

# Security of Quantum Key Distribution with Imperfect Devices

Hoi-Kwong Lo

Dept. of Electrical & Comp. Engineering (ECE); &

Dept. of Physics

University of Toronto

Email: [hklo@comm.utoronto.ca](mailto:hklo@comm.utoronto.ca)

URL: <http://www.comm.utoronto.ca/~hklo>

Joint work with

Daniel Gottesman

Norbert Lütkenhaus

John Preskill

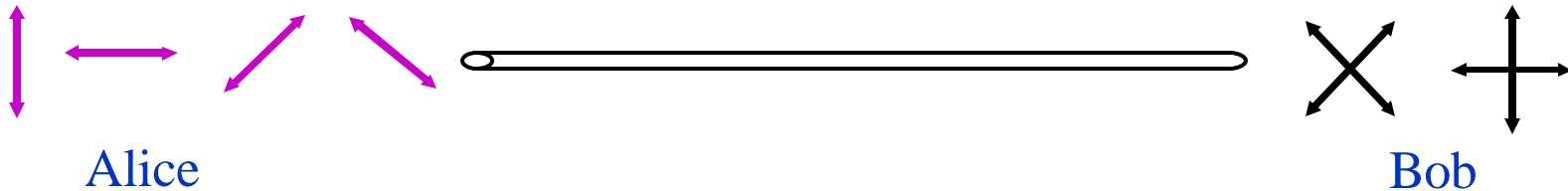
<http://xxx.lanl.gov/abs/quant-ph/0212066>

# Outline

1. Motivation and Summary of Results: Quantum Key Distribution (QKD): Theory and Practice
2. Entanglement distillation approach to security proof of QKD
3. Shor-Preskill's proof of security of BB84
4. Security of QKD with imperfect devices

# QKD : Theory

## Bennett and Brassard's scheme (BB84)



### ASSUMPTIONS:

1. Source: Emits perfect single photons. (No multi-photons)
2. Channel: **Noisy** but lossless. (No absorption in channel)
3. Detectors: a) Perfect detection efficiency. (100 %)
4. Basis Alignment: Perfect. (Angle between X and Z basis is exactly 45 degrees.)

Assumptions lead to security proofs:

Mayers (BB84), Lo and Chau (quantum-computing protocol), Biham et al. (BB84), Ben-Or (BB84), Shor-Preskill (BB84), ...

Conclusion: QKD is secure in theory.

# QKD : Practice

e.g., weak coherent state implementation of BB84

## Reality:

1. Source: Weak coherent states of bosonic modes. (Double photons may be emitted.)
2. Channel: Absorption inevitable. (e.g. 0.25 dB/km)
3. Detectors: efficiency  $\sim 15\%$  for Telecom wavelengths
4. Basis Alignment: Minor misalignment inevitable.

Question: Is QKD is secure in practice?

# Our assumptions

Assumptions:

1. Both Source and detector are under LIMITED control of an adversary.
2. Allow basis-dependent, individual flaws.

Comparison: (Either source or detectors is perfect in prior art.)

Mayers: perfect source but arbitrary detector.

Kaoshi-Preskill: arbitrary basis-independent source and perfect detector.

Inamori, Lutkenhaus, and Mayers: weak coherent states with perfect phase randomization, perfect basis alignment and basis-independent detection efficiency.

# Applications of our results

- 1 *Tagging*: A faulty source may “tag” some of the qubits with information, readable by the eavesdropper, that reveals the basis used in preparation. (Special case: Inamori, Lutkenhaus, and Mayers considered weak coherent states. Multi-photons reveal basis information).



- 2 *Basis-dependent detector efficiency*: The probability that a qubit is detected may depend on the basis used. An adversary may control whether the detector fires to disguise eavesdropping.

