Title: Experimental decoy state quantum key distribution

Date: Dec 13, 2006 04:00 PM

URL: http://pirsa.org/06120044

Abstract:

Experimental Decoy State Quantum Key Distribution

Yi Zhao

Joint work with Bing Qi, Xiongfeng Ma, Hoi-Kwong Lo, and Li Qian

Center for Quantum Information and Quantum Control (CQIQC)

Dept. of Electric and Computer Engineering, and Dept. of Physics

University of Toronto

Canada Research Chairs

NSERC CRSNG

ICIP CIPI

Ontario Innovation Trust

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

premier's research excellence awards

CIAR Canadian Institute for Advanced Research

Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

One-time pad

XOR=
Exclusive-OR

If Alice and Bob share a common long random string of secret, then One-time-pad method is perfectly secure. (Shannon 1949)

QUESTION: How to transfer the key?

One-time pad

XOR = Exclusive-OR

If Alice and Bob share a common long random string of secret, then One-time-pad method is perfectly secure. (Shannon 1949)

QUESTION: How to transfer the key?

Key Distribution Problem

Classical Key Distribution

Eve's copying machine

Bob

(representable as a string of Number: 01101.....)

Eve

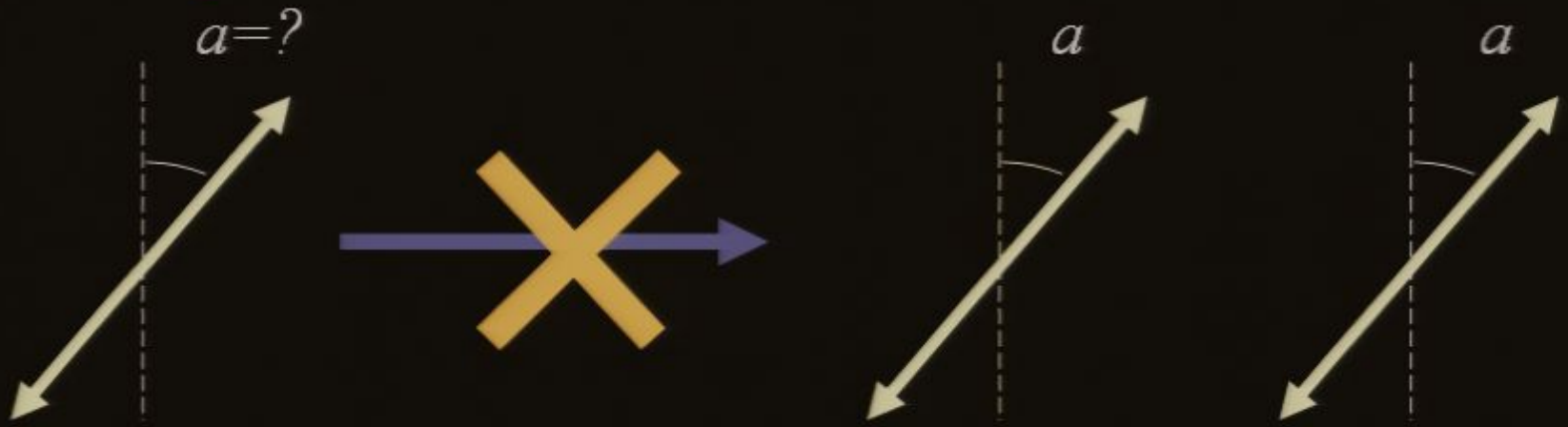
- All CLASSICAL key distribution schemes are fundamentally INSECURE.

Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Quantum Key Distribution (QKD)

Consider a single photon in an arbitrary polarization:



IMPOSSIBLE

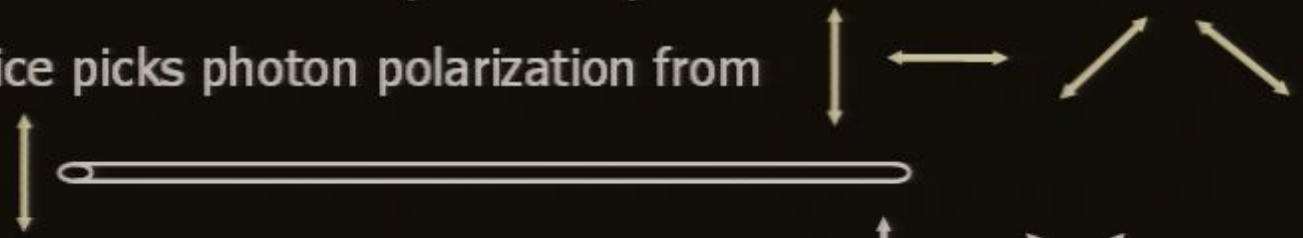
Quantum No-cloning Theorem

It is impossible to copy the state of
a single photon in an arbitrary polarization.

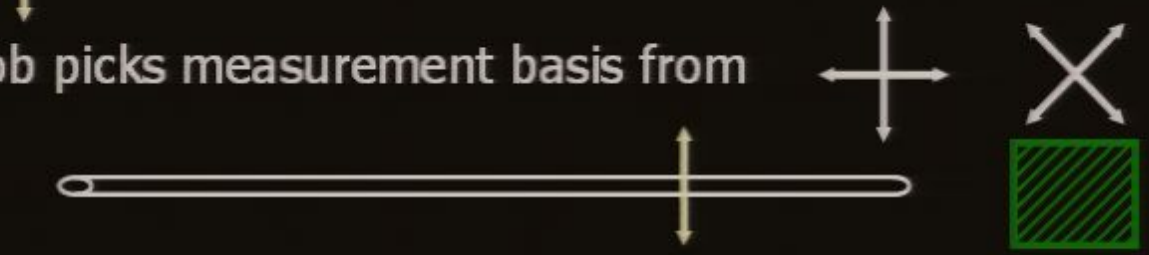
Procedure of standard BB84 QKD scheme

(Sketch)

Step 1: Alice picks photon polarization from



Step 2: Bob picks measurement basis from



Step 3: Bob records his basis and measurement outcome.

Step 4: Alice and Bob announce their bases publicly. They keep only the polarization data when they have used the same basis.

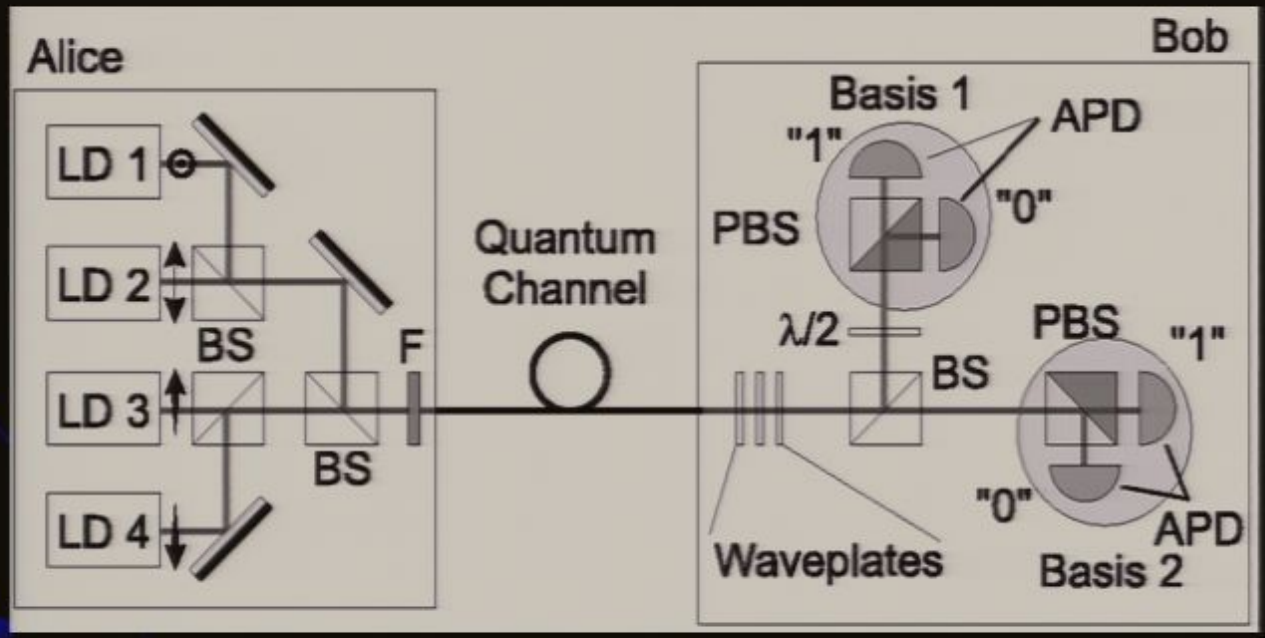
Step 5: Test for tampering by random sampling and computing quantum bit error rate. If error rate is OK, apply error correction and "privacy amplification".

Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

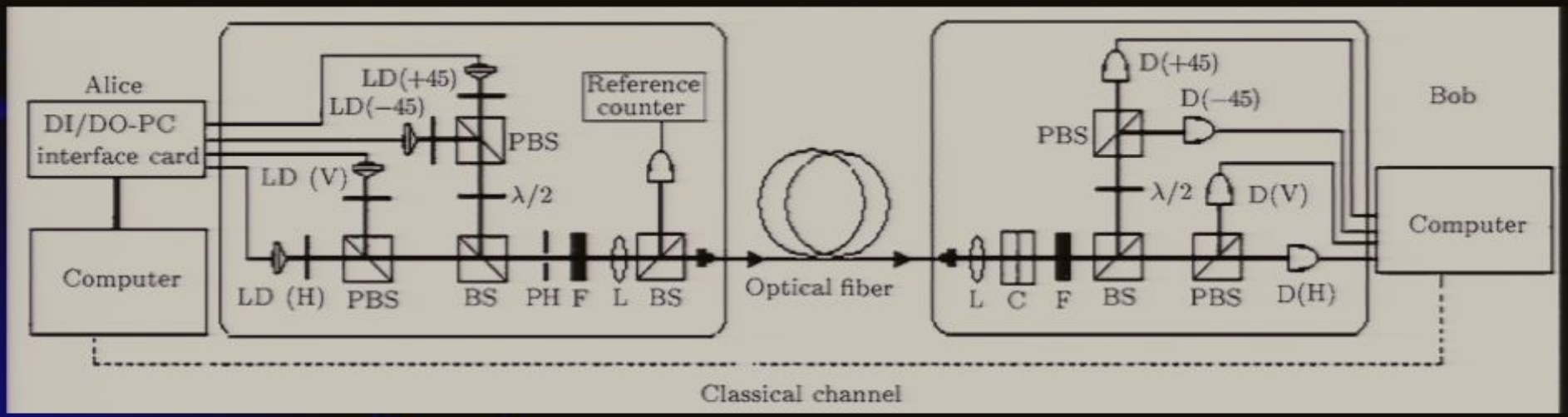
Set-up of polarization-encoding QKD (Conceptual)

- Alice prepares one photon with polarization of Q, R, H, or V randomly.
- Alice sends the photon through the quantum channel.
- Bob chooses a random basis, and perform measurement.



