Decoy State Quantum Key Distribution (QKD)

Hoi-Kwong Lo
Center for Quantum Information and Quantum Control
Dept. of Electrical & Comp. Engineering (ECE); &
Dept. of Physics
University of Toronto

Joint work with:
Xiongfeng Ma
Kai Chen
[Paper in preparation]

Supported by CFI, CIPI, CRC program, NSERC, OIT, and PREA.

Outline

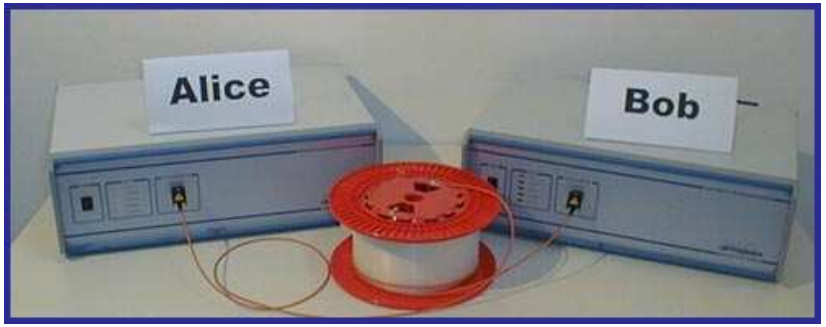
1. Motivation and Introduction
2. Problem
3. Our Solution and its significance

1. Motivation and Introduction

Commercial Quantum Crypto products available on the market Today!

MAGIQ TECH.

- Distance over 100 km of commercial Telecom fibers.



ID QUANTIQUE

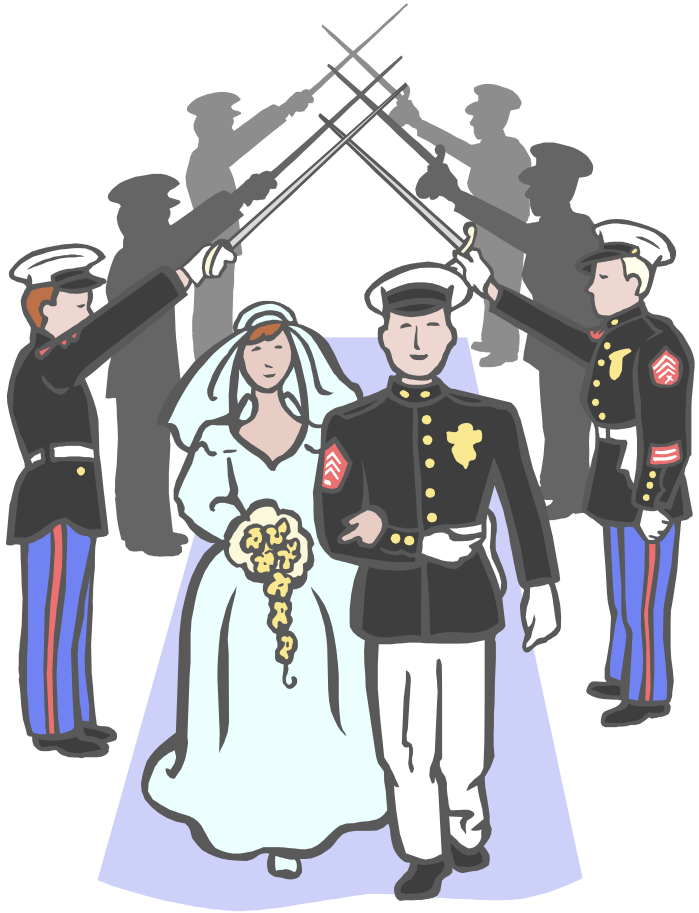
Bad News (for theorists)

Theory of quantum key distribution (QKD) is **behind** experiments.

Opportunity:

By developing theory, one can bridge gap between theory and practice.

Happy Marriage



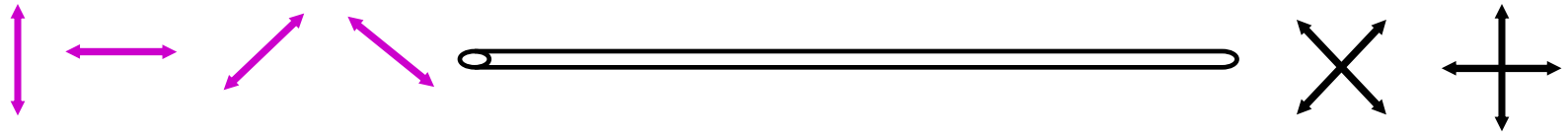
Theory and Experiment go hand in hand.

