Quantum Key Distribution (QKD): Assumptions and Detection Efficiency Loophole

Hoi-Kwong Lo

Center for Quantum Information and Quantum Control (CQIQC)

Department of Electrical & Computer Engineering

and Department of Physics

University of Toronto

KITP, UC Santa Barbara, Oct. 28, 2009

People in my Group

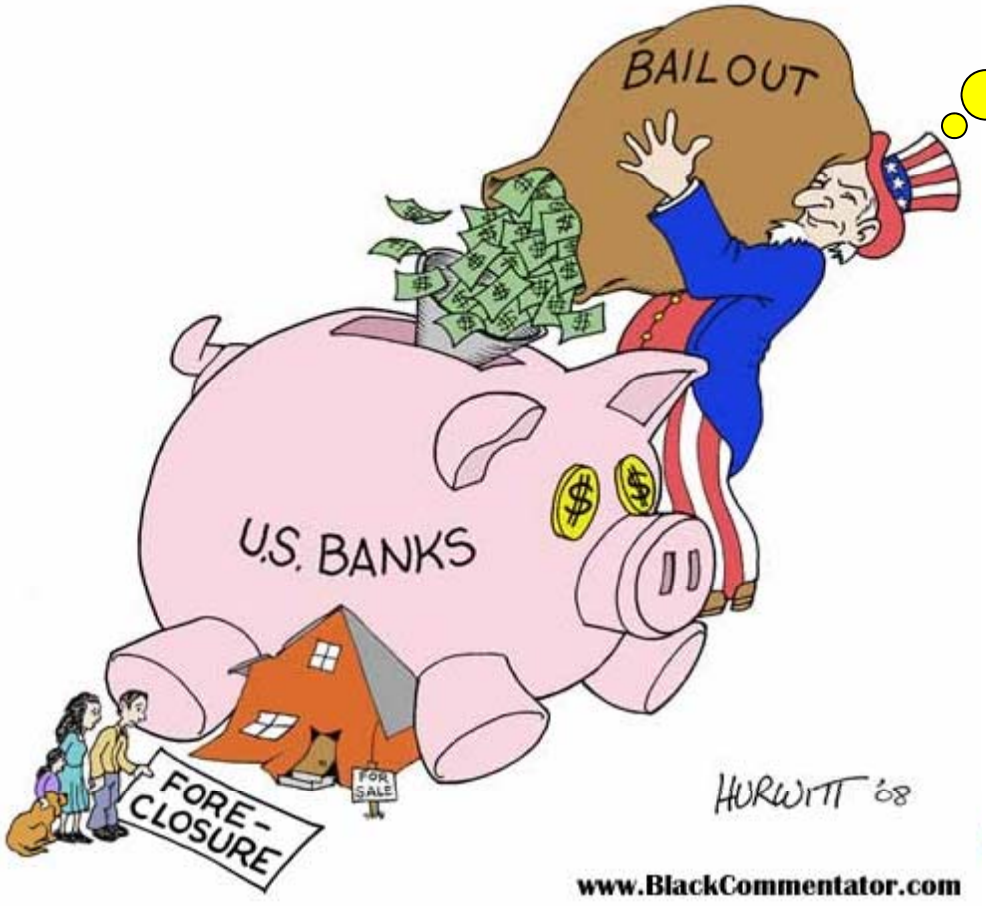
- Principle Investigator
  - Hoi-Kwong Lo
- Senior Research Associate
  - **Bing Qi**
- Grad Students
  - Viacheslav Burenkov
  - Yuemeng Chi
  - Wei Cui
  - Wolfram Helwig
  - Kero Lau
  - Feihu Xu
  - **Yi Zhao**
- Collaborators
  - Prof. Li Qian
  - …
  - …

**I thank Yi Zhao and Bing Qi for preparing most of the slides.

Theory

Experiment

Shall I (really) use QKD?



Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Side channels

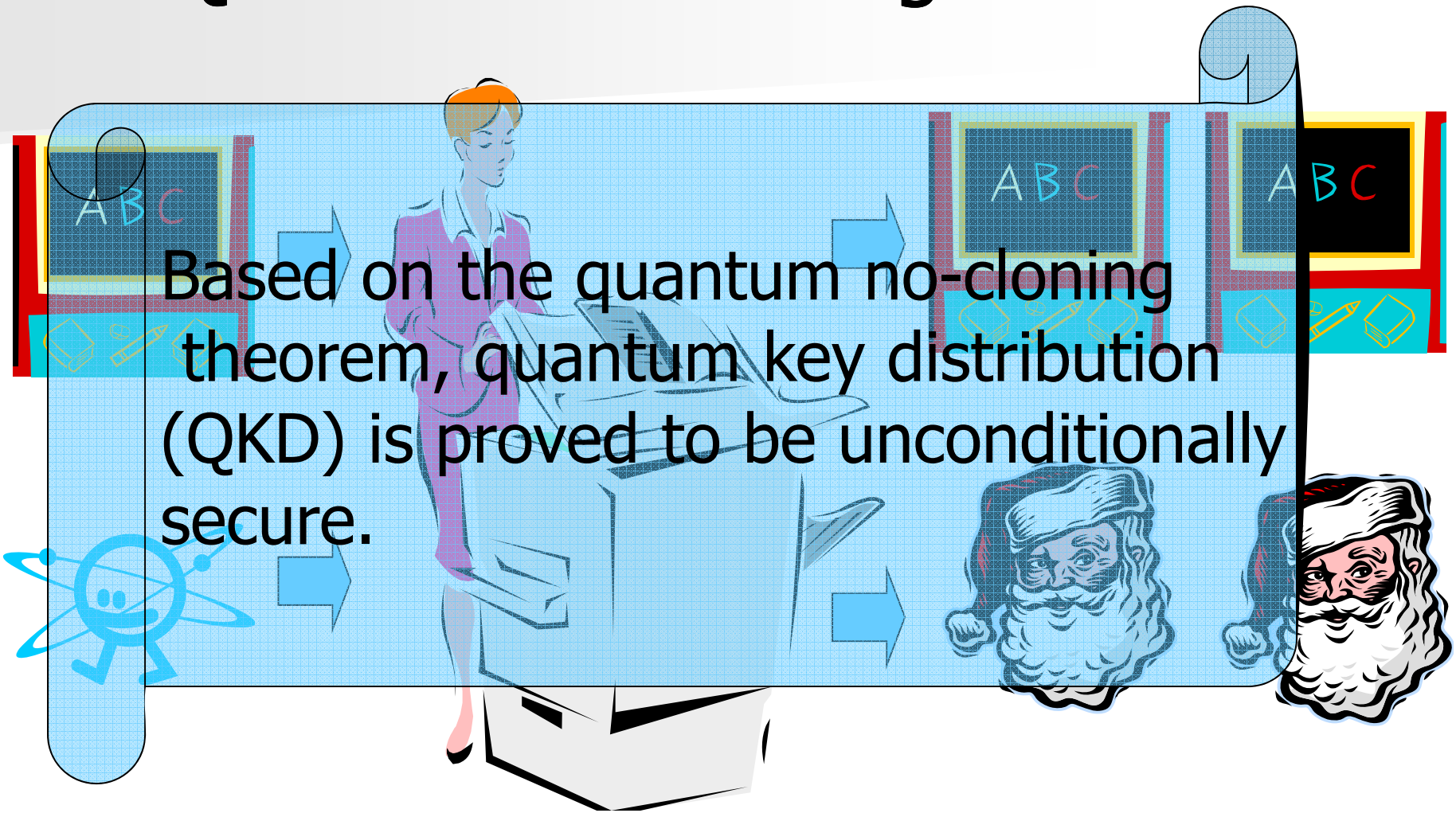
  Detection efficiency loophole
- Future Directions

Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Side channels

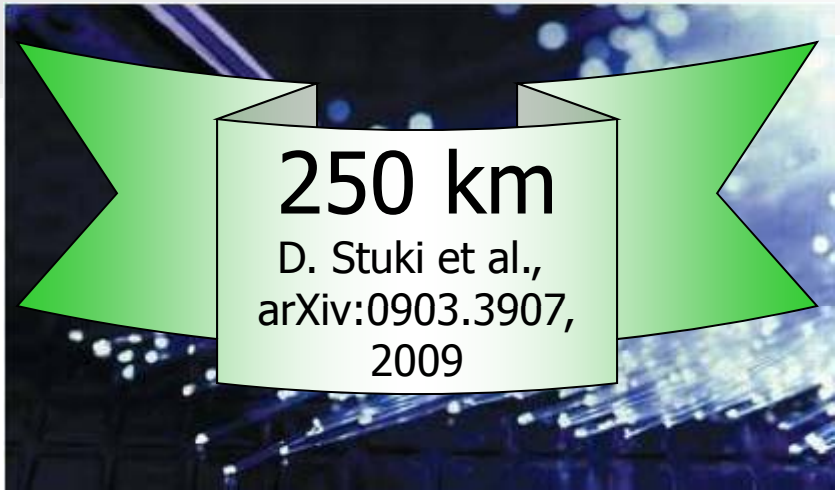
  Detection efficiency loophole
- Future Directions

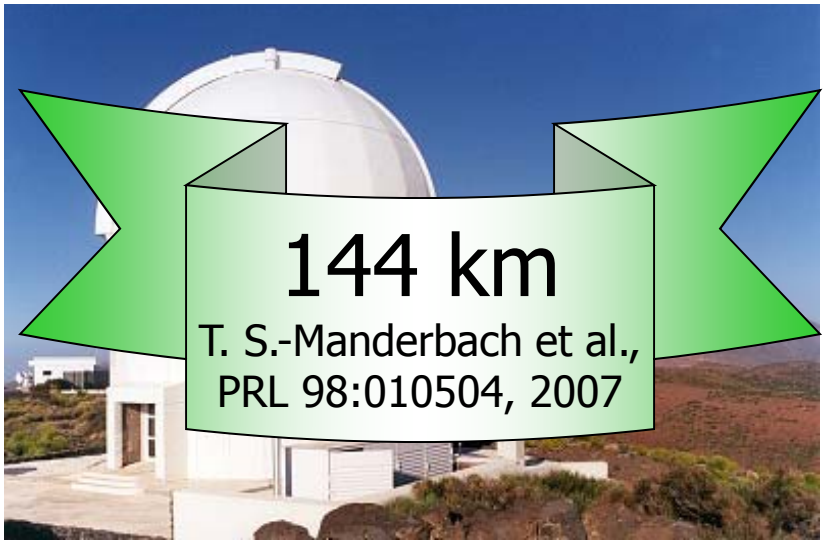
Quantum No-cloning Theorem



Based on the quantum no-cloning theorem, quantum key distribution (QKD) is proved to be unconditionally secure.

Quantum Cryptography: Today and Tomorrow





Commercial Quantum Crypto products available on the market Today!

MAGIQ TECH.

Distance over 100 km of commercial Telecom fibers.

ID QUANTIQUE

SmartQuantum : One Of the best **IPO** on the NYSE-Euronext Marché Libre of 2007

Swiss election uses quantum cryptography

Science & Technology

Quantum cryptography

Heisenberg's certainty principle

Oct 18th 2007

From *The Economist* print edition

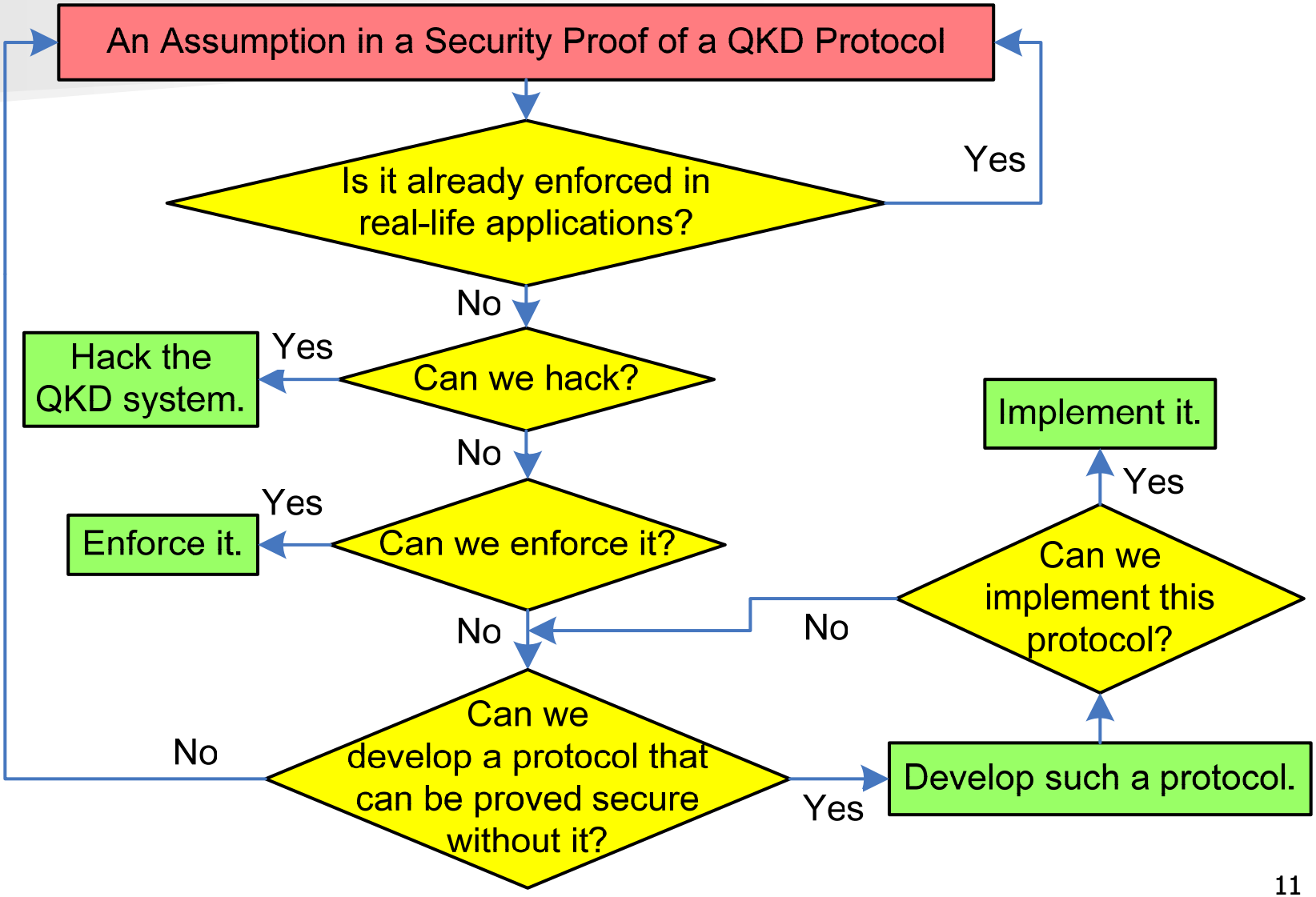
The Swiss are using quantum theory to make their election more secure

HANGING chads. Ballot stuffing. Gerrymandering. Such dirty tricks enfeeble democracy. But the security of the votes cast in Geneva during Switzerland's general election on October 21st is guaranteed. The authorities will use quantum cryptography—a way to transmit information that detects eavesdroppers and errors almost immediately—to ensure not only that votes are kept secret but also that they are all counted.

Assumptions and Security

- Security proof is based on some assumptions.
- Security proof falls apart if the assumptions are violated.
- Do such assumptions apply to real-life applications?