Set-up of polarization-encoding QKD (Experimental)

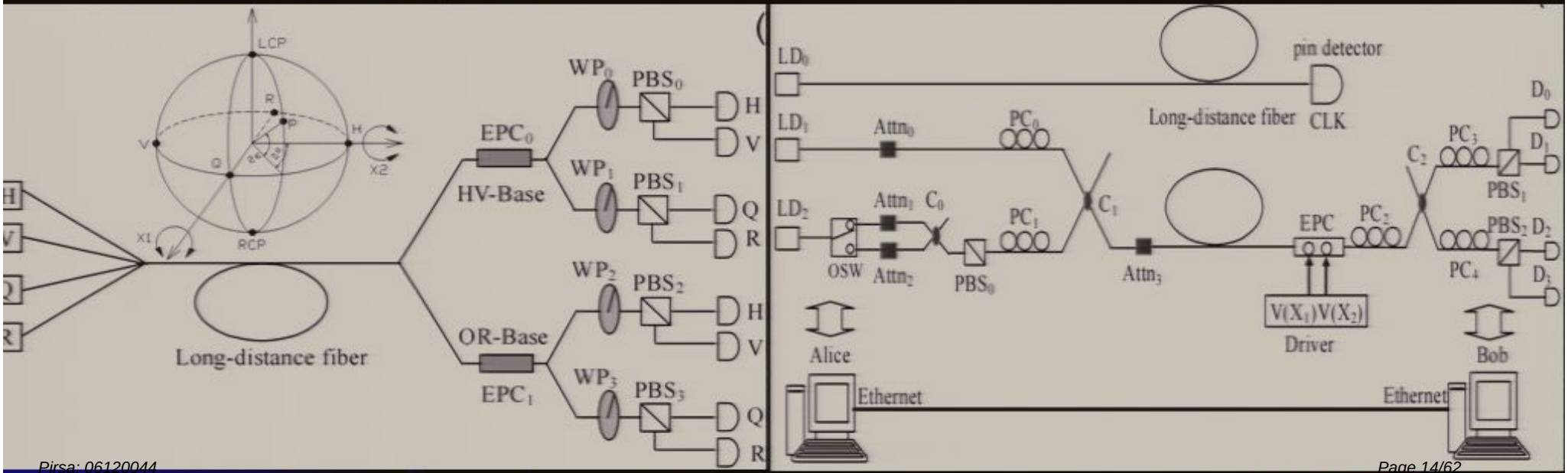
- Quantum Channel: Optical Fiber
  - Advantage: fiber network has been established.
  - Disadvantage: unpredictable polarization change due the birefringence of the fiber.
- Active polarization compensation?



W. –T. Liu *et. al.*, Chin. Phys. Lett., **23,** 287-289 (2006)

Set-up of polarization-coding QKD (with dynamic compensation)

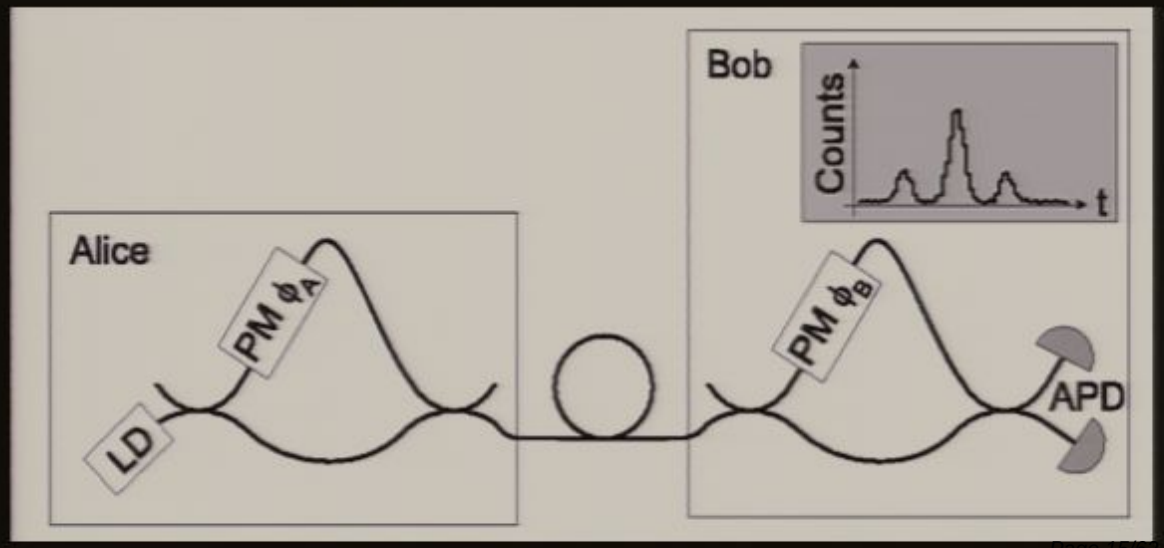
- Active polarization compensation
- Advantage: insensitive to length change
- Disadvantage: need many APDs; slow modulation, etc.



G. Wu, J, Chen, Y. Li, and H. Zeng, quant-ph/0606108

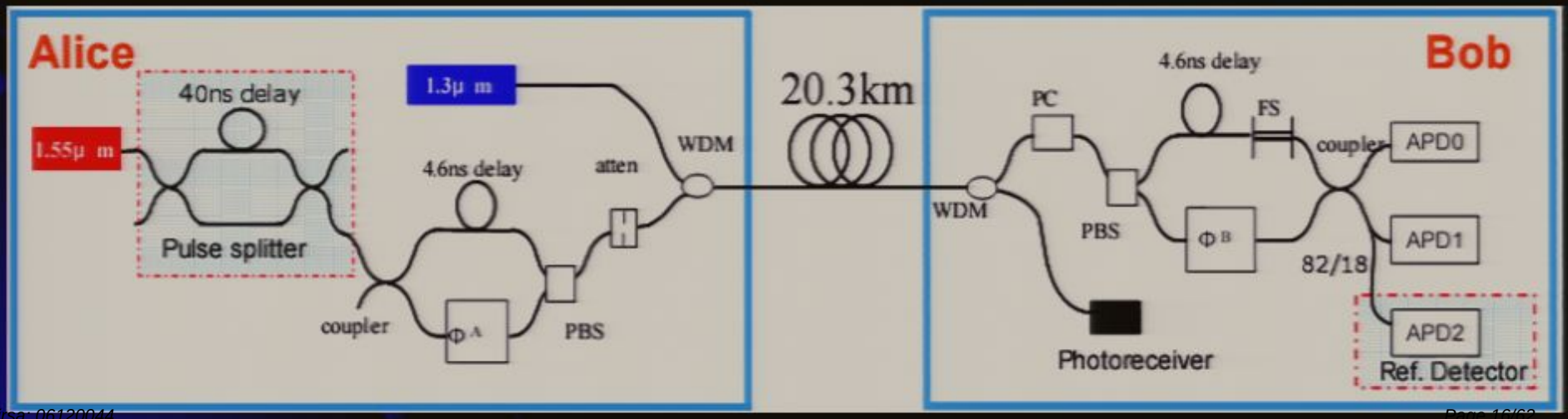
Set-up of phase-coding QKD (conceptual)

- Easy to be implemented by SMF components
- Much less dependent on polarization control
- Mismatches of the two Mach-Zenhder interferometers must be almost identical – local compensation is necessary.



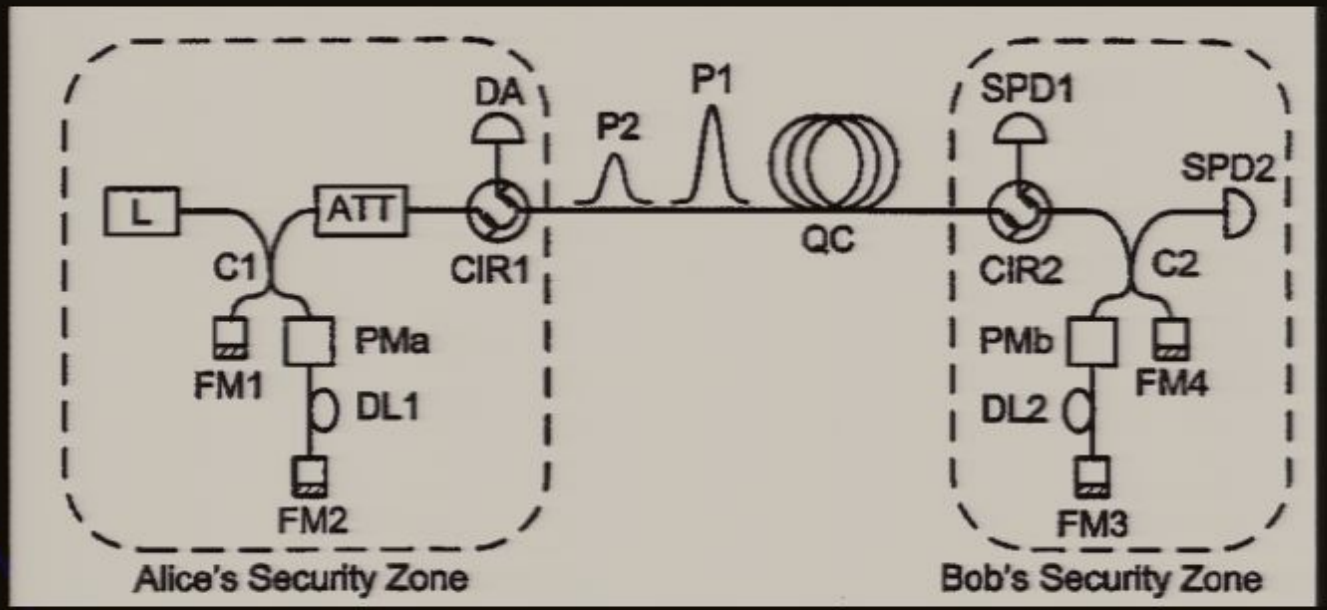
Set-up of phase-coding QKD (experimental)

- Active length drift compensation is achieved by introducing a reference detector.
- Still need polarization compensation…