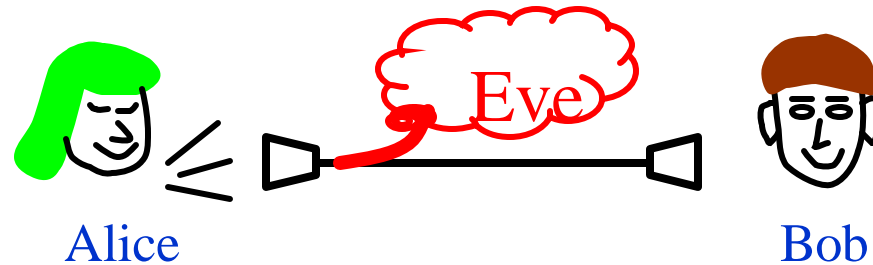
Bob's basis:  fire ;  pass.

- 3 *Basis-dependent misalignment in source/detector*: Source and detector not perfectly aligned. Eavesdropper can exploit her freedom to rotate these devices to reduce the disturbance caused by her eavesdropping.



# Conceptual interest of our result

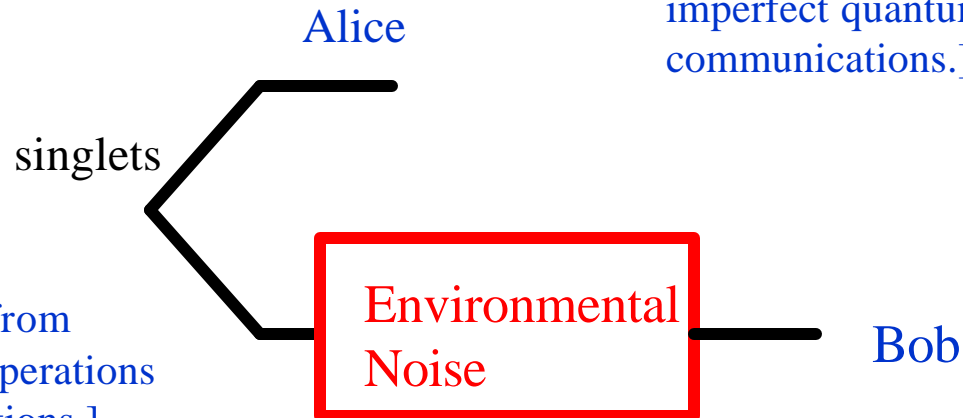
Quantum  
Key  
Distribution  
(QKD):



[Distill a secure key from  
imperfect quantum  
communications.]

Entanglement  
Distillation  
Protocol (EDP):

[Distill better “singlets” from  
imperfect ones by local operations  
and classical communications.]



