols that do not have certain “symmetry” properties?
- What about a finite-key analysis?

Thank you! Questions?

References

[2] M. Boyer, D. Kenigsberg, T. Mor. Quantum key distribution with classical Bob. PRL 99:140510, 2007

[5] W. O. Krawec. Restricted attacks on semi-quantum key distribution protocols. Quantum Information Processing. 13(11):2417-2436,2014.

[14] W. O. Krawec. Security proof of a semi-quantum key distribution protocol. In IEEE ISIT 2015, 686-690.

[17] W. O. Krawec. Quantum key distribution with mismatched measurements over arbitrary channels. Quantum Information and Computation. 17 (3&4) 209-241. 2017.

[21] N. Beaudry, M. Lucamarini, S. Mancini, and R. Renner. Security of two-way quantum key distribution. PRA 88(6)062302, 2013

[23] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. Proc. Royal Society A 461(2053) 207-235, 2005.

[24] M. Berta, M. Christandl, R. Colbeck, J. Renes, R. Renner. The uncertainty principle in the presence of quantum memory. Nature Physics 6(9):659-662, 2010.

[25] A. Winter. Tight uniform continuity bounds for quantum entropies: conditional entropy, relative entropy distance and energy constraints. Communications in Mathematical Physics. 347(1):291-313,2016.

References (cont.)

- 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.
- M. Christandl, R. Renner, and A. Ekert, A generic security proof for quantum key distribution.
- I. Devetak and A. Winter, Distillation of secret key and entanglement from quantum states. Proc. R. Soc. A 2005 461.
- W.O. Krawec, 2014, Restricted attacks on semi-quantum key distribution protocols. Quantum Information Processing, 13(11):2417-2436.

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.