

# Breaking the Unbreakable Quantum Key Distribution



Design ©2008 Vadim Makarov

Lars Lydersen

Kjeller  
23. September 2010



Norwegian University of  
Science and Technology



# Quantum Hacking group

NTNU, Trondheim & UNIK, Kjeller



[www.iet.ntnu.no/groups/optics/qcr/](http://www.iet.ntnu.no/groups/optics/qcr/)

Prof. Johannes Skaar

Postdoc Vadim Makarov

PhD students Qin Liu,

Lars Lydersen,

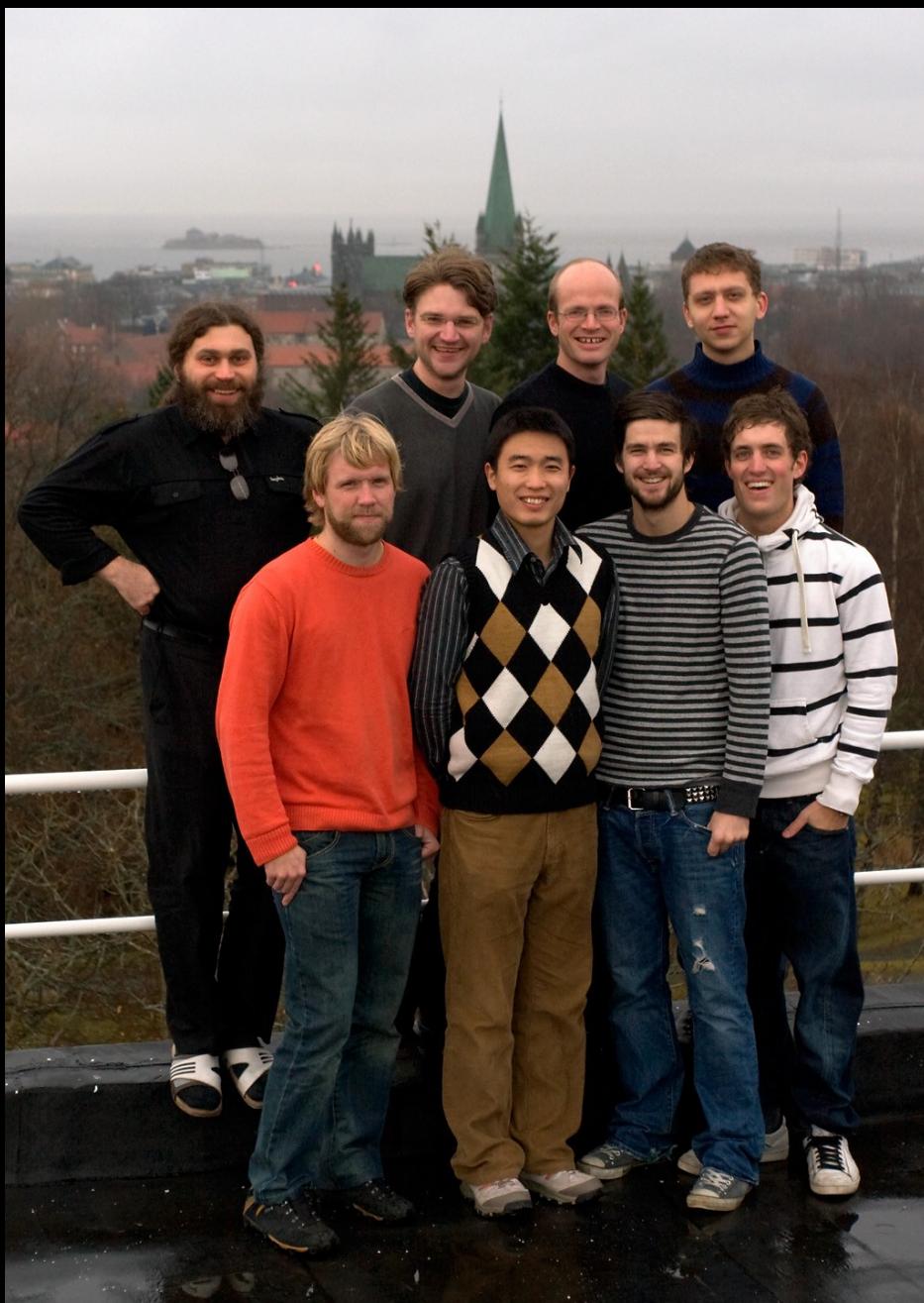
Øystein Marøy

Collaborations:

CQT Singapore,

KTH Stockholm,

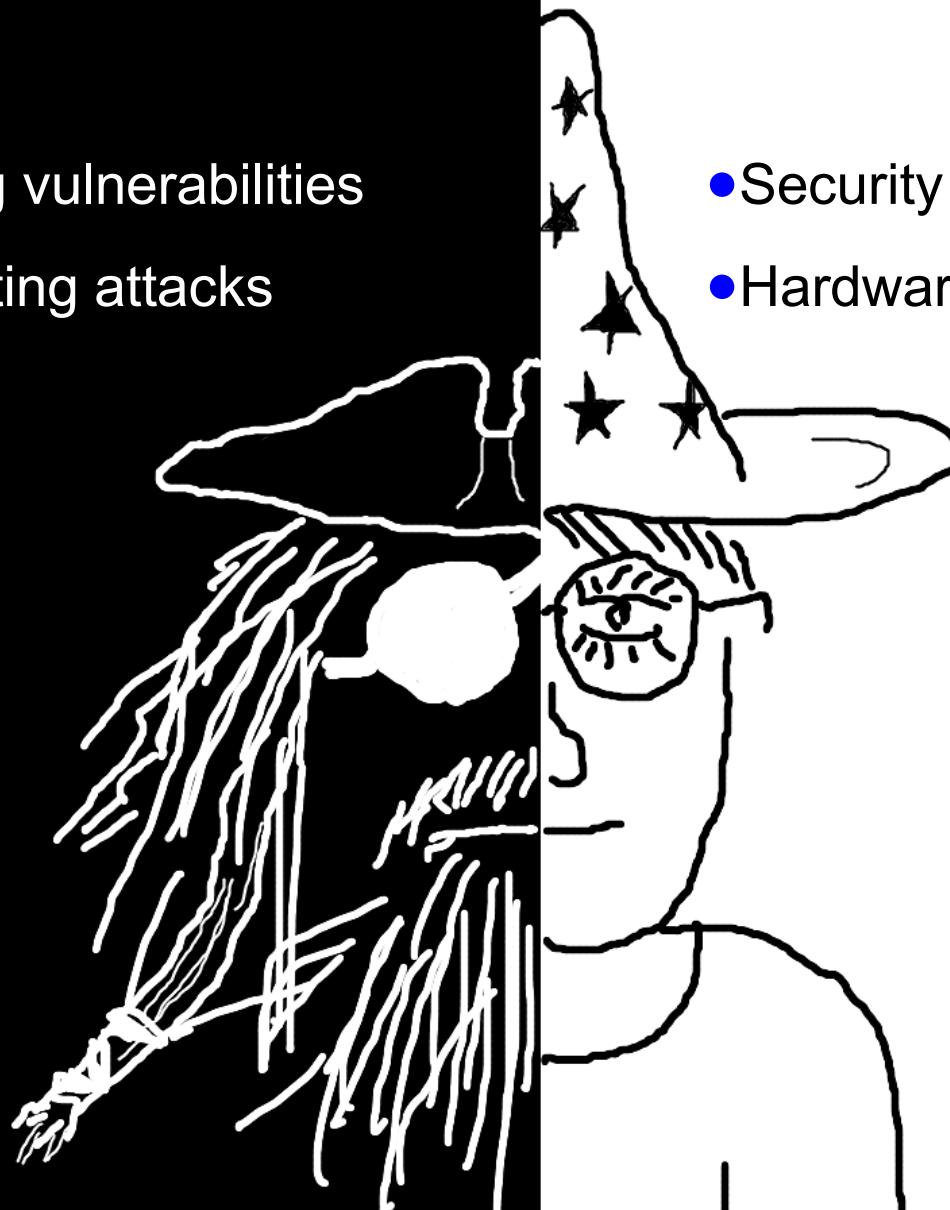
Max Planck inst. Erlangen...



