Seminar at AlbaNova University Center, Stockholm, October 23, 2008

Eve strikes back:* attacks exploiting component imperfections

Vadim Makarov

NTNU
Det skapende universitet

*Title idea ©Claude Crépeau

Quantum cryptography timeline

ca. **1970** Concept ("money physically impossible to counterfeit")

1984 First key distribution protocol (BB84)

1989 Proof-of-the-principle experiment

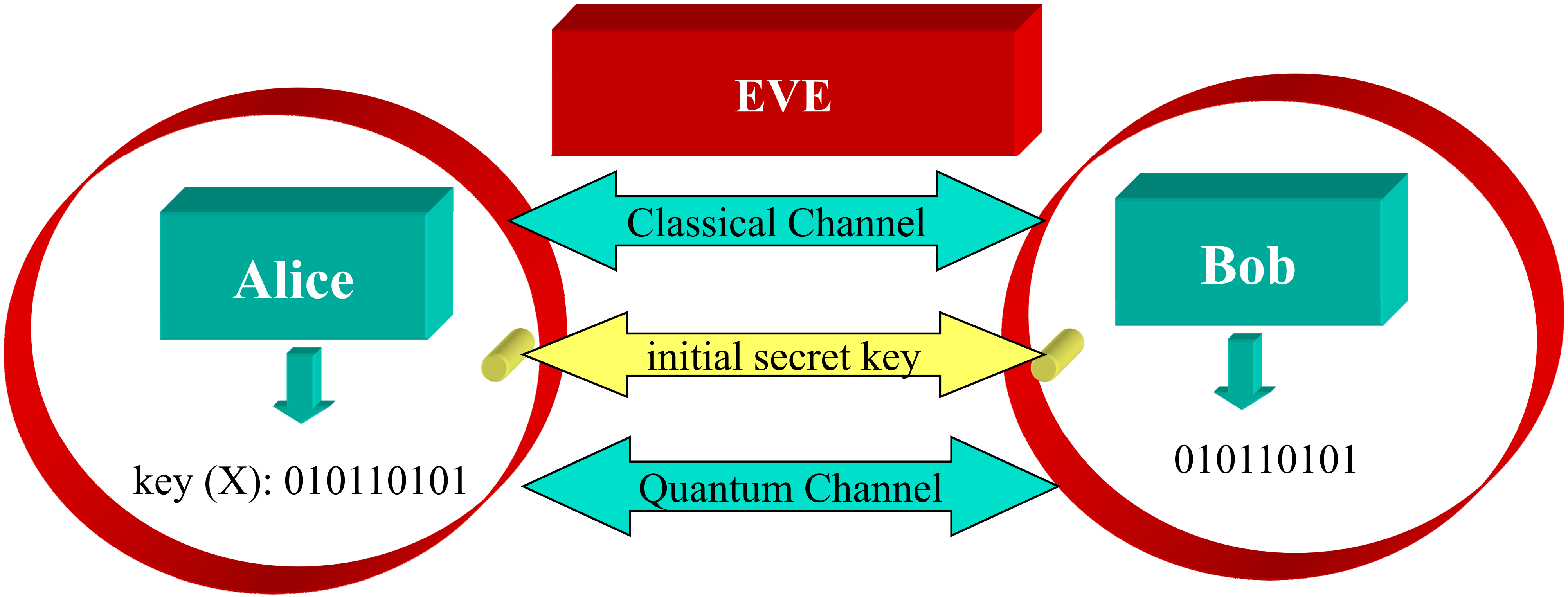
1993 Key transmission over fiber optic link

2004 First commercial offers (20~50 km fiber links)

2007 200 km in fiber, 144 km free-space demonstrated

... Market? And, what's the *real* level of security?

