Title: Practical quantum-key-distribution systems with detector efficiency mismatch: attacks and secret key rates

Date: Jun 04, 2007 10:50 AM

URL: http://pirsa.org/07060021

Abstract: Imperfections in devices are inevitable in practice. In this talk, we focus on the imperfection of QKD systems in the detectors, namely that the efficiencies of the detectors are not completely identical. We show some practical attacks that specifically exploit this efficiency mismatch and demonstrate how Eve may obtain some information on the final key if Alice and Bob are unaware of the attack. Also, we discuss the upper and lower bounds on the secret key rates both with and without the assumption of the efficiency mismatch

Quantum key distribution (QKD)

- Absolute security based on fundamental laws of quantum mechanics, rather than computational assumptions.
- Allow two persons who share a small amount of authentication information to communicate in absolute security in the presence of an eavesdropper.
- Any eavesdropping attack will essentially always be caught.

Quantum key distribution (QKD)

- Absolute security based on fundamental laws of quantum mechanics, rather than computational assumptions.
- Allow two persons who share a small amount of authentication information to communicate in absolute security in the presence of an eavesdropper.
- Any eavesdropping attack will essentially always be caught.

Quantum key distribution (QKD)

- Absolute security based on fundamental laws of quantum mechanics, rather than computational assumptions.
- Allow two persons who share a small amount of authentication information to communicate in absolute security in the presence of an eavesdropper.
- Any eavesdropping attack will essentially always be caught.

Intrusion alert! Eve Intrusion alert!

Are practical QKD systems really secure?

- QKD protocols have been proven to be unconditionally secure even with imperfect devices
  - Mayers, J. of ACM, 48, 351 (2001);
  - Lo and Chau, Science 283, 2050 (1999);
  - Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000);
  - Gottesman, Lo, Lütkenhaus, and Preskill, QIC 5, 325 (2004);
  - Renner, Gisin, and Kraus, PRA 72, 012332 (2005);
  - Kraus, Branciard, and Renato Renner, PRA 75, 012316 (2007)
  - ...
- Is this the end of security investigation for QKD?

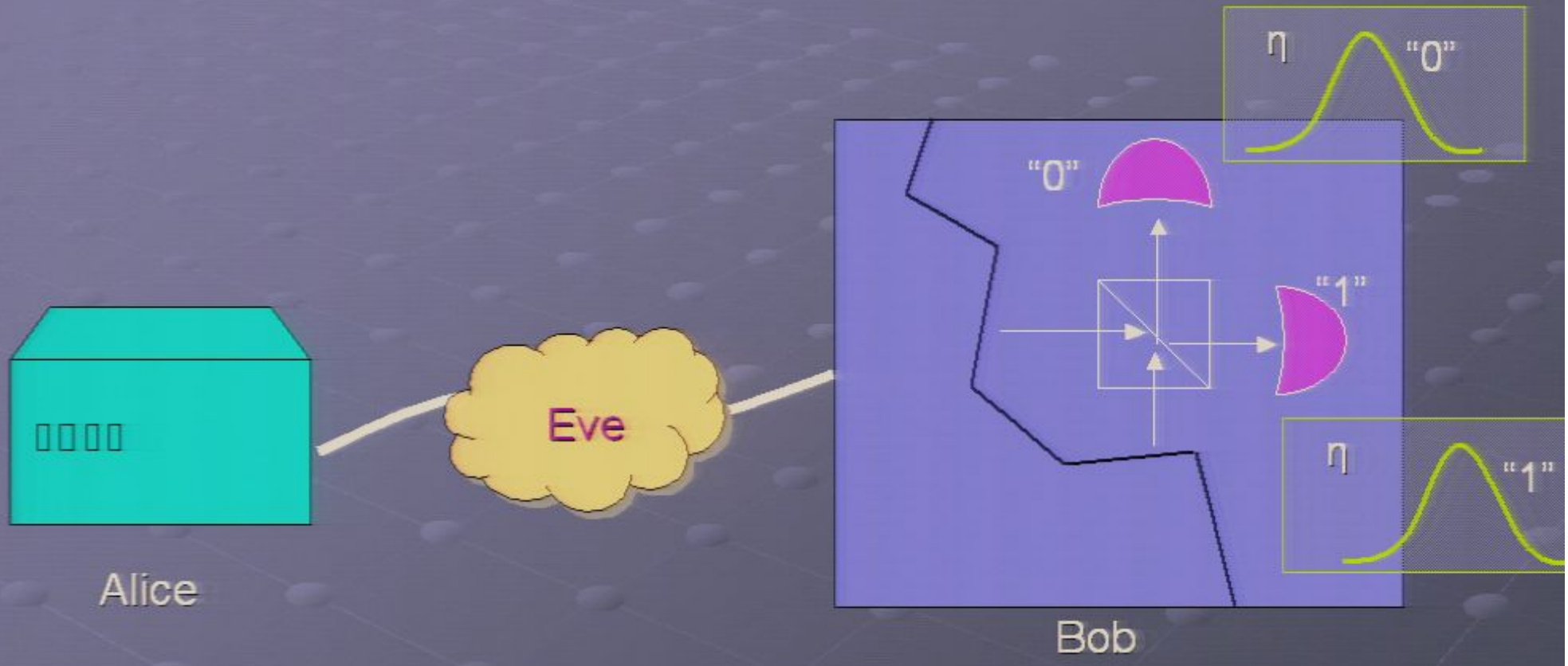
Are practical QKD systems really secure?