Key Distribution Problem

Alice and Bob would like to communicate in absolute security in the presence of an eavesdropper, Eve.

To do so, they need to share a common random string of number----key 

Bennett and Brassard's scheme (BB84)



Alice Bob

ASSSUMPTIONS:

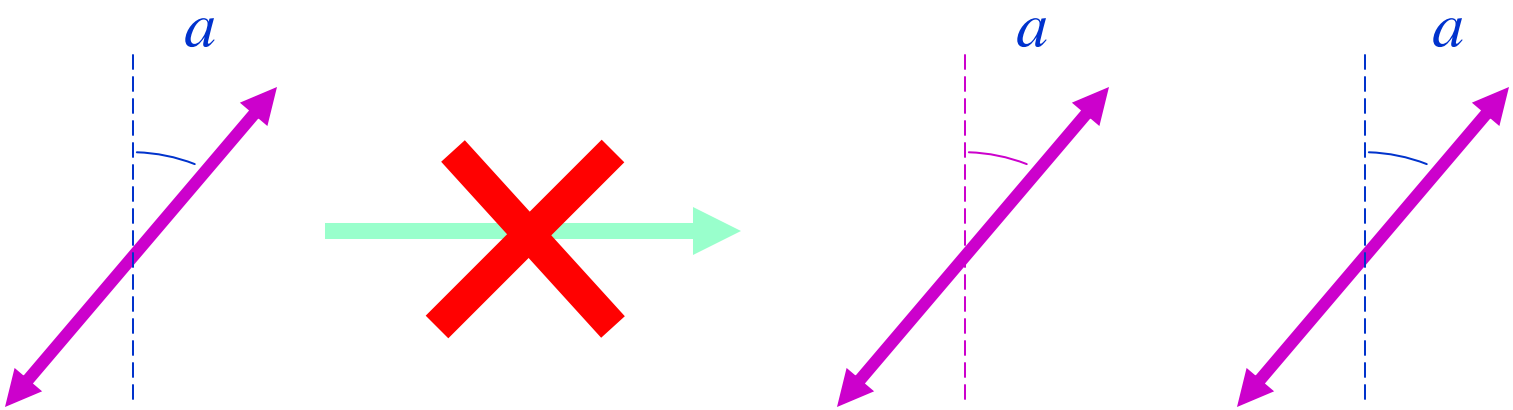
1. Source: Emits single photons. (No multi-photons)
2. Channel: noisy but . (No absorption in channel)
3. Detectors: a) detection efficiency. (100 %)
4. Basis Alignment: . (Angle between X and Z basis is exactly 45 degrees.)

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.