Set-up of phase-coding QKD (experimental)

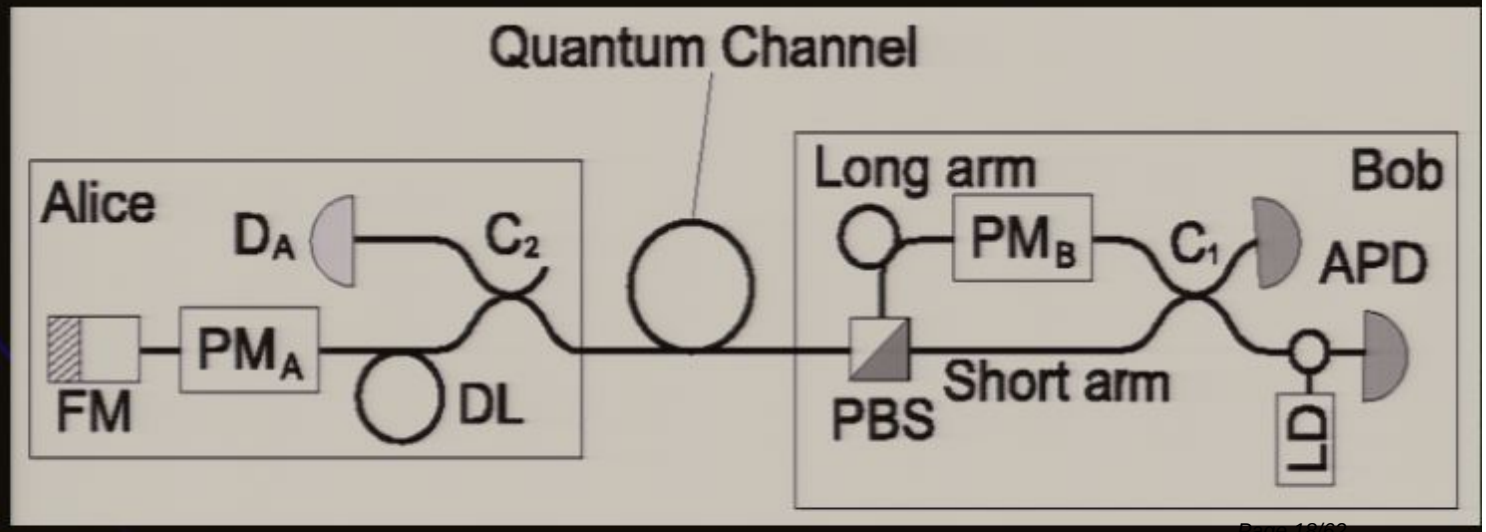
- Active polarization is no longer necessary by introducing the Faraday-Michelson system
- Active length compensation is still necessary.



X. –F. Mo *et al.*, Opt. Lett., **30**, 2632-2634 (2005)

“Plug & Play”?

- Laser pulse is generated by Bob, and travels through the same channel twice.
- Both polarization and length changes are compensated.
- Our Choice



Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Imperfections of Practical QKD Set-up

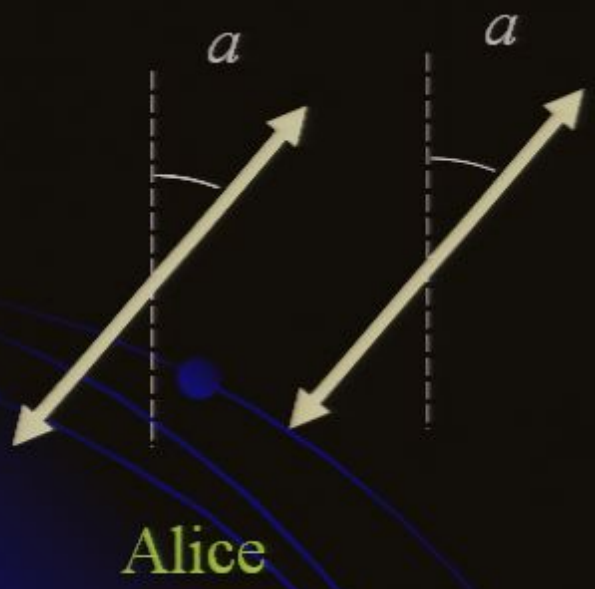
- Source: Attenuated Laser
  - Coherent State $|\mu\rangle$
  - Phase is uniformly randomized.
  - Photon Number Distribution: Possionian
- Occasional Generation of Multi-Photon Signals
- Channel: Lossy and Noisy.

Multi-photons are insecure

- A multi-photon signal CAN be split. (Therefore, insecure for BB84.)

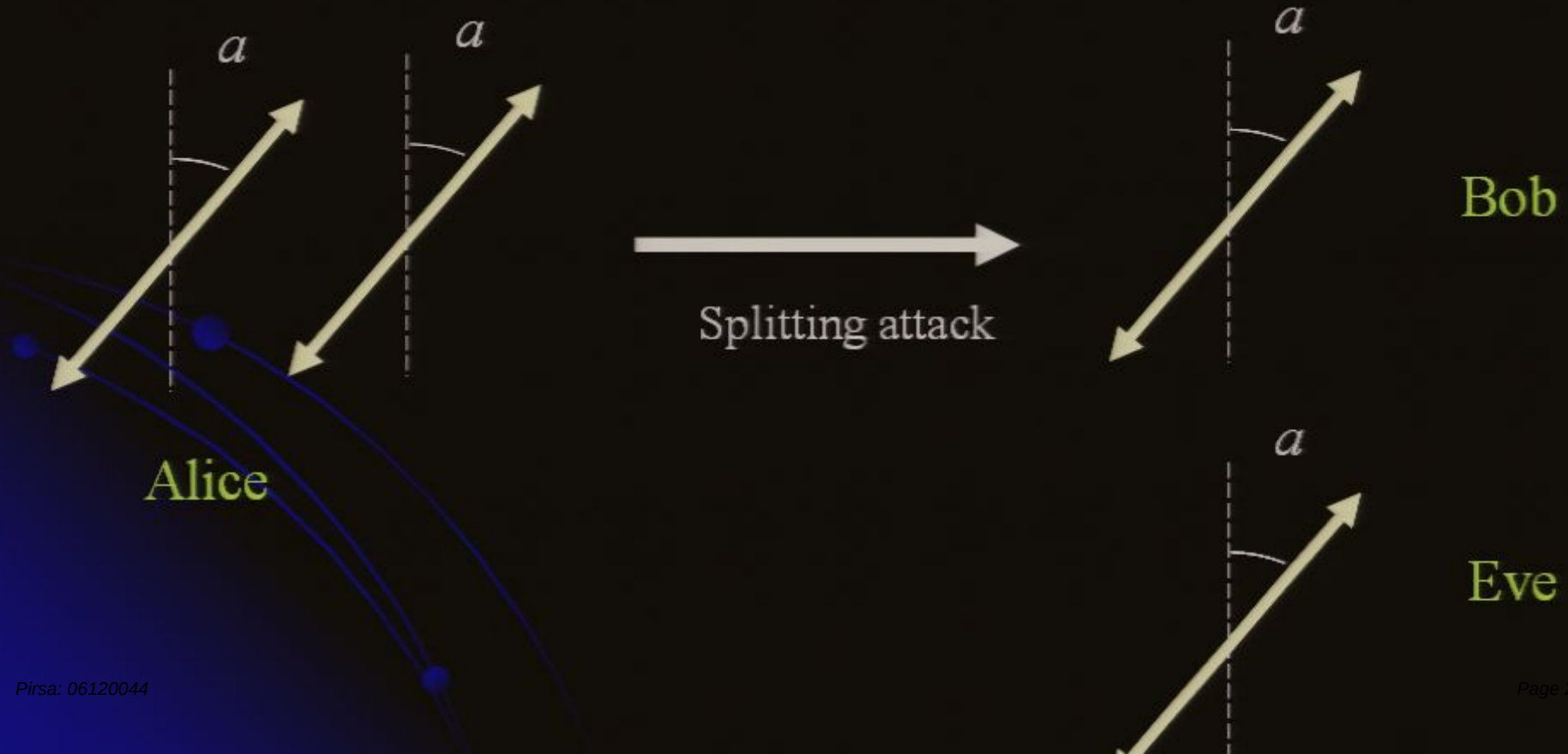
Multi-photons are insecure

- A multi-photon signal CAN be split. (Therefore, insecure for BB84.)



Multi-photons are insecure

- A multi-photon signal CAN be split. (Therefore, insecure for BB84.)



Photon-number splitting attack

- Eve measures the photon number, n.
- Single Photon States: Block
- Multi-Photon States: Split
- Eve has an identical copy of what Bob possesses.

Previous Solution

- Perfect Single Photon Source
  - Very Challenging to Build
  - Not Practical for Now
- Privacy Amplification
  - Estimate maximum information obtained by Eve
  - Imperfect set-up can be made secure
  - Very low key generation rate and very short transmission distance

Decoy State QKD: Basic Idea

- Signal state: Poisson photon number distribution μ (at Alice)
- Decoy states: different expected photon numbers $\nu_1, \nu_2, \nu_3 \cdots$
- Given an n-photon state, Eve cannot tell if it is from a decoy or a signal.
- Lower bound of key generation rate could be estimated from gains and QBERs of different states.
- Dramatic Performance Improvement

- W. -Y. Hwang, Phys. Rev. Lett., 91, 057901 (2003)
- H. -K. Lo, Proceedings of the International Symposium on Information Theory (ISIT) 2004 p137
- H. -K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. 94 230504 (2005).

Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Decoy State QKD: Method

1. Alice randomly sends either a signal state or decoy state to Bob.
2. Bob acknowledges receipt of signals.
3. Alice announces the Decoy Profile.
4. Alice and Bob compute the gains and QBERs for the signal state and the decoy states.
5. They estimate the lower bound of secure key generation rate.

