Semi-Quantum Key Distribution with Limited Measurement Capabilities

Walter O. Krawec

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

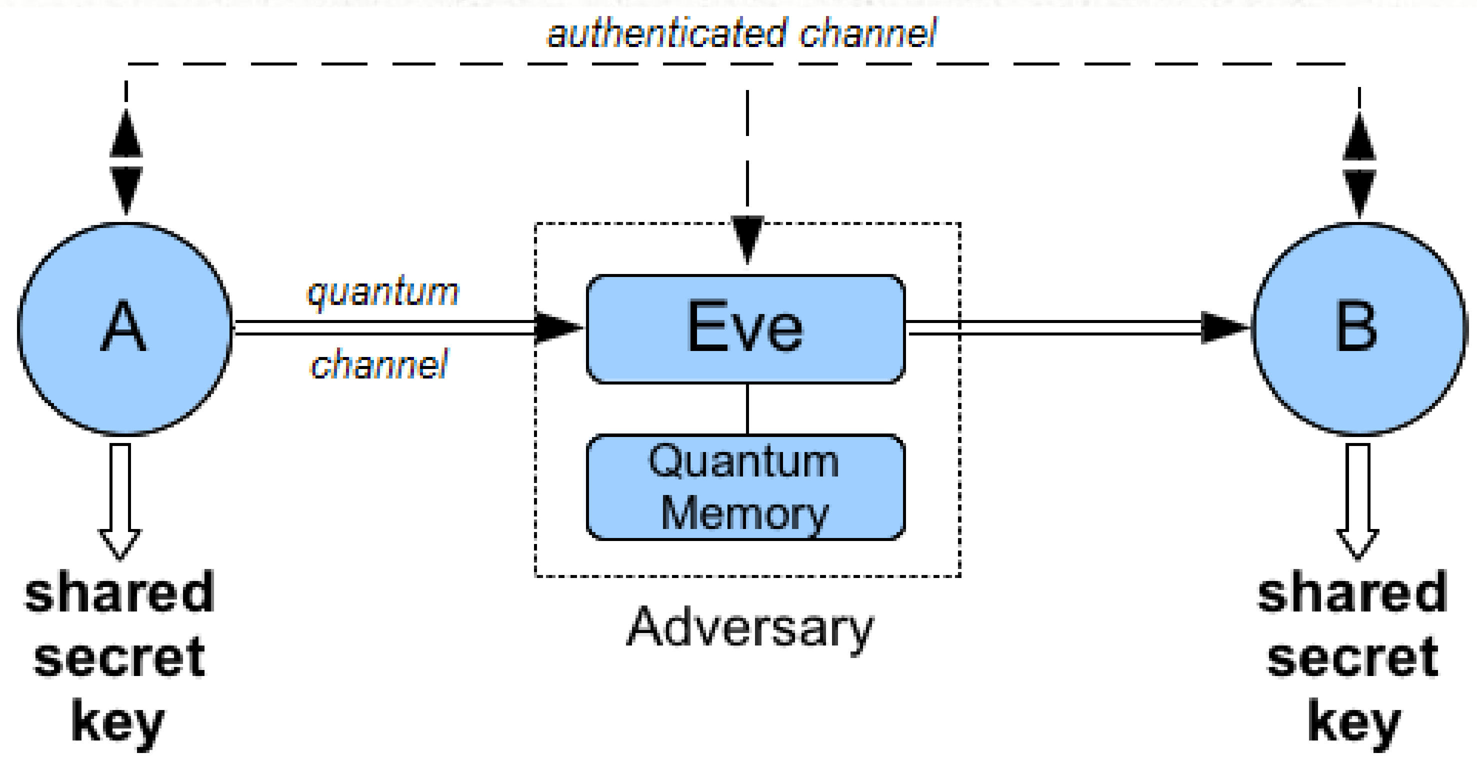
Email: walter.krawec@gmail.com

ISITA 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*

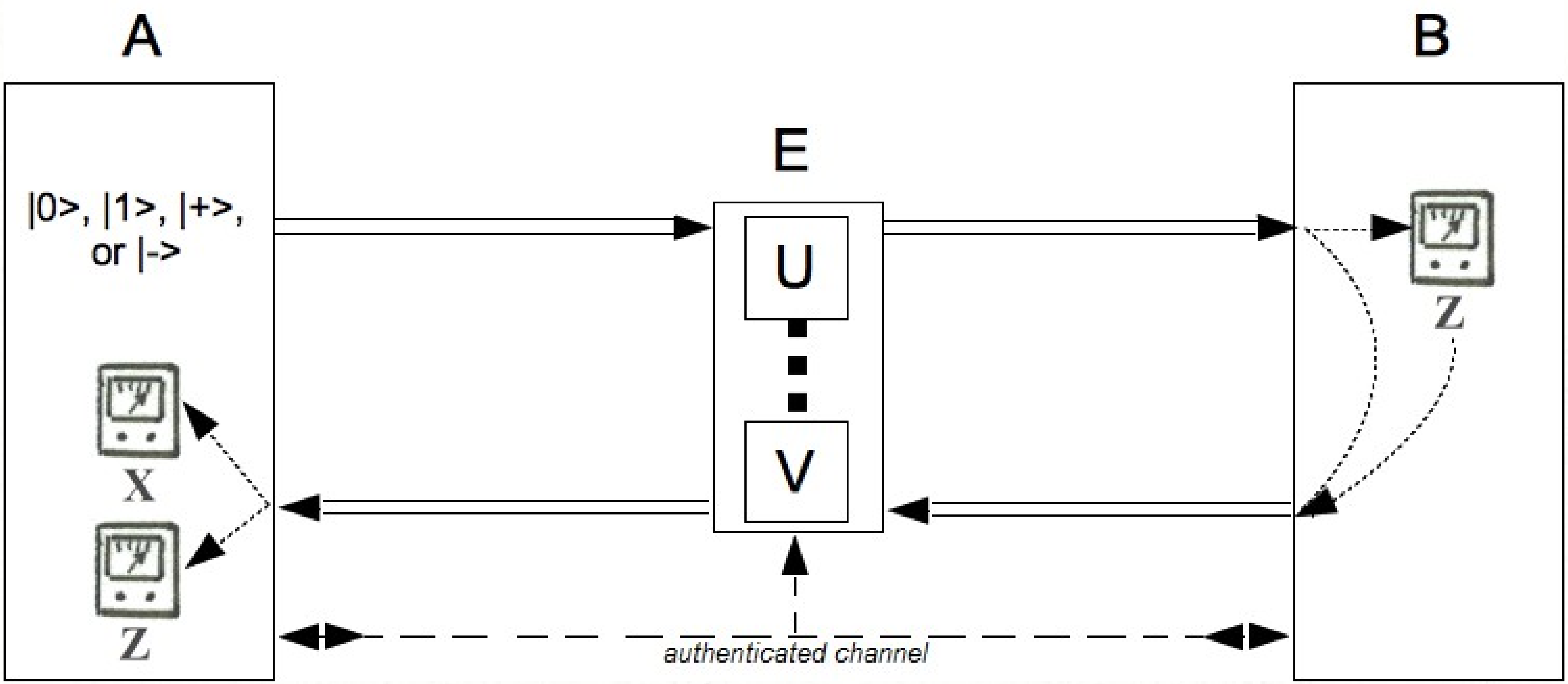
Quantum Key Distribution



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
  - Noise tolerance shown to be 6.1% if using only error-statistics
  - Tolerance is 11% if using **mismatched measurements** [5,9,10]
    - Requires 18 different measurement statistics