- QKD protocols have been proven to be unconditionally secure even with imperfect devices
  - Mayers, J. of ACM, 48, 351 (2001);
  - Lo and Chau, Science 283, 2050 (1999);
  - Shor and Preskill, Phys. Rev. Lett. 85, 441 (2000);
  - Gottesman, Lo, Lütkenhaus, and Preskill, QIC 5, 325 (2004);
  - Renner, Gisin, and Kraus, PRA 72, 012332 (2005);
  - Kraus, Branciard, and Renato Renner, PRA 75, 012316 (2007)
  - ...
- Is this the end of security investigation for QKD?

No really!

Practical systems may contain imperfections not considered by standard proofs that may lead to loophole.

Practical imperfection: detector efficiency mismatch

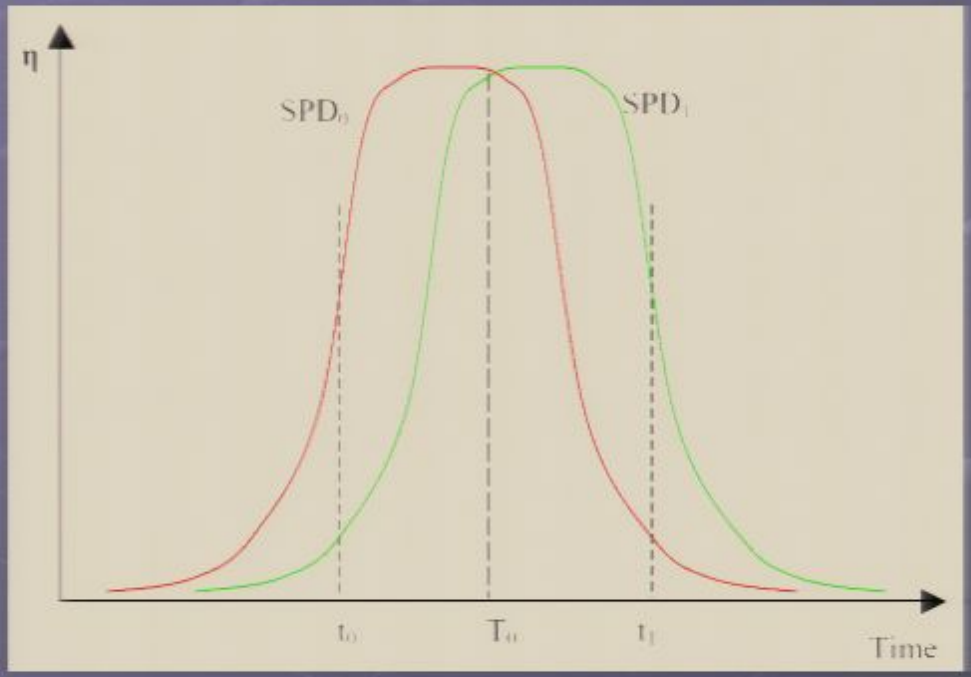


- In many QKD systems, there are two detectors for detecting bit "0" and bit "1".
- One imperfection is that these detectors respond differently.

Detector efficiency mismatch

- Detectors operating in gated mode may have different efficiencies.

η: detection efficiency



- Ideally, signals should arrive at Bob at time T_0
- Eve takes advantage of the efficiency mismatch by arranging signals to arrive at other times.

Attacks based on efficiency mismatch

Two attacks:

- Faked states attack

  [Makarov, Anisimov, and Skaar, PRA 74, 022313 (2006)]