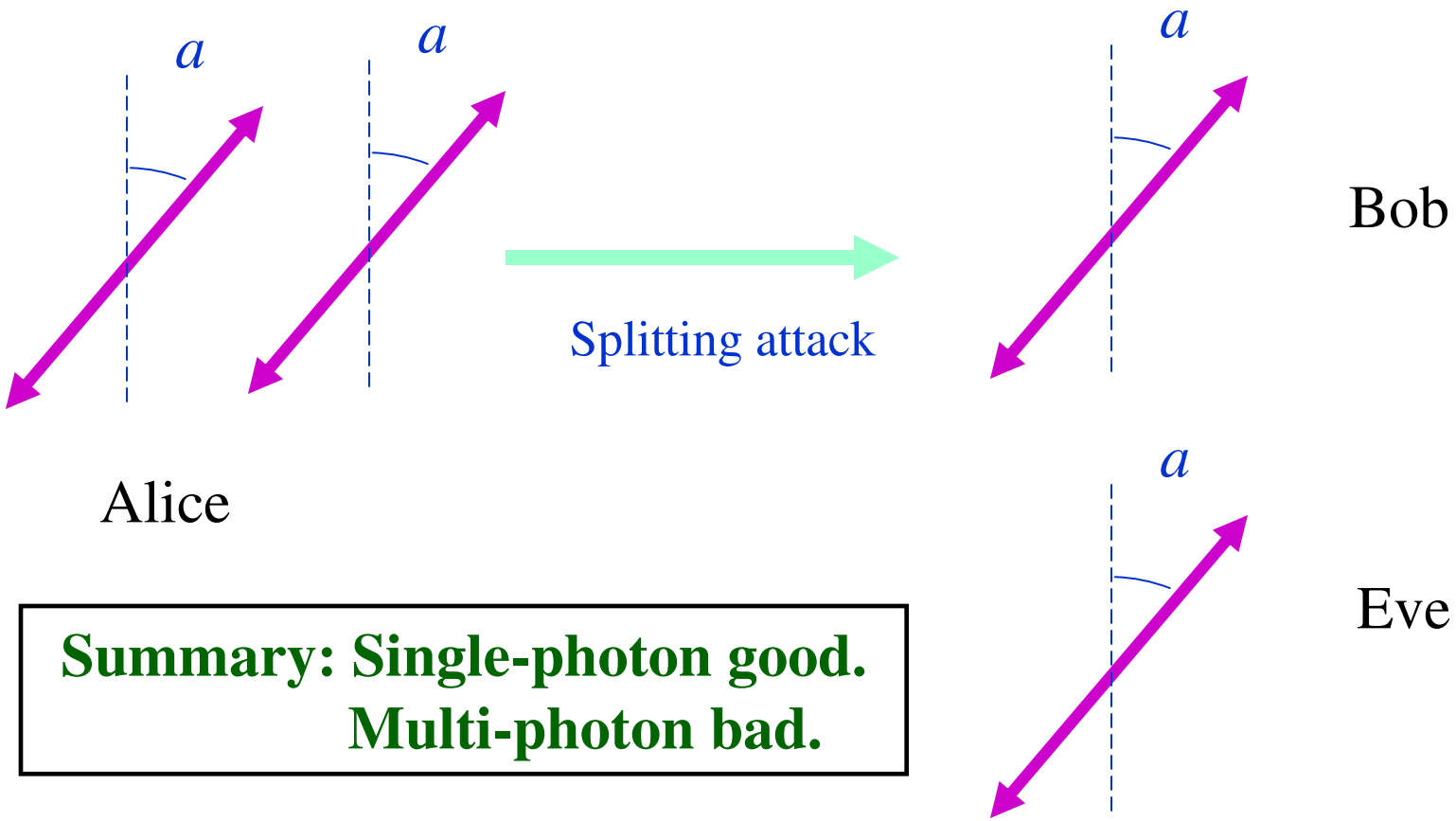
Reminder: Quantum No-cloning Theorem

- An unknown quantum state **CANNOT** be cloned. Therefore, eavesdropper, Eve, cannot have the same information as Bob.
- Single-photon signals are secure.



Photon-number splitting attack against multi-photons

A multi-photon signal CAN be split. (Therefore, insecure.)



Summary: Single-photon good.
Multi-photon bad.

QKD : Practice

Reality:

1. Source: (**Poisson photon number distribution**)
   Mixture. Photon number = k with probability: $\frac{\alpha^k}{k!}e^{-\alpha}$
   Some signals are, in fact, double photons!
2. Channel: Absorption inevitable. (e.g. 0.2 dB/km)
3. Detectors:
   (a) Efficiency ~15% for Telecom wavelengths
   (b) "Dark counts": Detector's erroneous fire.
   Detectors will claim to have detected signals with some probability even when the input is a vacuum.
4. Basis Alignment: Minor misalignment inevitable.

Question: Is QKD secure in practice?