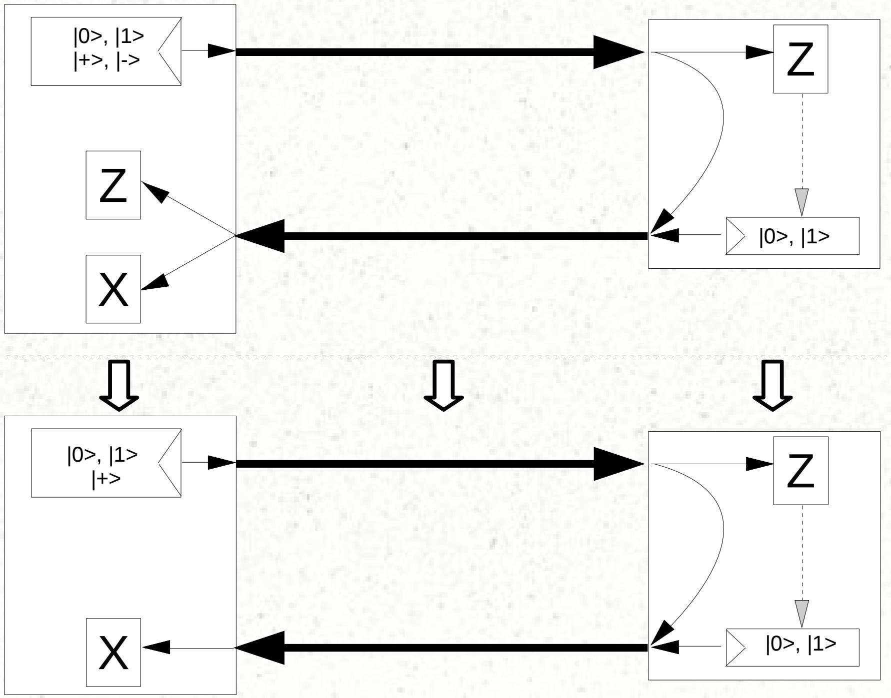
New Protocol

- All SQKD protocols require a two-way quantum channel
- All SQKD protocols so far have required the quantum user to measure in two (or more) bases
- We show this is not necessary
- Furthermore, the noise tolerance of our new protocol is just as high as BB84 assuming symmetric attacks!

New Protocol

Original:

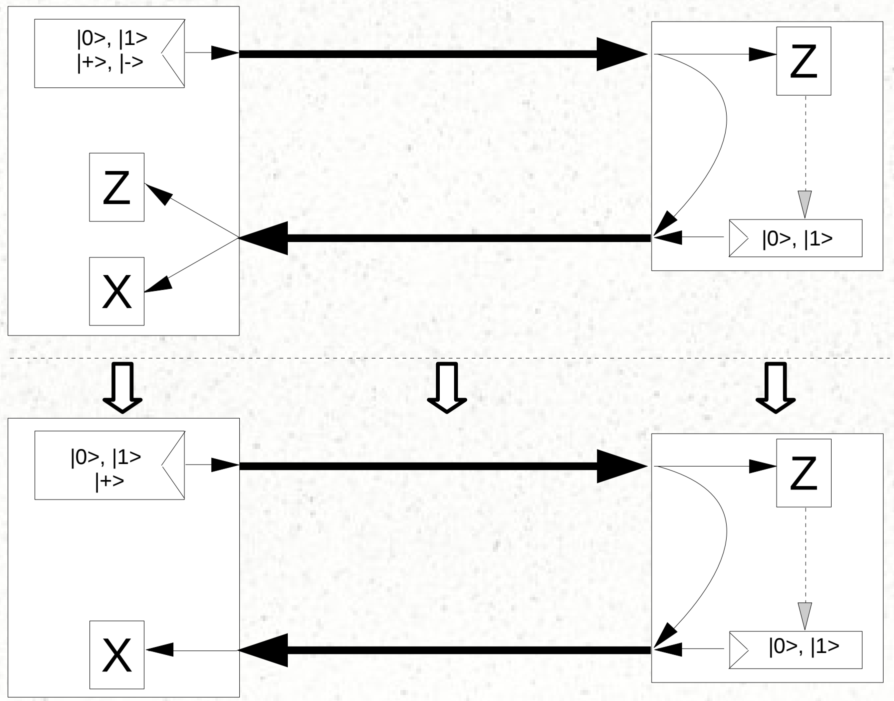
New:



New Protocol

Original:

New:



Interestingly, protocol is **insecure** if we only look at error rates – looking at mismatched measurements is **necessary** for security of this protocol!