Decoy State QKD: Protocols

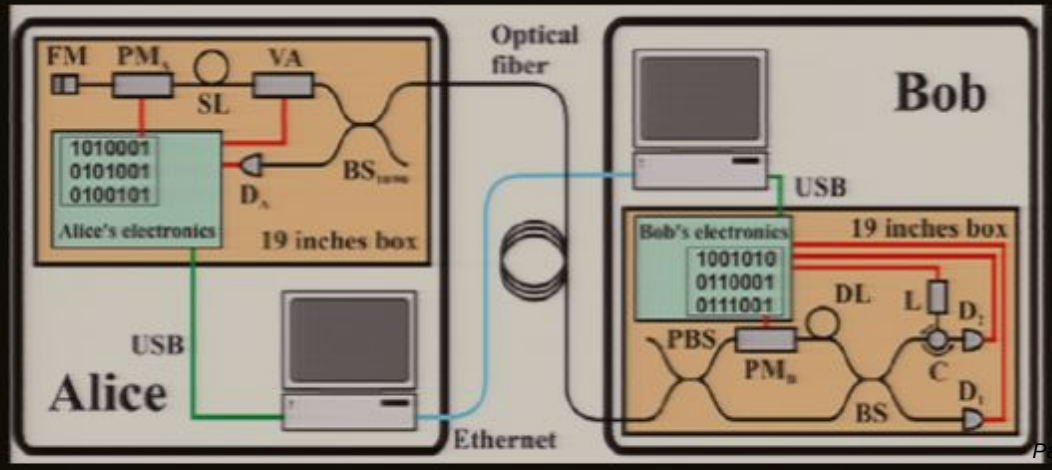
- One-Decoy Protocol
  - *One* Decoy State is Introduced
  - Easiest to Implement
- Weak+Vacuum Protocol
  - *Two* Decoy States are Introduced
  - Vacuum: No Photon (|0>)
  - Optimal in Asymptotic Case
- General Two-Decoy Protocol

Xiongfeng Ma, Bing Qi, Yi Zhao, and Hoi-Kwong Lo, Phys. Rev. A, 72, 012326 (2005).

See also: X. –B. Wang, Phys. Rev. Lett., 94, 230503 (2005); X. –B. Wang, Phys. Rev. A, 72, 012322 (2005)

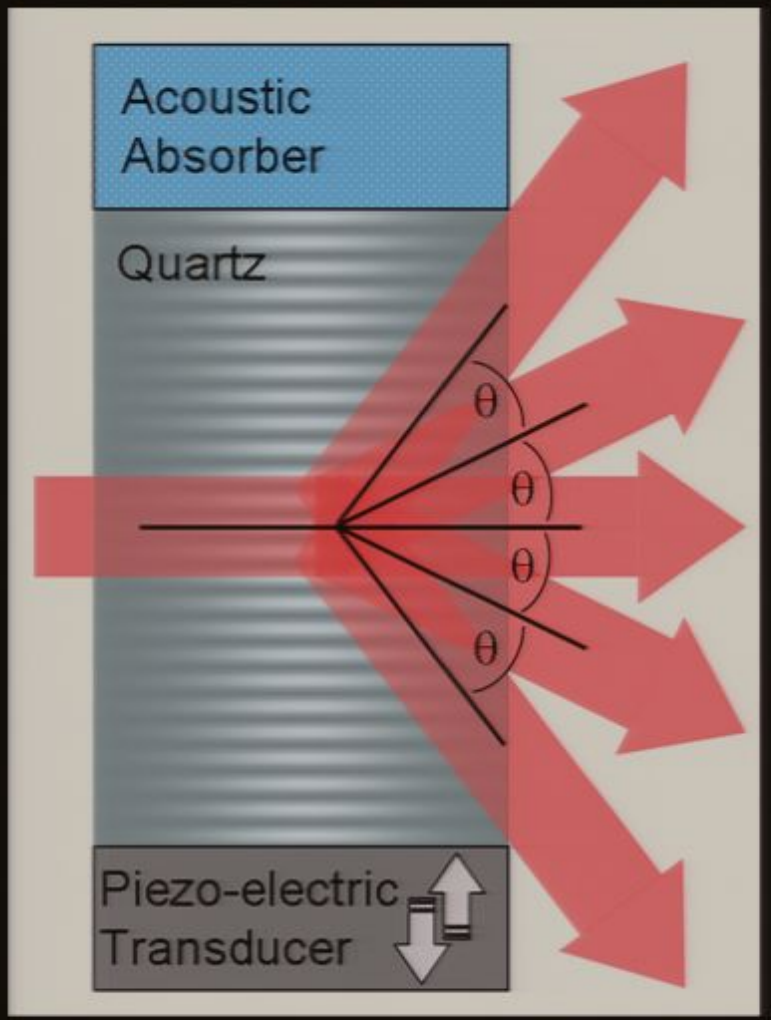
Requirements of Amplitude Modulator

- Our system: “P&P” system @ 5MHz
- The amplitude modulator should be able to work at the same frequency.
- The modulation should be insensitive to the polarization change of incoming light.



Choice of Amplitude Modulator

- Acousto-Optic Modulator (AOM)
- Principle: acoustic wave creates periodical refractive index change, forming a grating.
- Potential problem: frequency shift due to Doppler effect.



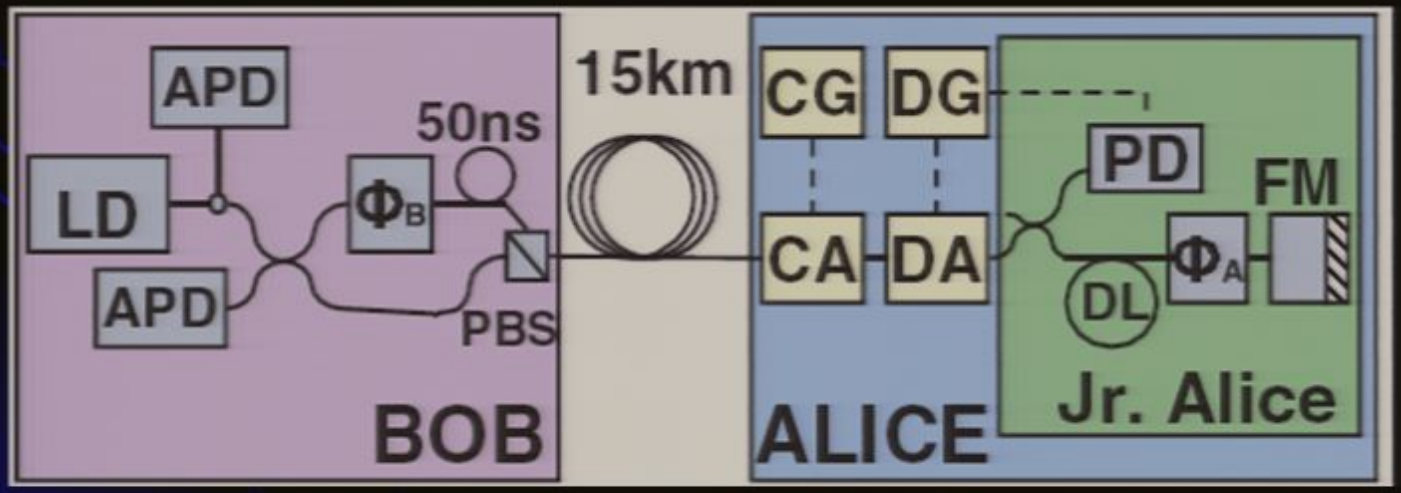
Borrowed from *Wikipedia*®

Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

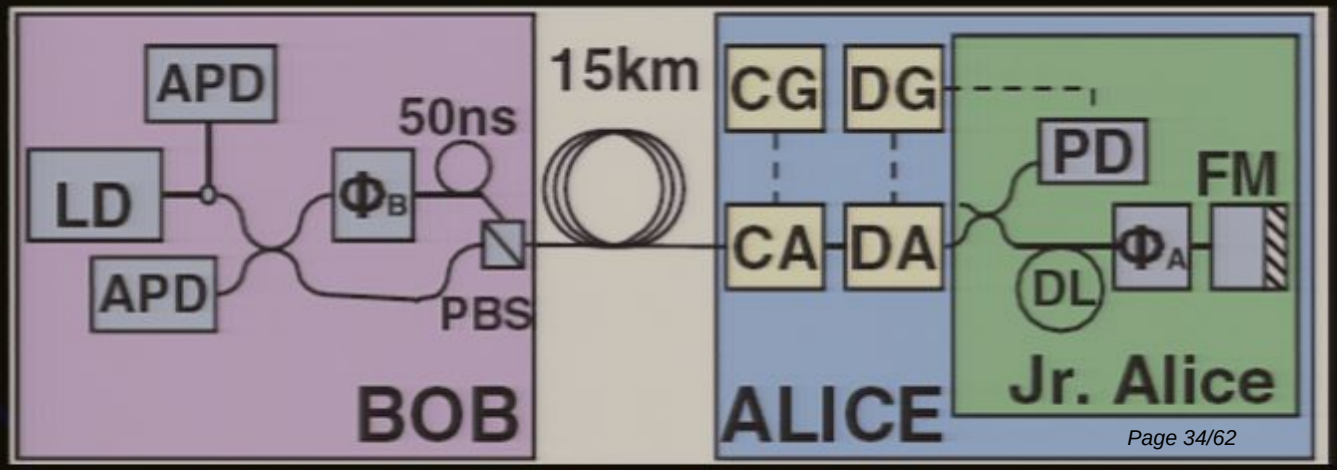
One-Decoy Protocol: Experiment

- First Decoy State QKD Experiment
- Based on Commercial "Plug & Play" QKD System
- First Application of AOM in QKD
- μ=0.80, v=0.12



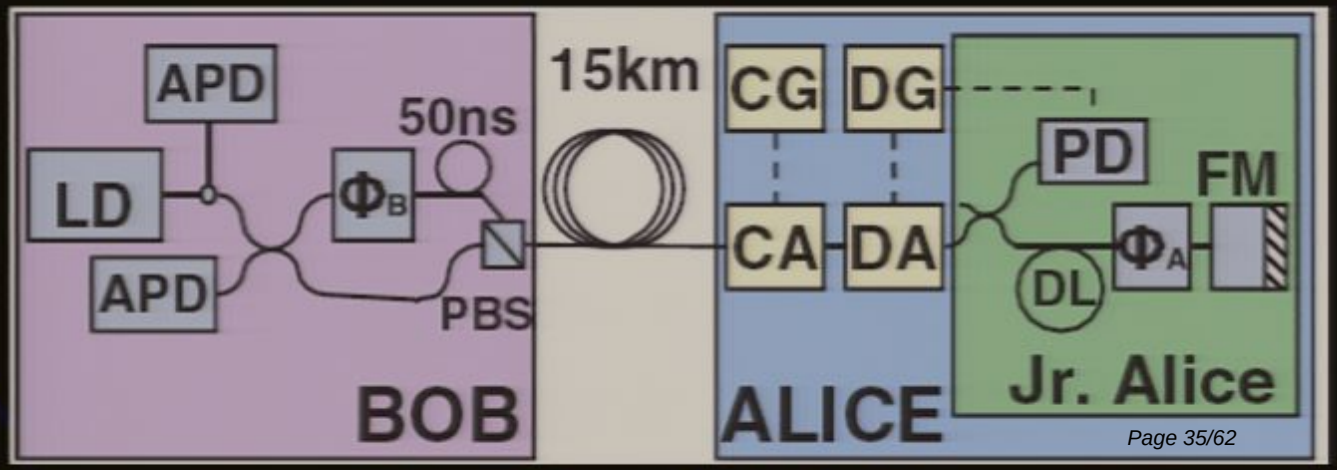
X. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. 96, 070502 (2006)