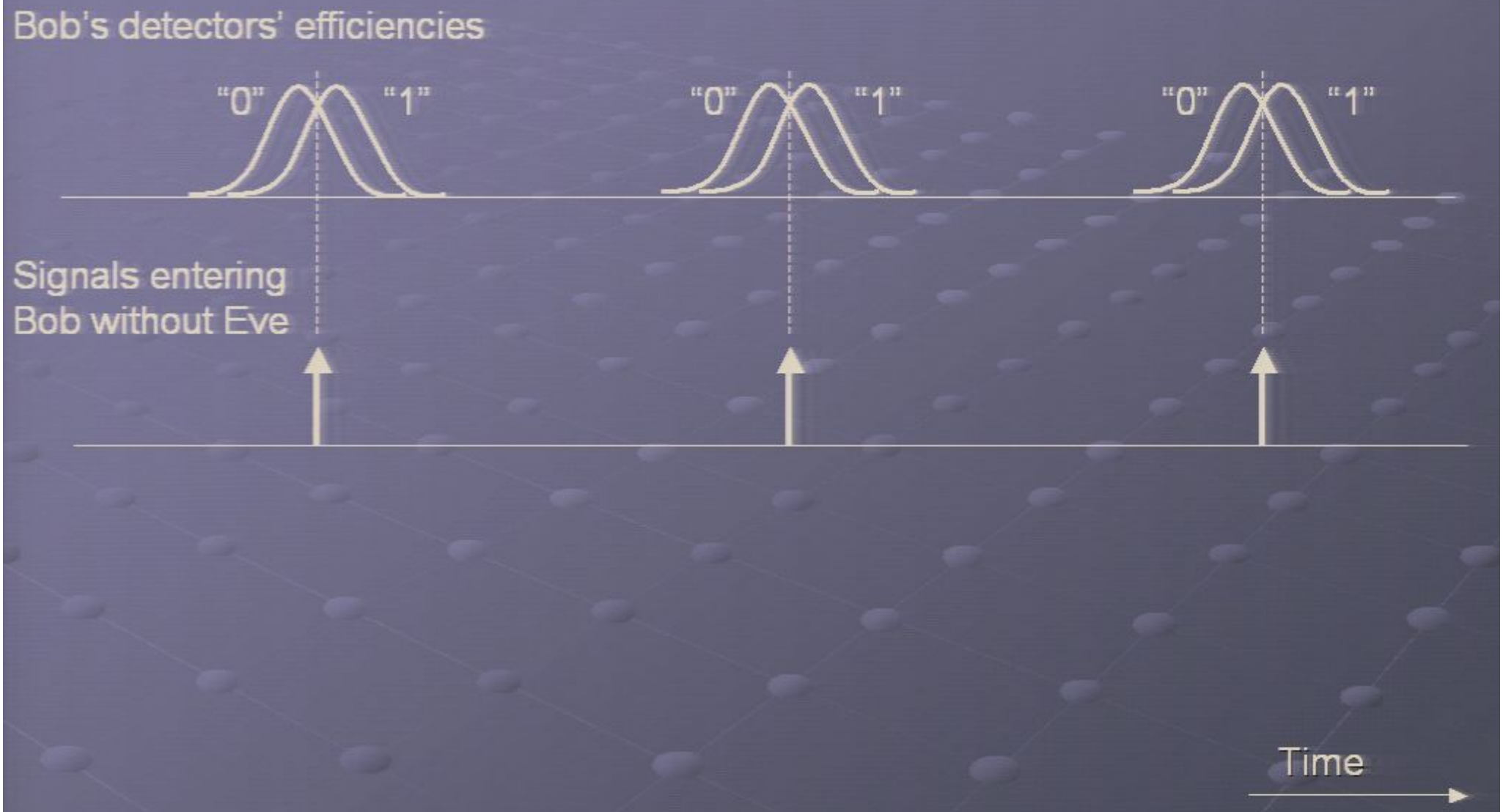
  - Eve measures Alice's signal and sends a time-shifted signal to Bob (intercept-and-resend attack).

- Time-shift attack