Our Contributions

- We propose a new SQKD protocols where **both** users have severe restrictions placed on their measurement capabilities
- We show how the technique of **mismatched measurements** [9,10] can be applied to this two-way protocol to produce very optimistic key-rate bounds
  - We also show that it is necessary to look at these mismatched statistics!
- We show our protocol has the same noise tolerance as other SQKD and **fully-quantum** QKD protocols

[9] S. M. Barnett, B. Huttner, and S. J. Phoenix, “Eavesdropping strategies and rejected-data protocols in quantum cryptography,” Journal of Modern Optics, vol. 40, no. 12, pp. 2501–2513, 1993.

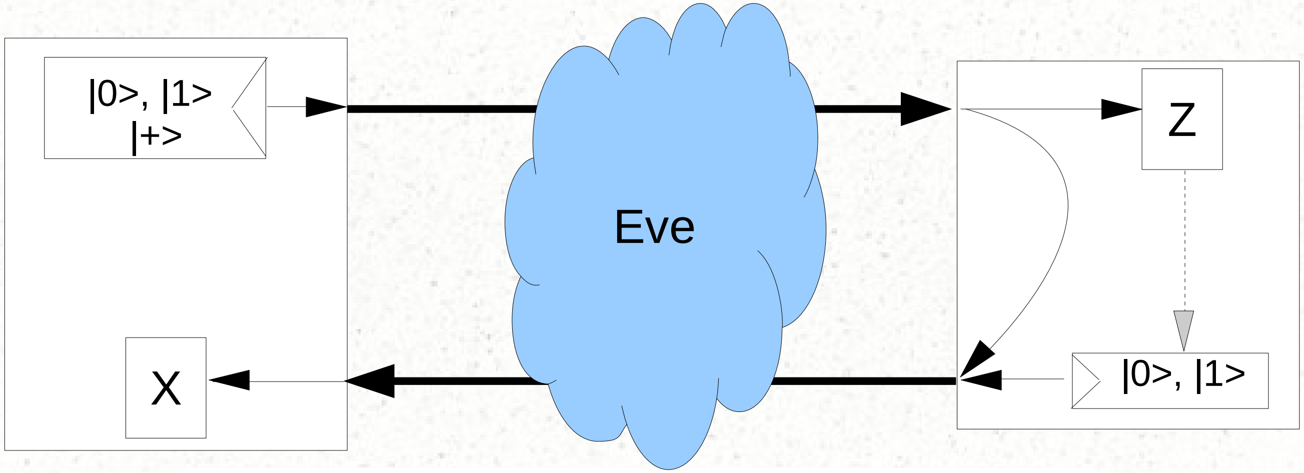
[10] S. Watanabe, R. Matsumoto, and T. Uyematsu, “Tomography increases key rates of quantum-key distribution protocols,” Physical Review A, vol. 78, no. 4, p. 042316, 2008.

The Protocol

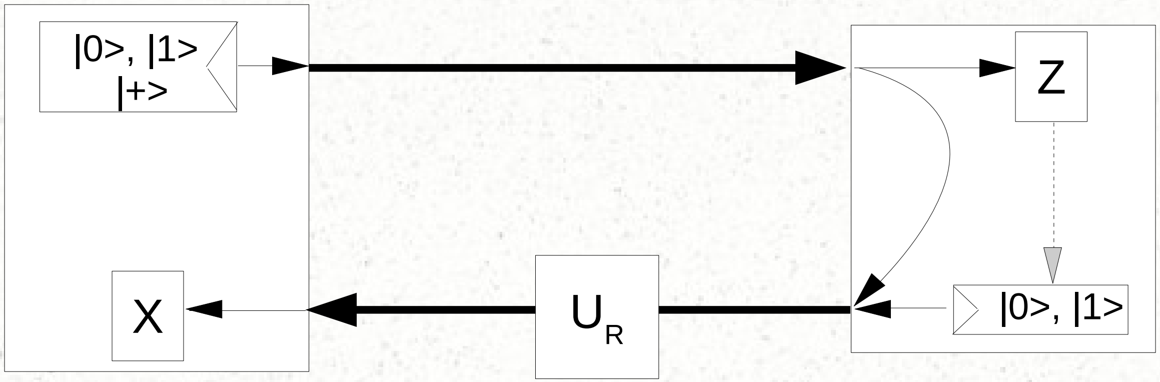
The Protocol

- Alice's Restrictions:
  - Can only send |0>, |1>, or |+>
  - Can only measure in the X basis {|+>, |->}
- Bob's Restrictions:
  - **Measure-and-Resend**: Measure in the Z basis and resend the observed result
  - **Reflect**: Disconnect from the quantum channel and ignore the incoming state

The Protocol (in a nutshell)