One-Decoy Protocol: Experiment



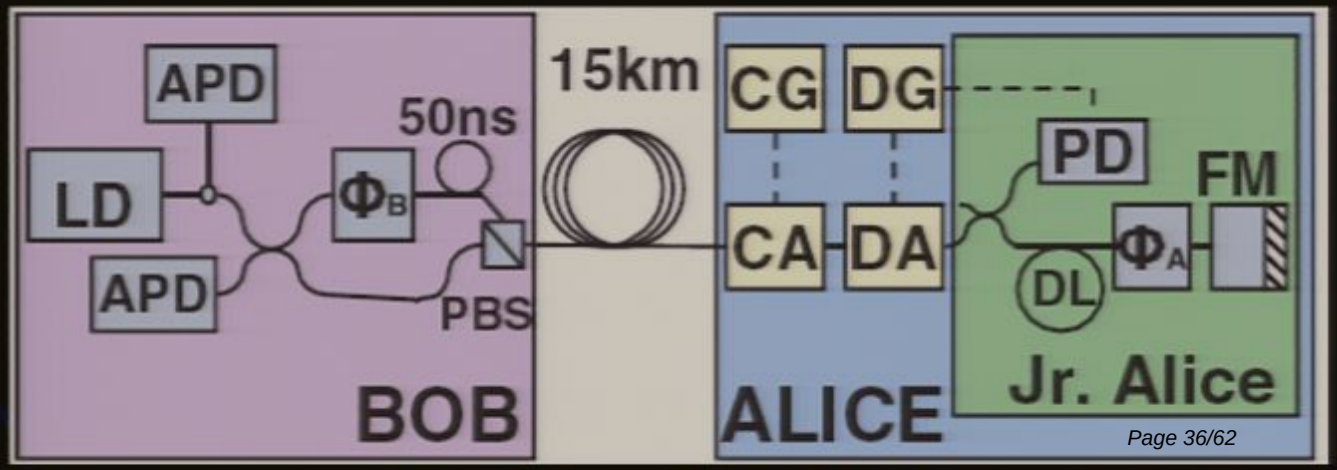
One-Decoy Protocol: Experiment

- Bob generates strong laser pulses.



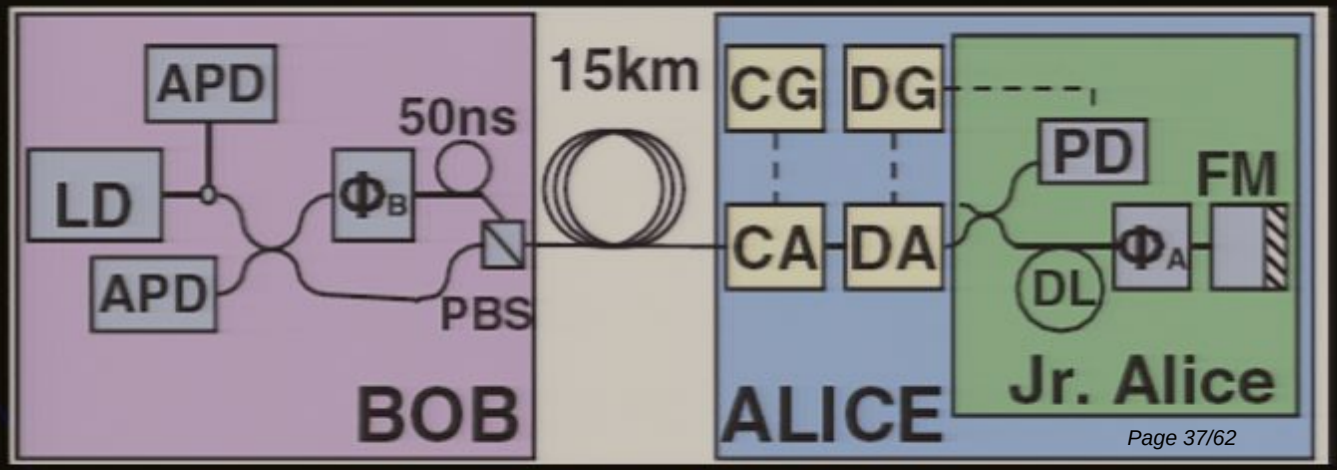
One-Decoy Protocol: Experiment

- Bob generates strong laser pulses.
- Alice encodes her information.



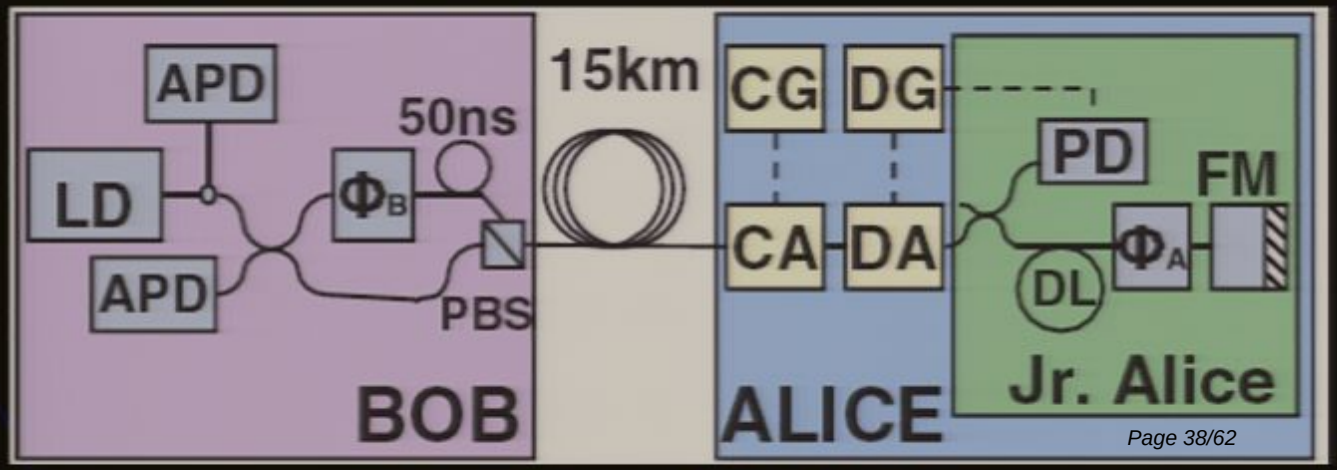
One-Decoy Protocol: Experiment

- Bob generates strong laser pulses.
- Alice encodes her information.
- Meanwhile, a synchronization signal is generated to trigger the functional generator.



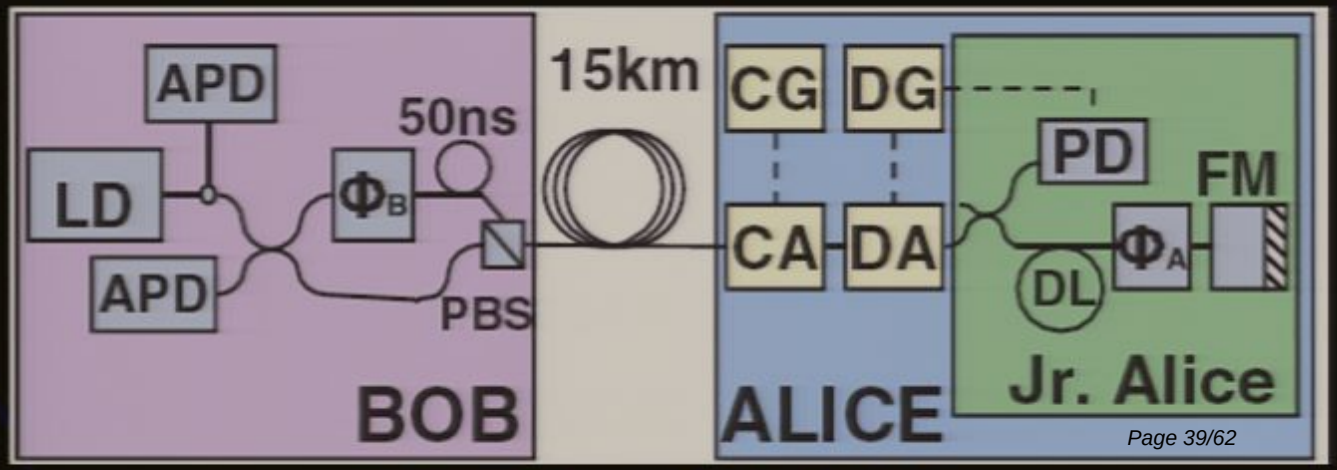
One-Decoy Protocol: Experiment

- Bob generates strong laser pulses.
- Alice encodes her information.
- Meanwhile, a synchronization signal is generated to trigger the functional generator.
- The generator drives the AOM to modulate the intensities of pulses randomly when they propagate through the AOM.



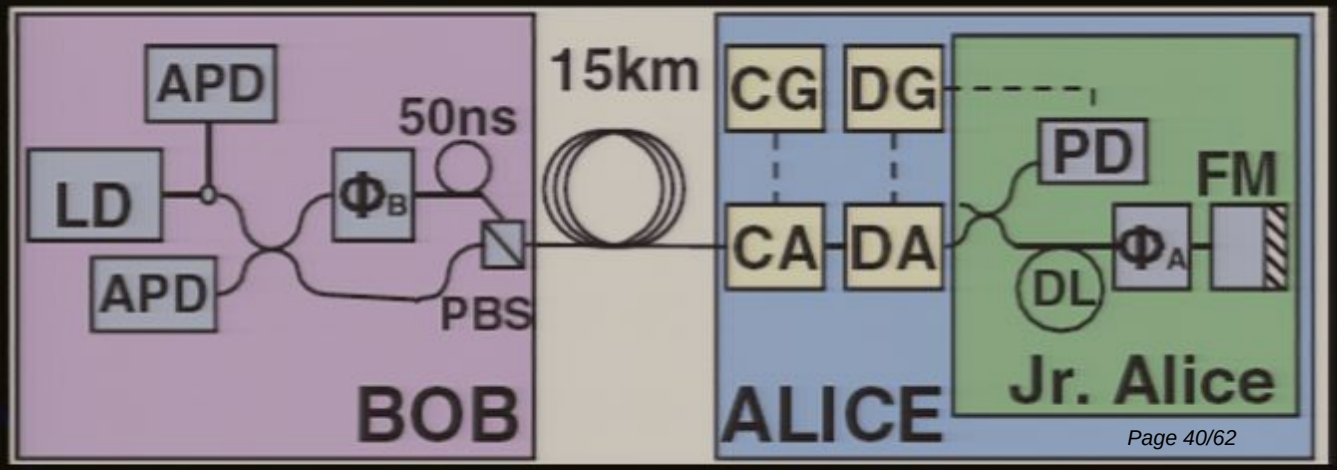
One-Decoy Protocol: Experiment

- Bob generates strong laser pulses.
- Alice encodes her information.
- Meanwhile, a synchronization signal is generated to trigger the functional generator.
- The generator drives the AOM to modulate the intensities of pulses randomly when they propagate through the AOM.
- Bob decodes the information.