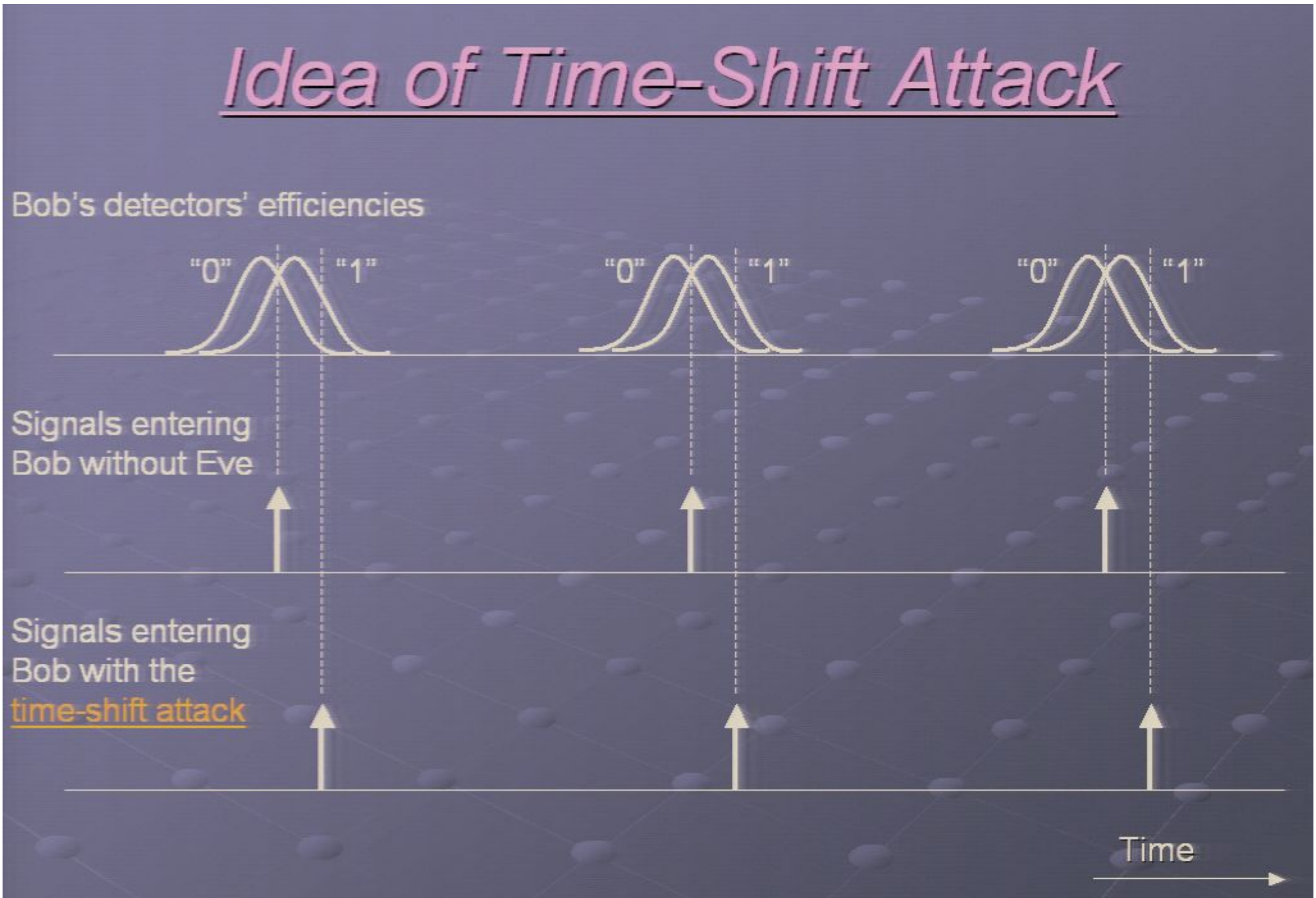
  [Qi, Fung, Lo, and Ma, QIC 7, 73 (2007); Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, arXiv:0704.3253]