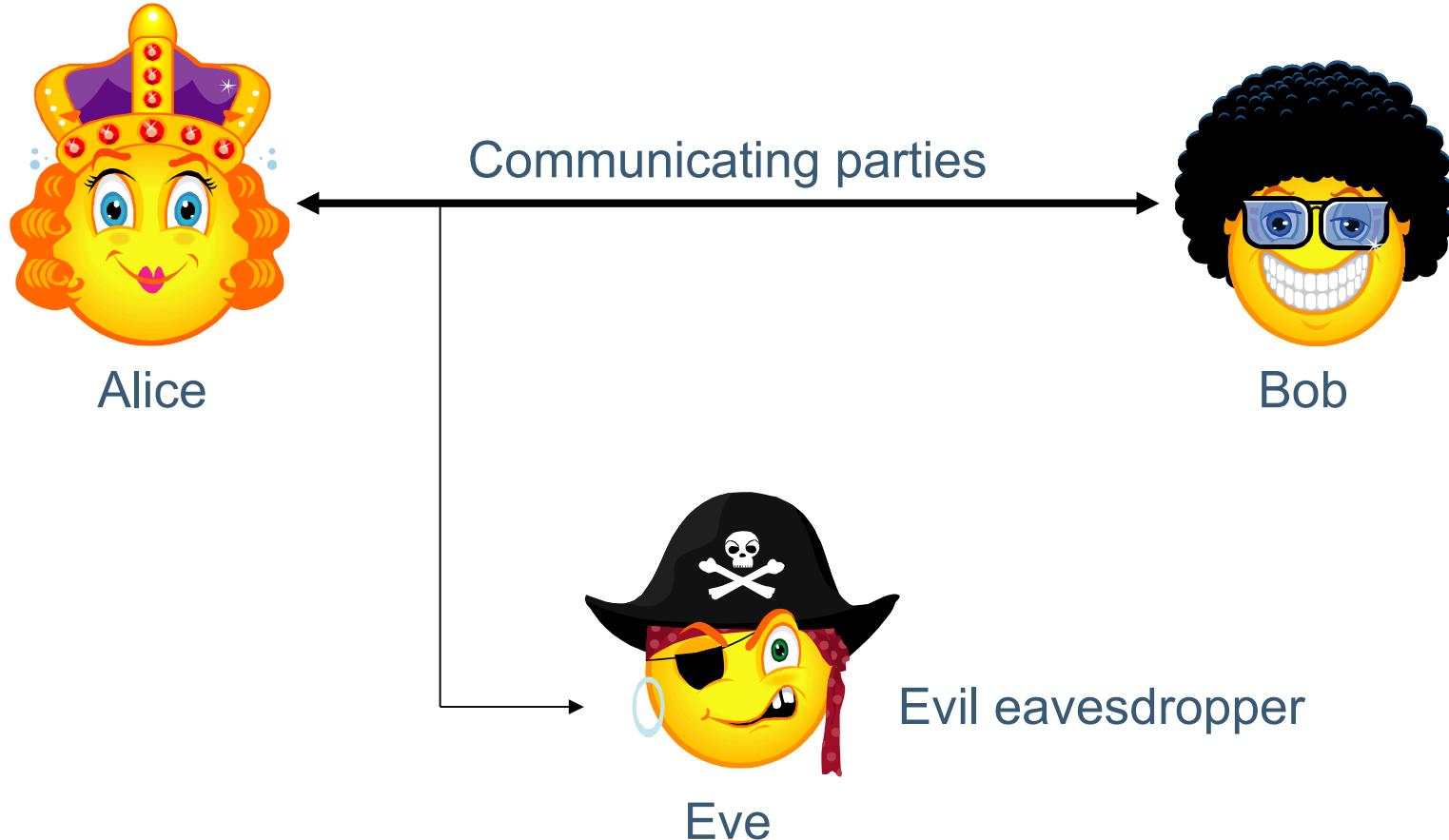
# Quantum Hacking group.

- Discovering vulnerabilities
- Demonstrating attacks

- Security proofs
- Hardware countermeasures

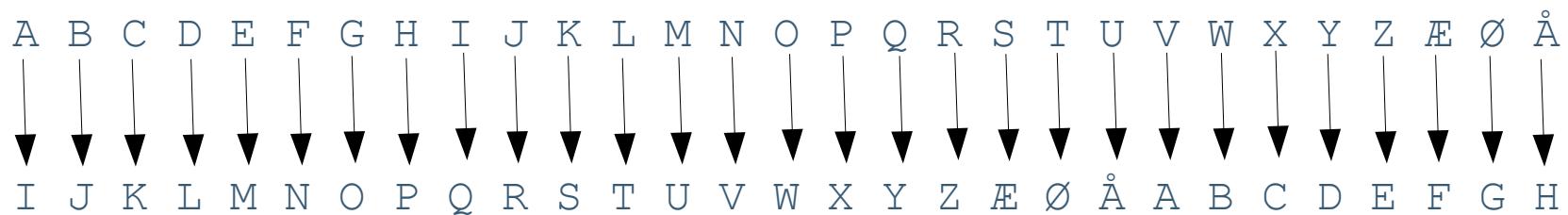


# Name convention



# Private key cryptography

- Alice and Bob agree on a secret key in advance
- Example: mono-alphabetic substitution cipher



- Breakable by frequency analysis
- For perfect security: need new “mapping” for each letter
- One-time pad.

# Private key: one-time pad

- 100 % secure (Eve's best attempt to break the cryptography is to try to guess the message)
- The key can only be used once! How many bits should the key be?
- What if the two parties cannot meet to agree on a key?

# Quantum key distribution

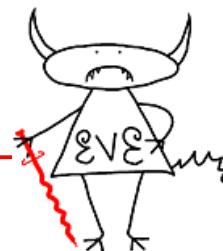
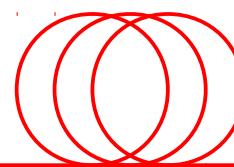
Alice