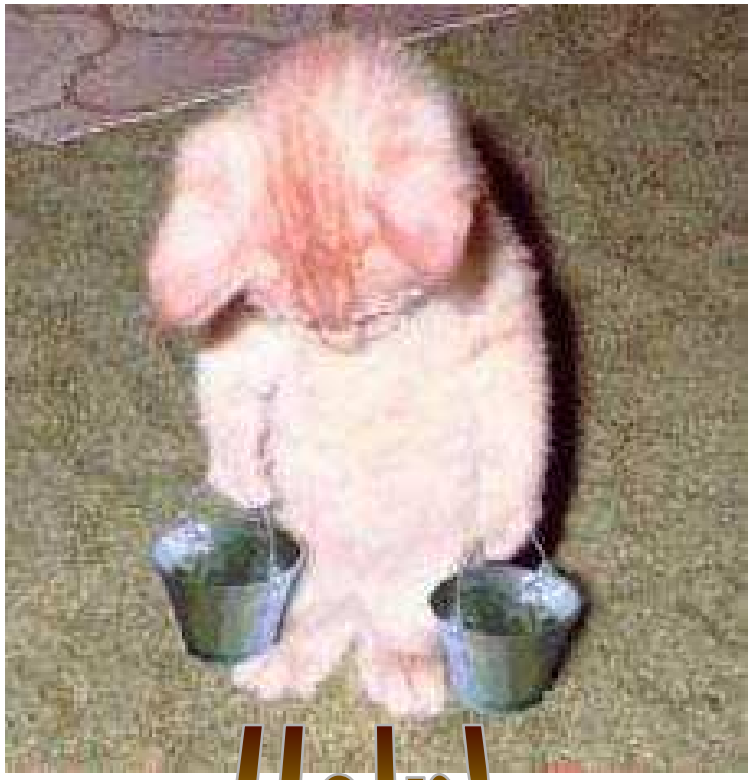
Prior art on BB84 with imperfect devices

1. Inamori, Lutkenhaus, Mayers (ILM)
2. Gottesman, Lo, Lutkenhaus, Preskill (GLLP)

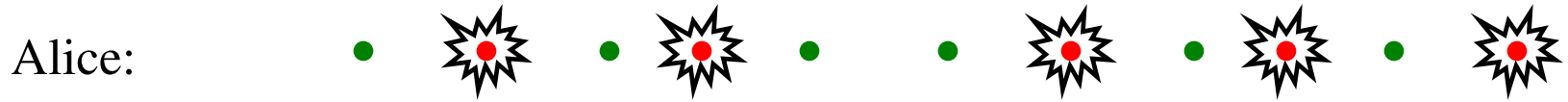
GLLP: Under (semi-) realistic assumptions,
if imperfections are sufficiently small,
then BB84 is secure.

Question: Can we go beyond these results

2. Problem

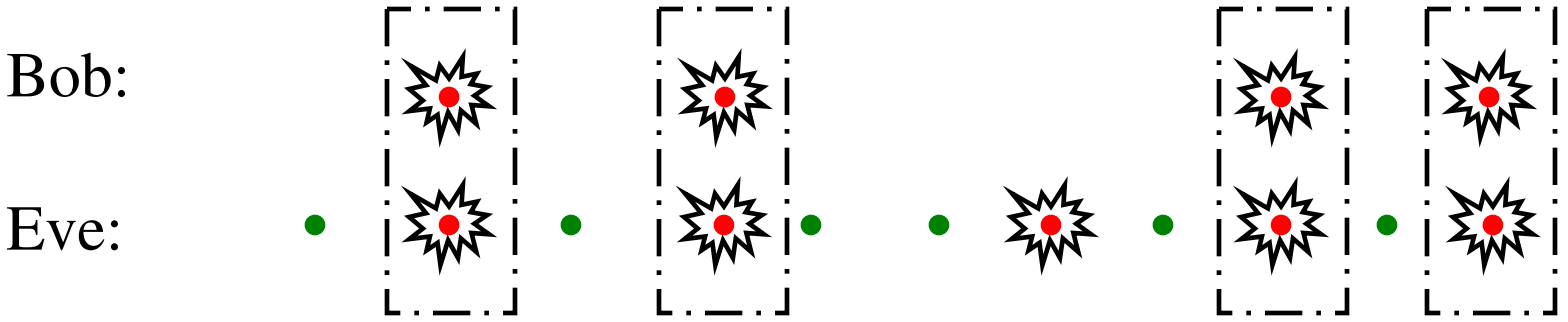


Big Problem: Nice guys come last



Problems: 1) Multi-photon signals (bad guys) can be split.

2) Eve may suppress single-photon signals (Good guys).