A Flow-chart of Assumptions and Security



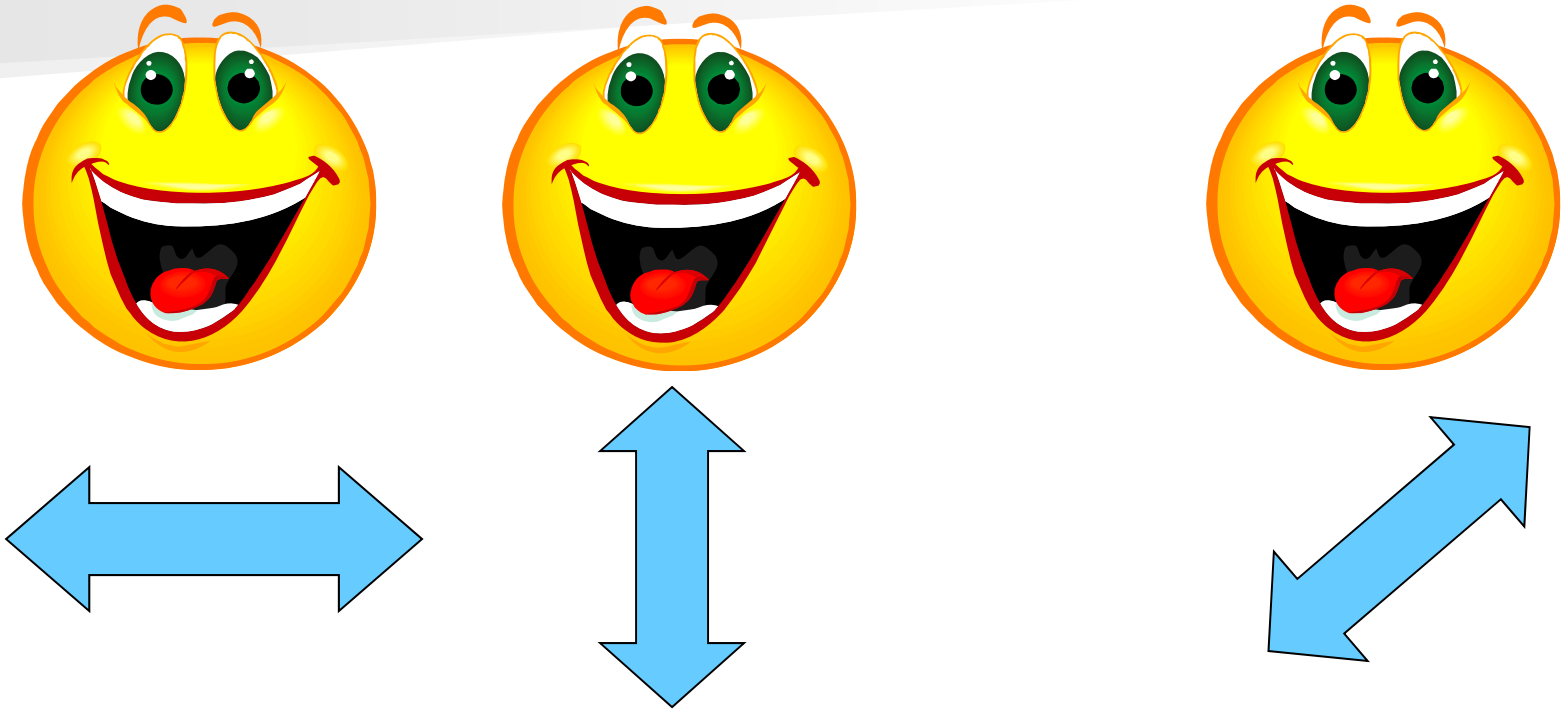
Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Side channels

  Detection efficiency loophole
- Future Directions

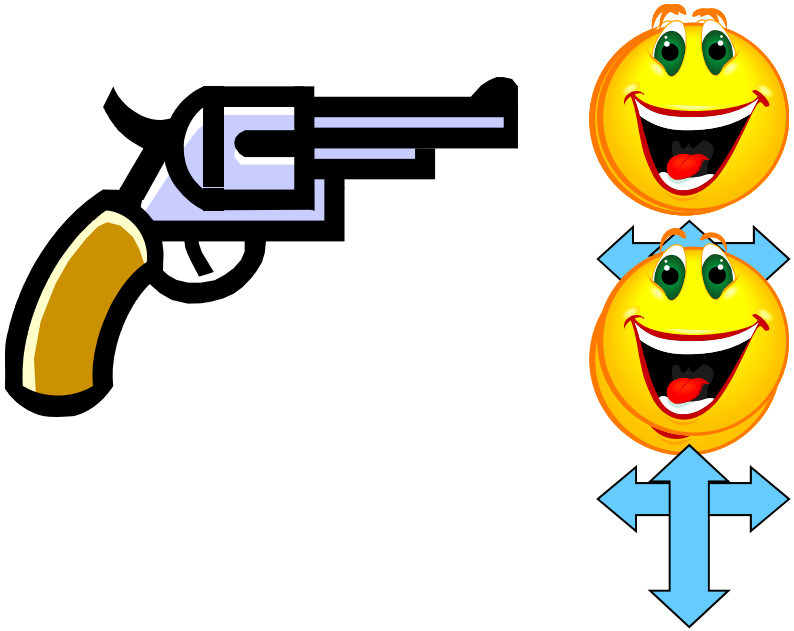
Single Mode in QKD

Qubit in Polarization Coding



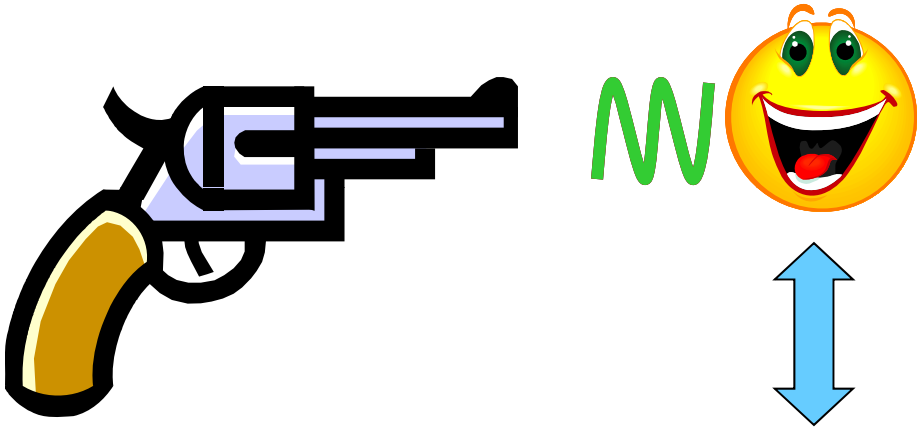
|0> |1> a|0>+b|1>

A Laser can Emit Multi-photon



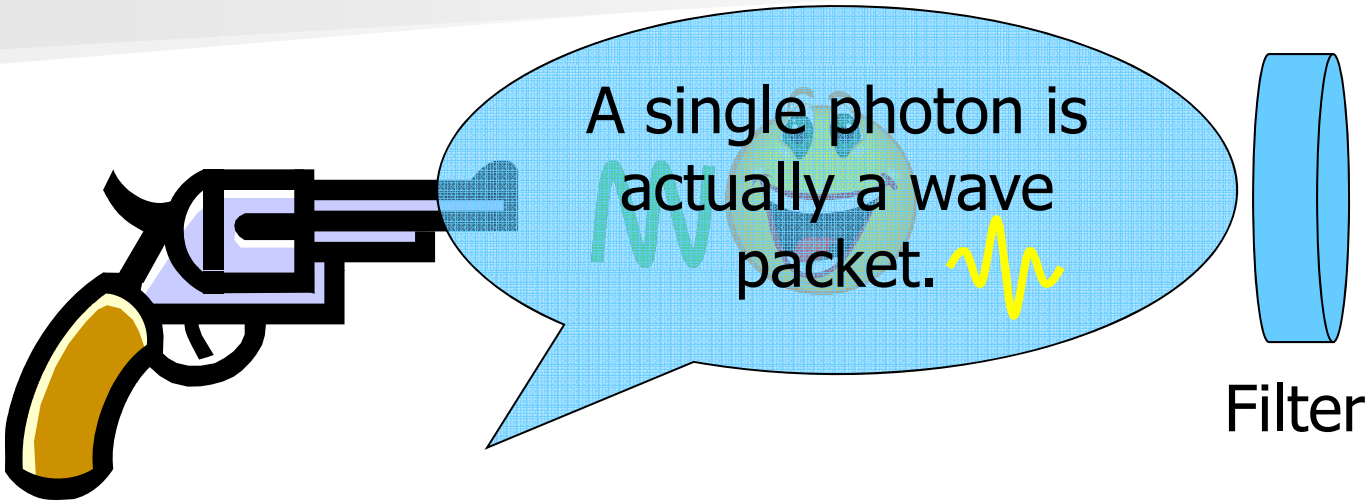
- Two modes: $|n_H, n_V\rangle$. n_H and n_V are natural numbers representing the number of horizontal and vertical photons respectively.

Side Channels



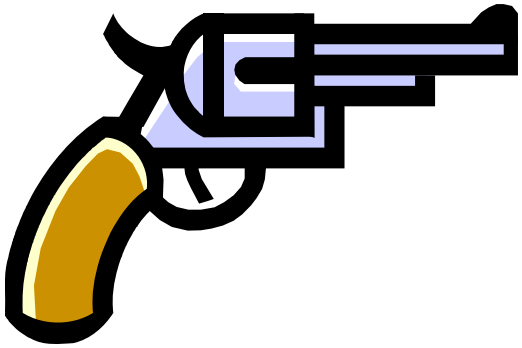
- Now, we will suppress the polarization.
- Single mode assumption may be violated!
- E.g. frequency info. can be a side channel.

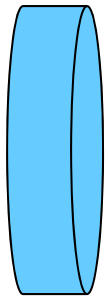
What is a Single Mode?



- A multi-mode has basis vectors $|n_{H1}, n_{H2}, \ldots, n_{V1}, n_{V2}, \ldots\rangle$
- A two-mode has basis vectors $|n_H, n_V\rangle$.
- To reduce a multi-mode to a two-mode, an ideal filter is applied to kill all other modes.

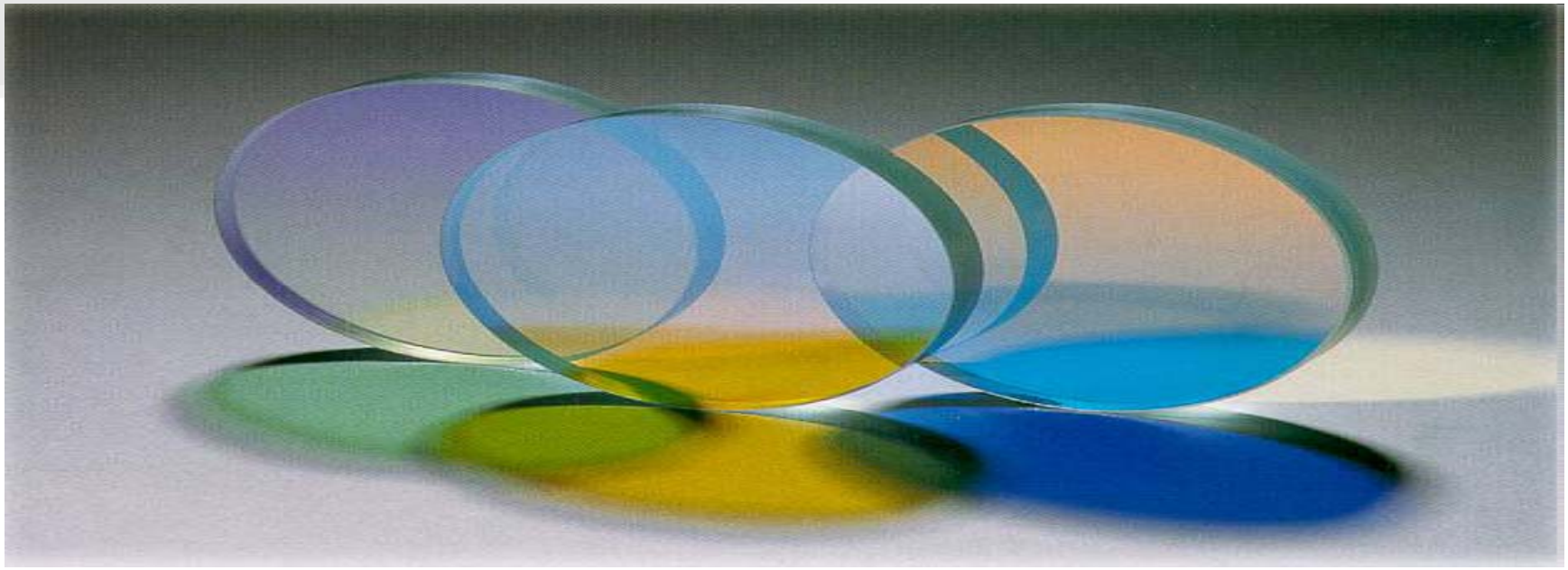
A Problem: How to Construct such a Filter?





Filter

Practical Filters are Imperfect!

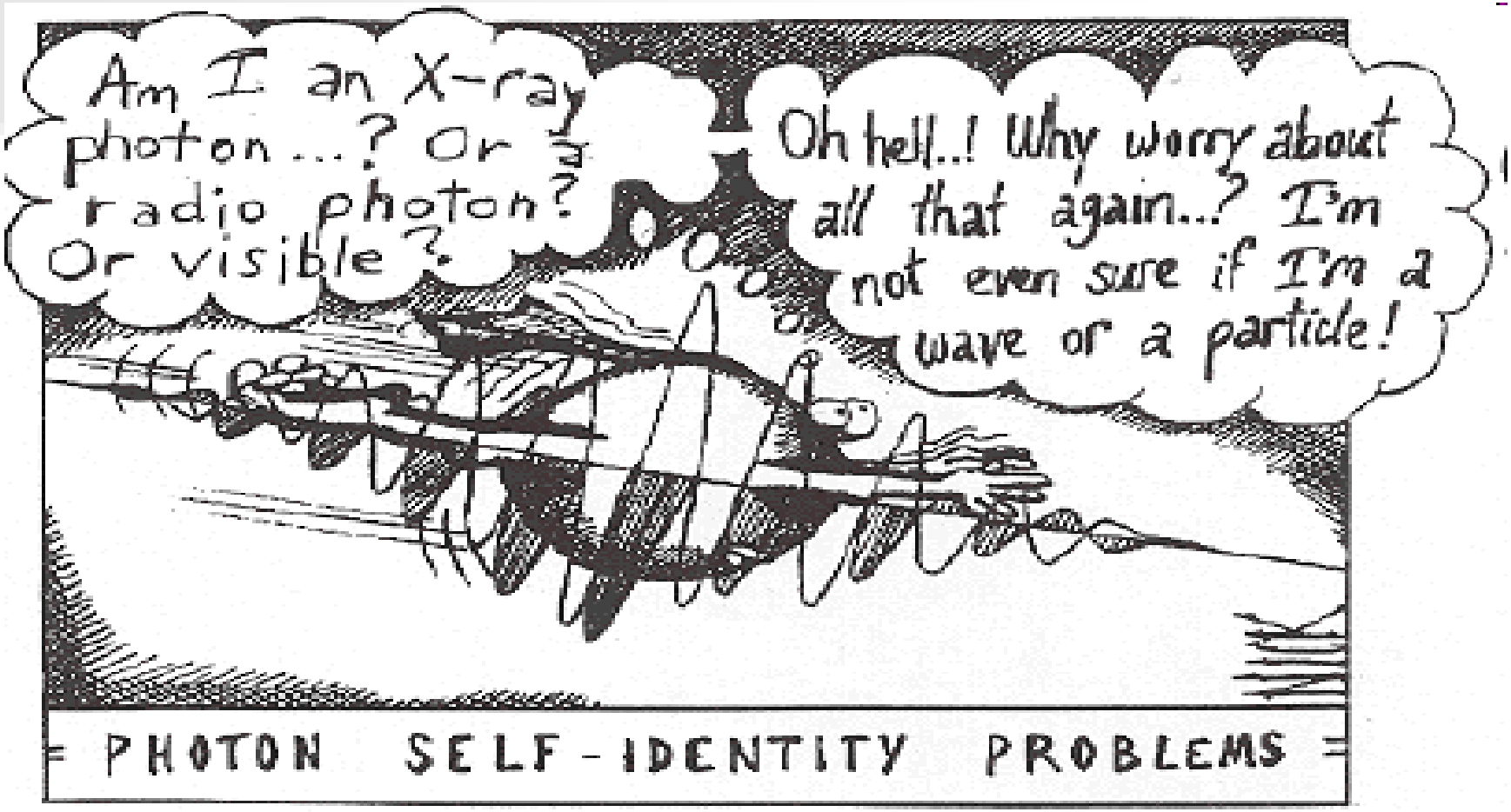


Advanced Image Quality Space-Qualified Ultraviolet Interference Filter
(Courtesy-NASA/JPL/Caltech)

Future Direction: Need to **quantify** imperfections in filters and take care of them in security proofs.