  - Eve simply time shifts the signal sent out by Alice.
  - No error introduced.

Idea of Time-Shift Attack

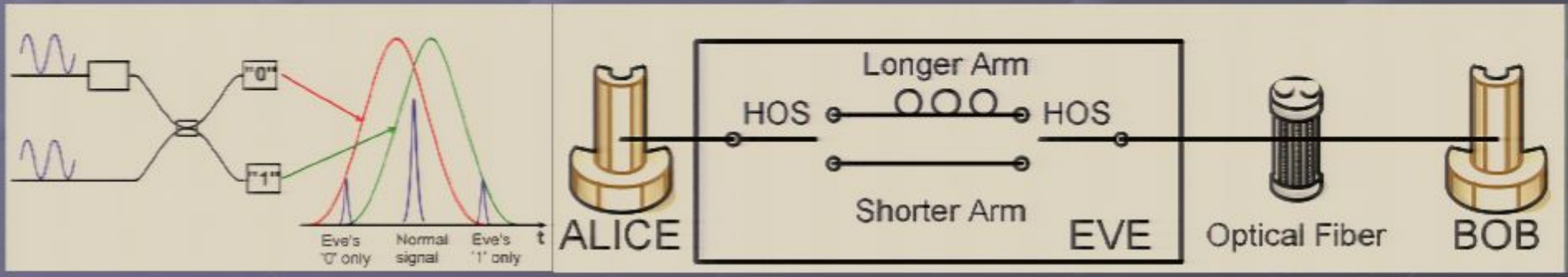


Idea of Time-Shift Attack



Time-Shift Attack: Strategy

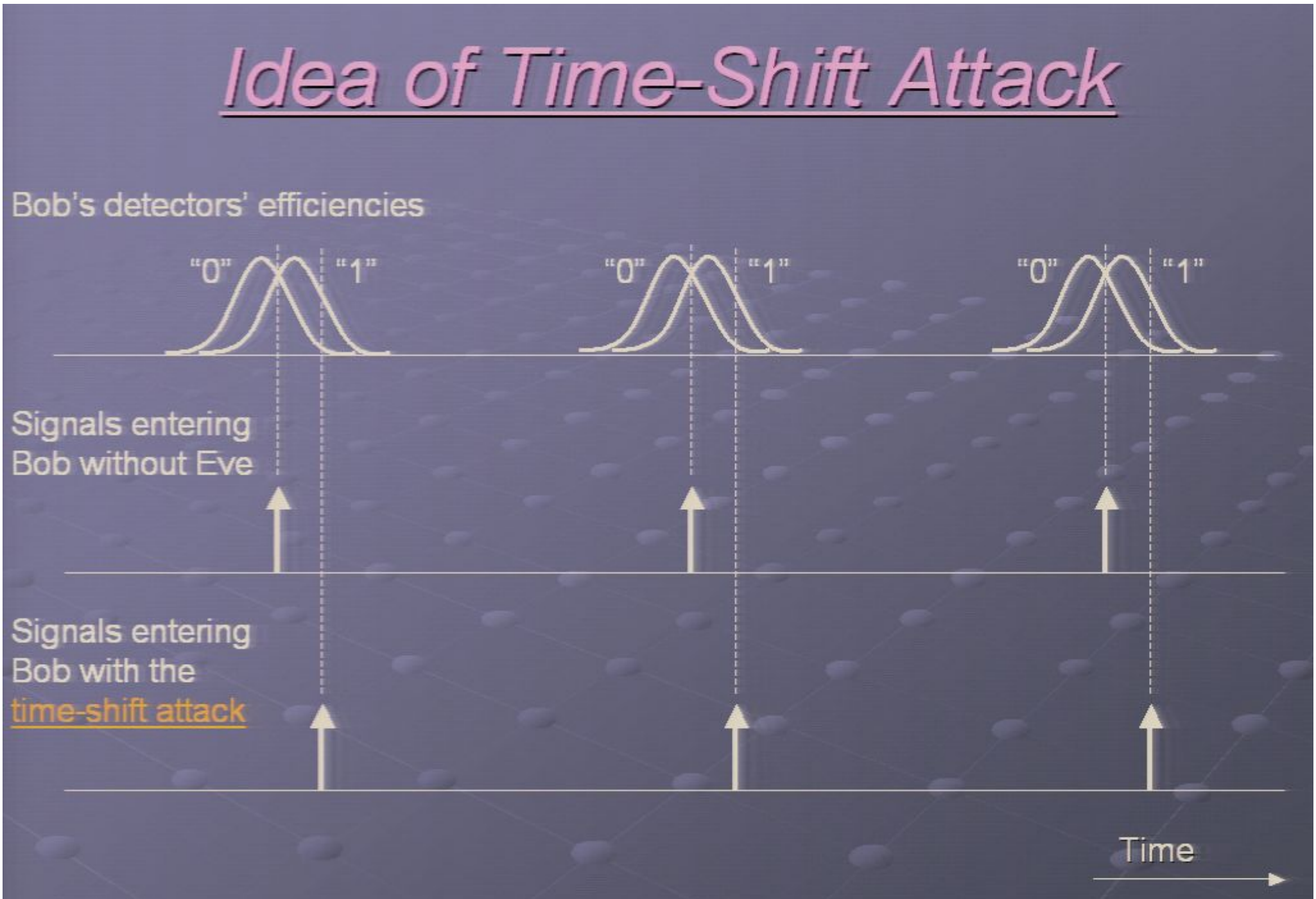
- Eve finds two shifts with large efficiency mismatches.
- Eve randomly shifts the arrival time of each signal to either of the two.
- The probability of choosing either shift is carefully chosen so that Bob will receive similar number of “0”s and “1”s.



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

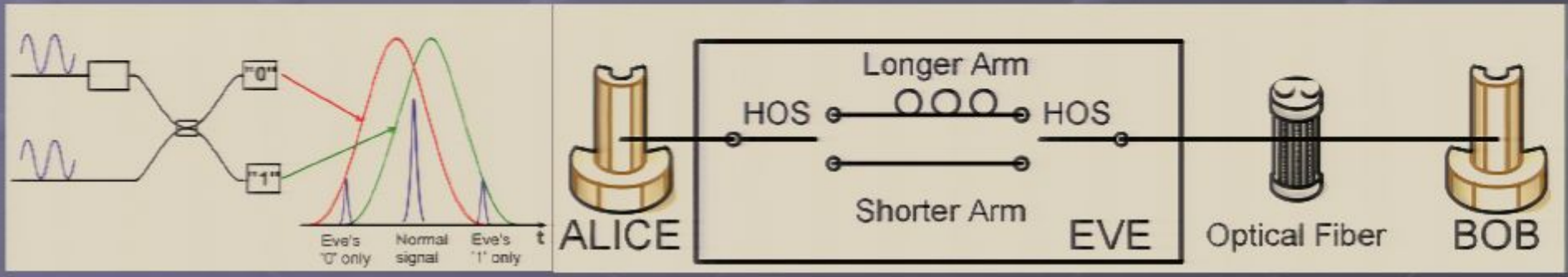
Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, arXiv:0704.3253.

Idea of Time-Shift Attack



Time-Shift Attack: Strategy

- Eve finds two shifts with large efficiency mismatches.
- Eve randomly shifts the arrival time of each signal to either of the two.
- The probability of choosing either shift is carefully chosen so that Bob will receive similar number of “0”s and “1”s.



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

Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, arXiv:0704.3253.

Theoretical analysis

- Analysis of efficiency mismatch, assuming BB84 and no error.

  1. Alice and Bob unaware of efficiency mismatch (standard security proof):

0 Key generation rate 1

Theoretical analysis

- Analysis of efficiency mismatch, assuming BB84 and no error.