Bob

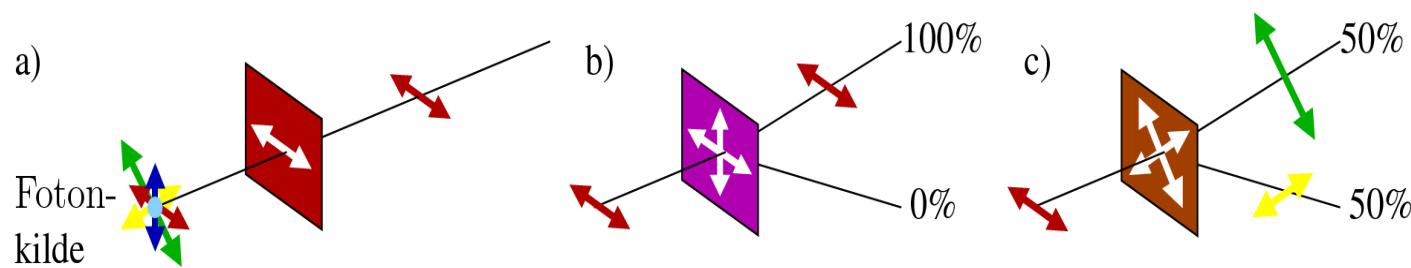
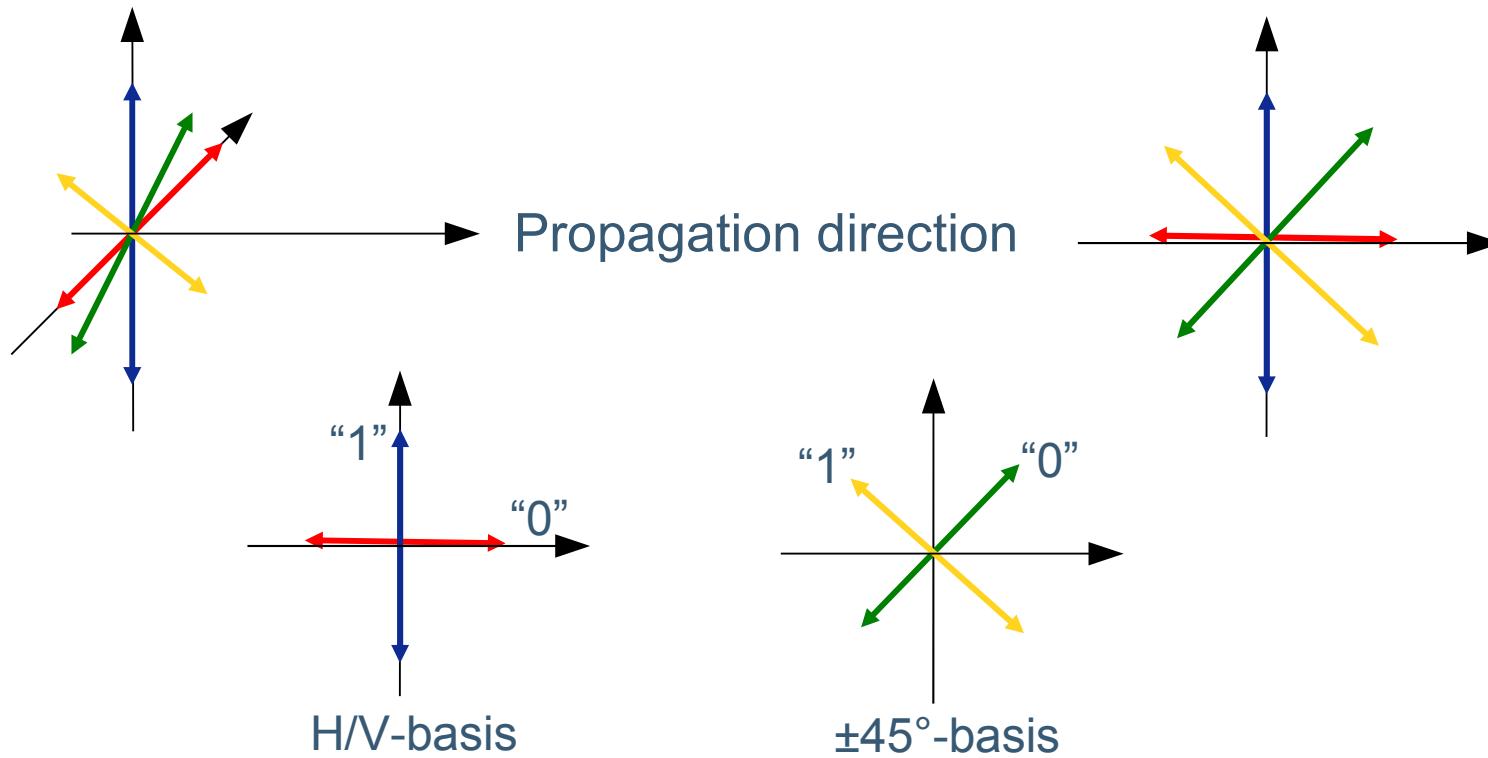


Optical fiber

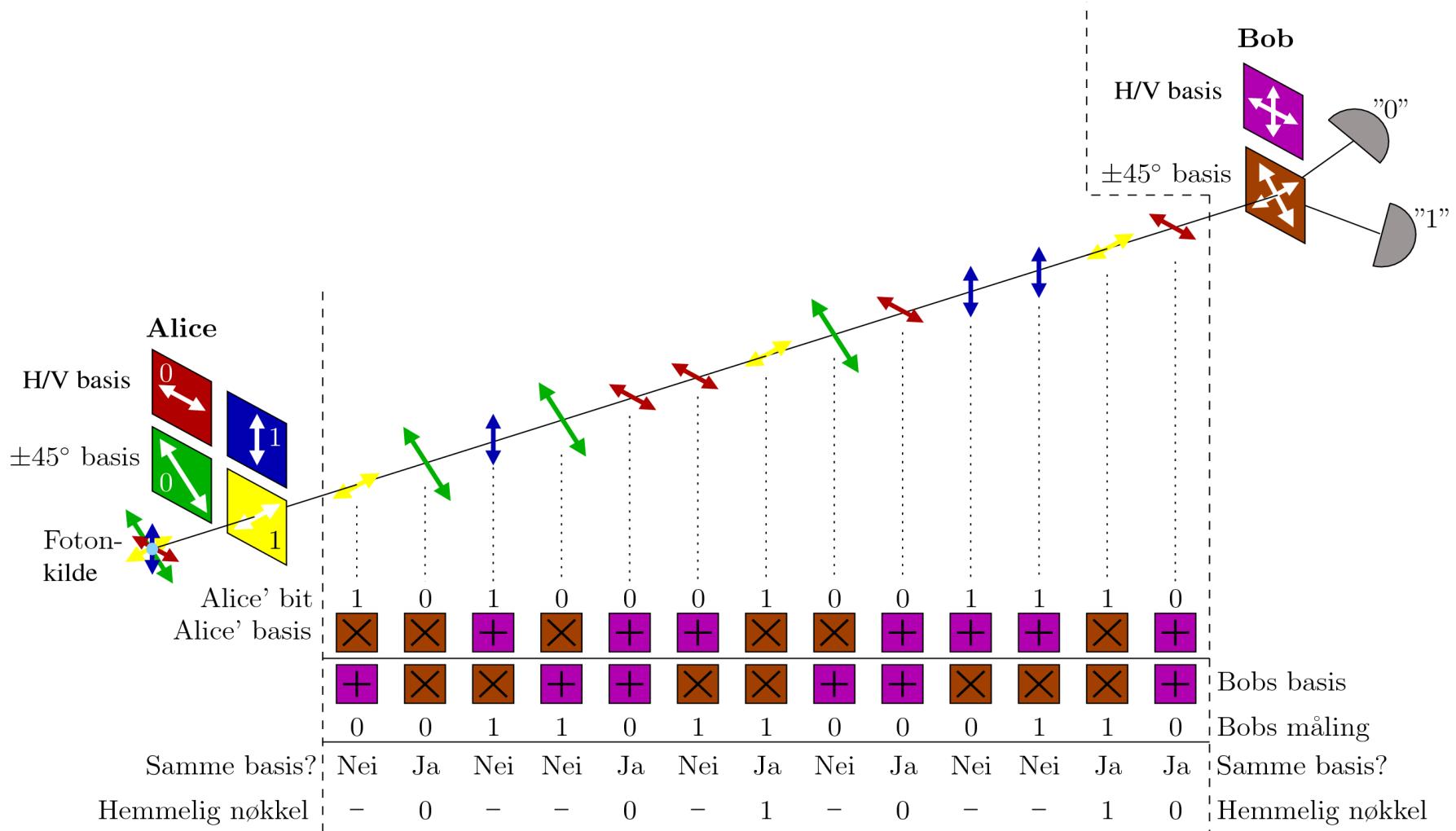


Internet (authenticated)