Phase Randomization in QKD

Duality of Photon



- A photon is a particle as well as a wave packet.
- From the "wave" view, it has a phase.

Example: phase randomization

- Standard assumption made in many security proofs
- Until recently, had ever been strictly implemented
- If phase is not randomized, existing security proof gives a lower key rate. [Lo and Preskill, QIC 7, 431 (2007).]
- We demonstrated the first experimental QKD with active phase randomization.

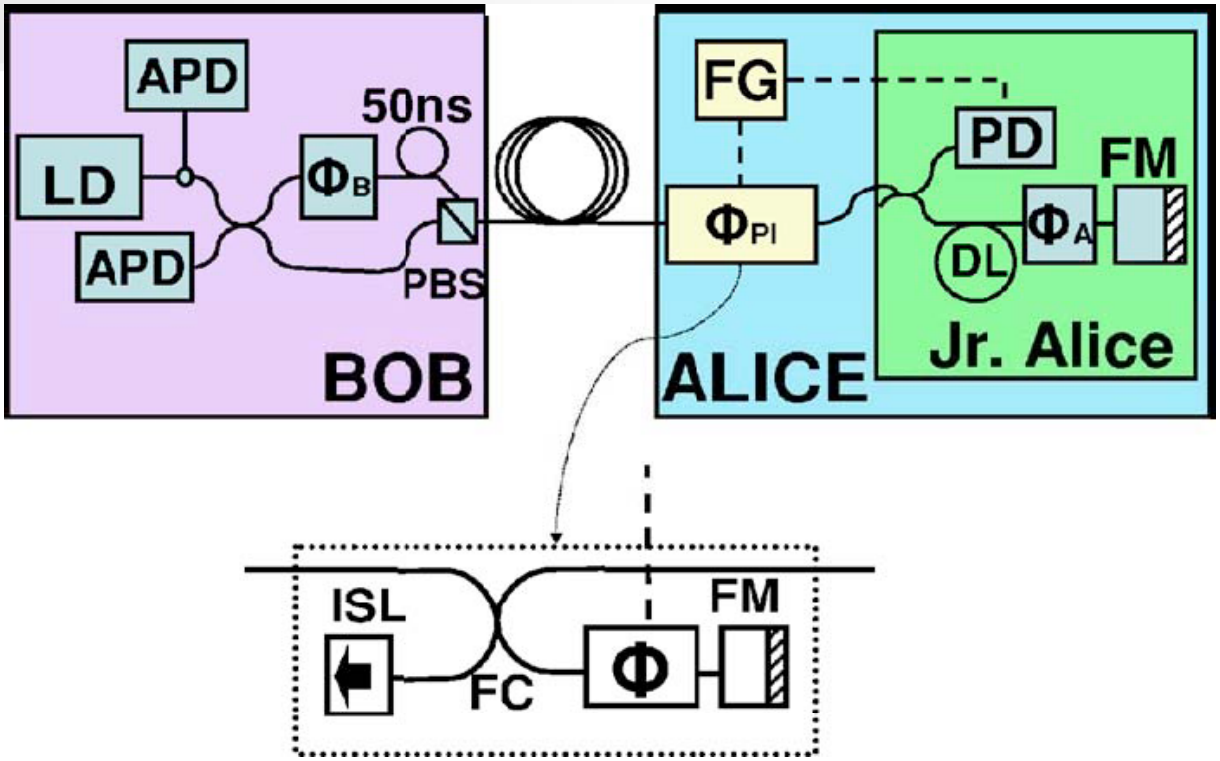
APPLIED PHYSICS LETTERS **90**, 044106 (2007)

Experimental quantum key distribution with active phase randomization

Yi Zhao,[a)] Bing Qi, and Hoi-Kwong Lo
Center for Quantum Information and Quantum Control, Department of Physics, University of Toronto, Toronto, Ontario M5S 1A7, Canada and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada

(Received 6 November 2006; accepted 15 December 2006; published online 22 January 2007)

Active phase randomization



Y. Zhao, B. Qi, and H.-K. Lo, Applied Physics Letters **90** 044106 (2007)

Brief Summary

- Single Mode Assumption

- Phase Randomization Assumption

Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Side channels

  Detection Efficiency Loophole
- Future Directions

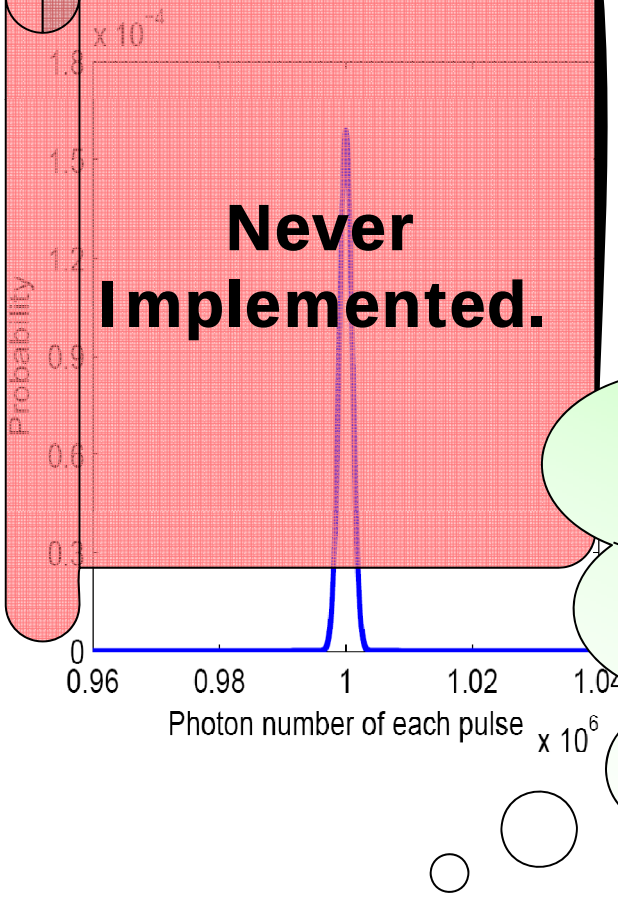
Untrusted Source QKD

Photon number distribution

Ideal laser source:
Photon number per pulse obeys Poisson distribution.

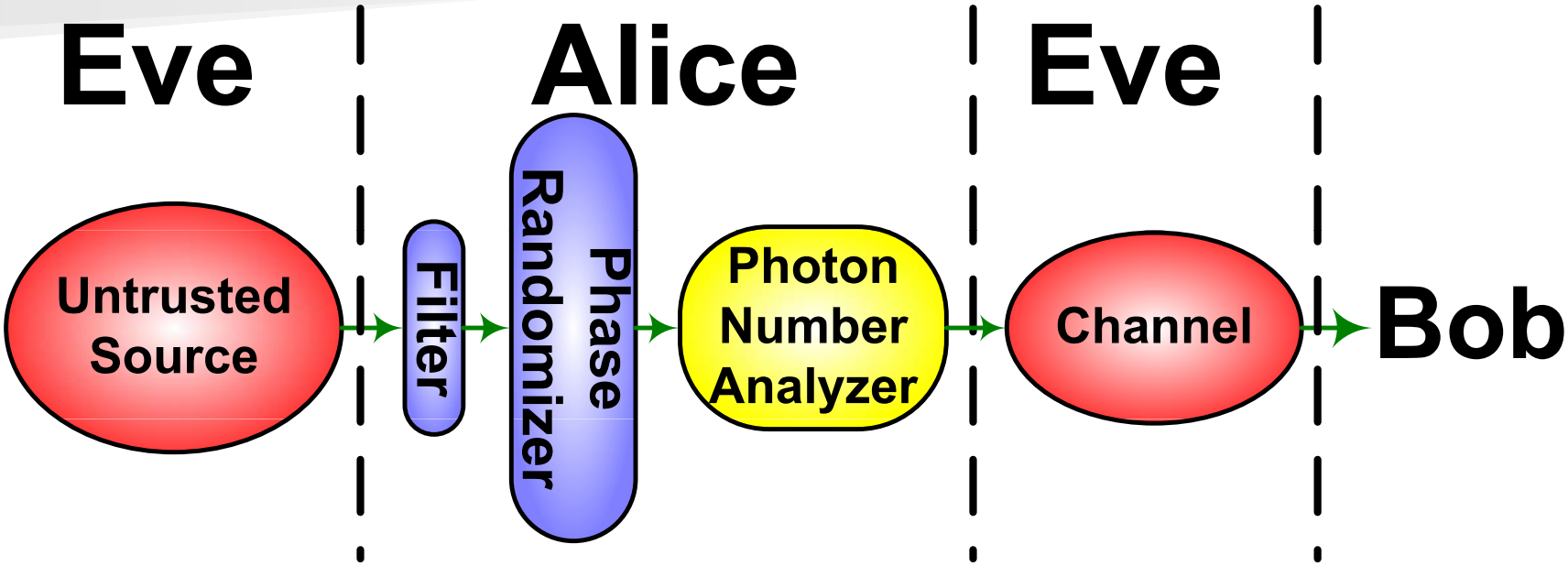
Never Implemented.

Widely Implemented. But, assumption on photon number distribution Violated. No Security Proof.



Can we prove the security of QKD **without** assuming a Poissonian photon number distribution?

Our Approach: A General Model

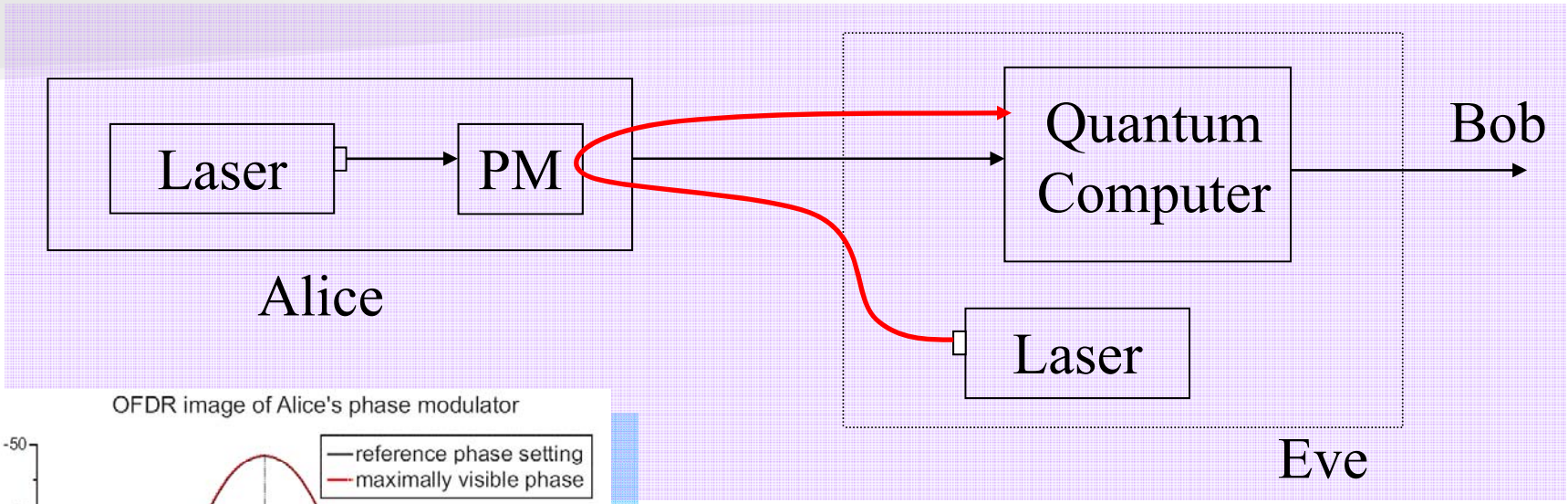


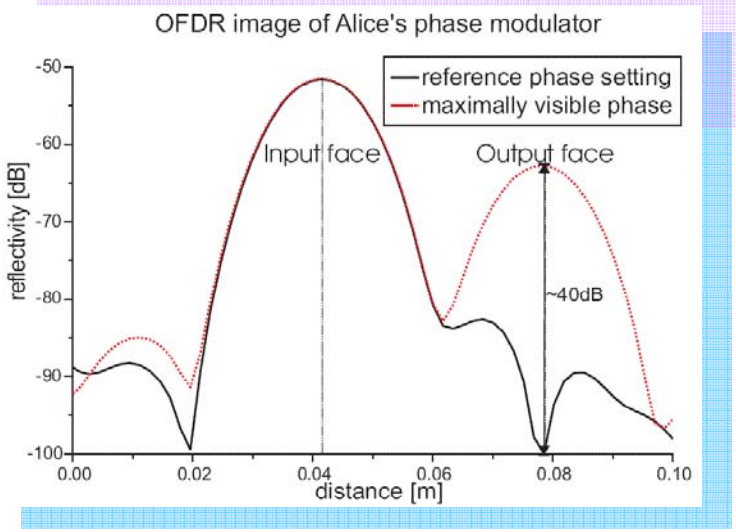
- Photon Number Analyzer: Analyzes input photon number distribution.

Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A, 77, 052327 (2008)
Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, arXiv:0905.4225 (2009).

Trojan Horse Attack

Beyond standard attacks: strong pulse attack as an example





- Eve sends a strong pulse to read off the setting of Alice's PM.

[Gisin, Fasel, Kraus, Zbinden, and Ribordy, PRA 73, 022320 (2006)]

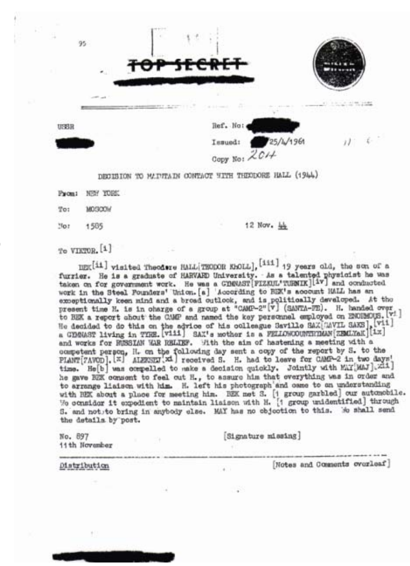
Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Side channels (i.e. Silly bugs)

  Detection efficiency loophole
- Future Directions

VENONA Project: Silly Bugs Can Kill Serious Cryptosystems

- Soviet Union spied in Manhattan project!
- Spies' communications with Moscow were encrypted by one-time pad.
  - One-time pad is theoretically impossible to decrypt (Shannon, 1948).
  - Quantum cryptography is also based on one-time pad.
- Owing to procedural errors, Soviet re-used one-time-pad!
- From 1948 to 1951, numerous Soviet spies were uncovered and prosecuted.
- Today, everyone can view these encrypted cables.