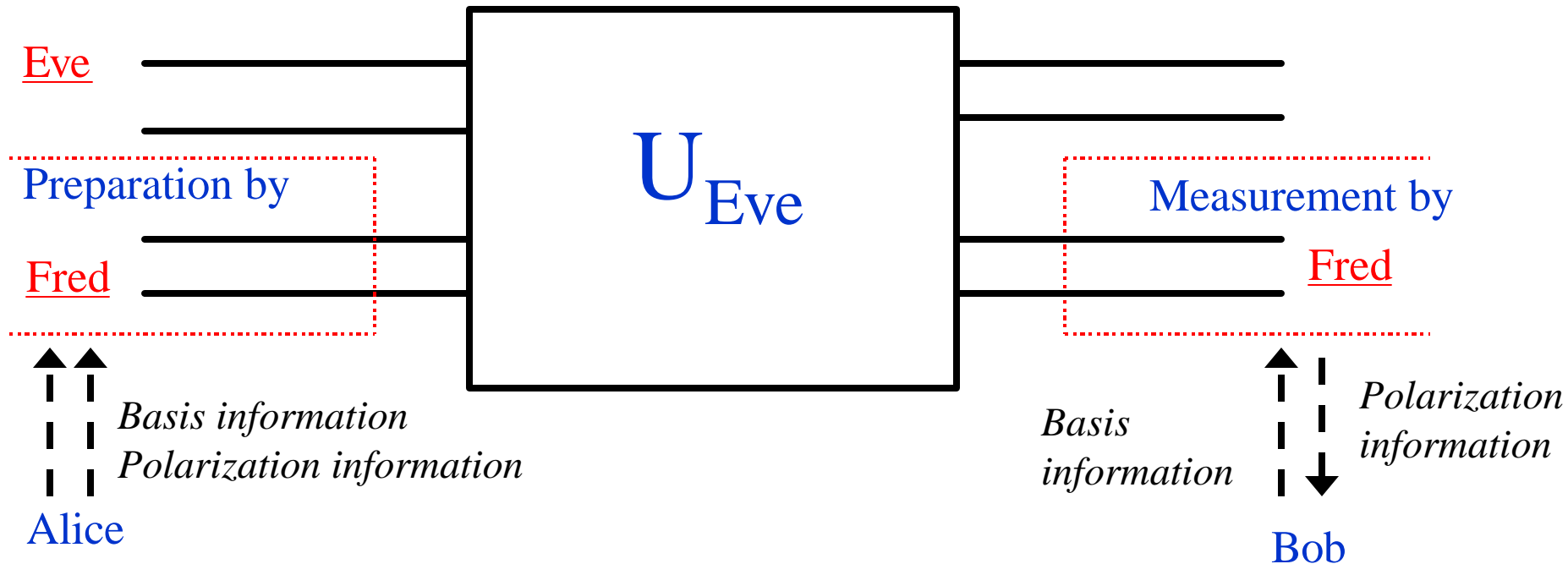
Connecting two big ideas in quantum information: EDP with  
PRACTICAL QKD.

## Our general framework: Eve and Fred (Intuition)

Imagine two collaborating adversaries, Eve and Fred, try to foil QKD.

Eve: does not know the basis used by Alice and Bob and has no direct control on source/detector.

Fred: knows the basis used by Alice and Bob and has limited control on source/detector for each signal individually.