1. Alice and Bob unaware of efficiency mismatch (standard security proof):

0 Key generation rate 1

2. Maximum key rate allowed with efficiency mismatch:

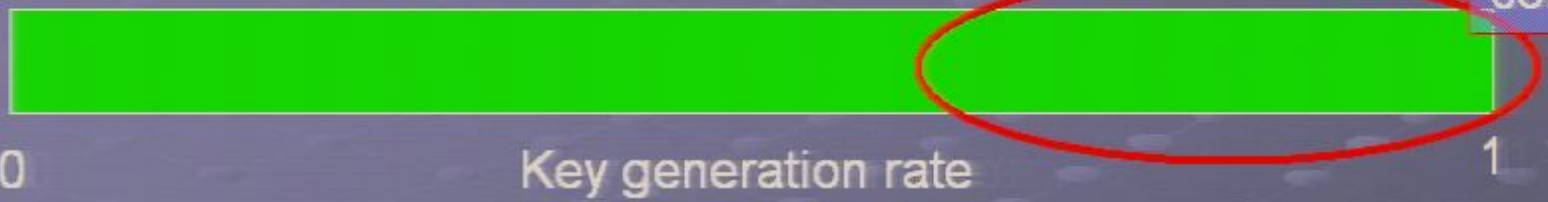
0 1

$$\min_t \; H_2\left(\frac{\eta_0(t)}{\eta_0(t)+\eta_1(t)}\right)$$

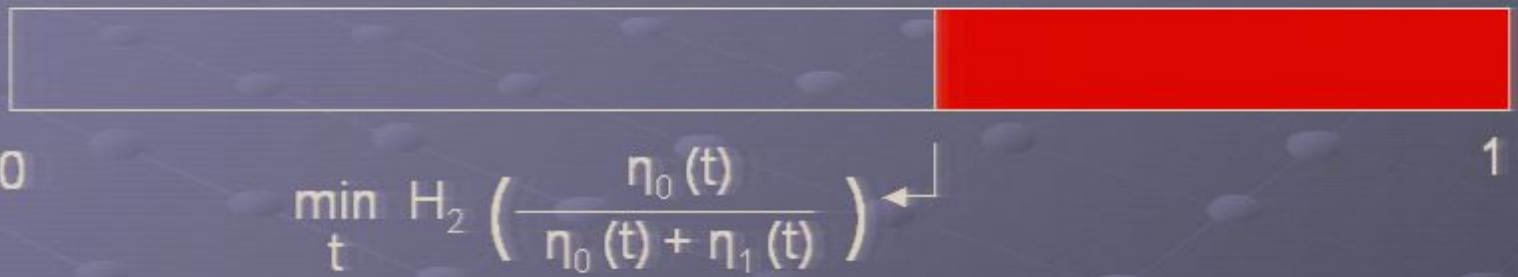
Theoretical analysis

- Analysis of efficiency mismatch, assuming BB84 and no error.

1. Alice and Bob unaware of efficiency mismatch (standard security proof):



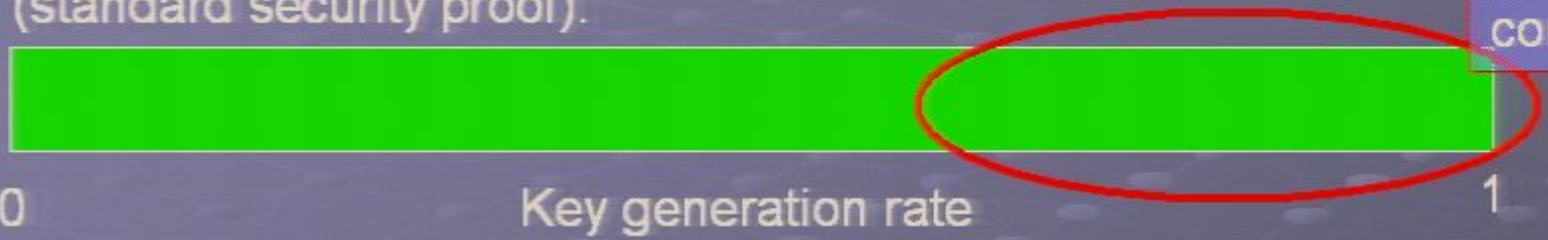
2. Maximum key rate allowed with efficiency mismatch:



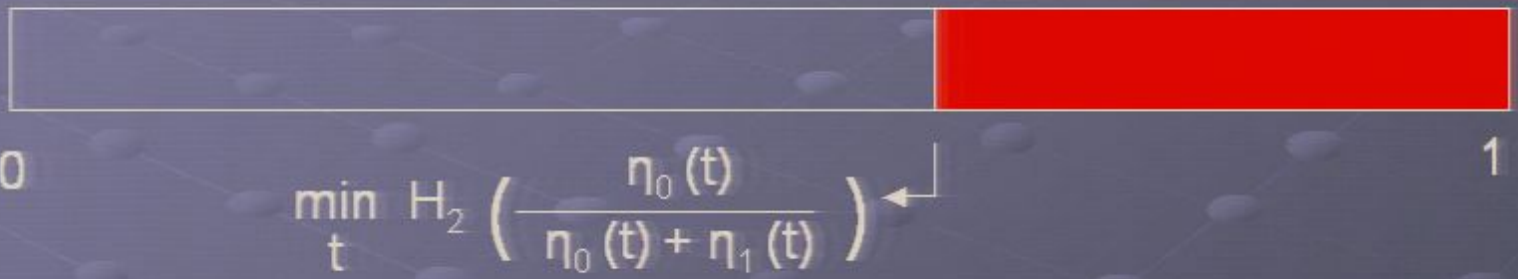
Theoretical analysis

- Analysis of efficiency mismatch, assuming BB84 and no error.