95

~~TOP SECRET~~

[redacted]

USSR

[redacted]

Ref. No: [redacted]

Issued: [redacted]25/4/1961

Copy No: 204

DECISION TO MAINTAIN CONTACT WITH THEODORE HALL (1944)

From: NEW YORK

To: MOSCOW

No: 1585 12 Nov. 44

To VIKTOR.[i]

BEK[ii] visited Theodore HALL[TEODOR KhOLL],[iii] 19 years old, the son of a furrier. He is a graduate of HARVARD University. As a talented physicist he was taken on for government work. He was a GYMNAST[FIZKUL'TURNIK][iv] and conducted work in the Steel Founders' Union.[a] According to BEK's account HALL has an exceptionally keen mind and a broad outlook, and is politically developed. At the present time H. is in charge of a group at "CAMP-2"[v] (SANTA-FE). H. handed over to BEK a report about the CAMP and named the key personnel employed on ENORMOUS.[vi] He decided to do this on the advice of his colleague Saville SAX[SAVIL SAKS],[vii] a GYMNAST living in TYRE.[viii] SAX's mother is a FELLOWCOUNTRYMAN[ZEMLYaK][ix] and works for RUSSIAN WAR RELIEF. With the aim of hastening a meeting with a competent person, H. on the following day sent a copy of the report by S. to the PLANT[ZAVOD].[x] ALEKSEJ[xi] received S. H. had to leave for CAMP-2 in two days' time. He[b] was compelled to make a decision quickly. Jointly with MAY[MAJ][xii] he gave BEK consent to feel out H., to assure him that everything was in order and to arrange liaison with him. H. left his photograph and came to an understanding with BEK about a place for meeting him. BEK met S. [1 group garbled] our automobile. We consider it expedient to maintain liaison with H. [1 group unidentified] through S. and not to bring in anybody else. MAY has no objection to this. We shall send the details by post.

No. 897
11th November

[Signature missing]

Distribution

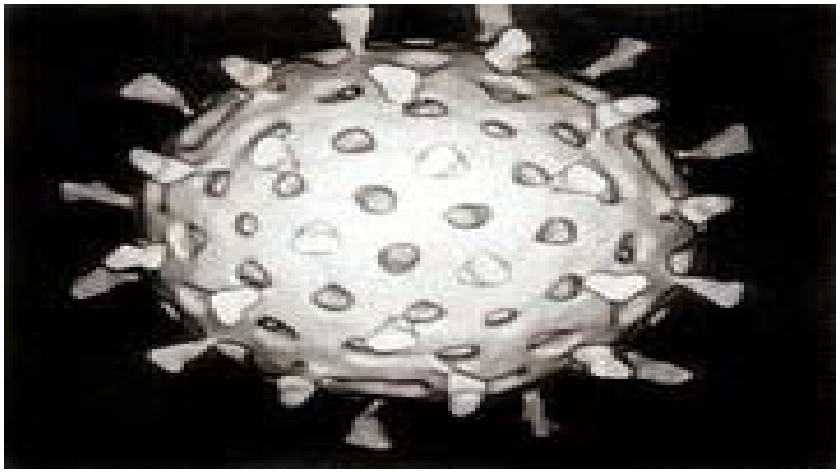
[Notes and Comments overleaf]

[redacted]

Why silly bugs exist in QKD?

A) Unintentional bugs

B) Intentional bugs (Quantum Crypto-virology)



Unintentional Bugs

- QKD systems often use commercial off-the-shelf components (lasers, detectors, time interval analyzers, etc)

- Those components are NOT originally designed for security applications.

- Seemingly innocent short-cuts in design can prove fatal in QKD applications.

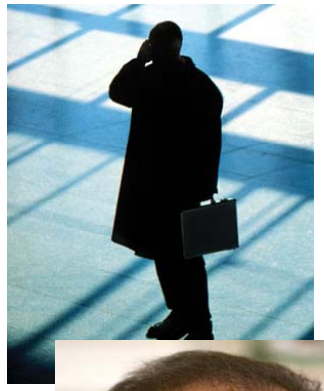
Intentional Bugs
(Quantum Crypto-Virology)

- Malicious QKD designers may hide backdoors in QKD systems.

- In current QKD experiments, most assumptions in security proofs are not verified.

Greek telephone tapping case 2004-05

- Illegal tapping of over 100 mobile phones on Vodafone Greece network during Olympic Game 2004.
- Phones tapped included that of Greek Prime Minister Kostas Karamanlis.
- Foreign and Greek media have raised United States intelligence agencies as the main suspects
- Ericsson switches used by Vodafone Greece were compromised and unauthorized software was installed.
- Exploited lack of monitering in usage of "lawful interception" module.
- Network Planning Manager for Vodafone - Greece, Kostas Tsalikidis, was found dead in an apparent suicide.



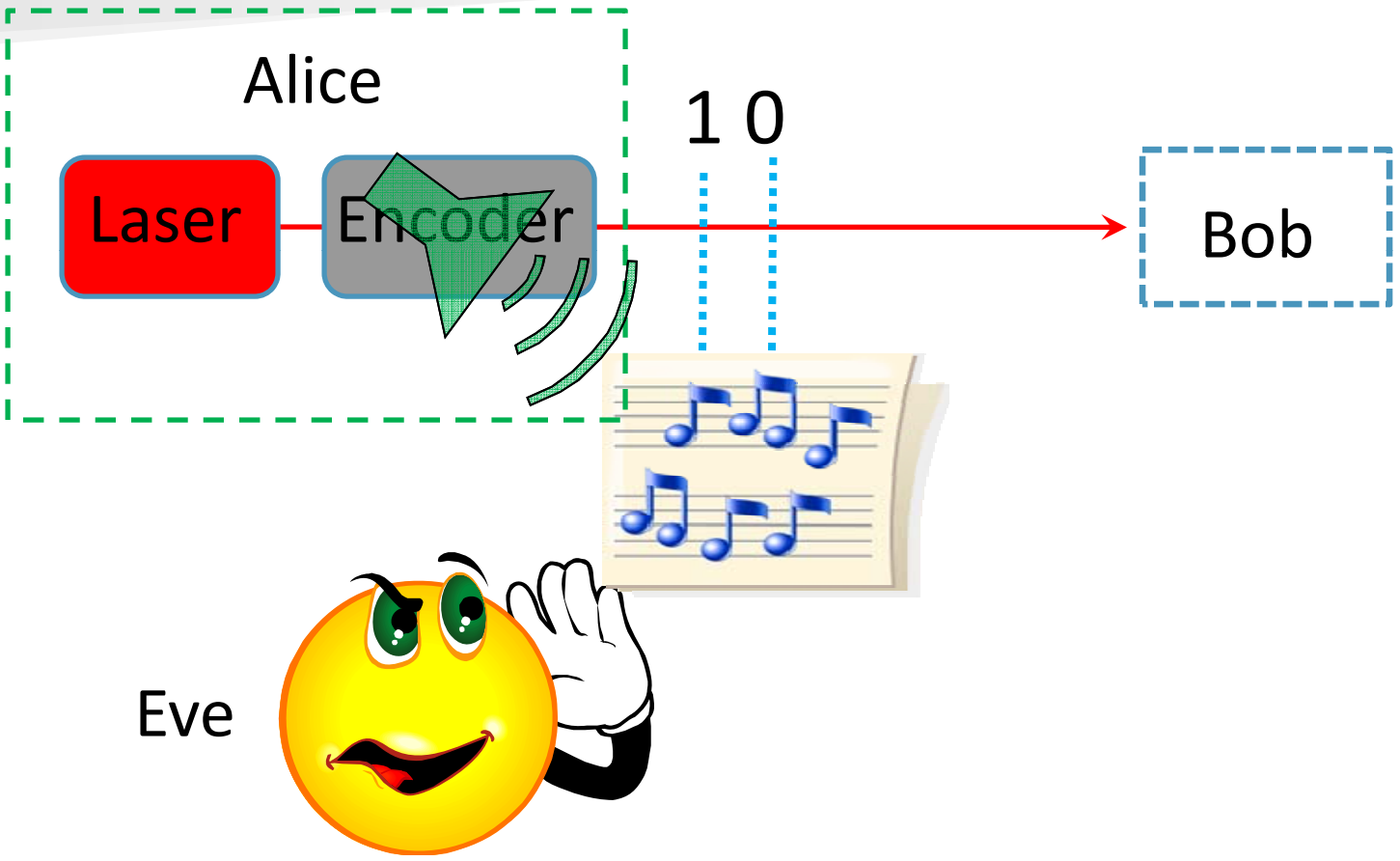
Lesson from history

"... unconditionally secure against any eavesdropper who happened to be **deaf**!"

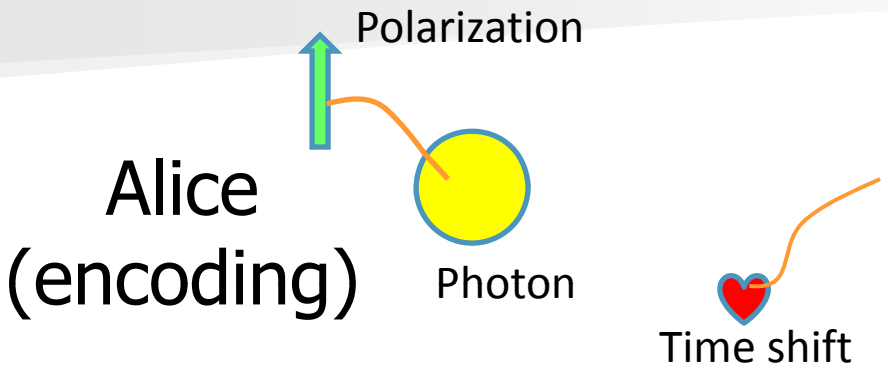
Gilles Brassard

describing the first QKD experiment

Passive side-channel attack



Our Focus: **Active** side-channel attack



Bob
(measurement)

Eve
(encoding)

- Eve encodes random bit on other quantum variables
- Originally, no correlation between Alice's and Eve's bits
- Bob's measurement could build the correlation.

B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 73 (2007).

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

Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Side channels (i.e. Silly bugs)

  Detection efficiency loophole
- Future Directions

Connection of QKD with foundations of QM

- Proposals for self-testing of QKD systems (Mayers and Yao), e.g. based on violation of Bell inequalities (Ekert91 protocol).

- QKD protocol built from data violating the CHSH Bell inequality

  $-2 \leq S \leq 2$ where

  $S = E(a, b) - E(a, b') + E(a', b) + E(a' b')$.

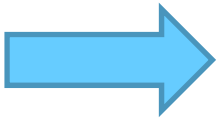
  where a and a' are detector settings on side A, b and b' on side B and $E(a, b)$ etc. are the expectation value of the products of the outcome.

Loopholes in Bell test experiments

1. Locality loophole (not that relevant to QKD).

2. Detection efficiency loophole

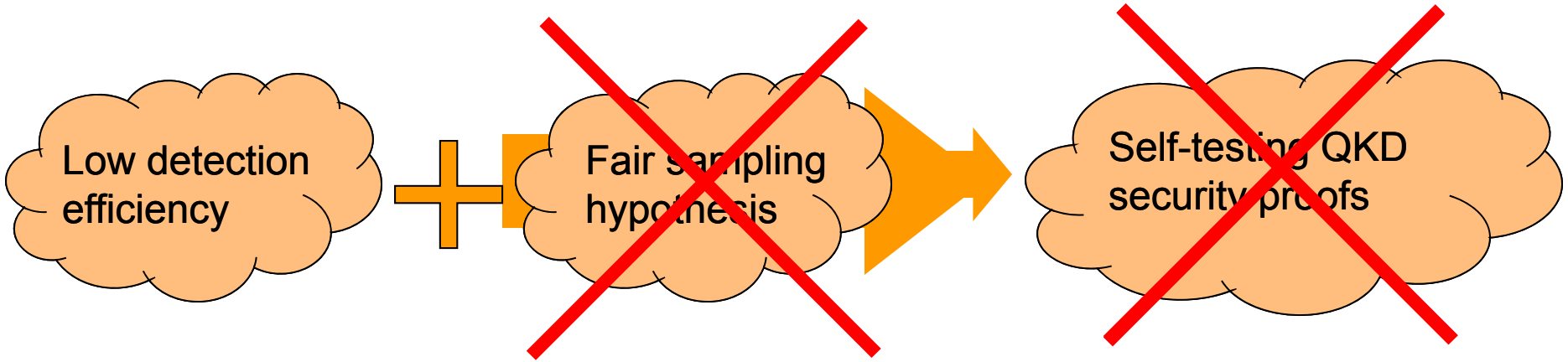
3. Freedom-of-choice loophole



need **true** random numbers in QKD

Detection efficiency loophole

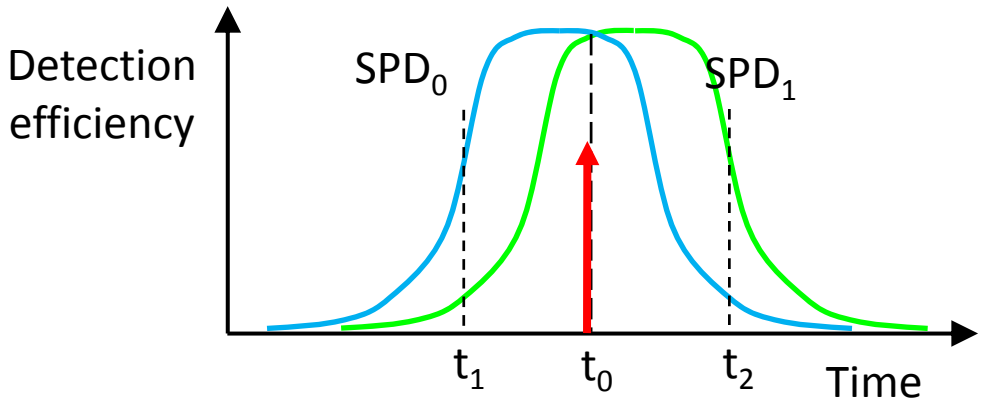
- Self-testing idea may not work when detection efficiency is low!
- Local hidden variables model can be constructed when detection efficiency < 82.8% for maximally entangled states.
- In telecom wavelengths, detection efficiency ~10%.



- The fair sampling hypothesis may come to rescue.
- **However, I will show that the fair sampling hypothesis is NOT reasonable for untrusted devices!**

Detector Efficiency Loophole in QKD

- Most QKD systems have two or more detectors.
- Efficiency *mismatch* could exist in the time, spatial, or spectral domains, etc.

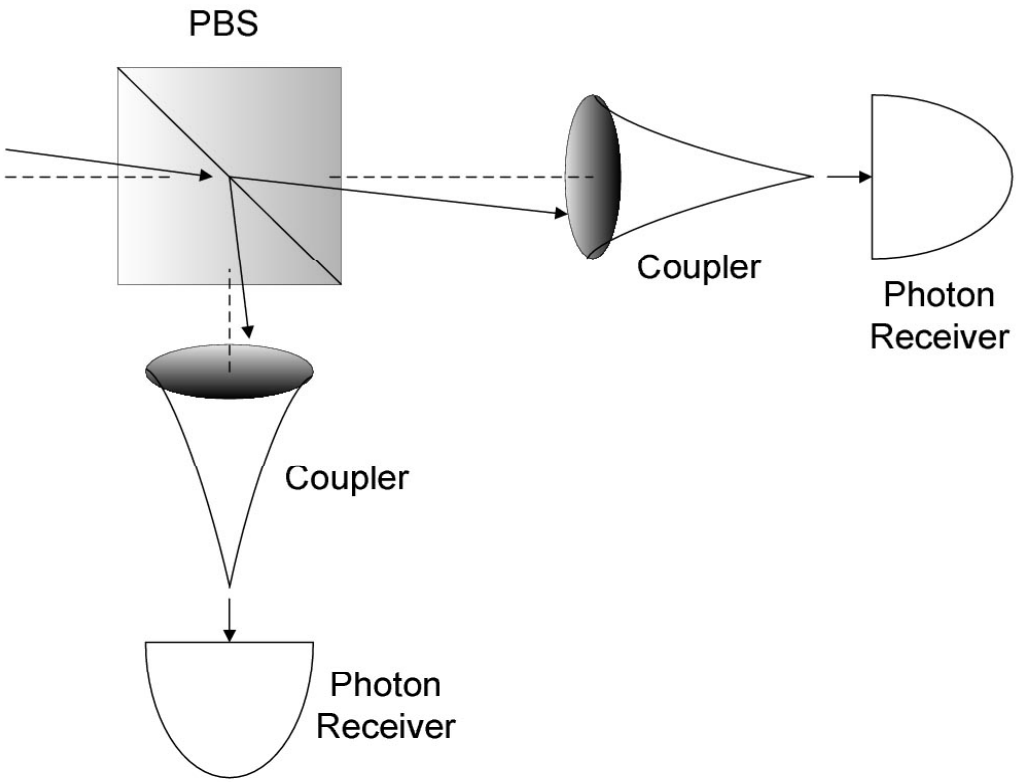


V. Makarov, A. Anisimov, and J. Skaar, Phys. Rev. A 74, 022313 (2006).
B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 73 (2007).