Set up a “Chinese Wall” to separate information between Eve and Fred. 8

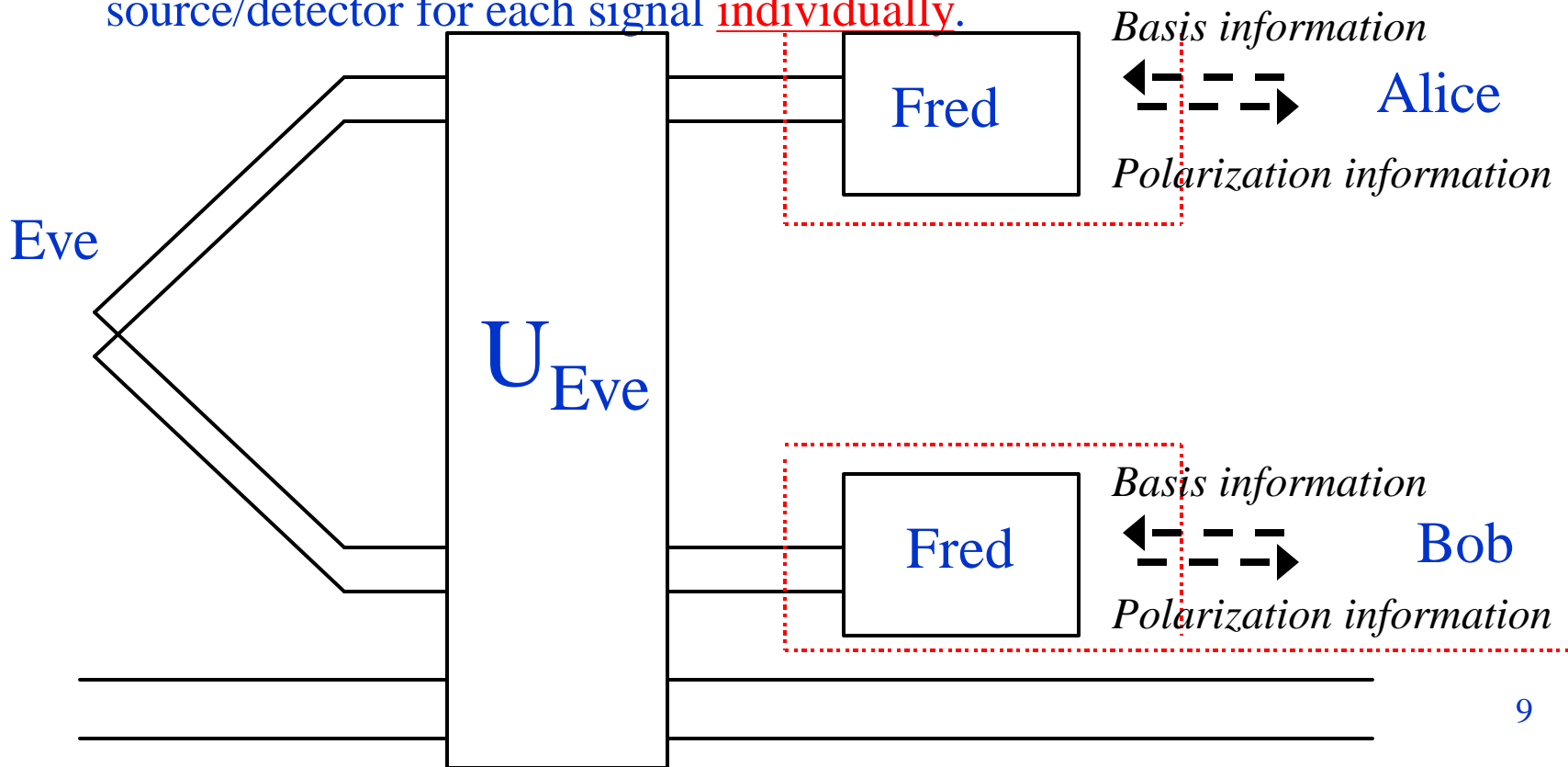


# Our general framework: Eve and Fred (More Precise)

Imagine two collaborating adversaries, Eve and Fred, try to foil QKD.

Eve: does not know the basis used by Alice and Bob and has no direct control on source/detector.

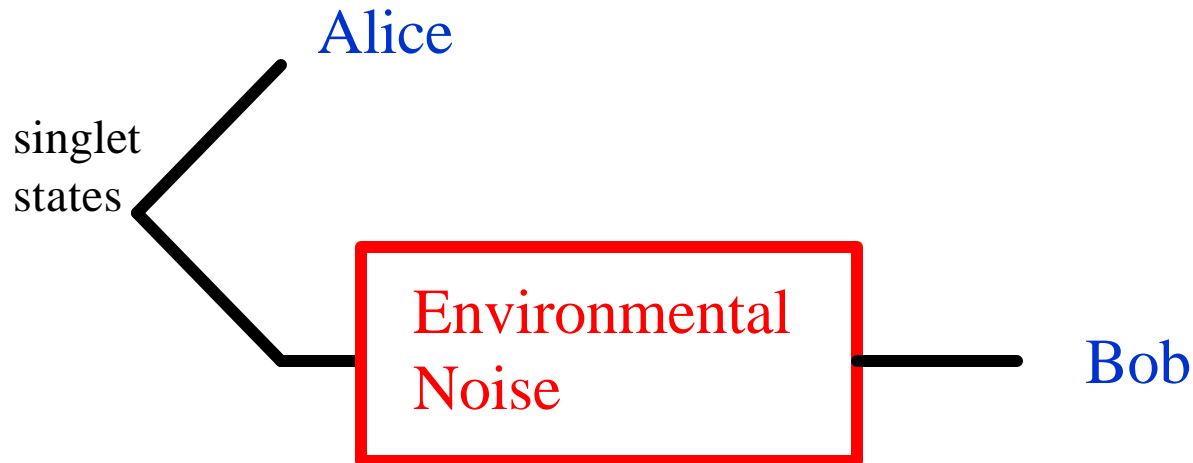
Fred: knows the basis used by Alice and Bob and has limited control on source/detector for each signal individually.