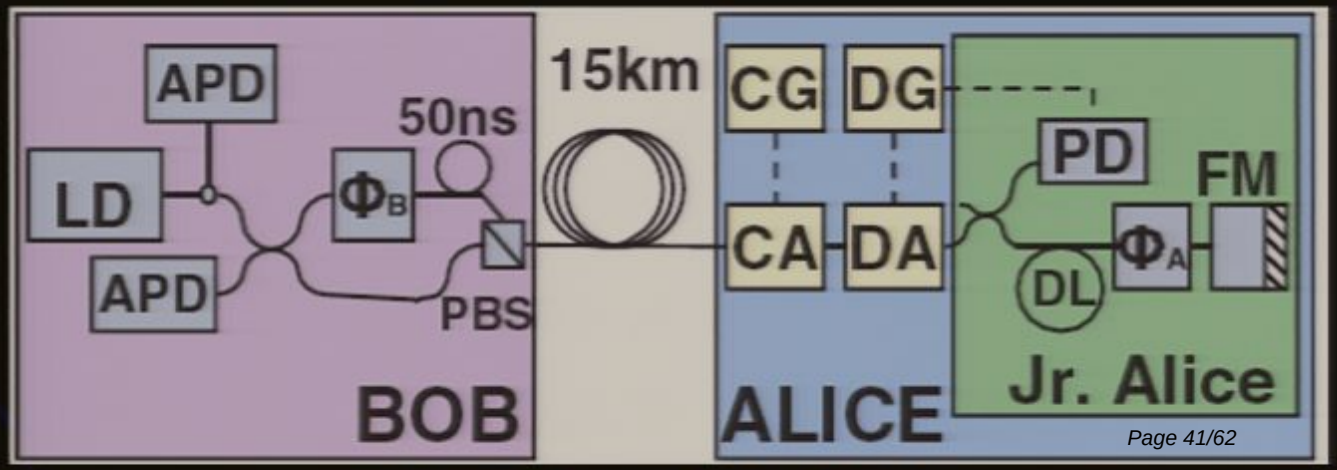
One-Decoy Protocol: Experiment

- Bob generates strong laser pulses.
- Alice encodes her information.
- Meanwhile, a synchronization signal is generated to trigger the functional generator.
- The generator drives the AOM to modulate the intensities of pulses randomly when they propagate through the AOM.
- Bob decodes the information.
- Alice broadcasts the basis information as well as the decoy profile.



One-Decoy Protocol: Experiment

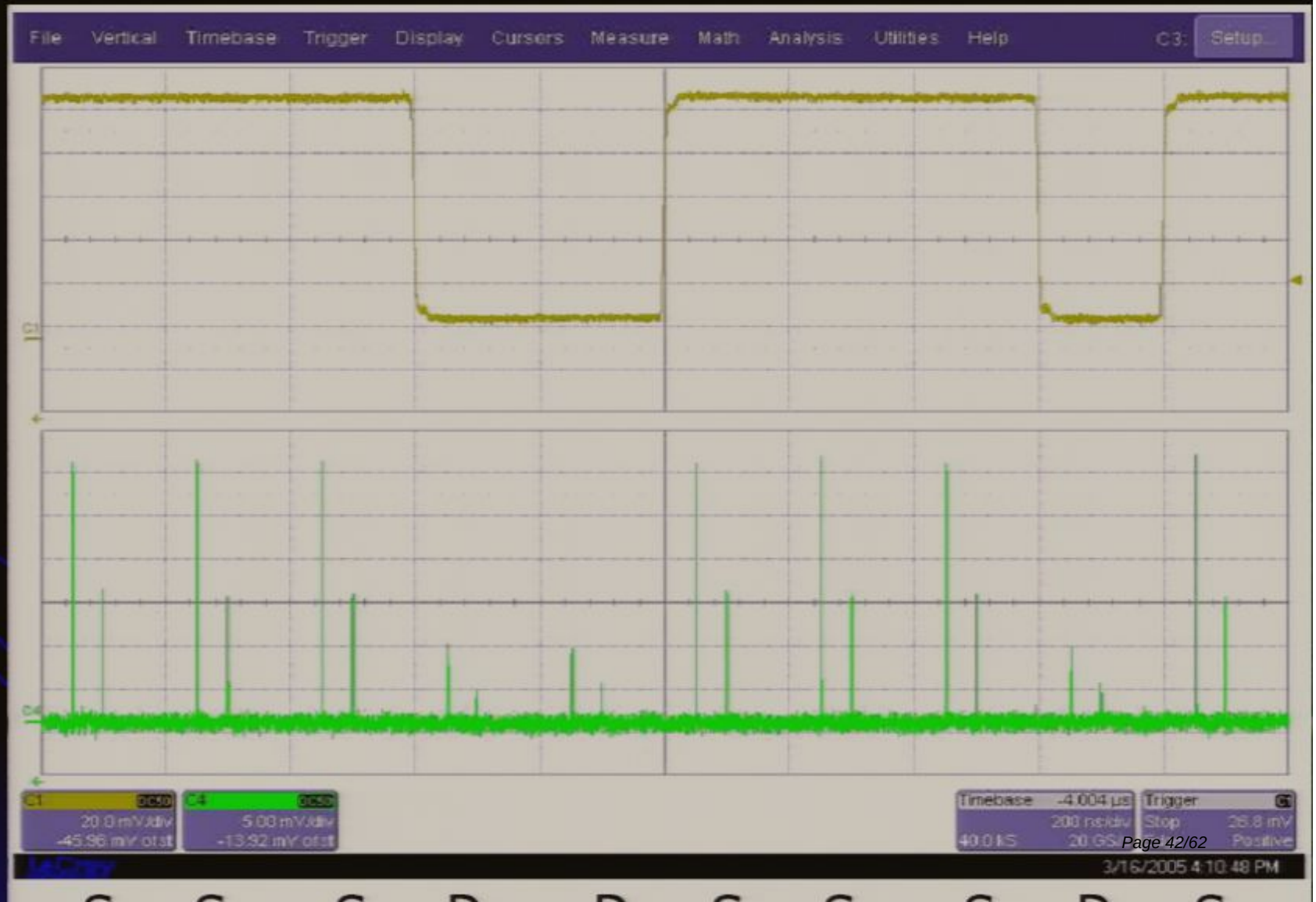
- Bob generates strong laser pulses.
- Alice encodes her information.
- Meanwhile, a synchronization signal is generated to trigger the functional generator.
- The generator drives the AOM to modulate the intensities of pulses randomly when they propagate through the AOM.
- Bob decodes the information.
- Alice broadcasts the basis information as well as the decoy profile.
- Bob computes the gains and QBERs of different states.



The Decoy is in the Data!

Modulation Voltage

Intensity of Laser Pulse

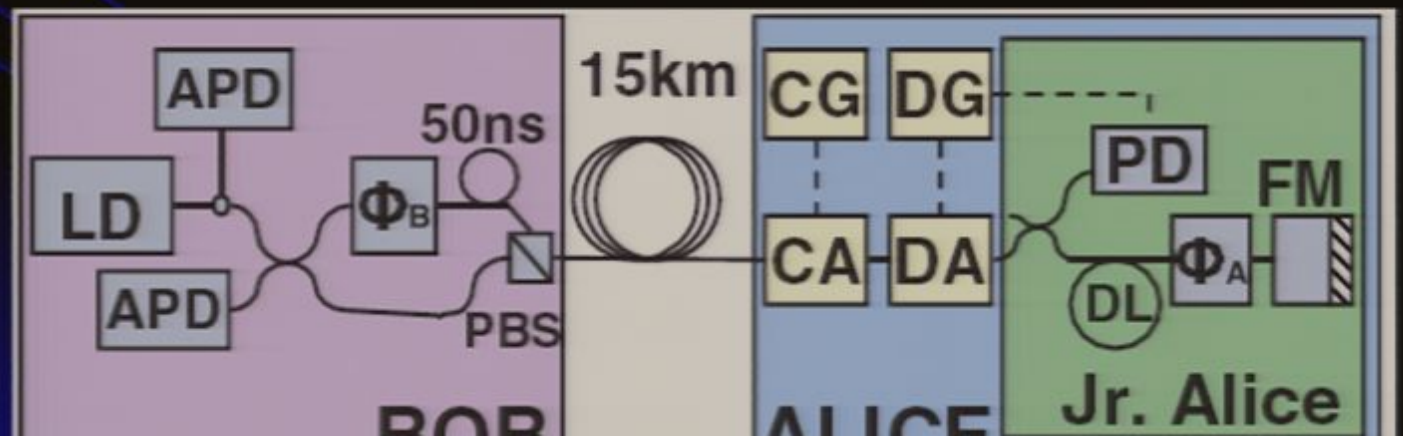


One-Decoy Protocol: Experiment

- 15km Optical Fiber
- Key Rate: 3.6e-4 per pulse, ¼ of Theoretical Limit

The Frequency-Shift

- The frequency shift results in phase shift due to the asymmetric Mach-Zenhder interferometer.
- Very high QBER
- Compensation: introducing another AOM
- Can we remove this AOM?