Attacks Targeting Detector Efficiency Mismatch

- Temporal attack
  - Time-shift the signal (in gated single photon detector (SPD). We will discuss more here).
- Spectral attack
  - Frequency-shift the signal (in up-conversion SPD)
- Spatial attack
  - Change the spatial mode (in free space QKD).

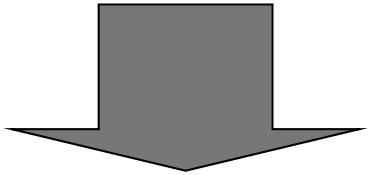
Spatial Attack



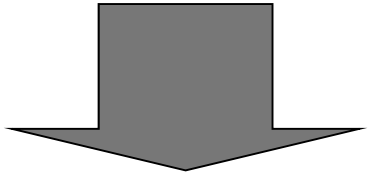
Change in incident angle $\Rightarrow$ different coupling losses

Perspectives of Quantum Hacking

Hard to build two identical detectors in practice



Hard to remove detector efficiency mismatch



Security Loopholes

Eve strikes back!

Eve lost the battle in security proofs,
but came back via loopholes.

Stealing an idea from Claude Crepeau's slides in a CIAR meeting

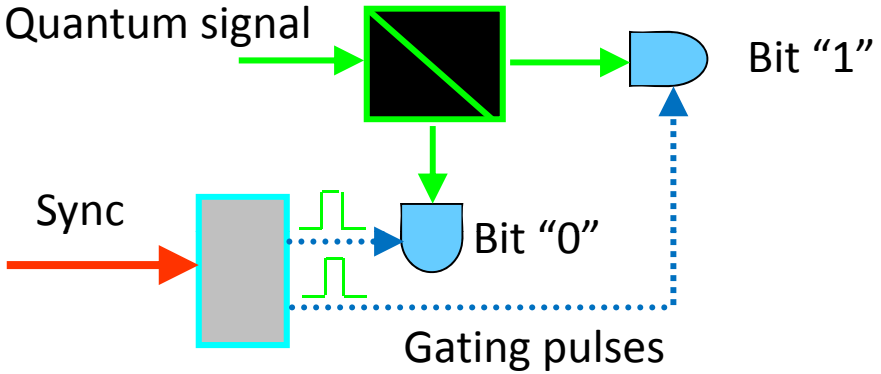
Quantum hacking: How to cheat in a Swiss election?

First experimental demonstration of a feasible attack against a commercial QKD system.

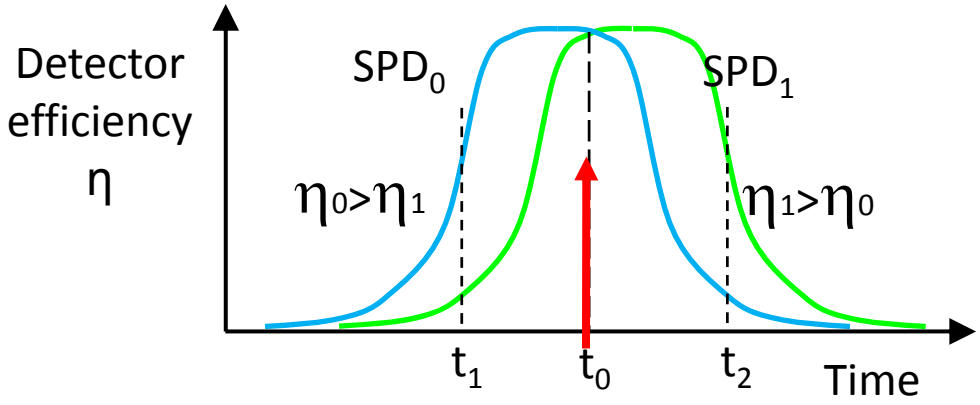
1. B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. (QIC) 7, 73 (2007)
2. Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, Phys. Rev. A 78, 042333 (2008)
3. C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, QIC 9,131(2009).

Time-shift attack: Basic idea

1. Single photon detector in **gated** mode



2. Detection Efficiency mismatch



B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 73 (2007).

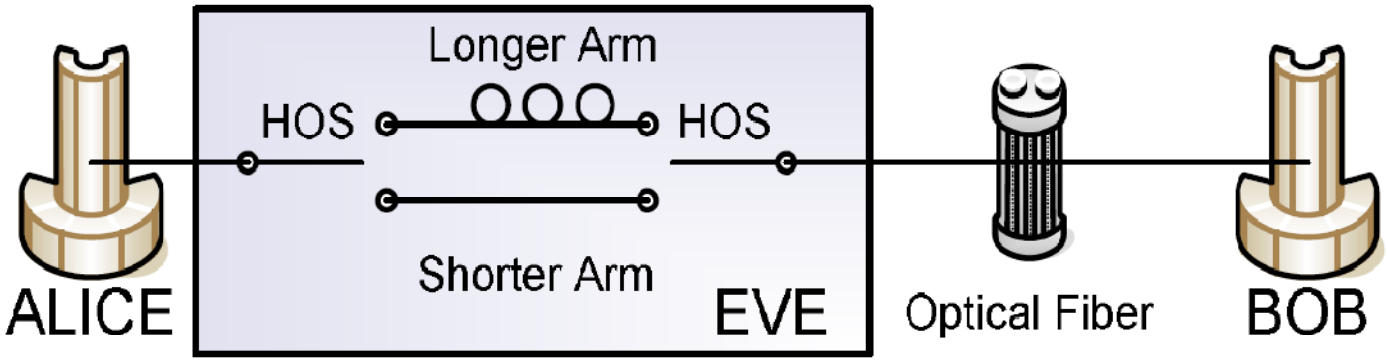
Time-shift attack: strategy

Eve randomly time-shifts signal

→ $\eta_0 > \eta_1$ or $\eta_1 > \eta_0$

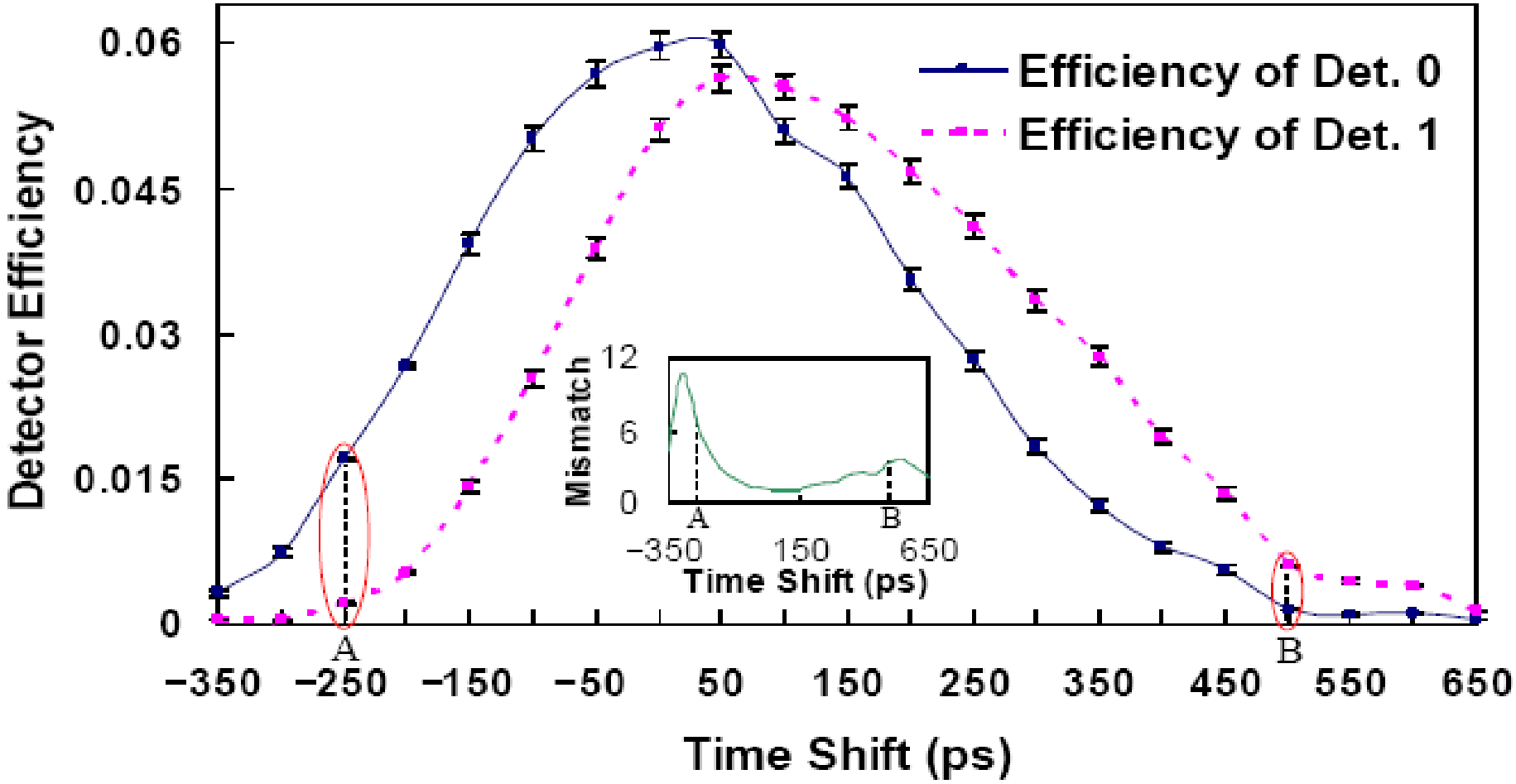
→ With a high probability, Eve knows which detector clicks

→ Eve acquires partial information of the key



B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 73 (2007).

Experimental results



Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, PRA 78:042333 (2008).

Time-shift attack works

Lower bound		Upper bound
(ignoring the attack 1297 bits)	>	(considering the attack 1131 bits)

- Final key shared between Alice and Bob is compromised by Eve!
- Information leaked to Eve without Alice and Bob noticing.

The first experimental demonstration of a technologically feasible attack against a commercial QKD system.

Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, PRA 78:042333 (2008).

Faked States Attack

- Measure-and-resend Scheme (therefore, challenging to implement).
- Eve first measures the input signal in some basis.
- Eve resends the signals with wrong bit values, wrong basis, and wrong arrival times.
  - V. Makarov, A. Anisimov, J. Skaar, PRA, 74:022313 (2006).
  - V. Makarov, J. Skaar, QIC, 8:622 (2008).

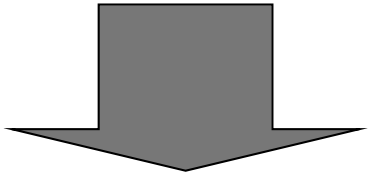
Other Attacks

- Active attack: Controlling Bob's detectors.
  - Eve can manipulate Bob's detectors by sending intense laser pulse into Bob.
  - Eve may even **permanently** change some components' properties of e.g. **commercial** PerkinElmer SPCM-AQR
    - V. Makarov, NJP, 11:065003 (2008).
    - V. Makarov, A. Anisimov, S. Sauge, arXiv:0809.3408, 2008.
- Passive Attack: Monitoring the Communication about Detection Time.
  - But, the detection time may not be broadcasted by Alice and Bob…
  - A. Lamas-Linares and C. Kurtsiefer, Opt. Express 15:9388, 2007.

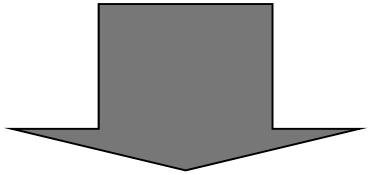
Counter Measures

Perspectives of Quantum Hacking

Hard to build two identical detectors in practice



Hard to remove detector efficiency mismatch

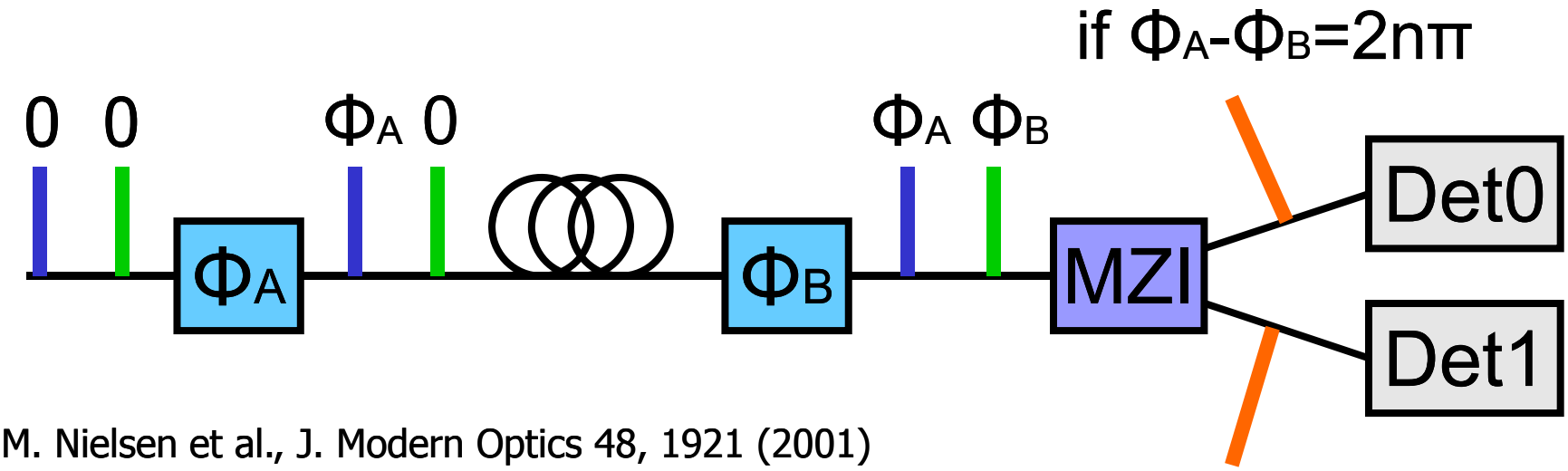


Security Loopholes

Solution: Randomization of Detectors

Counter Measure: Four-state Modulation at Bob's Side

- Bob's phase modulator could also use four settings.
  - $\Phi_A \in \{0, \pi/2, \pi, 3\pi/2\}$, $\Phi_B \in \{0, \pi/2, \pi, 3\pi/2\}$.
- Each detector is randomly assigned with a bit value.



P. M. Nielsen et al., J. Modern Optics 48, 1921 (2001)
M. J. LaGasse, US patent application 20050190922 (2005)
C.-H. F. Fung et al., QIC 9:131 (2009).

Other Counter Measures

- Check timing of incoming pulses.
- Randomly shifting gating window of SPD to smooth out the efficiency.
- Security proof for detectors with different efficiencies — more privacy amplification*.

*C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, QIC 9:131 (2009).

Outline

- Introduction
- Assumptions and Security
  - Assumptions: single mode, phase randomization, …
  - Security: untrusted source, Trojan horse, …
- Detection Efficiency Mismatch
- Future Directions

Fundamental research (e.g. based on the testing of the Bell's inequalities) that does not have practical applications.

V. Scarani, C. Kurtsiefer, arXiv:0906.4547, 2009.

Future Direction

Security proofs with **testable** assumptions!

Practical research that can only provide some "reasonable" security.

Future Direction I

- Security proofs with testable assumptions:
  - Assumptions in security proofs should be explicitly stated and experimentally verified.
  - Until experimental verification has been done, one can never be sure about security of real QKD systems.

Future direction II

- Battle-testing:

  Imperative to study eavesdropping attacks and counter measures more carefully and extensively.
  - This involves both theory and experiment.
  - Needs collaboration between theorists and experimentalists.