Need for Mismatched Measurements

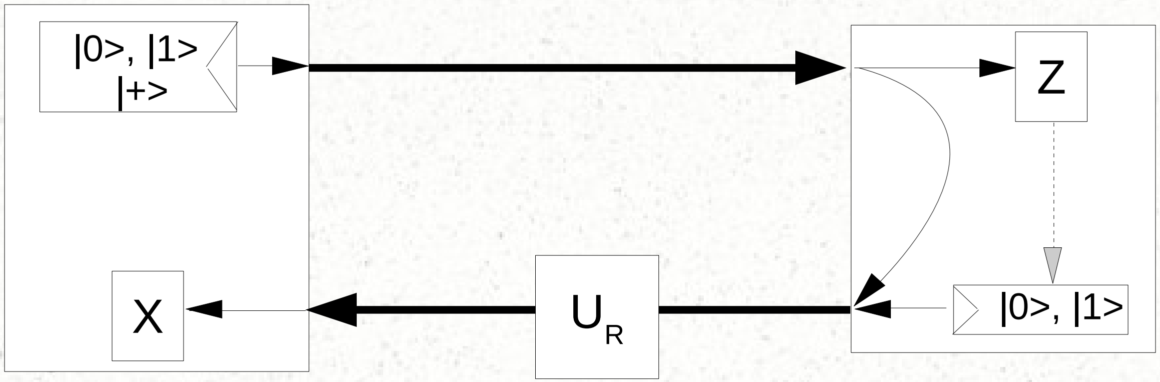


Forward Channel: Ignore (no noise)

Reverse Channel, apply U_R:

$$U_R|+>=|+,0>$$
$$U_R|->=|+,1>$$

Need for Mismatched Measurements



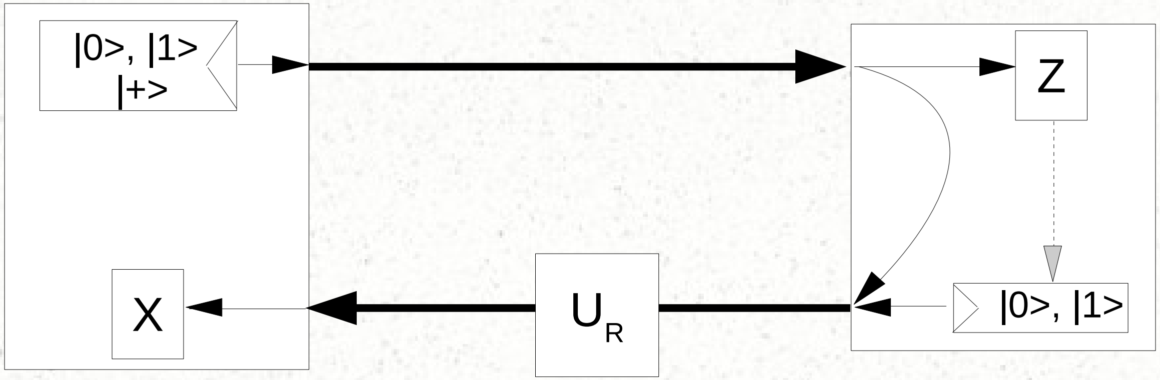
Forward Channel: Ignore (no noise)

Reverse Channel, apply U_R:

$$U_R|+>=|+,0>$$
$$U_R|->=|+,1>$$

No detectable noise!

Need for Mismatched Measurements

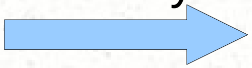


Forward Channel: Ignore (no noise)

Reverse Channel, apply U_R:

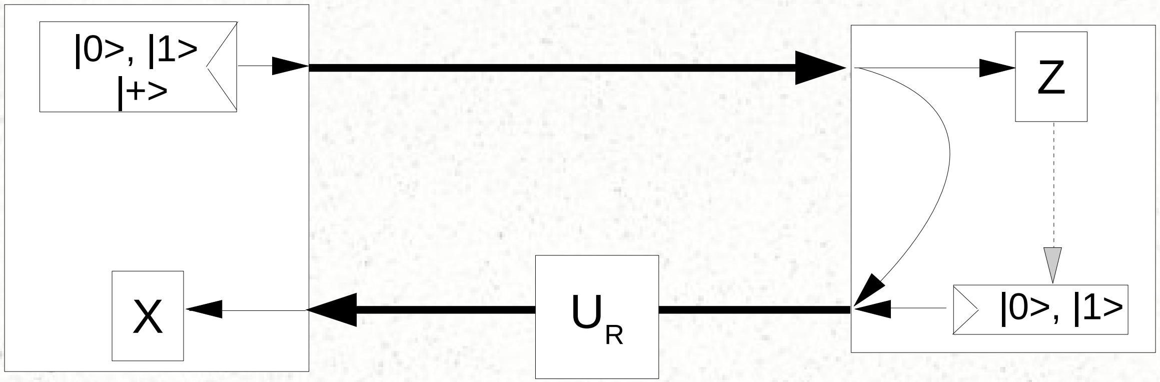
$$U_R|+\rangle = |+,0\rangle$$
$$U_R|-\rangle = |+,1\rangle$$

Linearity



$$U_R|0\rangle = |+,+\rangle$$
$$U_R|1\rangle = |+,-\rangle$$

Need for Mismatched Measurements



$$U_R|+\rangle=|+,0\rangle$$
$$U_R|-\rangle=|+,1\rangle$$

$$U_R|0\rangle=|+,+\rangle$$
$$U_R|1\rangle=|+,-\rangle$$

Two Fixes:

•Increase complexity of protocol by having A send |->

•Use **mismatched measurements** [5,9,10]

Security Proof

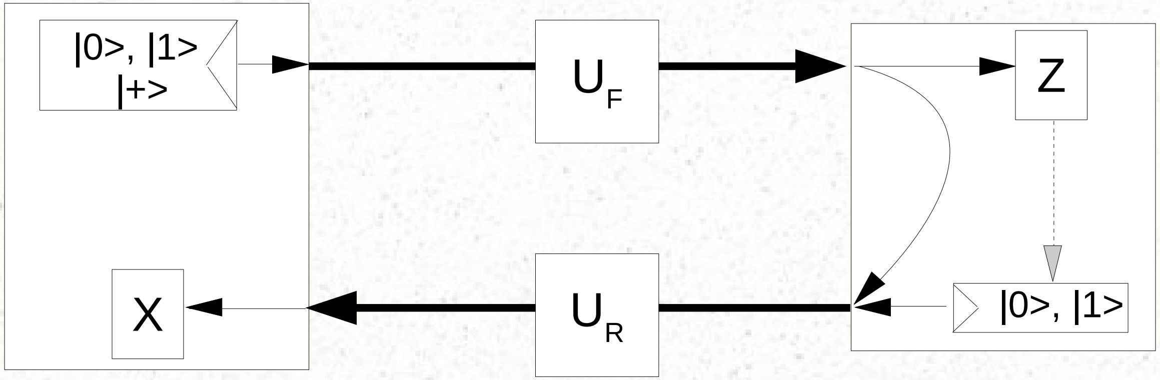
General QKD Security

- 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:

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

Two Attacks

Eve is allowed to opportunities to probe the qubit:

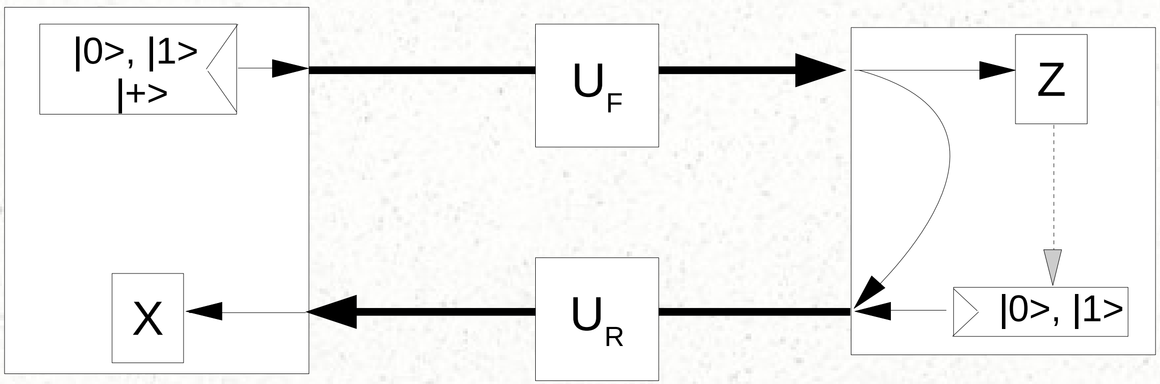


Forward:
$$U_F|0,0>_{TE}=|0,e_0>+|1,e_1>$$
$$U_F|1,0>_{TE}=|1,e_2>+|1,e_3>$$

Reverse:
$$U_R|i,e_j>_{TE}=|0,e_{i,j}^0>+|1,e_{i,j}^1>$$

Two Attacks

Eve is allowed to opportunities to probe the qubit:



Forward:

$$U_F|0,0>_{TE}=|0,e_0>+|1,e_1>$$
$$U_F|1,0>_{TE}=|1,e_2>+|1,e_3>$$

Not necessarily normalized or orthogonal

Reverse:

$$U_R|i,e_j>_{TE}=|0,e^0_{i,j}>+|1,e^1_{i,j}>$$

Quantum State ABE

- With this notation, simple algebra allows us to derive the following density operator describing one iteration (conditioning on a key-bit being distilled):

$$\rho_{ABE} = \frac{1}{2}[0,0]_{AB} \otimes \left([e^{0}_{0,0}] + [e^{1}_{0,0}]\right) + \frac{1}{2}[0,1]_{AB} \otimes \left([e^{0}_{1,1}] + [e^{1}_{1,1}]\right)$$
$$+ \frac{1}{2}[1,0]_{AB} \otimes \left([e^{0}_{0,2}] + [e^{1}_{0,2}]\right) + \frac{1}{2}[1,1]_{AB} \otimes \left([e^{0}_{1,3}] + [e^{1}_{1,3}]\right)$$

Note: $[x] = |x\rangle\langle x|$

$$\rho_{ABE}=\frac{1}{2}[0,0]_{AB}\otimes([e^0_{0,0}]+[e^1_{0,0}])+\frac{1}{2}[0,1]_{AB}\otimes([e^0_{1,1}]+[e^1_{1,1}])$$
$$+\frac{1}{2}[1,0]_{AB}\otimes([e^0_{0,2}]+[e^1_{0,2}])+\frac{1}{2}[1,1]_{AB}\otimes([e^0_{1,3}]+[e^1_{1,3}])$$

Using a result in [5] allows us to bound:

$$S(A|E)\geq\frac{<e^0_{0,0}|e^0_{0,0}>+<e^1_{1,3}|e^1_{1,3}>}{2}\left(h\left(\frac{<e^0_{0,0}|e^0_{0,0}>}{<e^0_{0,0}|e^0_{0,0}>+<e^1_{1,3}|e^1_{1,3}>}\right)-h(\lambda_1)\right)$$
$$+\frac{<e^1_{0,0}|e^1_{0,0}>+<e^0_{1,3}|e^0_{1,3}>}{2}\left(h\left(\frac{<e^1_{0,0}|e^1_{0,0}>}{<e^1_{0,0}|e^1_{0,0}>+<e^0_{1,3}|e^0_{1,3}>}\right)-h(\lambda_2)\right)$$
$$+\frac{<e^1_{1,1}|e^1_{1,1}>+<e^0_{0,2}|e^0_{0,2}>}{2}\left(h\left(\frac{<e^1_{1,1}|e^1_{1,1}>}{<e^1_{1,1}|e^1_{1,1}>+<e^0_{0,2}|e^0_{0,2}>}\right)-h(\lambda_3)\right)$$
$$+\frac{<e^0_{1,1}|e^0_{1,1}>+<e^1_{0,2}|e^1_{0,2}>}{2}\left(h\left(\frac{<e^0_{1,1}|e^0_{1,1}>}{<e^0_{1,1}|e^0_{1,1}>+<e^1_{0,2}|e^1_{0,2}>}\right)-h(\lambda_4)\right)$$