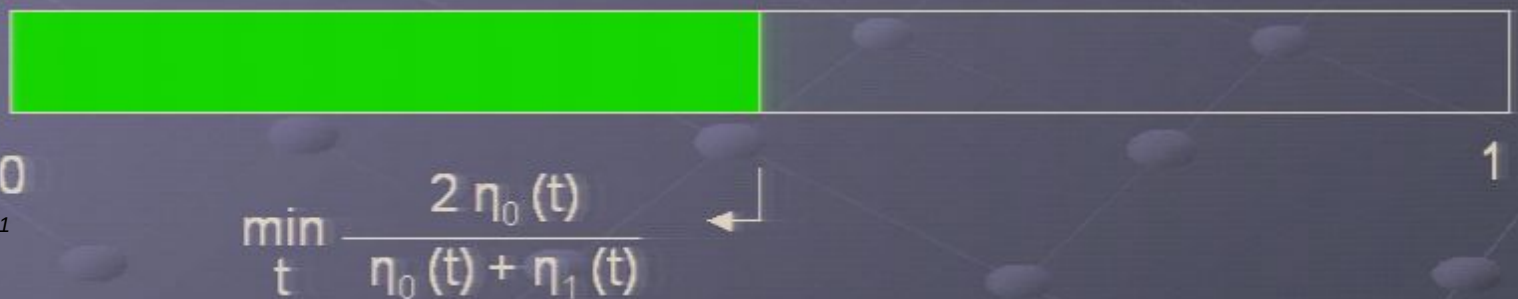
1. Alice and Bob unaware of efficiency mismatch (standard security proof):