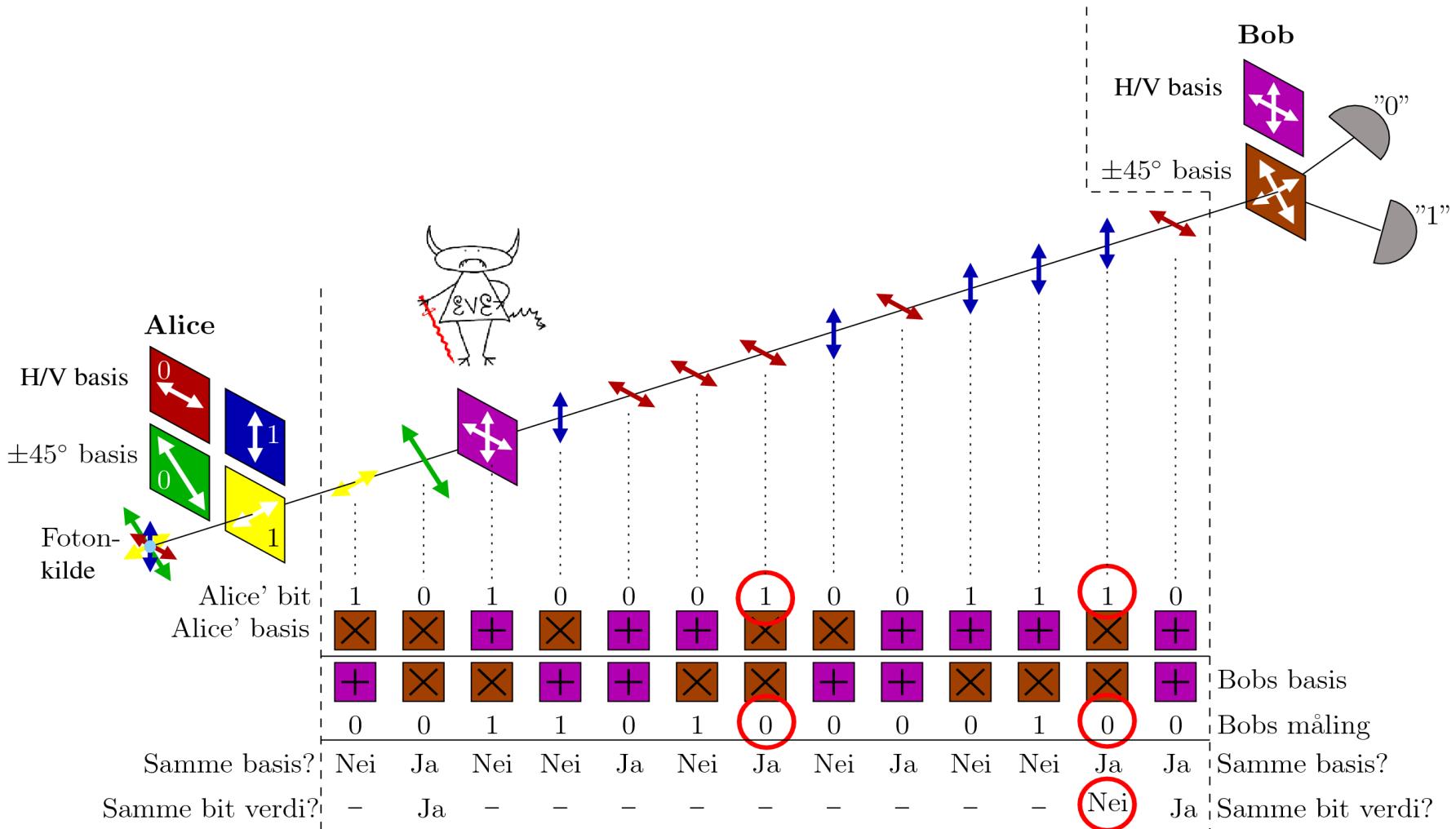
# Photons as quantum bits



# BB84



# What about Eve?



Eve causes 25% QBER  
(Quantum bit error rate)

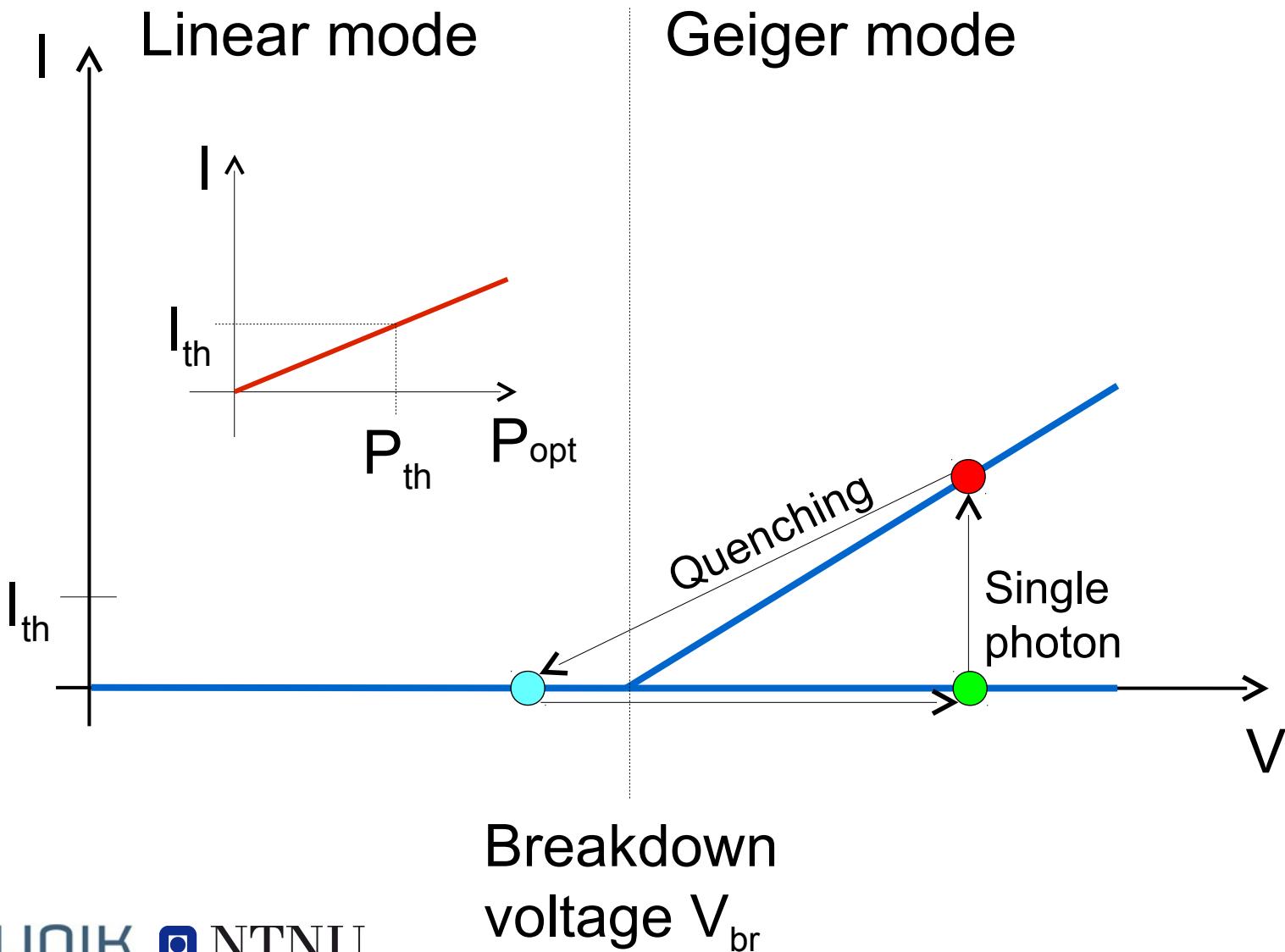
# How to hack the system?

- Secure with QBER < 11 % without imperfections
- What about imperfections?