# Outline

1. Motivation and Summary of Results: Quantum Key Distribution (QKD): Theory and Practice
- 2. Entanglement distillation approach to security proof of QKD**
3. Shor-Preskill's proof of security of BB84
4. Security of QKD with imperfect devices

## 2. EDPs (Entanglement distillation protocols)

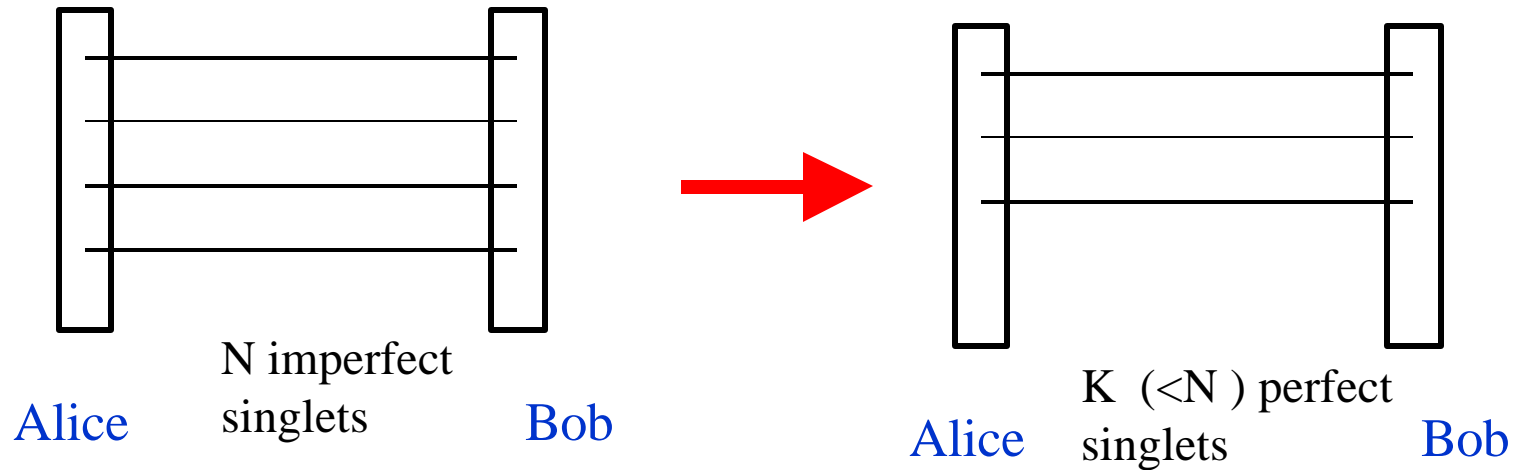


Distill better singlets from imperfect ones by local operations and classical communications (LOCCs).

Remark: A singlet is a pair of qubits in the standard state  $|01\rangle - |10\rangle$ . It exhibits perfect quantum correlations (i.e., entanglement).

# Entanglement Distillation Protocol (EDP)

Distant laboratory paradigm



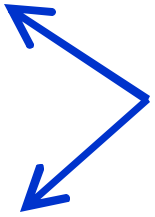
Local operations and classical communications (LOCCs)



## Classification of errors acting on spin-1/2 system

A) **Bit flip error:**  $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$

B) **Phase error:**  $Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$



Two types of truly independent errors

C) Simultaneous Bit-flip and Phase error:

$$Y = XZ$$

For N spin-1/2 objects, consider the tensor product error operator.