Unlike past SQKD protocols, we can only bound these
(based on the noise in the **forward channel**)

$$S(A|E) \geq \frac{<e^0_{0,0}|e^0_{0,0}> + <e^1_{1,3}|e^1_{1,3}>}{2}\left(h\left(\frac{<e^0_{0,0}|e^0_{0,0}>}{<e^0_{0,0}|e^0_{0,0}> + <e^1_{1,3}|e^1_{1,3}>}\right) - h(\lambda_1)\right)$$

$$+ \frac{<e^1_{0,0}|e^1_{0,0}> + <e^0_{1,3}|e^0_{1,3}>}{2}\left(h\left(\frac{<e^1_{0,0}|e^1_{0,0}>}{<e^1_{0,0}|e^1_{0,0}> + <e^0_{1,3}|e^0_{1,3}>}\right) - h(\lambda_2)\right)$$

$$+ \frac{<e^1_{1,1}|e^1_{1,1}> + <e^0_{0,2}|e^0_{0,2}>}{2}\left(h\left(\frac{<e^1_{1,1}|e^1_{1,1}>}{<e^1_{1,1}|e^1_{1,1}> + <e^0_{0,2}|e^0_{0,2}>}\right) - h(\lambda_3)\right)$$

$$+ \frac{<e^0_{1,1}|e^0_{1,1}> + <e^1_{0,2}|e^1_{0,2}>}{2}\left(h\left(\frac{<e^0_{1,1}|e^0_{1,1}>}{<e^0_{1,1}|e^0_{1,1}> + <e^1_{0,2}|e^1_{0,2}>}\right) - h(\lambda_4)\right)$$

Function of $\Re < e^0_{0,0} | e^1_{1,3} >$

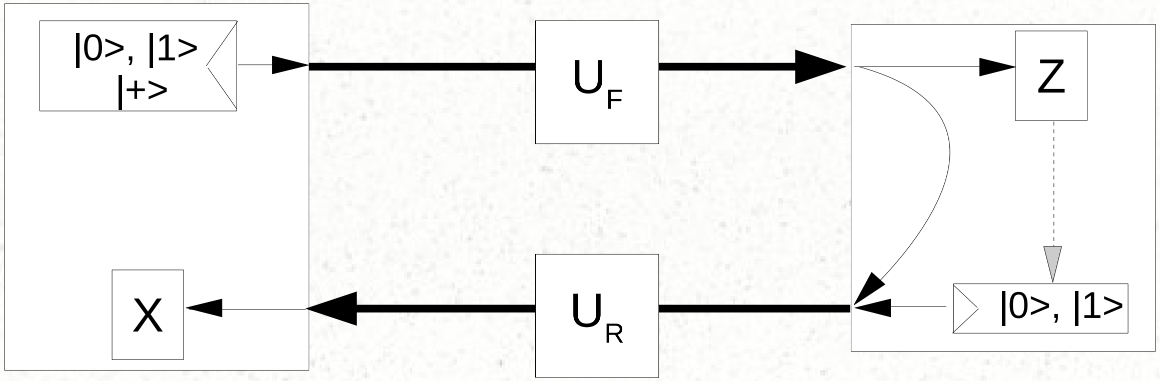
$$S(A|E) \geq \frac{< e^0_{0,0} | e^0_{0,0} > + < e^1_{1,3} | e^1_{1,3} >}{2} \left(h\left(\frac{< e^0_{0,0} | e^0_{0,0} >}{< e^0_{0,0} | e^0_{0,0} > + < e^1_{1,3} | e^1_{1,3} >} \right) - h(\lambda_1) \right)$$

$$+ \frac{< e^1_{0,0} | e^1_{0,0} > + < e^0_{1,3} | e^0_{1,3} >}{2} \left(h\left(\frac{< e^1_{0,0} | e^1_{0,0} >}{< e^1_{0,0} | e^1_{0,0} > + < e^0_{1,3} | e^0_{1,3} >} \right) - h(\lambda_2) \right)$$

$$+ \frac{< e^1_{1,1} | e^1_{1,1} > + < e^0_{0,2} | e^0_{0,2} >}{2} \left(h\left(\frac{< e^1_{1,1} | e^1_{1,1} >}{< e^1_{1,1} | e^1_{1,1} > + < e^0_{0,2} | e^0_{0,2} >} \right) - h(\lambda_3) \right)$$

$$+ \frac{< e^0_{1,1} | e^0_{1,1} > + < e^1_{0,2} | e^1_{0,2} >}{2} \left(h\left(\frac{< e^0_{1,1} | e^0_{1,1} >}{< e^0_{1,1} | e^0_{1,1} > + < e^1_{0,2} | e^1_{0,2} >} \right) - h(\lambda_4) \right)$$

Parameter Estimation



Forward:

$$U_F|0,0>_{TE}=|0,e_0>+|1,e_1>$$
$$U_F|1,0>_{TE}=|1,e_2>+|1,e_3>$$

Reverse:

$$U_R|i,e_j>_{TE}=|0,e^0_{i,j}>+|1,e^1_{i,j}>$$

$$p^{A\rightarrow B}_{0,0}=<e_0|e_0>$$

$$p^{A\rightarrow B}_{0,0}=<e^0_{0,0}|e^0_{0,0}>+<e^1_{0,0}|e^1_{0,0}>$$

Bound based on $p_{0,0}^{A\rightarrow B} = <e_{0,0}^{0}|e_{0,0}^{0}> + <e_{0,0}^{1}|e_{0,0}^{1}>$

$$S(A|E) \geq \frac{<e_{0,0}^{0}|e_{0,0}^{0}> + <e_{1,3}^{1}|e_{1,3}^{1}>}{2}\left(h\left(\frac{<e_{0,0}^{0}|e_{0,0}^{0}>}{<e_{0,0}^{0}|e_{0,0}^{0}> + <e_{1,3}^{1}|e_{1,3}^{1}>}\right) - h(\lambda_1)\right)$$