Comparison of QKD *vs.* Boxing

Boxing

Player A Tyson

Player B Holyfield

General rules

1.Fair game
2.Safe (hopefully)
3.……

Detailed rules

1.Eye punching Yes
2.Ear biting No
3.……

Make sure rules are followed

referee

QKD

Team A Alice/Bob

Team B Eve

General assumptions

1.Single quantum state
2.No side channel
3.……

Testable assumptions

1.Average photon number
2.Efficiency of SPD
……

Make sure assumptions are valid

calibrating systems

Our goal

Acknowledgements

Canada Research Chairs

Ontario Innovation Trust

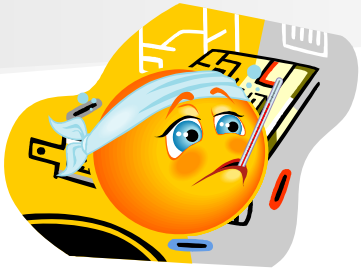
cifar Canadian Institute for Advanced Research

Thank you!

67

Trojan Horse: Eve's Probing Signal

Encoder



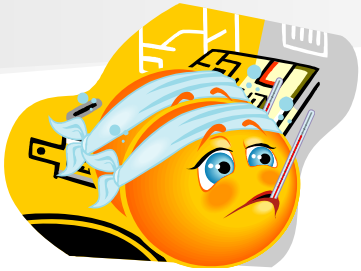
Bob

Alice

- Alice encodes her information with an encoder.
- Then Alice sends the encoded signal to Bob.

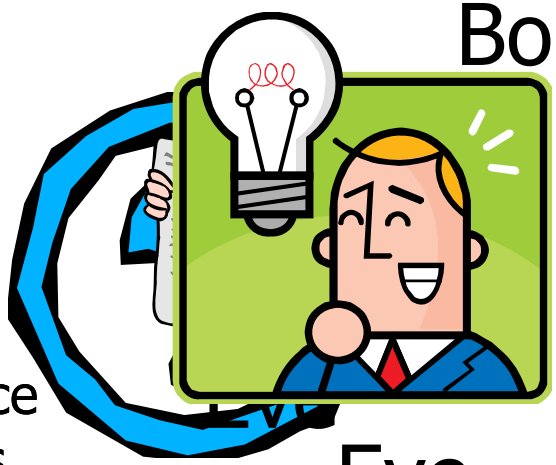
Trojan Horse: Eve's Probing Signal

Encoder



Bob

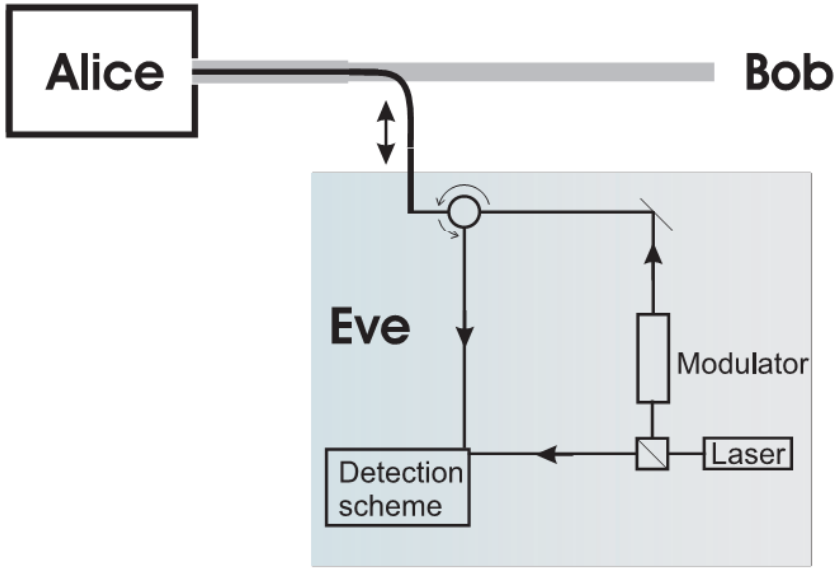
Alice



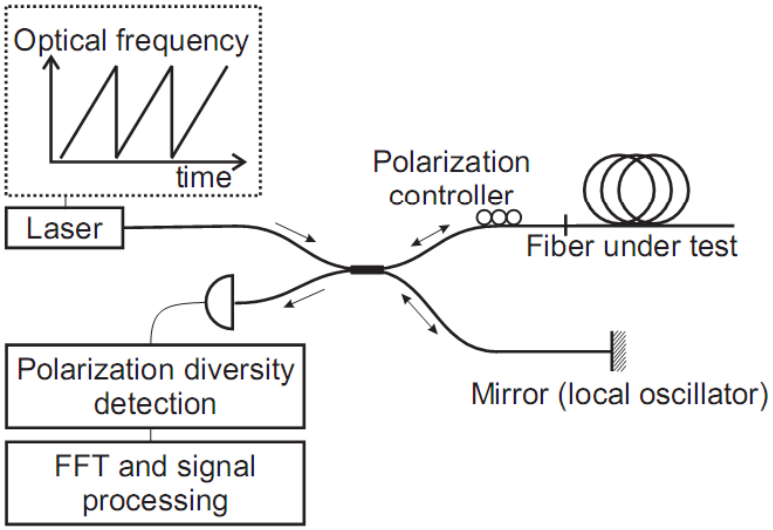
Eve

- Eve can send in some strong signals to Alice
- Eve can then collect some reflected signals and extract Alice's encoder information.
- This attack has been experimentally demonstrated.

Experimental Demonstration of Trojan Horse Attack



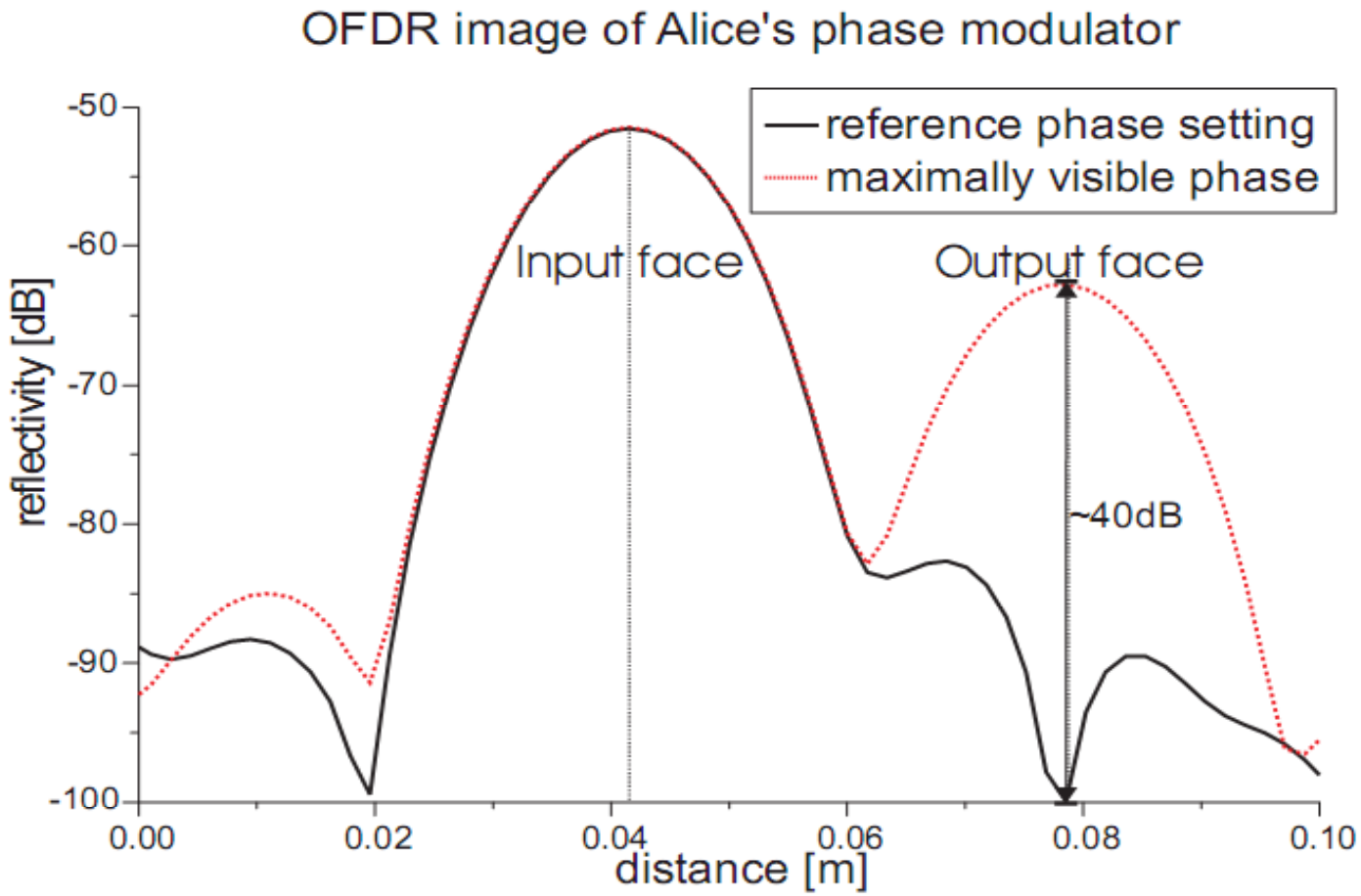
Basic Schematic



Optimal Scheme: Optical Frequency Domain Reflectometry (OFDR)

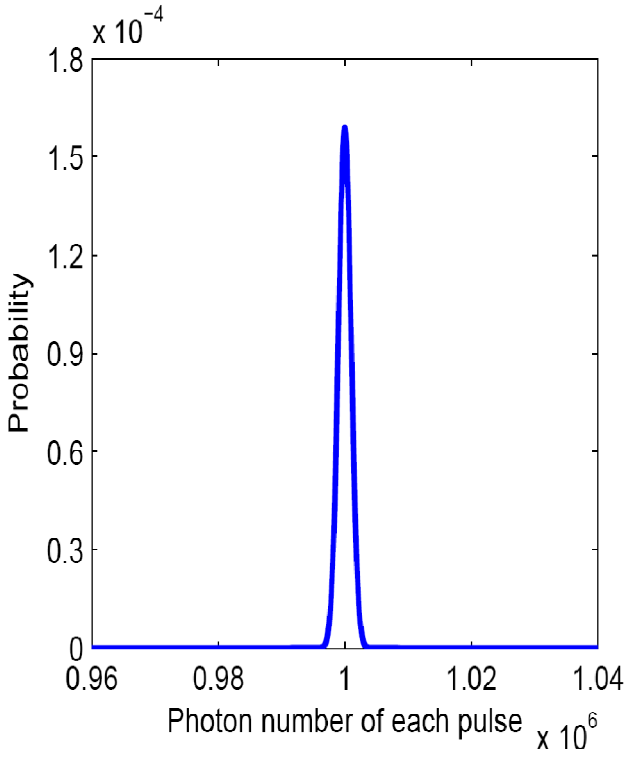
N. Gisin et al., Phys. Rev. A **73**, 022320 (2006)

Experimental Results

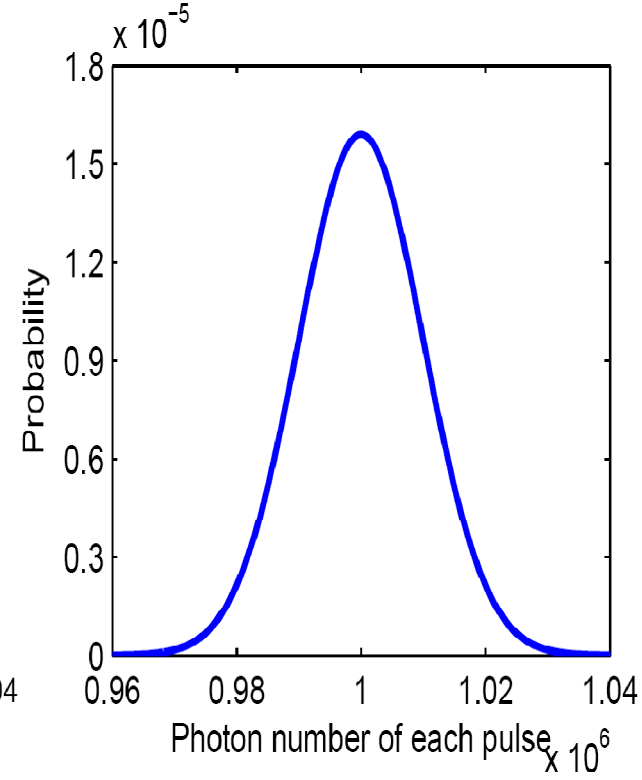


Photon number distribution

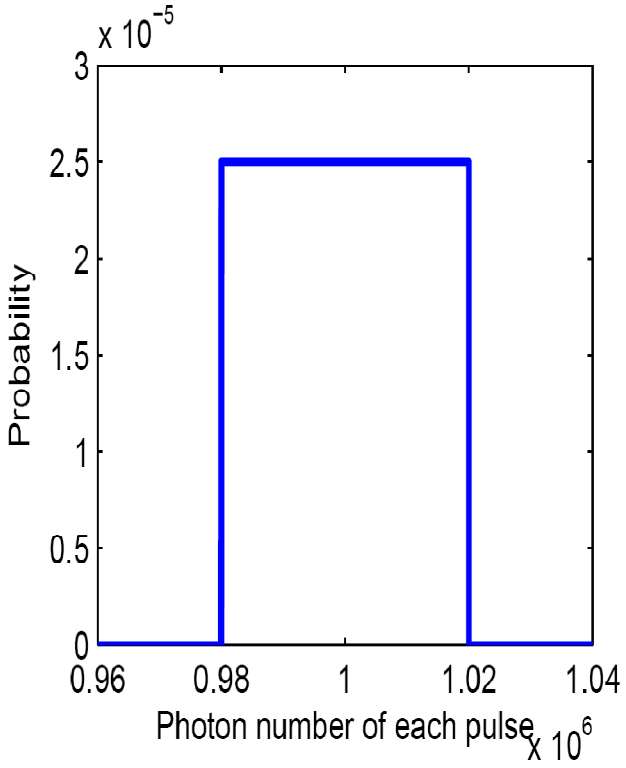
Ideal laser source: Photon number per pulse obeys Poisson distribution.



Imperfect laser source: Photon number distribution is unknown. E.g. Pulsed laser diode.