Remark: If an entanglement distillation protocol can correct up to t errors acting on N spin-1/2 objects of the tensor product form in X, Y and Z types of errors, then it can correct a **general** error acting on up to t out of the N spin-1/2 objects. (This is because I, X, Y, and Z generate the most general 2 x 2 unitary matrix.)

## EDP-based QKD scheme (Deutsch et al.; Lo-Chau)

1. (Testing error rate) Suppose Alice and Bob share  $2N$  noisy singlets. Alice and Bob can test their purity by randomly choosing say  $N$  out of the  $2N$  pairs and measuring either  $X X$  or  $Z Z$ . If error rate not too big, go to Step 2.

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \quad Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

2. (Entanglement Distillation) Alice and Bob can apply local operations and classical communications to distill out a smaller number, say  $k$ , almost perfect singlets from the  $N$  remaining pairs.
3. (Key generation) They can then measure those  $k$  singlets, say along the  $Z$  axis, to generate a secret key.

Remark: Key generation along  $Z$  axis only.

# Question

- How can one remove the assumption of quantum computers in security proof of QKD?

Solution: Shor-Preskill's proof....

# Outline

1. Motivation and Summary of Results: Quantum Key Distribution (QKD): Theory and Practice
2. Entanglement distillation approach to security proof of QKD
- 3. Shor-Preskill's proof of security of BB84**
4. Security of QKD with imperfect devices



# Overall Strategy of Shor-Preskill's proof

Use Entanglement Distillation Protocols (EDPs) to prove security of BB84:



Procedure:

1. Construct EDP-based QKD scheme and prove its security.
2. Show that security of EDP-based QKD scheme **implies** Security of BB84.

Result: A simple proof of **unconditional security** of BB84.

(Cf. Mayers' proof, the first proof for BB84, is hard for many people.)

Remark: Unconditional security means security against the most general type of attacks---`joint attacks`. Holy Grail of Quantum Crypto.17

# Correspondence between CSS codes and BB84 (Shor-Preskill's proof)

CSS codes

BB84

bit flip error correction



error correction

phase error correction



privacy amplification

(to remove Eve's info.)

N.B.: CSS stands for Calderbank-Shor-Steane codes.  
It is a common class of quantum codes.

# Intuition of Shor-Preskill's proof

- Shor-Preskill use CSS codes which have the nice properties that their generators are of the form X-type or Z-type. i.e., the bit-flip and phase error correction procedures are **decoupled**.
- In EPP-based QKD protocol, the key is generated by measuring Z's. Therefore, value of the key is **not** affected by phase error correction.
- Therefore, Alice and Bob do **NOT** need to compute the phase error syndrome. Consequently, no quantum computers are needed.
- If Alice and Bob do not announce the phase error syndrome, it can be shown that the density matrix prepared by Alice is the **same** as in BB84. From Eve's view, Alice and Bob could have prepared the state by using EDPs.
- What is important is not phase error correction is actually performed, but that it **could have been** successful, if it had been performed.

# Outline

1. Motivation and Summary of Results: Quantum Key Distribution (QKD): Theory and Practice
2. Entanglement distillation approach to security proof of QKD
3. Shor-Preskill's proof of security of BB84
- 4. Security of QKD with imperfect devices**

## Error Rates of tested and untested pairs

Tested Pairs:  $\mathbf{d}_X$  , X-basis error rate (of tested signals)  
 $\mathbf{d}_Z$  , Z-basis error rate (of tested signals)

Key generation Pairs:  $\mathbf{d}$  , bit-flip error rate.  
 $\mathbf{d}_p$  , phase error rate.

[Key generation rate:  $R = 1 - H_2(\mathbf{d}) - H_2(\mathbf{d}_p)$  ]

Question: How to relate  $(\mathbf{d}_X, \mathbf{d}_Z)$  to  $(\mathbf{d}, \mathbf{d}_p)$  ?