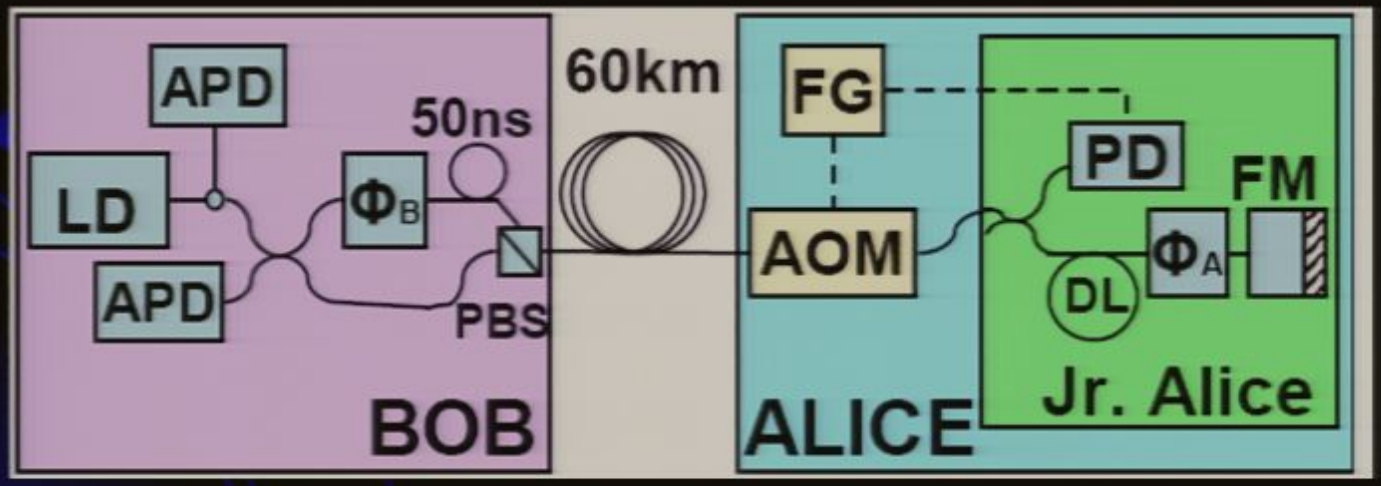


Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Weak+Vacuum Protocol: Experiment

- More Complicated than One-Decoy Protocol
- But with Simpler Set-up
- Over 60km Fiber
- Secure Key Rate: 8.5e-5 per pulse



Y. Zhao, B. Qi, X. Ma, H. –K. Lo, and L. Qian, in Proceedings of *IEEE ISIT*, 2094-2098 (2006)

Outline

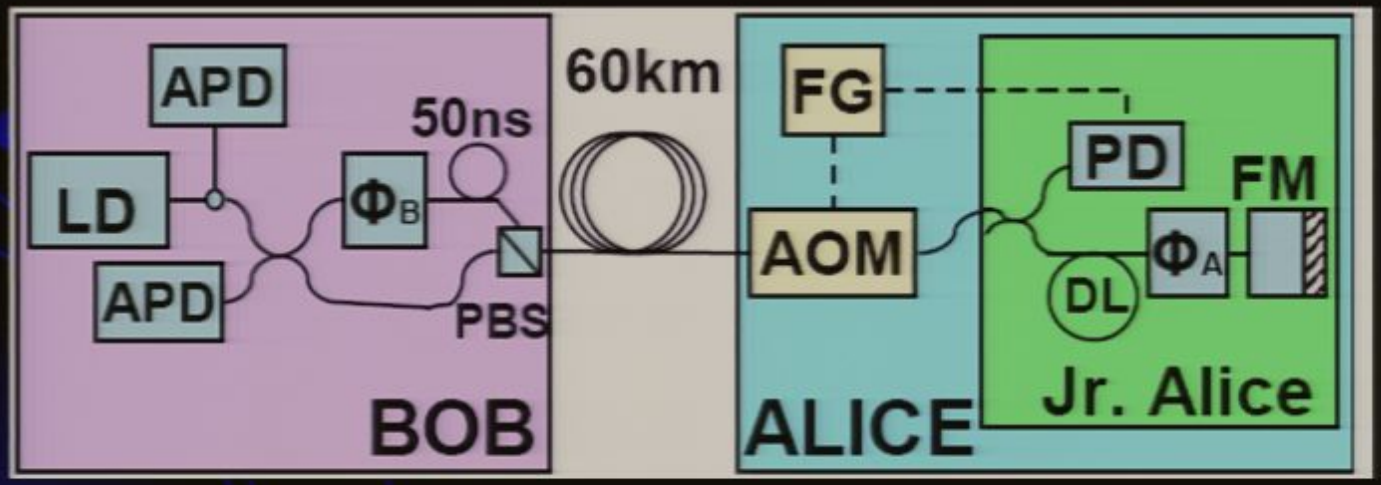
- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Numerical Simulation: Necessity

- How many bits should be assigned as decoys/signals?
- How to choose the intensity of each state?
- How long the channel should be?

Weak+Vacuum Protocol: Experiment

- More Complicated than One-Decoy Protocol
- But with Simpler Set-up
- Over 60km Fiber
- Secure Key Rate: 8.5e-5 per pulse



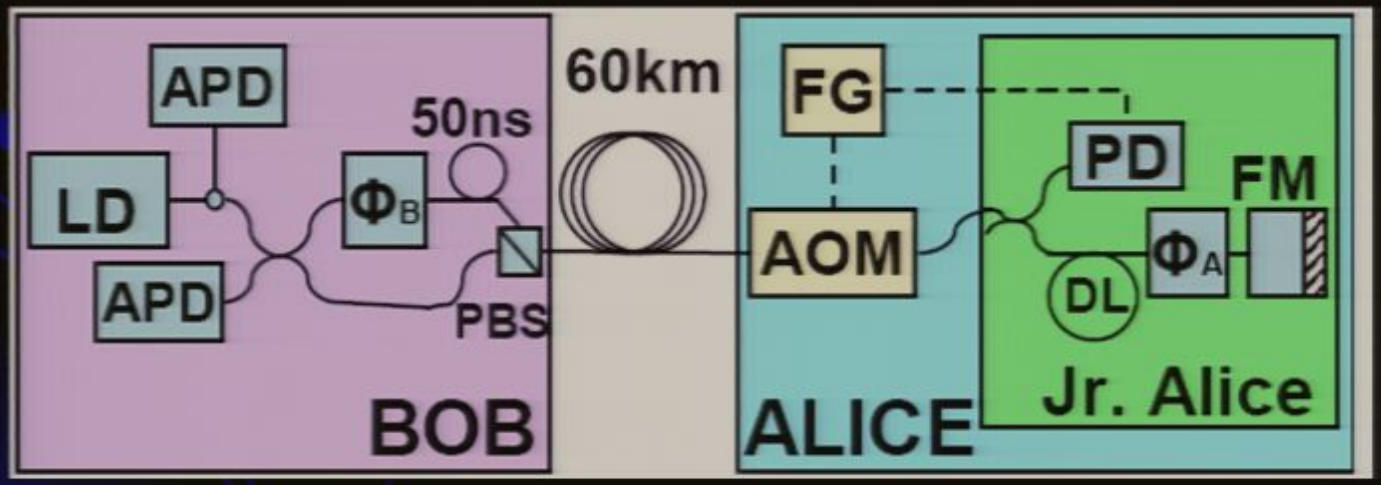
Y. Zhao, B. Qi, X. Ma, H. –K. Lo, and L. Qian, in Proceedings of *IEEE ISIT*, 2094-2098 (2006)

The Frequency-Shift

- The frequency shift results in phase shift due to the asymmetric Mach-Zenhder interferometer.
- Very high QBER
- Compensation: introducing another AOM
- Can we remove this AOM?

Weak+Vacuum Protocol: Experiment

- More Complicated than One-Decoy Protocol
- But with Simpler Set-up
- Over 60km Fiber
- Secure Key Rate: 8.5e-5 per pulse



Y. Zhao, B. Qi, X. Ma, H. –K. Lo, and L. Qian, in Proceedings of *IEEE ISIT*, 2094-2098 (2006)

Outline

- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Numerical Simulation: Necessity

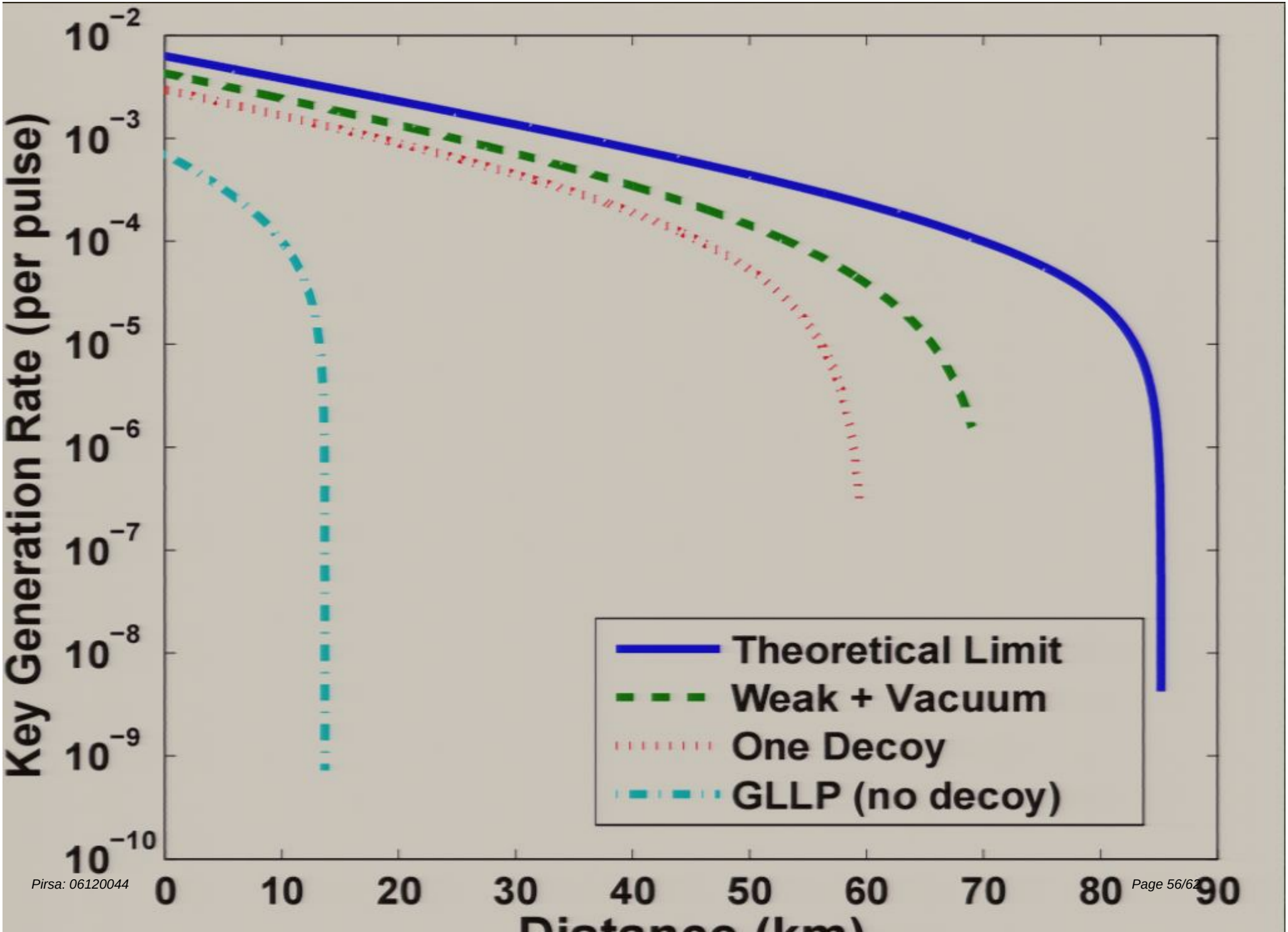
- How many bits should be assigned as decoys/signals?
- How to choose the intensity of each state?
- How long the channel should be?