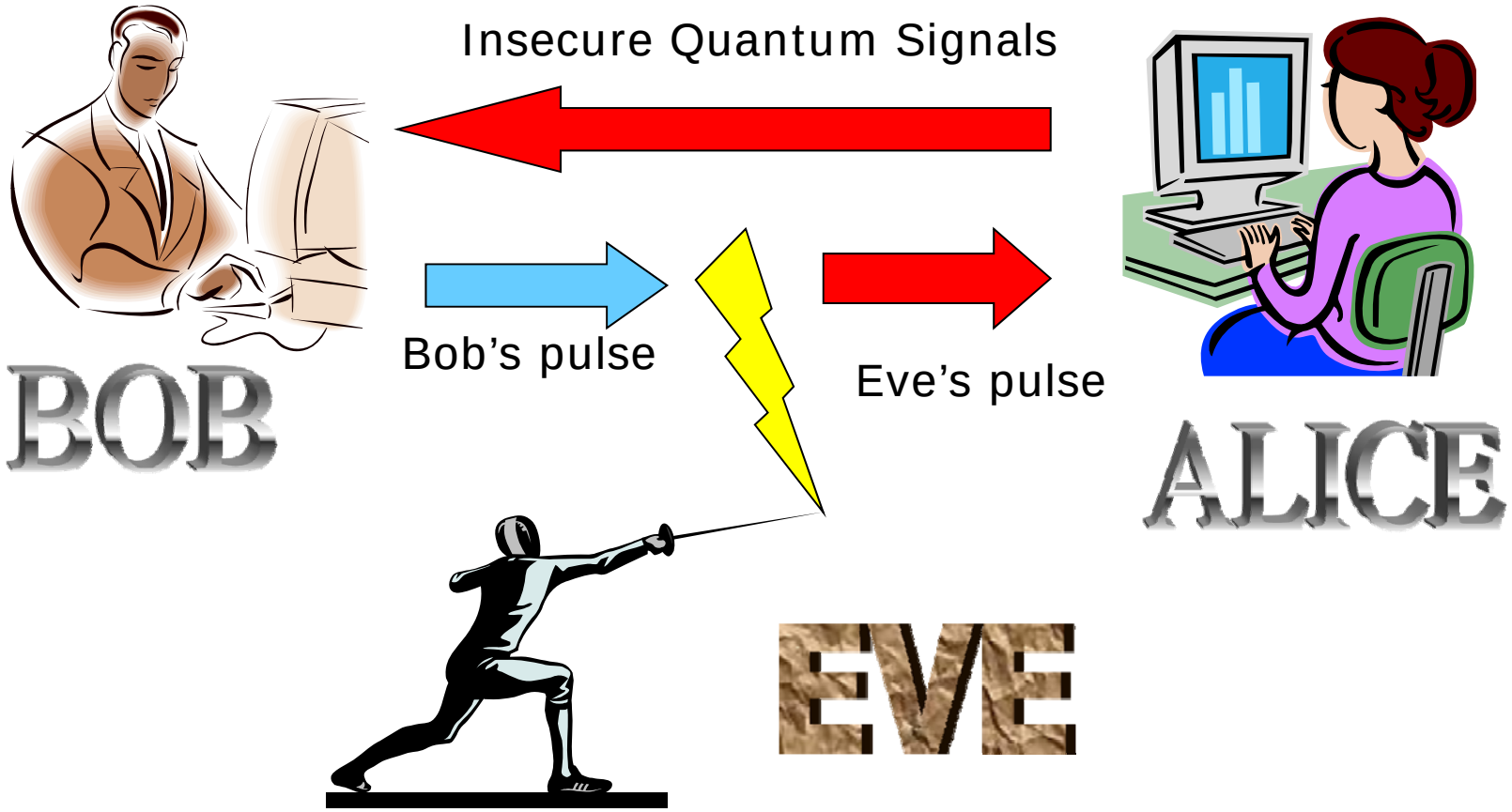


Plug & Play QKD: Photon number distribution is determined by Eve as Eve can control the source.



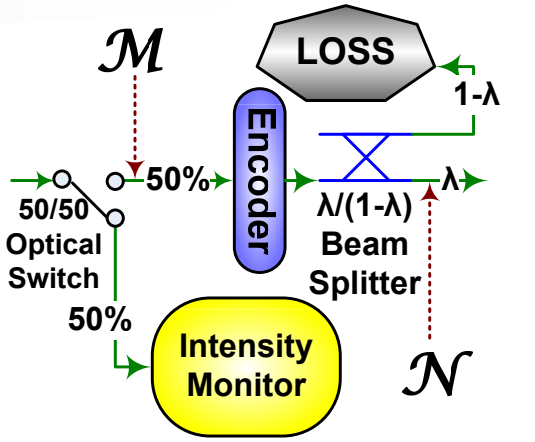
Security Risk in Plug & Play QKD

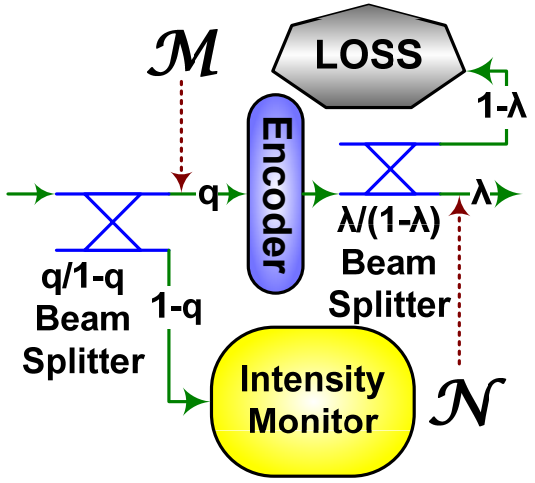
Plug & play structure is adopted by most commercial QKD systems.



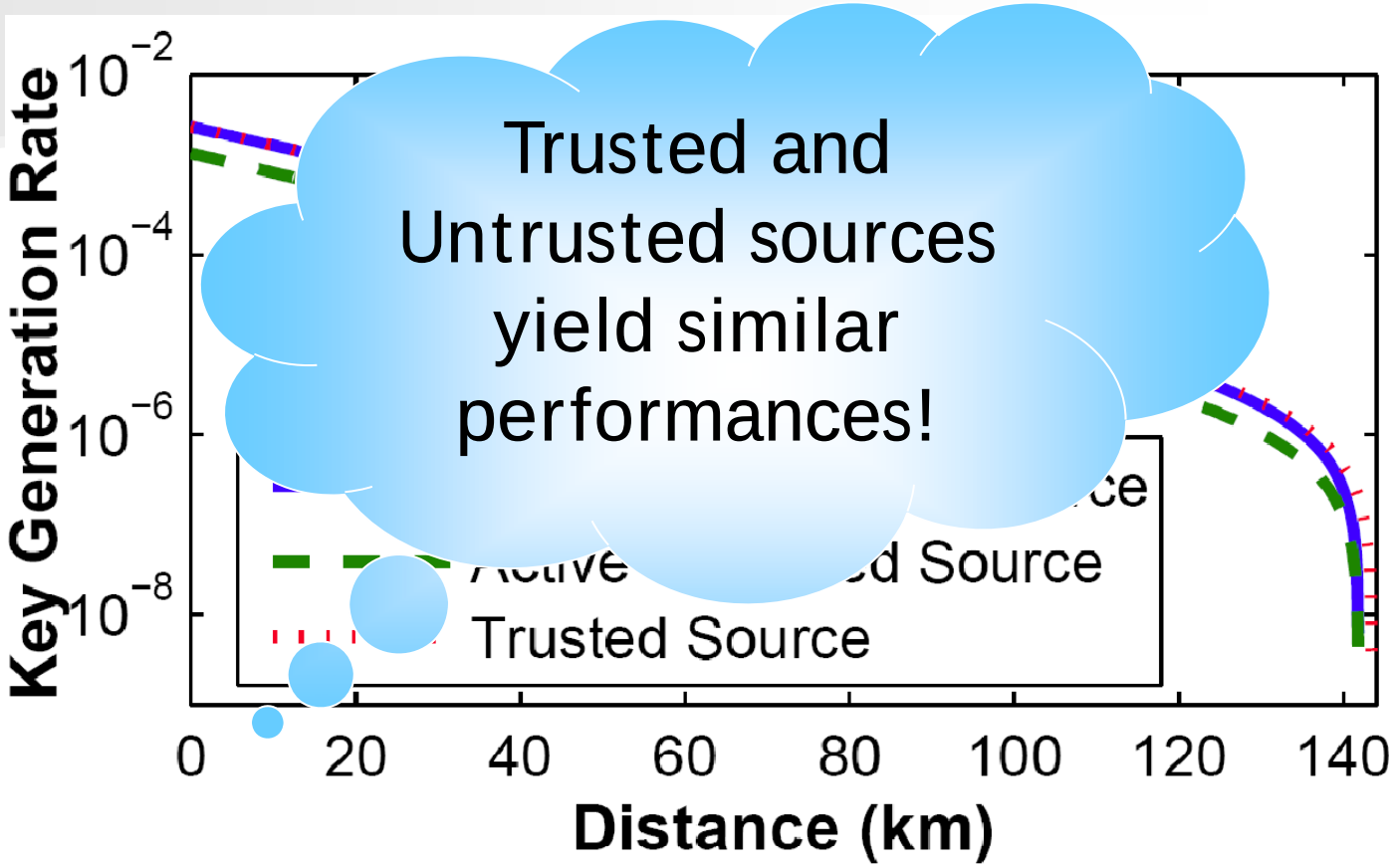
Estimating the Input Photon Number Distribution

- Active Estimate
  - Random Sampling.
  - Challenging to implement experimentally.
  - Y. Zhao, B. Qi, and H.-K. Lo, Phys. Rev. A, 77, 052327 (2008).
- Passive Estimate
  - Easy to implement.
  - Cross Sampling.
  - Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, arXiv:0905.4225 (2009).
  - See also X. Peng, Optics Letters, Vol. 33, Issue 18, pp. 2077-2079 for a preliminary experiment.





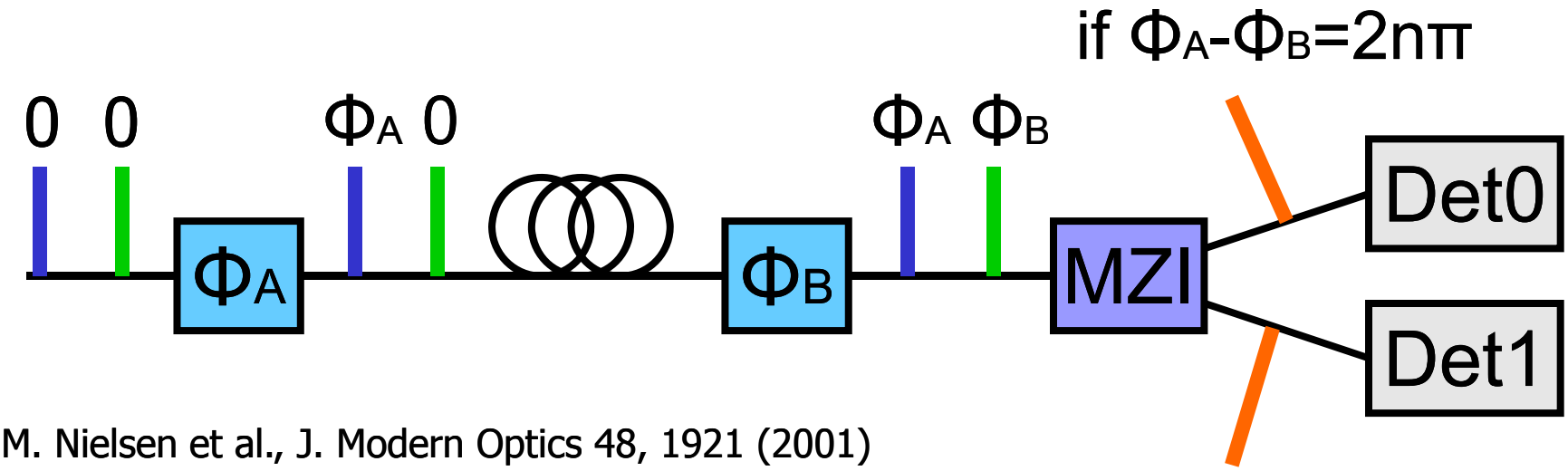
Numerical Simulation: Decoy State QKD



- Based on Toshiba group's experimental parameters.
  - C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. 84, 3762 (2004).

Counter Measure: Four-state Modulation at Bob's Side (Cont'd)

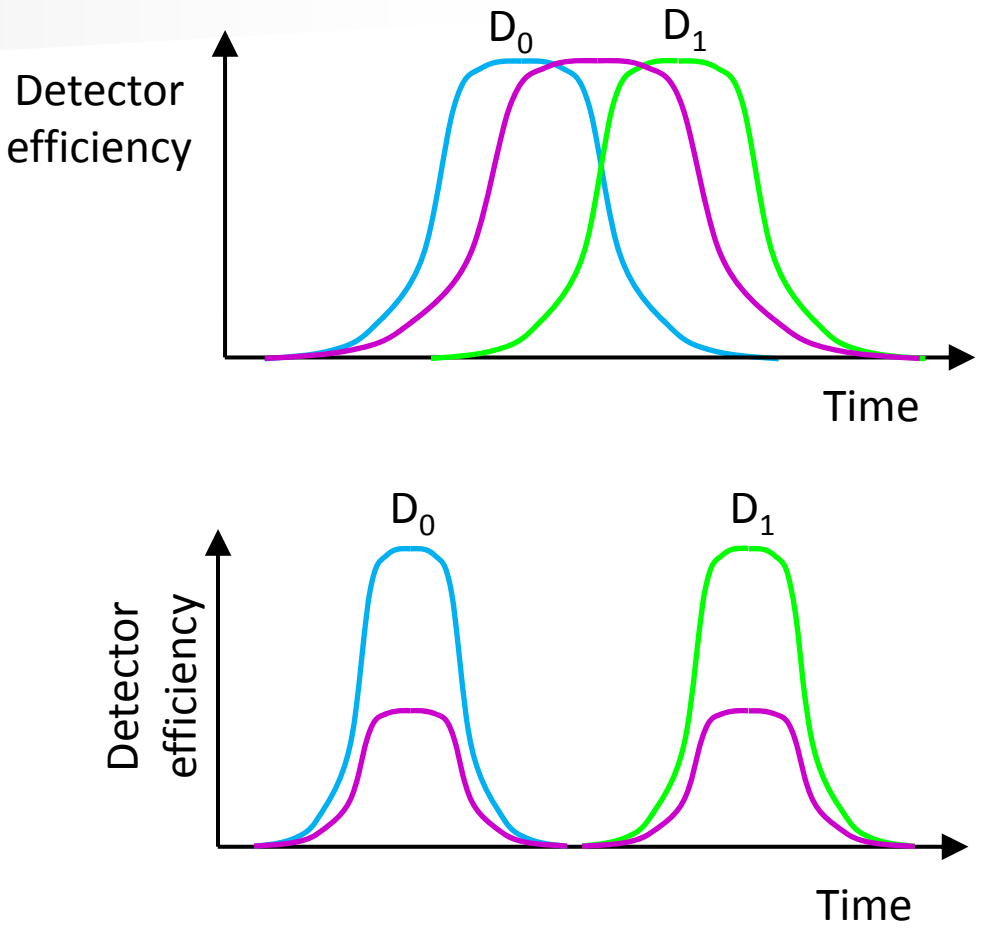
- Eve may predict which detector fires for certain bit.
- But, she does not know the bit value of the firing detector for this bit.



P. M. Nielsen et al., J. Modern Optics 48, 1921 (2001)
M. J. LaGasse, US patent application 20050190922 (2005)
C.-H. F. Fung et al., QIC 9:131 (2009).

Power of Four State Modulation

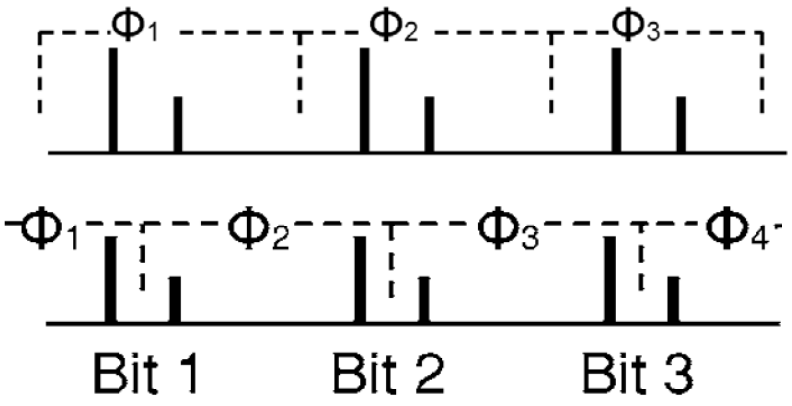
- It removes the detection efficiency mismatch in time, frequency, and spatial domains.
- It removes the detection efficiency mismatch due to detector dead time.

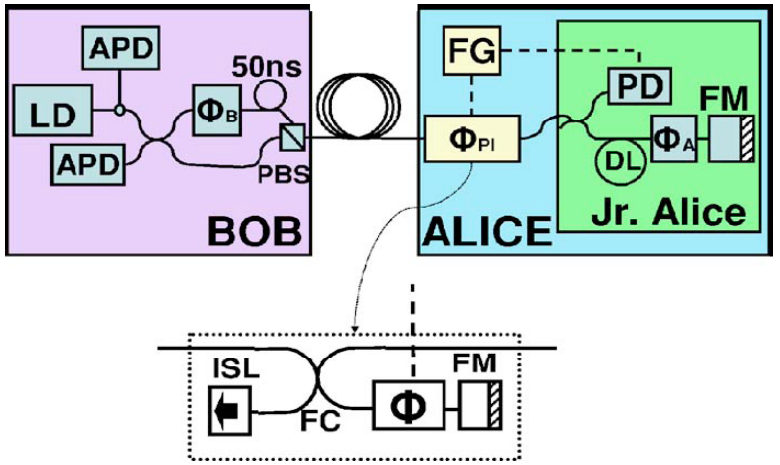


*C.-H. F. Fung, K. Tamaki, B. Qi, H.-K. Lo, and X. Ma, QIC 9:131 (2009).