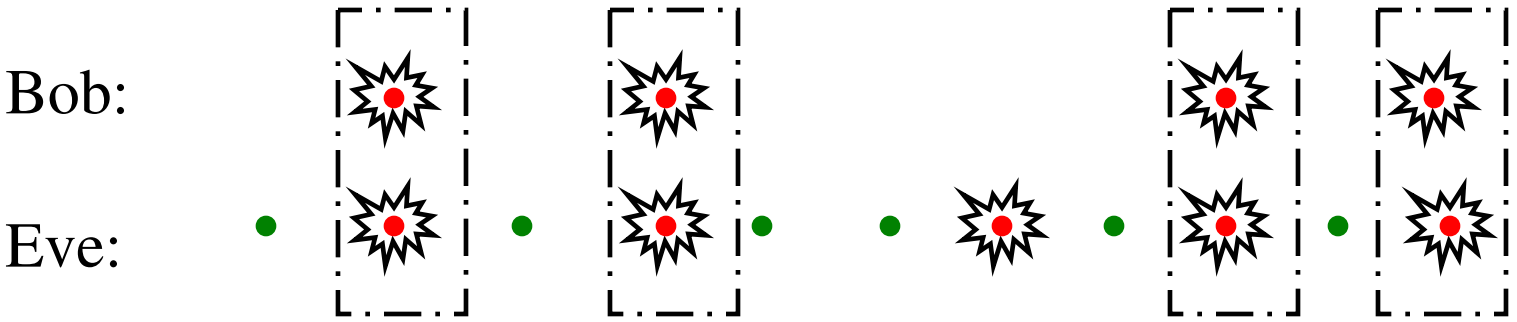


Eve may disguise herself as absorption in channel.
QKD becomes INSECURE as Eve has whatever Bob has.

Signature of this attack: Multi-photons are much more likely to reach Bob than single-photons. (Nice guys come last).

Yield as a function of photon number

Let us define Y_n = yield
= conditional probability that a signal will be detected by Bob, given that it is emitted by Alice as an **n-photon** state.



For example, with photon number splitting attack:

$Y_2 = 1$: all two-photon states are detected by Bob.
$Y_1 = 0$: all single-photon states are lost.

Figures of merits in QKD

- # of Secure bits per signal (emitted by Alice).

  How long is the final key that Alice and Bob can generate?

- (Maximal) distance of secure QKD.

  How far apart can Alice and Bob be from each other?

Prior Art Result

Consider the worst case scenario where **all** signals received by Bob are bad guys. (Insecure.)

To prevent this from happening, we need:

# of signals received by Bob

> # of multi-photon signals emitted by Alice.

Consider **channel transmittance η**.
For security, we use **weak** Poisson photon number distribution: $\mu = O(\eta)$.

Secure bits per signal $S = O(\eta^2)$.

Big Gap between theory and practice of BB84

	Theory	Experiment
Key generation rate:	S = O (η^2).	S= O (η).
Maximal distance:	d ~ 35km.	d >120km.

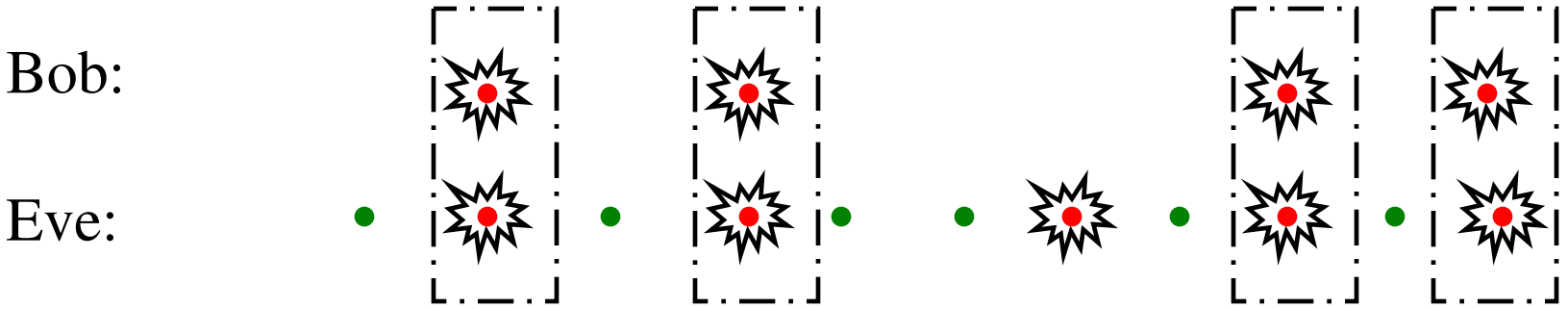
Prior art solutions (All bad):

1) Use Ad hoc security: Defeat main advantage of Q. Crypto. : unconditional security. (Theorists unhappy L .)
2) Limit experimental parameters: Substantially reduce performance. (Experimentalists unhappy L .)
3) Better experimental equipment (e.g. Single-photon source. Low-loss fibers. Photon-number-resolving detectors): Daunting experimental challenges. Impractical in near-future. (Engineers unhappy L .)