Numerical Simulation: Model

- Source: Coherent States $|\mu\rangle$
- Channel: Single-Mode Fiber
  - Channel Transmittance: $\eta = \mathrm{Exp}(\alpha L)$
- Detector: Threshold
  - Efficiency: η_{Bob}
  - Error Rate: $e_{detector}$
  - Dark Count Rate: Y_0

Numerical Simulation: Principle

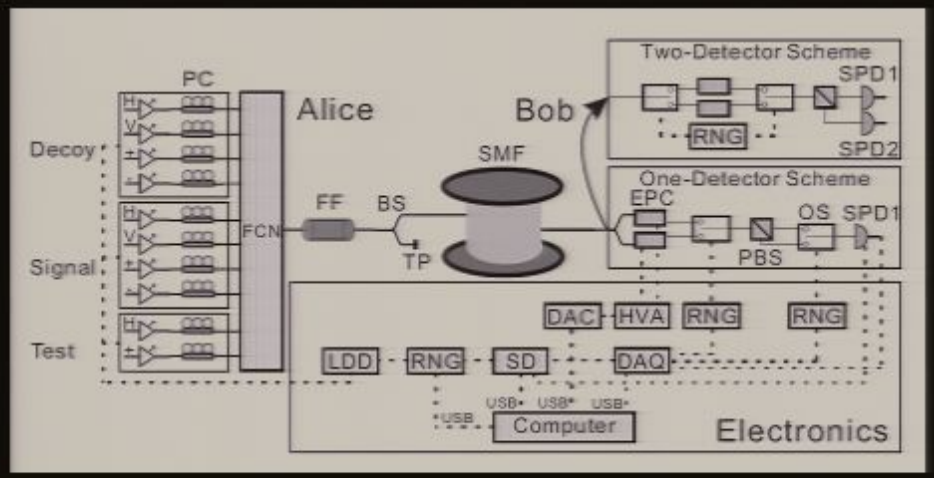
- Experimental Results can be Simulated
  - Gain: $Q(Y_0, \eta_{Bob}, \alpha, L, \mu)$
  - QBER: $E(Q, Y_0, e_{detector}, \eta_{Bob}, \alpha, L, \mu)$
- Key Generation Rate can be extracted with trial values of percentages and intensities of different states.
- At a certain distance (i.e., a certain channel loss), we can find the optimal combination of percentages and intensities of different states by exhaustive search.


Key Generation Rate (per pulse)
10^{-2}
10^{-3}
10^{-4}
10^{-5}
10^{-6}
10^{-7}
10^{-8}
10^{-9}
10^{-10}
0
10
20
30
40
50
60
70
80
90
Distance (km)
Theoretical Limit
Weak + Vacuum
One Decoy
GLLP (no decoy)

Outline

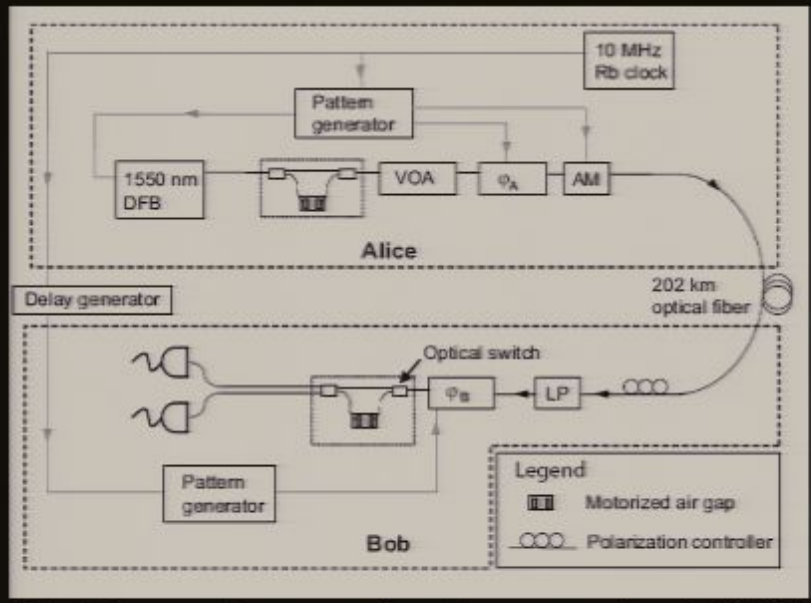
- Introduction
  - What is Quantum Key Distribution (QKD)?
  - Typical set-ups
  - Why do we need Decoy States?
- Experimental Implementations
  - One-Decoy Protocol
  - Weak+Vacuum Protocol
- Numerical Simulation
- Recent works and Summary

Some recent works

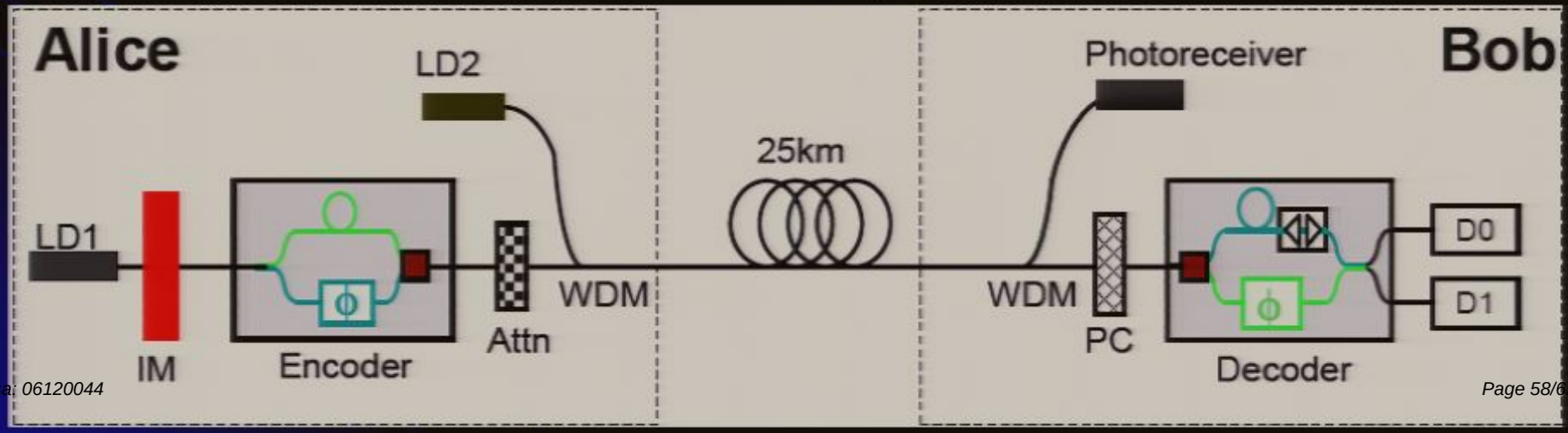


C. –Z. Peng *et. al.*, quant-ph/0607129

(USTC, China)



D. Rosenberg *et. al.*, quant-ph/0607186
(Los Alamos & NIST, US)



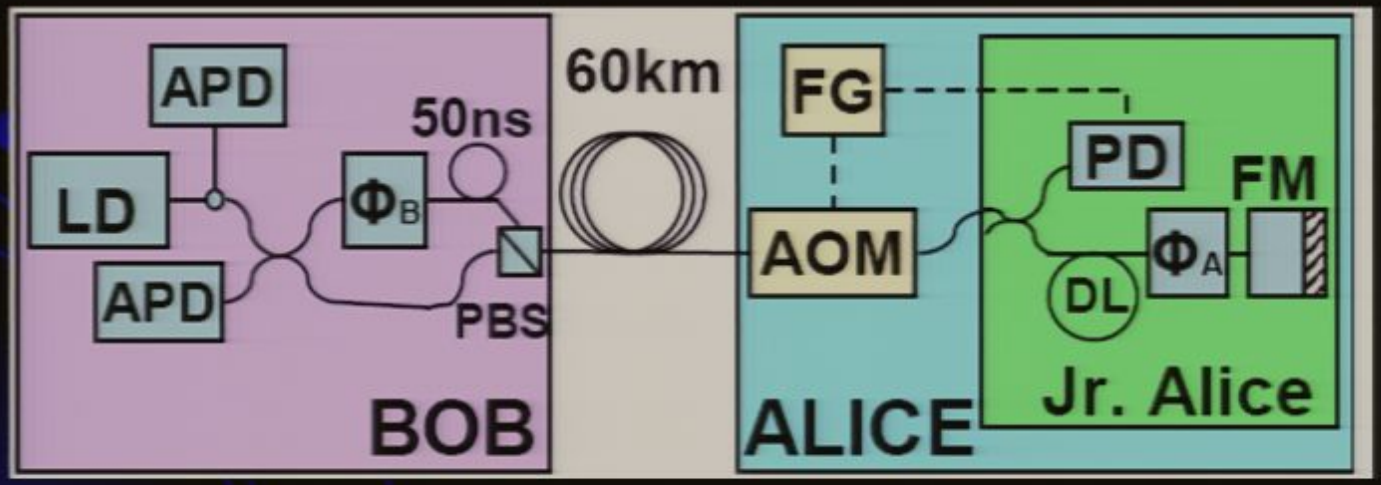
Summary

- The First Experimental Implementation of Decoy State QKD
- Dramatic Performance Improvement with Simple Modification on Commercial QKD System
- Decoy Method: Ready for Real-Life Application!

Thank You ☺

Weak+Vacuum Protocol: Experiment

- More Complicated than One-Decoy Protocol
- But with Simpler Set-up
- Over 60km Fiber
- Secure Key Rate: 8.5e-5 per pulse



Y. Zhao, B. Qi, X. Ma, H. –K. Lo, and L. Qian, in Proceedings of *IEEE ISIT*, 2094-2098 (2006)