Phase Randomization: Experiment

- Basic idea: active phase randomization
  - Careful synchronization → No mess-up!
- We demonstrated the first experimental QKD with reliable active phase randomization.
  - A polarization-insensitive phase modulator is developed.
  - Transmittance and error rate are not affected by the phase randomization.
- How can we verify that the phase is indeed random?

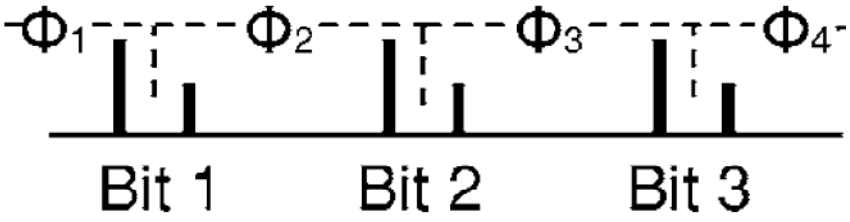


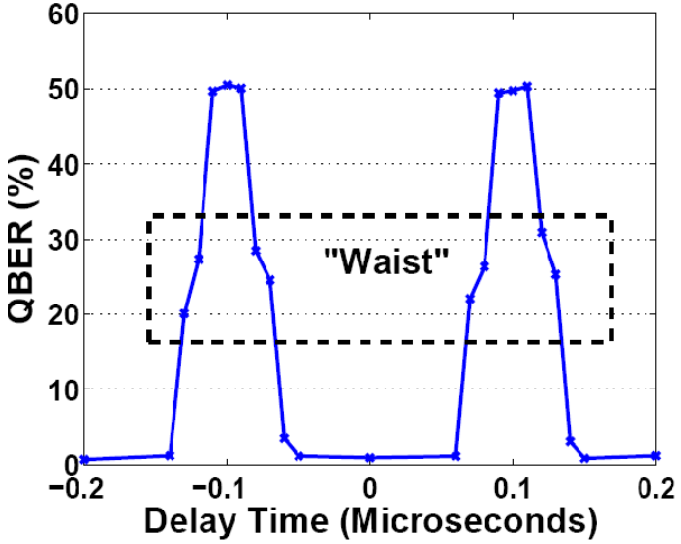


Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. 90:044106 (2007).

Phase Randomization: Verification

- Perhaps, we can “mess it up” a little…
- Shift the modulation period.
  - The relative phase is random.
  - A sharp increase of QBER to 50% is expected.
- A sharp increase of QBER to 50% is confirmed experimentally.

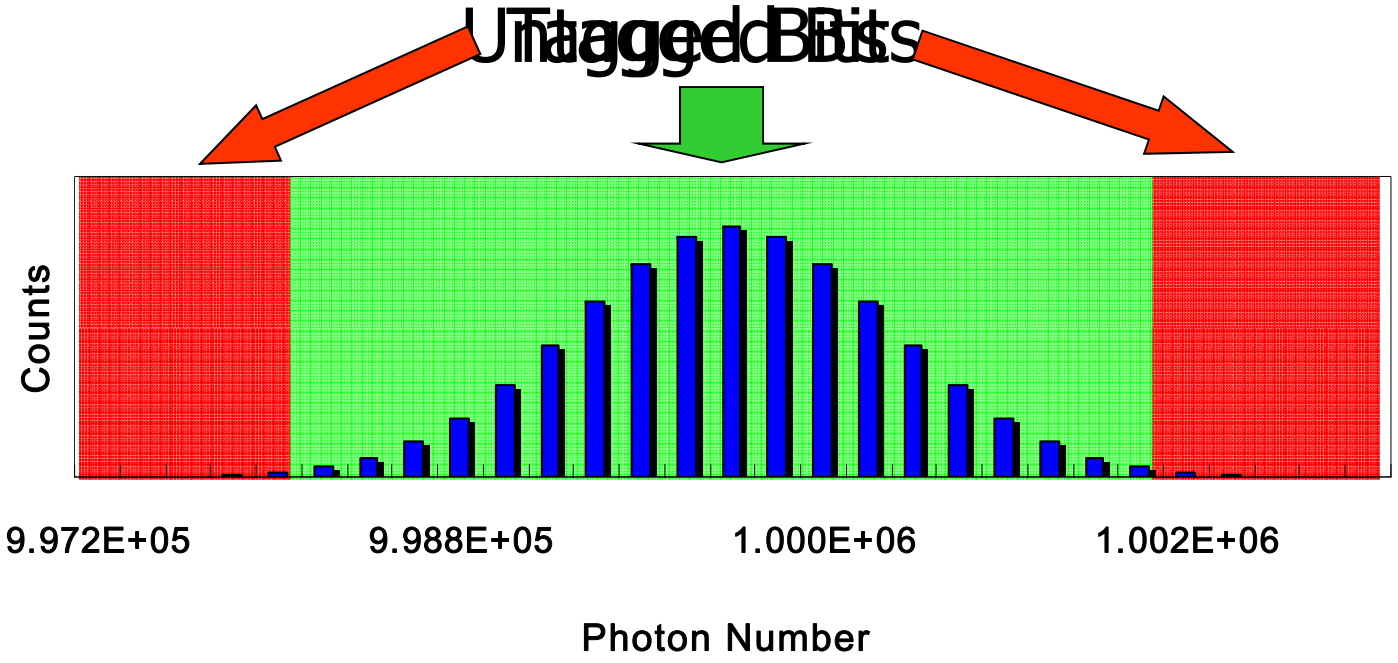




Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. 90:044106 (2007).

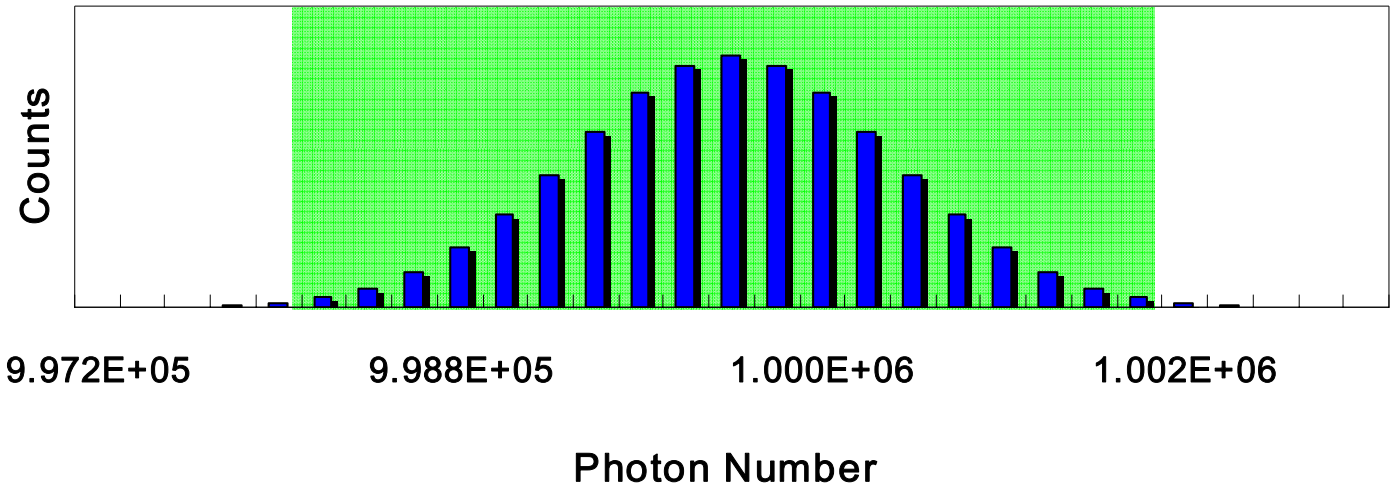
Main Concept: Untagged Bits

- One can arbitrarily set a range for input photon numbers.
- Pulses in this range are defined as Untagged Bits.
- Pulses outside of this range are defined as Tagged Bits.



Why are we interested in Untagged Bits?

- Untagged bits have clear upper and lower bounds of input photon numbers.
- One can estimate the minimum probability for an untagged bit to be secure.
- Question: How many untagged bits have been sent to Bob?



Time-Shift Attack: Analysis

- Probabilities of choosing the two shifts: 23:77
  - Two detectors receive the same counts.
- Lower bound of secure keys (ignoring the attack)
  - 1297 bits
- Upper bound of secure keys (knowing the attack)
  - 1131 bits

Data averaged over two shifts		
Data size	Gain	QBER
20.97Mbits	3.32e-4	5.68%

Experimental parameters	
Dark count rate	μ
2.26×10^{-5}	0.1

Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, PRA 78:042333 (2008).

Time-shift attack: advantages

- Easy to implement (optical switches, optical fibers)

  Cf. faked-state attack (Makarov et al.) is hard to implement because it involves measurements.

- Difficult to detect: NO extra quantum bit error rate (QBER=0)
- Bob's imperfect detectors (with time-polarization correlation) post-select photons which carry the same bit values from Alice and Eve.

B. Qi, C.-H. F. Fung, H.-K. Lo, and X. Ma, Quant. Info. Compu. 7, 73 (2007).

nature International weekly journal of science

Quantum cryptography: Seeking absolute security

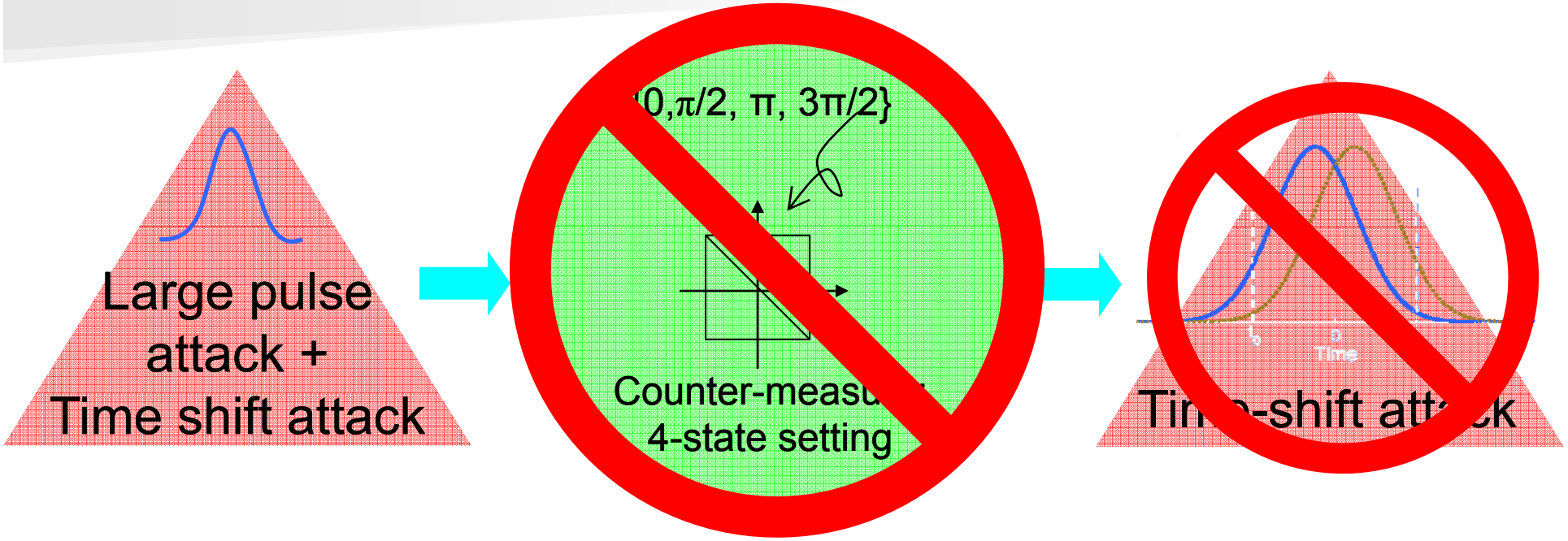
Quantum cryptography is theoretically unbreakable,
yet a handful of physicists are finding ways to hack into its secrets.
Geoff Brumfiel finds out how.

Nature **447**, 372-373 (24 May 2007)

Lesson One

- Once Alice and Bob are aware of an attack, it may not be too difficult for them to devise counter measures against it.
- Imperfections, once quantified, can be dealt with by additional privacy amplification.
- But, **Unanticipated** attacks can be fatal!

Lesson Two



Counter-measures may lead to new security loopholes!

Phase Randomization in Practice

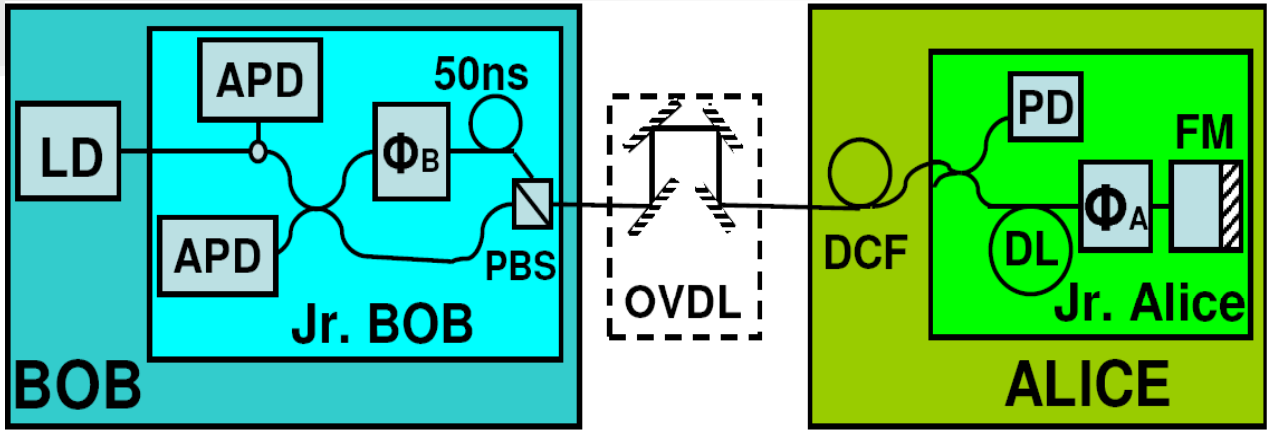
- In practice, the phase may not be random.
  - Uni-directional system: strong reference pulse, long coherent time.
  - Bi-directional system: strong classical pulse from Bob.
- If phase is not randomized, existing security proof gives a lower key rate.
  - Lo and Preskill, QIC 7, 431 (2007).
- We demonstrated the first experimental QKD with reliable active phase randomization.
  - **Y. Zhao**, B. Qi, and H.-K. Lo, Appl. Phys. Lett., 90:044106 (2007).

Previous Security Analysis (Not Proof!)

- Basic idea: Heavy attenuation can transform arbitrary photon number distribution to Poisson-like distribution.
- Bad News: Resulting distribution may not be "Poisson-like"!
- Hard to quantify how "likely" it is to Poisson distribution.
- Rigorous security proof has not been developed in this approach.

- N. Gisin et al., Phys. Rev. A **73**, 022320 (2006)

Time-shift attack: experiment



OVDL: optical variable delay line

- Commercial plug & play QKD system
- Scan the time shifts manually → find the two efficiency mismatch points
- Perform time-shift attack during QKD transmission
- Calculate how much information leaked to Eve

Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, PRA 78:042333 (2008).

Future Direction

- Research in the security of QKD has split into two directions.
  - Fundamental research (e.g. based on the testing of the Bell's inequalities) that does not have practical applications.
  - Practical research that can only provide some "reasonable" security.
- There will always be a gap between the two approaches.
- V. Scarani, C. Kurtsiefer, arXiv:0906.4547, 2009.