2. Maximum key rate allowed with efficiency mismatch:

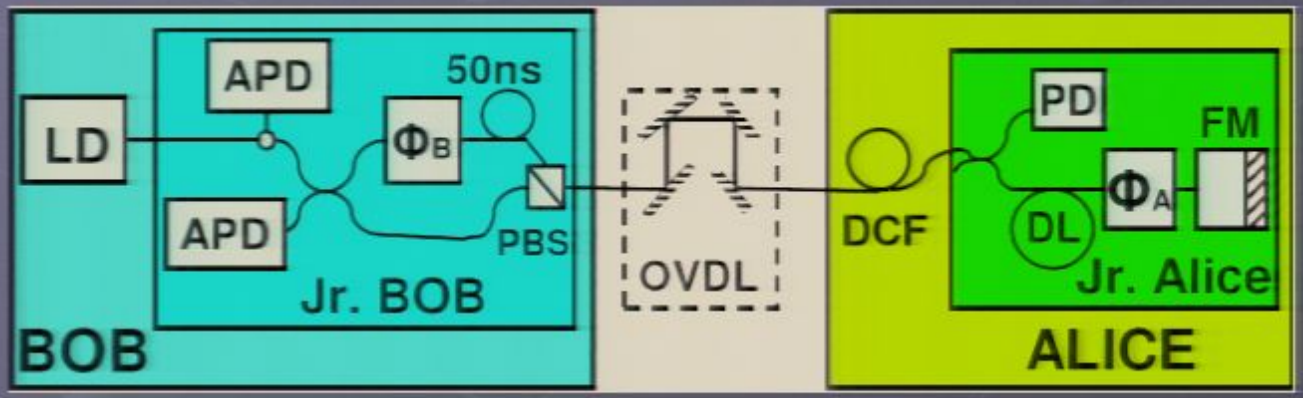


3. Alice and Bob aware of efficiency mismatch (new security proof):



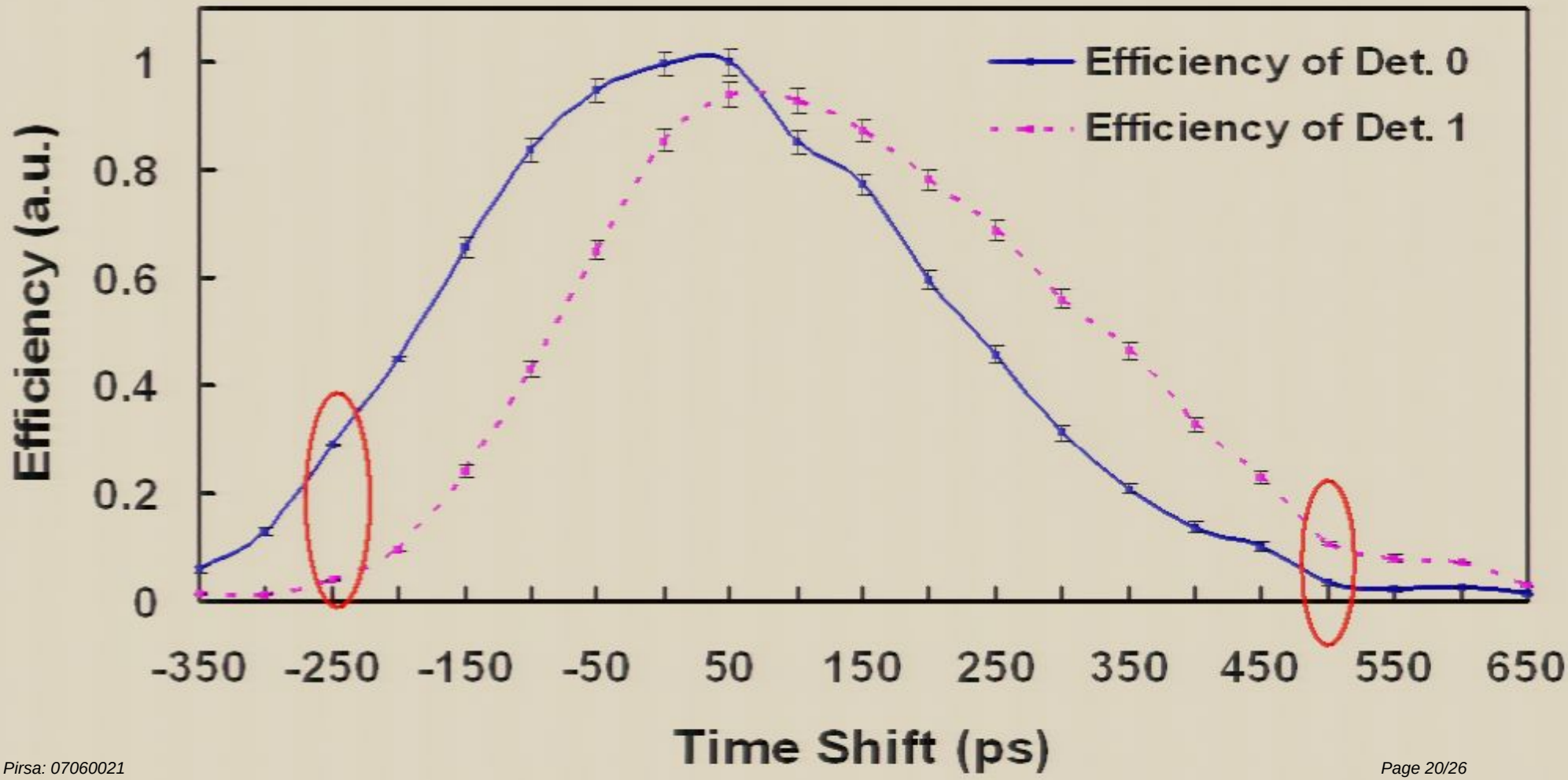
Time-Shift Attack: Experiment

- Perform detector activation time calibration using built-in calibration program from id Quantique ID-500 QKD system.
- Scan the time shifts manually.
- Exchange keys in each shift at μ=0.1.
- Calculate the counts of each detector and the error rate for each time shift.



Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, arXiv:0704.3253.

Time-Shift Attack: Result



Time-Shift Attack: Analysis

- Probabilities of choosing the two shifts: 23:77
  - Two detectors receive the same counts.
- Maximum key rate with efficiency mismatch: 6.08e-5
  - Given the information obtained by Eve.
- Key rate with standard security proof: 6.16e-5
  - Assuming Alice and Bob applied infinitely many decoy states.

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

Time-Shift Attack: Analysis

Key rate (6.16e-5) > Maximum possible (6.08e-5)

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

Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen, and H.-K. Lo, arXiv:0704.3253.

Countering attacks based on efficiency mismatch

- Both the faked states attack and the time-shift attack compromise the QKD system when Alice and Bob are not aware of the efficiency mismatch.

- Counter measures for both attacks:
  - Four-state measurement by Bob [M. J. LaGasse, US patent application]
  - Check timing of incoming pulses at Bob
  - Security proof for detectors with different efficiencies — more privacy amplification

Conclusions

- Time-shift attack by exploiting detectors' efficiency mismatch.
- When Alice and Bob are unaware of our attack, the final key may be compromised by Eve, without introducing any error.
- Demonstrated the time-shift attack in experiment and showed that final key is insecure.
- Need to verify that every assumption of a security proof holds in a practical QKD system.
- Blindly applying security proofs to a practical system may not work.

Thanks!

NSERC CRSNG

Canada Research Chairs

ICIP CIPI

cifar Canadian Institute for Advanced Research

Ontario Innovation Trust

premier's research excellence awards

Canada Foundation for Innovation
Fondation canadienne pour l'innovation

ROGERS

VELUT ARBOR ÆVO

Walter C. Sumner Memorial Fellowships

Shahid U.H. Qureshi Memorial Scholarship

MITACS

Time-Shift Attack: Result