Answer: In standard BB84, the tested pairs give a fair sample of the population. Therefore, the error rates of the tested and untested pairs are the same. i.e.,  $\mathbf{d} = \mathbf{d}_Z$  ,  
and  $\mathbf{d}_p = \mathbf{d}_X$  .

## Error Rates of tested and untested pairs

Tested Pairs:  $\mathbf{d}_X$  , X-basis error rate (of tested signals)  
 $\mathbf{d}_Z$  , Z-basis error rate (of tested signals)

Key generation Pairs:  $\mathbf{d}$  , bit-flip error rate.  
 $\mathbf{d}_p$  , phase error rate.

[Key generation rate:  $R = 1 - H_2(\mathbf{d}) - H_2(\mathbf{d}_p)$  ]

Question: How to relate  $(\mathbf{d}_X, \mathbf{d}_Z)$  to  $(\mathbf{d}, \mathbf{d}_p)$  ?

Answer: In standard BB84. The tested pairs give a fair sample of  
The population. Therefore, the error rates of the tested and  
Untested pairs are the same. i.e.,  $\mathbf{d} = \mathbf{d}_Z$  ,  
and  $\mathbf{d}_p = \mathbf{d}_X$  .

Question: What if we introduce imperfections?

## Error Rates of tested and untested pairs

Tested Pairs:  $\mathbf{d}_X$  , X-basis error rate (of tested signals)  
 $\mathbf{d}_Z$  , Z-basis error rate (of tested signals)

Key generation Pairs:  $\mathbf{d}$  , bit-flip error rate.  
 $\mathbf{d}_p$  , phase error rate.

[Key generation rate:  $R = 1 - H_2(\mathbf{d}) - H_2(\mathbf{d}_p)$  ]

Question: How to relate  $(\mathbf{d}_X, \mathbf{d}_Z)$  to  $(\mathbf{d}, \mathbf{d}_p)$  ?

Answer: With imperfection

$$\mathbf{d} = \mathbf{d}_Z$$

(Biased Sample)  $\mathbf{d}_p \not\approx \mathbf{d}_X$  .

Conclusion: Can reduce the whole question of dealing with imperfections to deriving constraints on  $\mathbf{d}_p$  from  $(\mathbf{d}_X, \mathbf{d}_Z)$  .

## Example I: Tagged qubits

- Suppose a fraction  $\Delta$  of the qubits are tagged by Fred.

The tag informs Eve which basis is used. So, Eve can learn polarizations without disturbing the qubits.

1. For untagged photons, Eve has no information on basis. Therefore, bit-flip and phase error rates are the same-----call it  $p$ .
2. For tagged photons, bit-flip error rate is 0 and phase error rate is at most 1. Therefore, taking the weighted average over tagged and untagged Photons, we have

$$\mathbf{d} = (1 - \Delta) p$$

$$\mathbf{d}_p = \underbrace{(1 - \Delta) p}_{\text{untagged}} + \underbrace{\Delta}_{\text{tagged}}$$

Example: In weak coherent state implementation, the tagging probability,  $\Delta = p_M / p_D$ , where

$p_M$  is probability for emitting a multi-photon and

$p_D$  is detection probability.



## Example II: Trojan Pony

- Suppose the detector is not perfectly efficient. A fraction  $\Delta$  of the signals that enter the detector fail to trigger it, resulting in no recorded outcome.
- Suppose Fred, who knows Bob's basis, controls whether the detector fires or not, subject to the constraint that at most a fraction,  $\Delta$  can be eliminated.
- In the worst case, every pair that Fred removes has a bit-flip error and no phase error.
- Before any pairs were eliminated, suppose the error rate was  $p$  in both cases.
- After elimination, the error rates are:

$$\mathbf{d} = \frac{p - \Delta}{1 - \Delta} \quad , \quad \mathbf{d}_p = \frac{p}{1 - \Delta}$$