$$+\frac{<e_{0,0}^{1}|e_{0,0}^{1}> + <e_{1,3}^{0}|e_{1,3}^{0}>}{2}\left(h\left(\frac{<e_{0,0}^{1}|e_{0,0}^{1}>}{<e_{0,0}^{1}|e_{0,0}^{1}> + <e_{1,3}^{0}|e_{1,3}^{0}>}\right) - h(\lambda_2)\right)$$

$$+\frac{<e_{1,1}^{1}|e_{1,1}^{1}> + <e_{0,2}^{0}|e_{0,2}^{0}>}{2}\left(h\left(\frac{<e_{1,1}^{1}|e_{1,1}^{1}>}{<e_{1,1}^{1}|e_{1,1}^{1}> + <e_{0,2}^{0}|e_{0,2}^{0}>}\right) - h(\lambda_3)\right)$$

$$+\frac{<e_{1,1}^{0}|e_{1,1}^{0}> + <e_{0,2}^{1}|e_{0,2}^{1}>}{2}\left(h\left(\frac{<e_{1,1}^{0}|e_{1,1}^{0}>}{<e_{1,1}^{0}|e_{1,1}^{0}> + <e_{0,2}^{1}|e_{0,2}^{1}>}\right) - h(\lambda_4)\right)$$

Similarly, we can look at: $p_{i,j}^{A\to B}$

$$S(A|E)\geq\frac{<e_{0,0}^0|e_{0,0}^0>+<e_{1,3}^1|e_{1,3}^1>}{2}\left(h\left(\frac{<e_{0,0}^0|e_{0,0}^0>}{<e_{0,0}^0|e_{0,0}^0>+<e_{1,3}^1|e_{1,3}^1>}\right)-h(\lambda_1)\right)$$

$$+\frac{<e_{0,0}^1|e_{0,0}^1>+<e_{1,3}^0|e_{1,3}^0>}{2}\left(h\left(\frac{<e_{0,0}^1|e_{0,0}^1>}{<e_{0,0}^1|e_{0,0}^1>+<e_{1,3}^0|e_{1,3}^0>}\right)-h(\lambda_2)\right)$$

$$+\frac{<e_{1,1}^1|e_{1,1}^1>+<e_{0,2}^0|e_{0,2}^0>}{2}\left(h\left(\frac{<e_{1,1}^1|e_{1,1}^1>}{<e_{1,1}^1|e_{1,1}^1>+<e_{0,2}^0|e_{0,2}^0>}\right)-h(\lambda_3)\right)$$

$$+\frac{<e_{1,1}^0|e_{1,1}^0>+<e_{0,2}^1|e_{0,2}^1>}{2}\left(h\left(\frac{<e_{1,1}^0|e_{1,1}^0>}{<e_{1,1}^0|e_{1,1}^0>+<e_{0,2}^1|e_{0,2}^1>}\right)-h(\lambda_4)\right)$$

Just leaves: $\Re < e_{0,0}^{0} | e_{1,3}^{1} >$

$$S(A|E) \geq \frac{<e_{0,0}^{0}|e_{0,0}^{0}> + <e_{1,3}^{1}|e_{1,3}^{1}>}{2} \left(h\left(\frac{<e_{0,0}^{0}|e_{0,0}^{0}>}{<e_{0,0}^{0}|e_{0,0}^{0}> + <e_{1,3}^{1}|e_{1,3}^{1}>} \right) - h(\lambda_1) \right)$$

$$+ \frac{<e_{0,0}^{1}|e_{0,0}^{1}> + <e_{1,3}^{0}|e_{1,3}^{0}>}{2} \left(h\left(\frac{<e_{0,0}^{1}|e_{0,0}^{1}>}{<e_{0,0}^{1}|e_{0,0}^{1}> + <e_{1,3}^{0}|e_{1,3}^{0}>} \right) - h(\lambda_2) \right)$$

$$+ \frac{<e_{1,1}^{1}|e_{1,1}^{1}> + <e_{0,2}^{0}|e_{0,2}^{0}>}{2} \left(h\left(\frac{<e_{1,1}^{1}|e_{1,1}^{1}>}{<e_{1,1}^{1}|e_{1,1}^{1}> + <e_{0,2}^{0}|e_{0,2}^{0}>} \right) - h(\lambda_3) \right)$$

$$+ \frac{<e_{1,1}^{0}|e_{1,1}^{0}> + <e_{0,2}^{1}|e_{0,2}^{1}>}{2} \left(h\left(\frac{<e_{1,1}^{0}|e_{1,1}^{0}>}{<e_{1,1}^{0}|e_{1,1}^{0}> + <e_{0,2}^{1}|e_{0,2}^{1}>} \right) - h(\lambda_4) \right)$$

Parameter Estimation

However, we show that techniques applying mismatched measurements for two-way semi-quantum protocols derived in [5] can be applied to this scenario.

By looking at the error-rate in the "reflection" case, we find:

$$p_{+,R,-}^{A \to A} = 1 - \frac{1}{2}(L_1 + L_2 + L_3 + L_4 + \eta_1 + \eta_2) - \frac{1}{2}(p_{0,R,+}^{A \to A} + p_{1,R,+}^{A \to A})$$

Parameter Estimation

However, we show that techniques applying mismatched measurements for two-way semi-quantum protocols derived in [5] can be applied to this scenario.

By looking at the error-rate in the "reflection" case, we find:

$$p_{+,R,-}^{A\rightarrow A} = 1 - \frac{1}{2}(L_1 + L_2 + L_3 + L_4 + \eta_1 + \eta_2) - \frac{1}{2}(p_{0,R,+}^{A\rightarrow A} + p_{1,R,+}^{A\rightarrow A})$$

Needed to compute λ_i

e.g., $L_1 = \Re < e_{0,0}^0 | e_{1,3}^1 >$

Parameter Estimation

However, we show that techniques applying mismatched measurements for two-way semi-quantum protocols derived in [5] can be applied to this scenario.