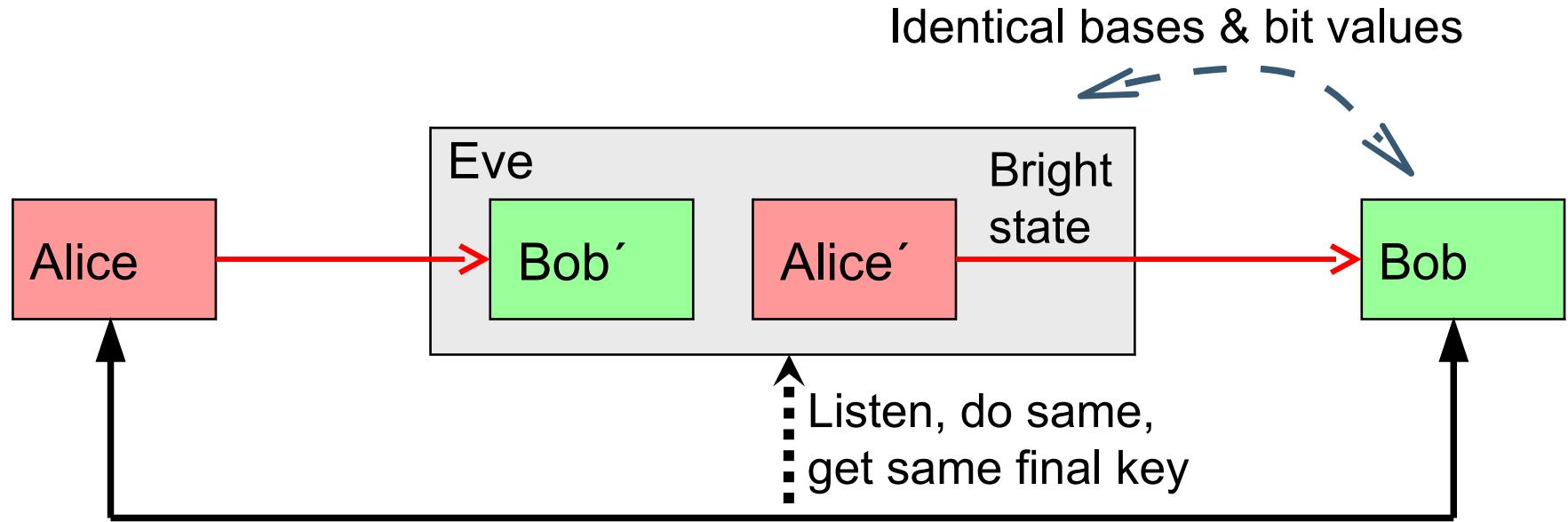
## Previous attempts:

- Cause a large QBER (i.e. 19.7%)
- Need equipment not available
- Gives only partial knowledge on the key

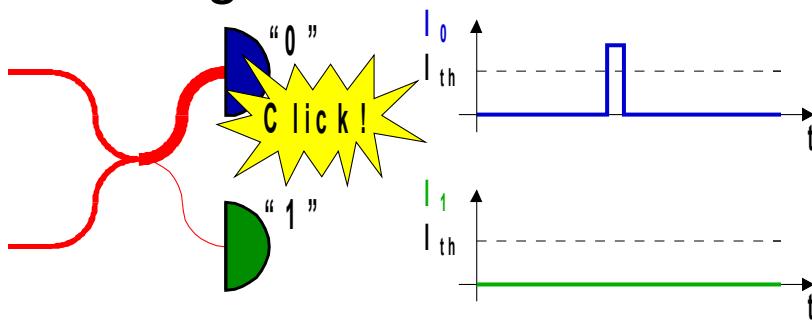
# How avalanche photo diodes (APDs) work



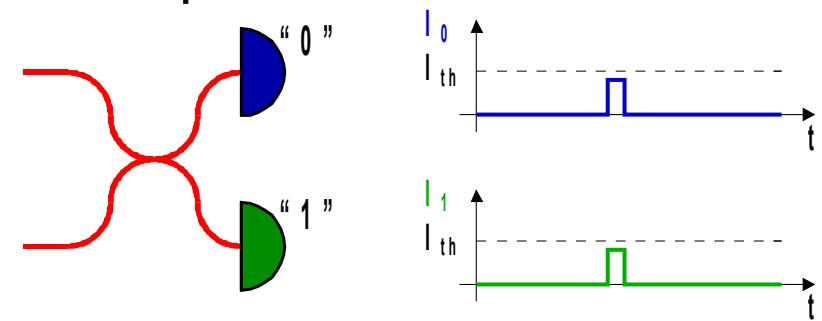
# Faked-state attack in APD linear mode



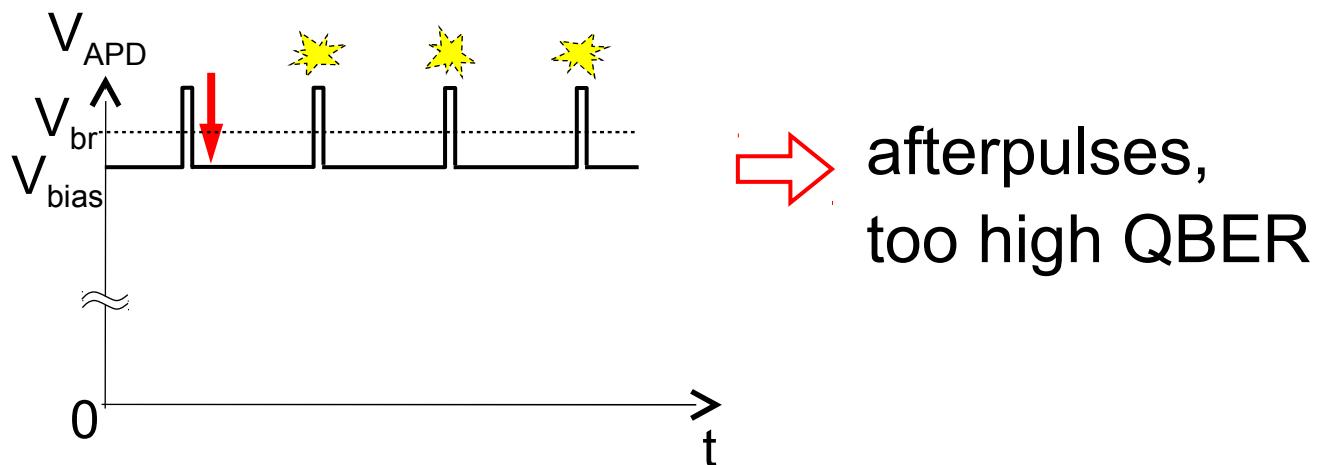
Matching basis:



Incompatible basis:



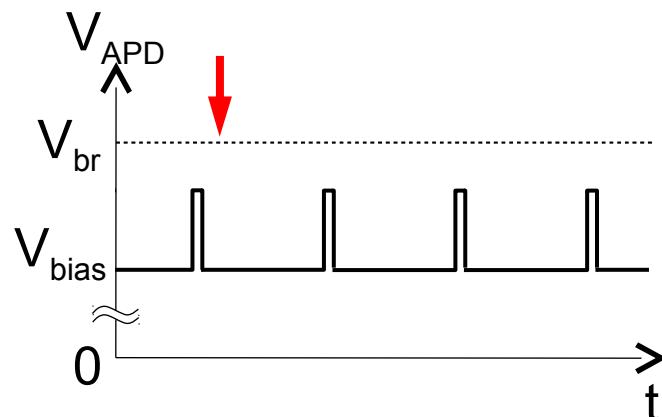
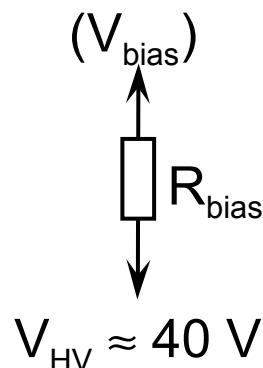
# Launching bright pulse after the gate...



afterpulses,  
too high QBER

Add CW light...