Our friend, Eve …

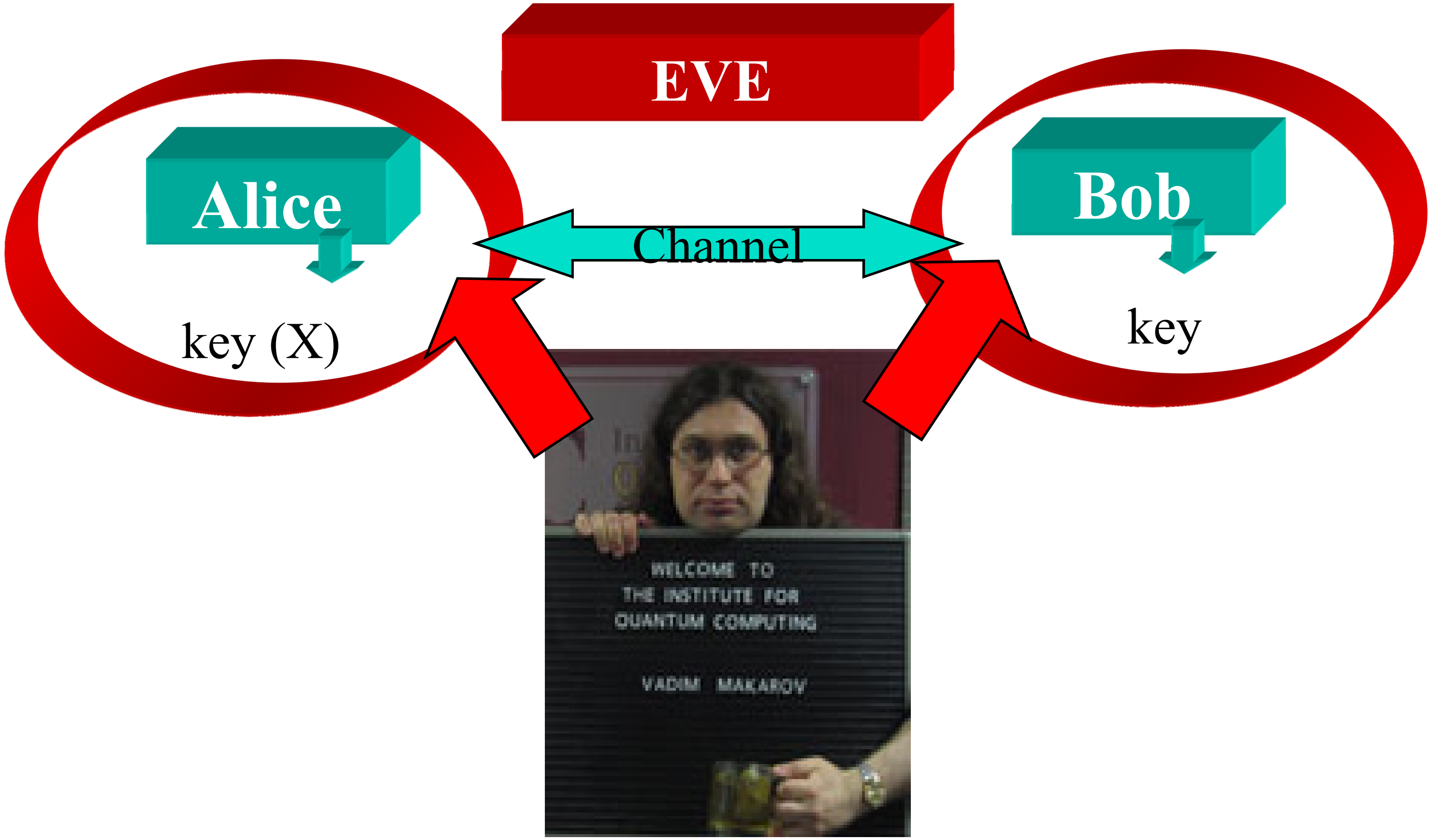


Alice and Bob's devices
- shielded from Eve
- work according to specification

Eve retired (Florida)

Slide courtesy Norbert Lütkenhaus

Not so friendly …



What Vadim does:

- find deviations of devices from model assumptions
- actively intrude devices via optical fibers!
- manipulate devices (blind, burn detectors)

Vadim’s complices: Hoi-Kwong Lo, Antia Lamas-Linares, Christian Kurtsiefer

Eve strikes back!