Question: How can we make everyone happy J ?

(Recall) Problem: Photon number splitting attack

Let us define Y_n = yield
= conditional probability that a signal will be detected by Bob, given that it is emitted by Alice as an **n-photon** state.



For example, with photon number splitting attack:

$Y_2 = 1$: all two-photon states are detected by Bob.
$Y_1 = 0$: all single-photon states are lost.

Yield for multi-photons may be much higher than single-photons.

Is there any way to detect this?

A solution: Decoy State (Toy Model)

Goal: Design a method to test experimentally the yield (i.e. transmittance) of multi-photons.

Method: Use two-photon states as decoys and test their yield.

Alice: N signals 

Bob: x signals 

Alice sends N two-photon signals to Bob.
Alice and Bob estimate the yield $Y_2 = x/N$.
If Eve selectively sends multi-photons, Y_2 will be abnormally large.
Eve will be caught!

Procedure of Decoy State QKD (Toy Model).

A) Signal state: Poisson photon number distribution α (at Alice).

B) Decoy state: = two-photon signals

1) Alice a state or state to Bob.
2) Bob acknowledges receipt of signals.
3) Alice publicly announces which are signal states and which are decoy states.
4) Alice and Bob compute the transmission probability for the signal states and for the decoy states respectively.

If Eve selectively transmits two-photons, an abnormally high fraction of the decoy state B) will be received by Bob. Eve will be caught.

Practical problem with toy model

- Problem: Making perfect two-photon states is hard, in practice

- Solution: Make **another mixture** of good and bad guys with a **different weight**.

Decoy state idea (Heuristic)

1) Signal state: Poisson photon number distribution: α (at Alice). Mixture 1.

2) **Decoy state: Poisson photon number distribution: $\mu \sim 2$ (at Alice). Mixture 2**

W.-Y. Hwang's **heuristic** idea (PRL):

- If Eve lets an abnormally high fraction of multi-photons go to Bob, then decoy states (which has high weight of multi-photons) will have an abnormally high transmission probability.
- Therefore, Alice and Bob can catch Eve!

Can we make things rigorous?

YES!

3. Our solution:

I Come!

Experimental observation

Yield: $$Q(\mu) = Y_0 e^{-\mu} + Y_1 e^{-\mu}\mu + Y_2 e^{-\mu}(\mu^2/2) + \ldots + Y_n e^{-\mu}(\mu^n/n!) + \ldots.$$

Error Rate $$E(\mu) = Y_0 e^{-\mu} e_0 + Y_1 e^{-\mu}\mu e_1 + Y_2 e^{-\mu}(\mu^2/2) e_2 + \ldots + Y_n e^{-\mu}(\mu^n/n!) e_n + \ldots.$$

If Eve cannot treat the decoy state any differently from a signal state

$$Y_n(\text{signal}) = Y_n(\text{decoy}),\ e_n(\text{signal}) = e_n(\text{decoy})$$

Y_n: yield of an *n*-photon signal

e_n : quantum bit error rate (QBER) of an *n*-photon signal.

Idea

Try **every** Poisson distribution μ!

We propose that Alice *switches power of her laser up and down*, thus producing as decoy states Poisson photon number distributions, μ's for **all** possible values of μ's.

Each μ gives Poisson photon number distribution:

$$Q(\mu), E(\mu) \forall \mu \Rightarrow Y_n, e_n \forall n$$

Our Contributions

1. *Making things rigorous* (Combine with entanglement distillation approach in Shor-Preskill's proof.)

2. *Constraining dark counts* (Detectors may claim to have registered events even when the input is a vacuum. These dark counts are often the limiting factor to the distance of secure QKD. Using vacuum as a decoy state to constrain the "dark count" rate.)