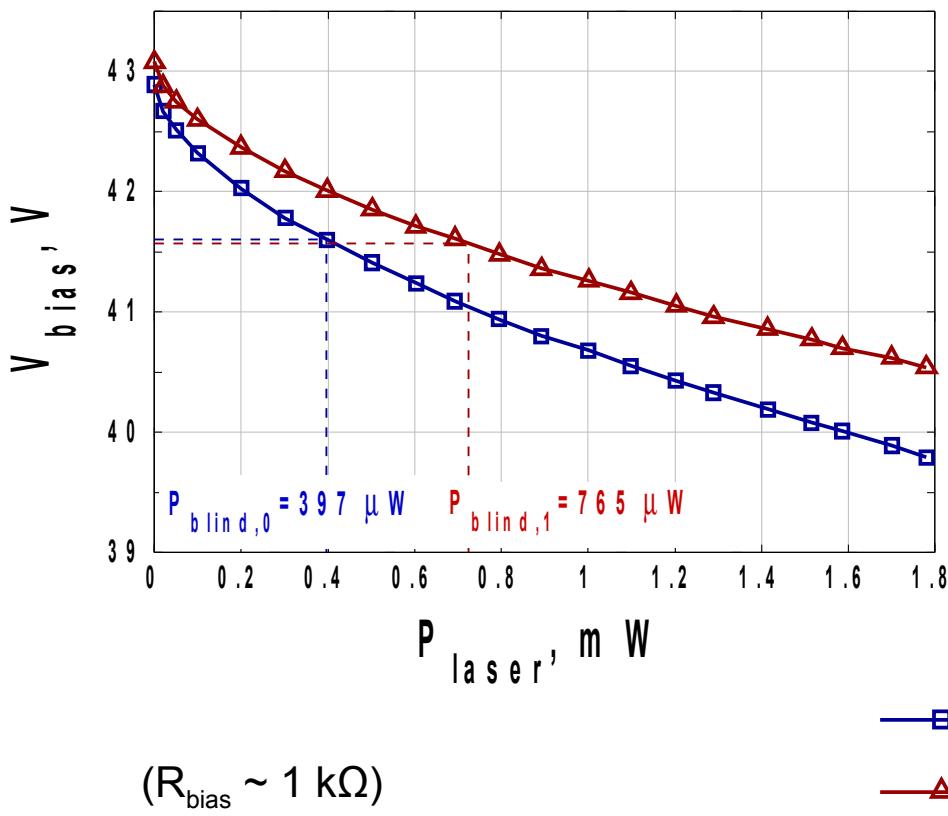
Bias to APD



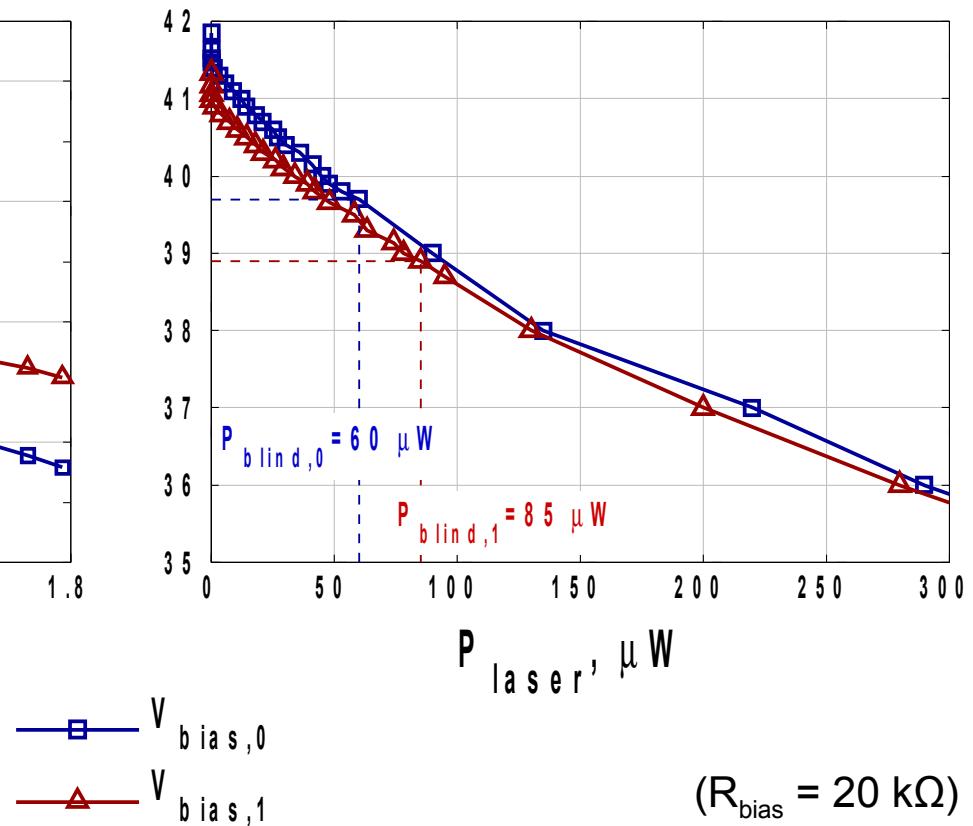
Detector blind!  
Zero dark count rate

# Detector blinding

ID Quantique  
Clavis2:

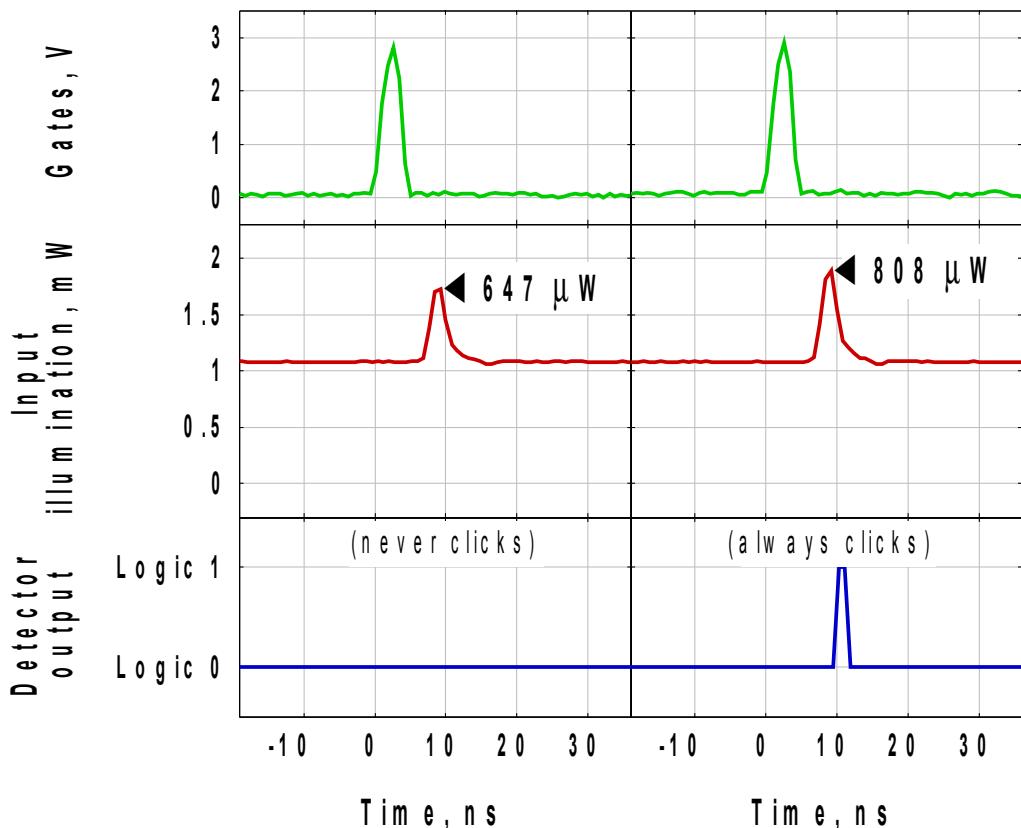


MagiQ Technologies  
QPN 5505:

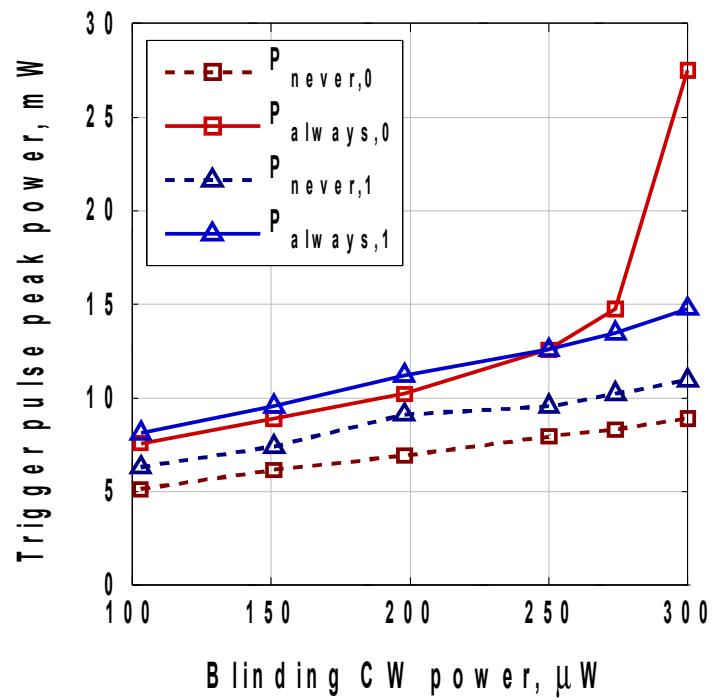


# Full detector control

ID Quantique  
Clavis2:



MagiQ Technologies  
QPN 5505:



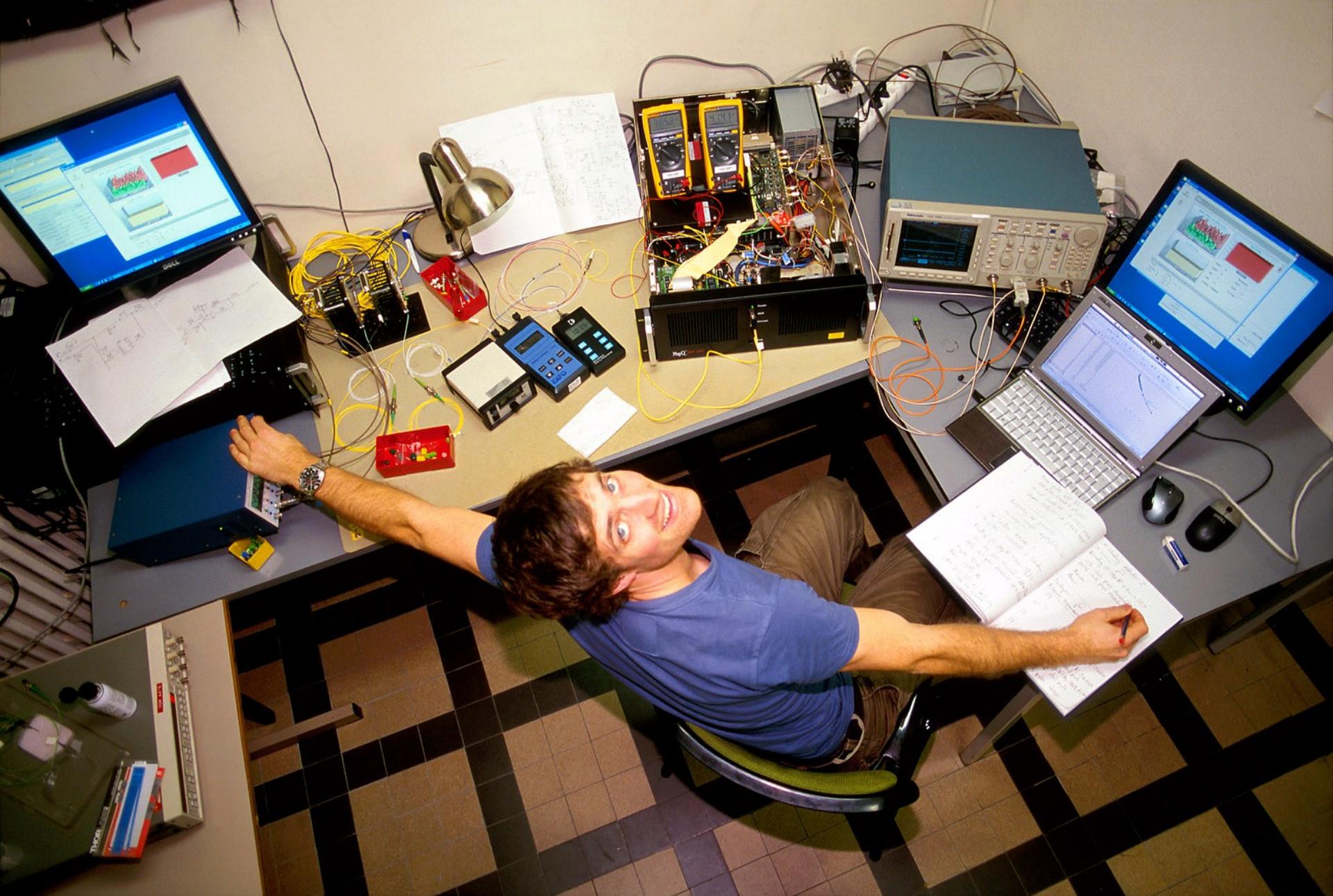
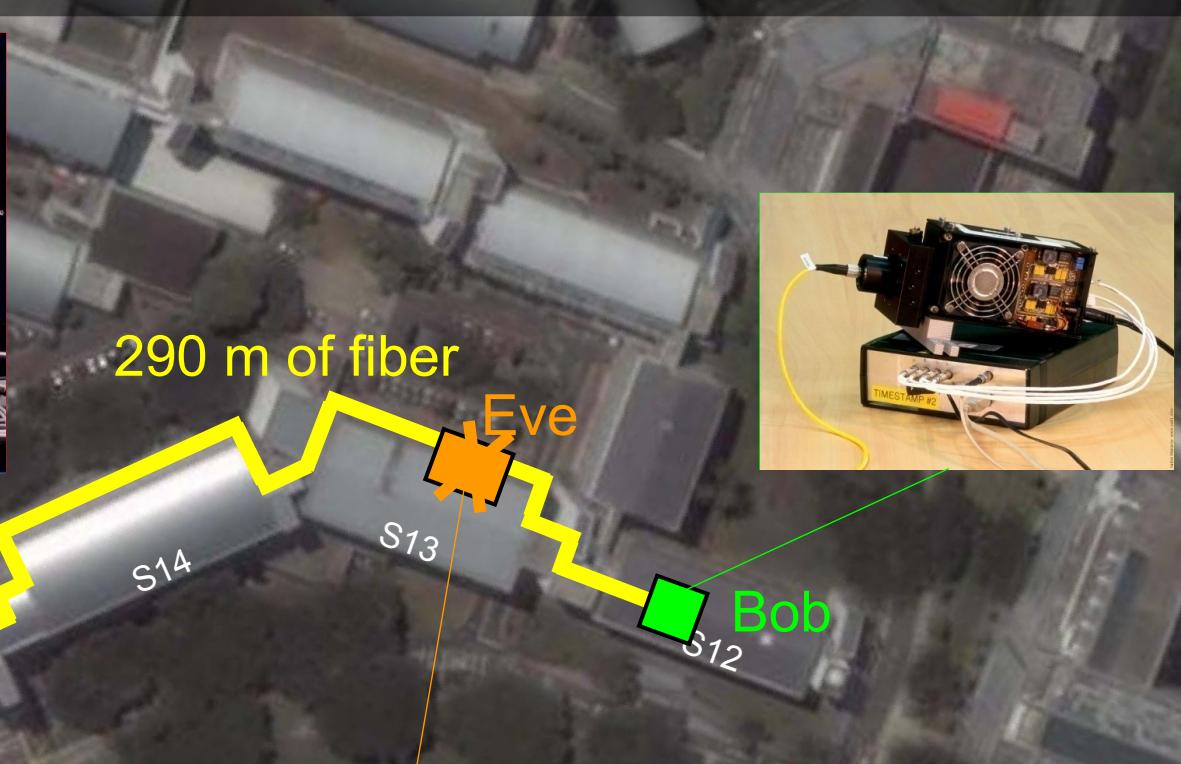
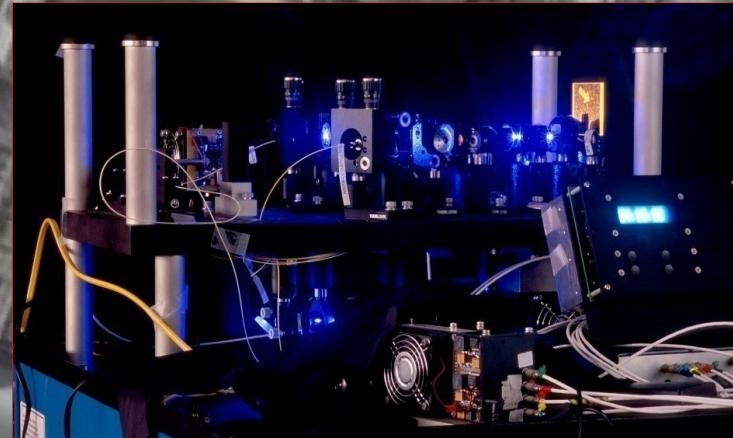