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

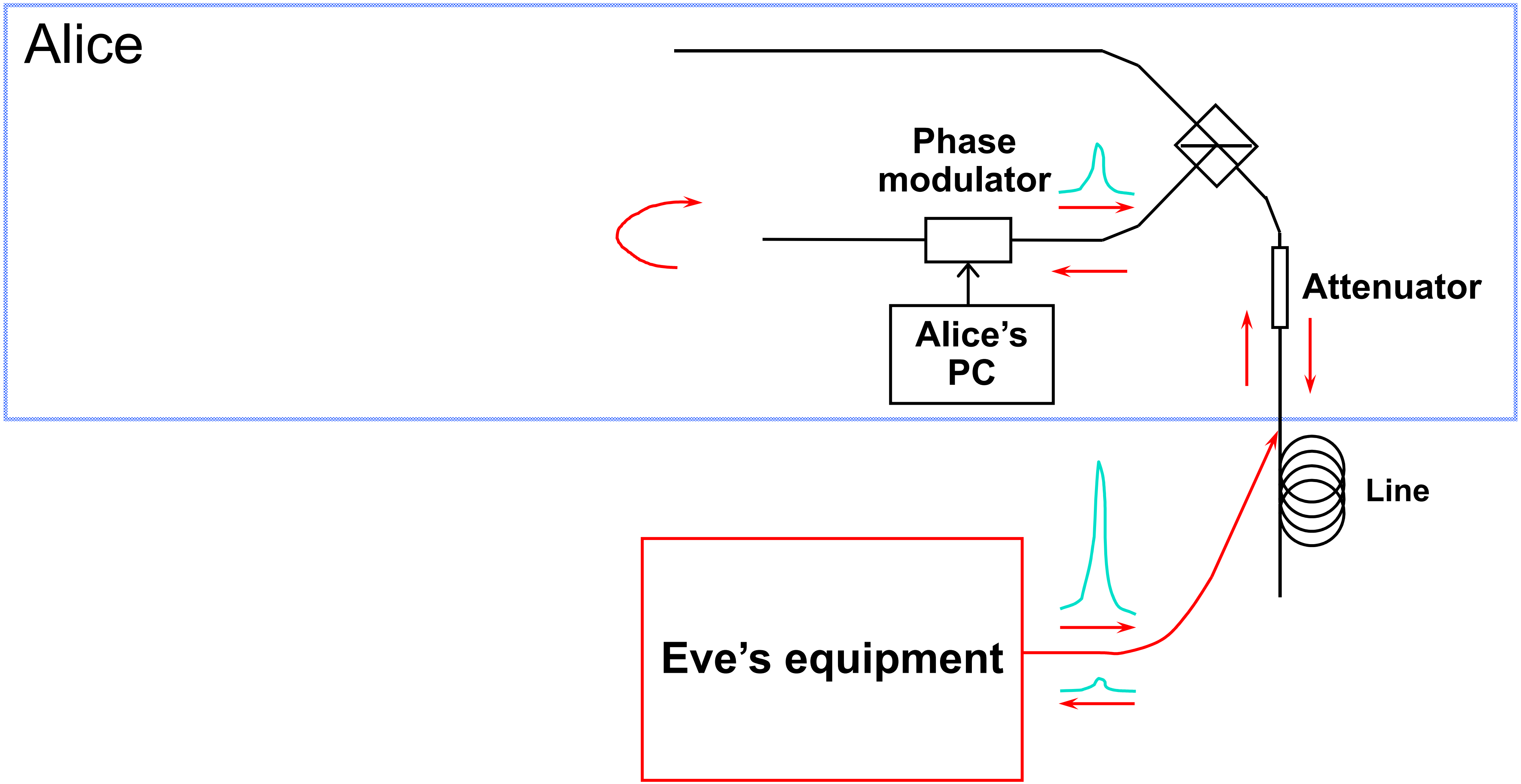
Stealing an idea from Claude Crepeau's slides in a CIAR meeting