3. *Constructing a general theory* (Infering **all** Y_n, e_n.)

$$Q(\mu), E(\mu) \forall \mu \Rightarrow Y_n, e_n \forall n$$

Conclusion: We severely limit Eve's eavesdropping strategies.

Any attempt by Eve to change <u>any</u> of Y_n, e_n 's will, in principle be caught.

Old Picture

	Theory	Experiment
Secure bits per signal:	$S = O(\eta^2)$.	$S = O(\eta)$.
Maximal distance:	d ~ 35km.	d >120km.

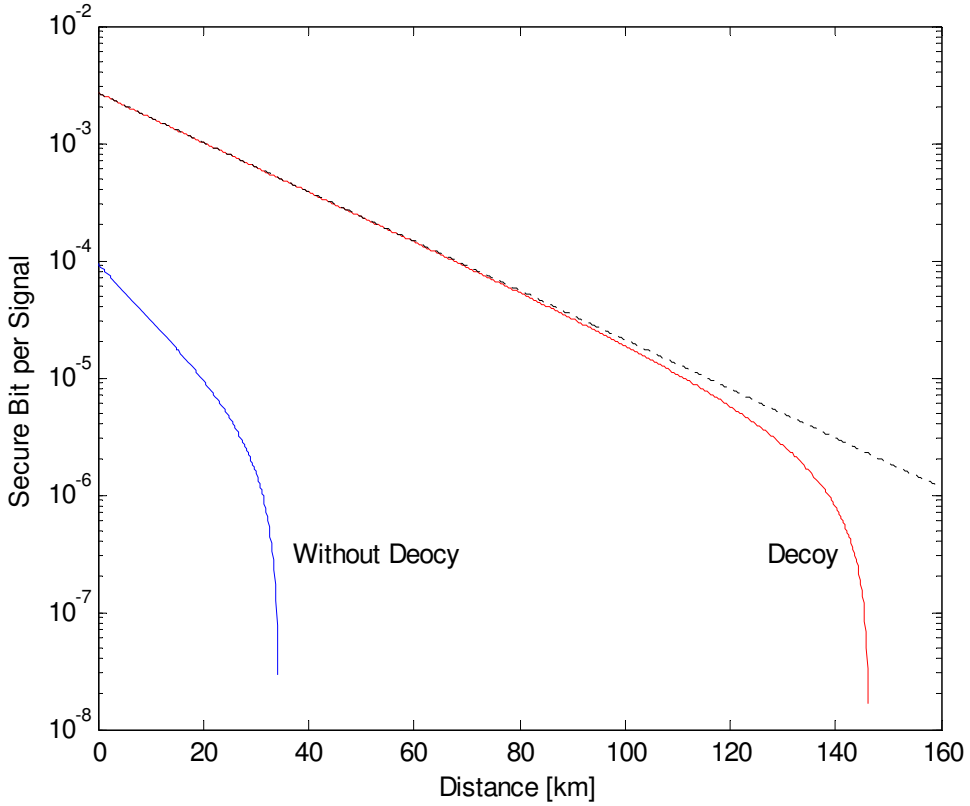
There is a big gap between theory and practice of BB84.

NEW Picture

	Theory	Experiment
Secure bits per signal:	$S = O(\eta)$.	$S = O(\eta)$.
Maximal distance:	d >120 km.	d >120km.

Even with imperfect devices, one gets highest performance possible **without** compromising security.

Compare the results with and without decoy states



Key parameter:

Wavelength: 1550nm

Channel loss: 0.21dB/km

Signal error rate: 3.3%

Dark count: $8.5*10^{-7}$ per pulse

Receiver loss and detection efficiency: 4.5%

The experiment data for the simulation come from the recent paper:
C. Gobby, Z. L. Yuan, and A. J. Shields, Applied Physics Letters, (2004)

Related Work

- Using another approach (strong reference pulse), another protocol (essentially B92) has recently been proven to be secure with $R=O(\eta)$. [Koashi, quant-ph/0403131]

- In future, it will be interesting to compare this approach with ours.

Summary

1. Decoy state BB84 allows:
   - Secure bits per signal: O (η)
     where η : channel transmittance.
   - Distance > 100km

2. Easy to implement. Alice just switches power of laser up and down (and measure transmittance and error rate).

3. Theory and experiment go hand-in-hand for standard BB84 quantum key distribution protocol.

THE END