## Example III: Misalignment

- Suppose Bob is unable to control his measurement basis perfectly. Instead of measuring a qubit along the Z-axis, he might be measuring it within a cone of angle  $\mathbf{q}$  from the desired axis.
- Similarly, instead of measuring along the X-axis, he might be measuring it within a cone of angle  $\mathbf{q}$  from the desired axis.
- The situation is equivalent to one in which Bob's measurement is perfect, but Fred is allowed to perform a rotation up to an angle depending on the basis used by Bob. Therefore, we have

$$\mathbf{r}_0 = (I \otimes U_0) \mathbf{r} (I \otimes U_0^{-1})$$

$$\mathbf{r}_1 = (I \otimes U_1) \mathbf{r} (I \otimes U_1^{-1})$$

where  $U = U_1 U_0^{-1}$  is a rotation of up to an angle  $2\mathbf{q}$  .

# Summary

- We have proven that QKD is secure even when both source and detector are imperfect and even when the flaws are adversarial and basis-dependent.

# Limitations

- Still, the model source and detectors are not completely general.
- Indeed, the flaws are assumed to be individual and limited.
- We have put aside the question of how Alice and Bob can verify our assumptions experimentally.
- We have not considered how to strengthen our results by using two-way classical communications. (Cf. Gottesman-Lo ).
- We have only considered the asymptotic case of an infinitely long key, but not the realistic case of a finitely long key.

# Correspondence between EDP and BB84 (Gottesman-Lo's proof)

EDP

BB84/six-state

bit-flip error <u>detection</u>	↔	“advantage distillation”
bit-flip error correction	↔	error correction
phase error correction	↔	privacy amplification

We proved BB84 is secure up to 18.9 percent bit error rate.  
“Security of quantum key distribution with two-way classical communications”,  
D. Gottesman and H.-K. Lo, IEEE Transactions on Information Theory,  
Vol. 49, No. 2, p. 457 (Feb., 2003). <http://xxx.lanl.gov/abs/quant-ph/0105121>

# Phenomenology of QKD

1. Design practical protocols for classical post-processing of QKD.
2. Model real-life QKD systems.
3. Study eavesdropping attacks.

# 1.Design practical protocols for classical post-processing of QKD.

Remark: ``Privacy amplification'' is the dual of error correction. (Cf. ``Generalized Hamming Weights for linear codes'', Wei, IEEE IT, 91)

1. **Finite size codes**: (convolutional codes or block codes?)

Security proofs usually deal with an infinitely long key.

In practice, it is necessary to consider a final key of finite length.

2. Fluctuations become very important.
3. Need **REAL-TIME** (hardware?) implementation.
4. Limited **REAL** random number generator rate.
5. Limited computational power.
6. Limited memory space.
7. Limited classical communication bandwidth.
8. Cost

## 2. Model real-life QKD systems.

1) All models of QKD are idealizations of real-life systems.

Real-life QKD system is a complex system with many degrees of freedom.

2) Imperfections:

- Imperfect single-photon sources
- Lossy channels
- Imperfect single-photon detection efficiency
- Detectors' dark counts
- Trojan Horse's attacks
- Denial-of-service attacks

How to quantify (experimentally) small imperfections and ensure security in the presence of those imperfections?

### 3. Study eavesdropping attacks.

The best way to build a secure cryptographic system is to try hard to break it.

Need to study theoretically and experimentally the feasibility and power of various eavesdropping attacks: beam-splitting attacks, unambiguous state determination, Trojan Horse attacks, etc.



# Security of Quantum Key Distribution with Imperfect Devices

Hoi-Kwong Lo

Dept. of Electrical & Comp. Engineering (ECE); &

Dept. of Physics

University of Toronto

Email: [hklo@comm.utoronto.ca](mailto:hklo@comm.utoronto.ca)

URL: <http://www.comm.utoronto.ca/~hklo>

Joint work with

Daniel Gottesman

Norbert Lütkenhaus

John Preskill

<http://xxx.lanl.gov/abs/quant-ph/0212066>