Photo ©2010 Vadim Makarov

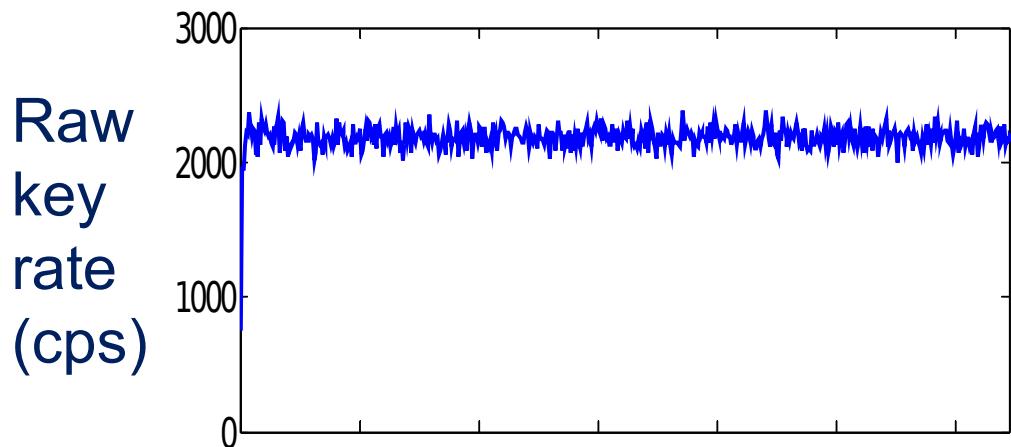
# Testing MagiQ Technologies QPN 5505

# Eavesdropping on installed QKD line on campus of the National University of Singapore

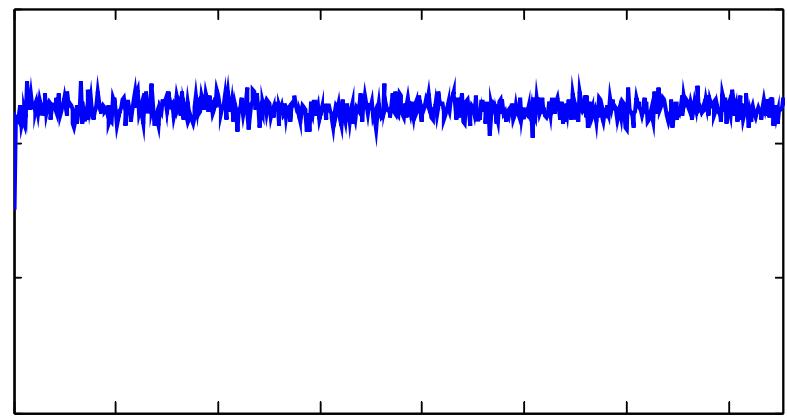


# Eve does not affect QKD performance

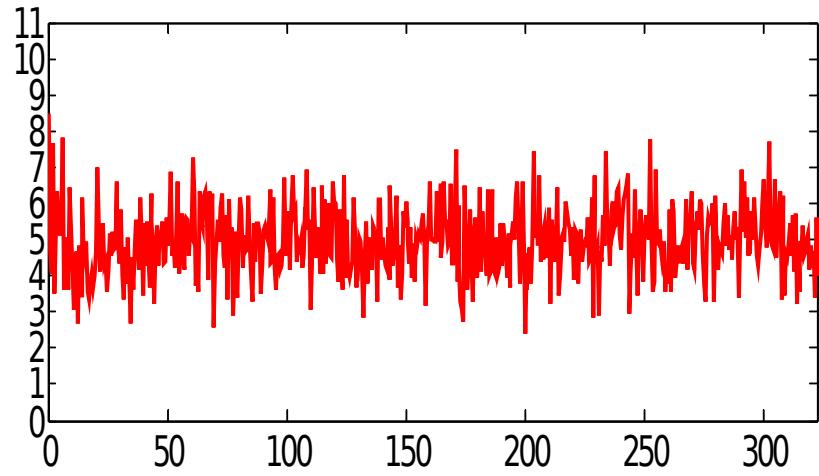
Before attack:



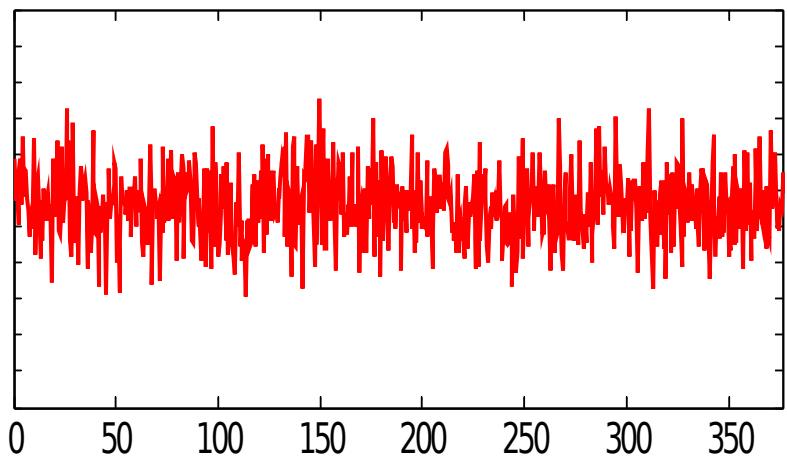
During attack:



QBER  
(%)



Time (s)



Time (s)

# Stages of secure technology

1. Idea / proof-of-the-principle

Quantum  
cryptography

1970–1993

2. Initial implementations

1994–2005

3. Weeding out implementation  
loopholes

(spectacular failures  patching)

◀ Now!

4. Good for wide use

# Summary



- Two commercial QKD systems fully cracked via demonstrating detector controllability
- Full attack demonstrated on a research QKD system under realistic conditions on installed line
- Vulnerabilities disclosed to vendors *responsibly*