By looking at the error-rate in the “reflection” case, we find:

$$p_{+,R,-}^{A\rightarrow A} = 1 - \frac{1}{2}(L_1 + L_2 + L_3 + L_4 + \eta_1 + \eta_2) - \frac{1}{2}(p_{0,R,+}^{A\rightarrow A} + p_{1,R,+}^{A\rightarrow A})$$

Mismatched Measurements – in a symmetric attack, these are ½ each

Parameter Estimation

However, we show that techniques applying mismatched measurements for two-way semi-quantum protocols derived in [5] can be applied to this scenario.

By looking at the error-rate in the “reflection” case, we find:

$$p_{+,R,-}^{A\to A} = 1 - \frac{1}{2}(L_1 + L_2 + L_3 + L_4 + \eta_1 + \eta_2) - \frac{1}{2}(p_{0,R,+}^{A\to A} + p_{1,R,+}^{A\to A})$$

Functions of five different mismatched statistics (each).

If symmetric attack, it holds that: $\eta_1 = \eta_2 = 0$

Entropy Computation

- Our entropy bound on S(A|E) is a function of eight variables:

$$<e^1_{0,0}|e^1_{0,0}>, <e^1_{1,3}|e^1_{1,3}>, <e^1_{0,2}|e^1_{0,2}>, <e^1_{1,1}|e^1_{1,1}>, L_1, L_2, L_3, L_4$$

- With restrictions:

Restriction	Reason
$<e^k_{i,j}\|e^k_{i,j}> \geq 0$	Property of inner-product
$<e^1_{0,0}\|e^1_{0,0}> \leq p^{A\to B}_{0,0}$ $<e^1_{1,3}\|e^1_{1,3}> \leq p^{A\to B}_{1,1}$ $<e^1_{0,2}\|e^1_{0,2}> \leq p^{A\to B}_{1,0}$ $<e^1_{1,1}\|e^1_{1,1}> \leq p^{A\to B}_{0,1}$	Unitarity of U_R
$\|L_1\| \leq \sqrt{<e^0_{0,0}\|e^0_{0,0}><e^1_{1,3}\|e^1_{1,3}>}$ $\|L_2\| \leq \sqrt{<e^1_{0,0}\|e^1_{0,0}><e^0_{1,3}\|e^0_{1,3}>}$ $\|L_3\| \leq \sqrt{<e^1_{1,1}\|e^1_{1,1}><e^0_{0,2}\|e^0_{0,2}>}$ $\|L_4\| \leq \sqrt{<e^0_{1,1}\|e^0_{1,1}><e^1_{0,2}\|e^1_{0,2}>}$	Cauchy-Schwarz
$p^{A\to A}_{+,R,-} = 1 - \frac{1}{2}(L_1 + L_2 + L_3 + L_4 + \eta_1 + \eta_2)$ $- \frac{1}{2}(p^{A\to A}_{0,R,+} + p^{A\to A}_{1,R,+})$	Mismatched Measurements

Evaluation + Summary

Results

- We numerically minimize S(A|E) based on the above constraints
  - Need to minimize as we must assume the worst case
- Computing H(A|B) is trivial given observable data
- Thus, we can compute the key-rate r = S(A|E) - H(A|B)

	Independent: $Q_X = 2Q(1-Q)$	Dependent: $Q_X = Q$
Max. Q:	$Q < 7.9\%$	$Q < 11\%$

Required Measurement Statistics

Error Rates

$p_{0,0}^{A \to B}$
$p_{0,1}^{A \to B}$
$p_{1,0}^{A \to B}$
$p_{1,1}^{A \to B}$

$p_{+,R,-}^{A \to A}$

Mismatched Events

$p_{+,0}^{A \to B}$
$p_{+,1}^{A \to B}$

$p_{0,R,+}^{A \to A}$
$p_{1,R,+}^{A \to A}$
$p_{+,0,+}^{A \to A}$
$p_{0,0,+}^{A \to A}$
$p_{1,0,+}^{A \to A}$
$p_{+,1,+}^{A \to A}$
$p_{0,1,+}^{A \to A}$
$p_{1,1,+}^{A \to A}$

Required Measurement Statistics

Error Rates

$p_{0,0}^{A \to B}$

$p_{0,1}^{A \to B}$

$p_{1,0}^{A \to B}$

$p_{1,1}^{A \to B}$

$p_{+,R,-}^{A \to A}$

Mismatched Events

$p_{+,0}^{A \to B}$

$p_{+,1}^{A \to B}$

$p_{0,R,+}^{A \to A}$

$p_{1,R,+}^{A \to A}$

$p_{+,0,+}^{A \to A}$

$p_{0,0,+}^{A \to A}$

$p_{1,0,+}^{A \to A}$

$p_{+,1,+}^{A \to A}$

$p_{0,1,+}^{A \to A}$

$p_{1,1,+}^{A \to A}$

While we only evaluated on a symmetric channel, our equations apply to arbitrary channels.

Future Work

- How does the protocol compare to others over non-symmetric attacks?
- We only considered collective attacks – does the usual techniques of applying de Finetti work here?
    - Or some other way to extend to general attacks
- What about a finite-key analysis?
    - Especially comparing with other SQKD or fully quantum protocols.

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, "Quantum key distribution with mismatched measurements over arbitrary channels," Quantum Information and Computation, vol. 17, pp. 209–241, 2017.

[9] S. M. Barnett, B. Huttner, and S. J. Phoenix, "Eavesdropping strategies and rejected-data protocols in quantum cryptography," Journal of Modern Optics, vol. 40, no. 12, pp. 2501–2513, 1993.

[10] S. Watanabe, R. Matsumoto, and T. Uyematsu, "Tomography increases key rates of quantum-key distribution protocols," Physical Review A, vol. 78, no. 4, p. 042316, 2008.

[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.