Slide courtesy Hoi-Kwong Lo

Loopholes

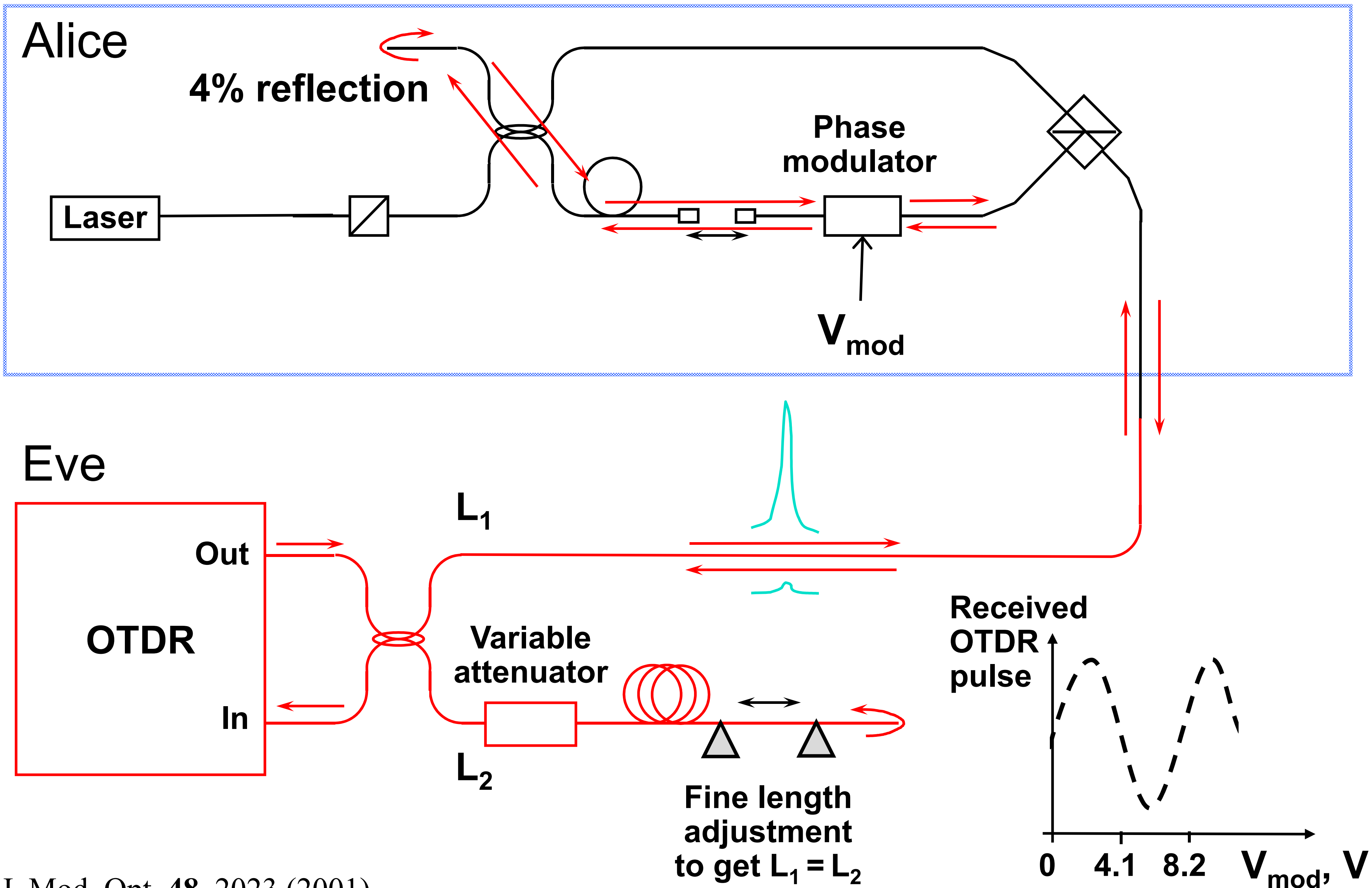
- **Large pulse attack**
- **Detector efficiency mismatch**
- **Control of passively-quenched detectors**
- **Control of PerkinElmer actively-quenched detector**

Large pulse attack

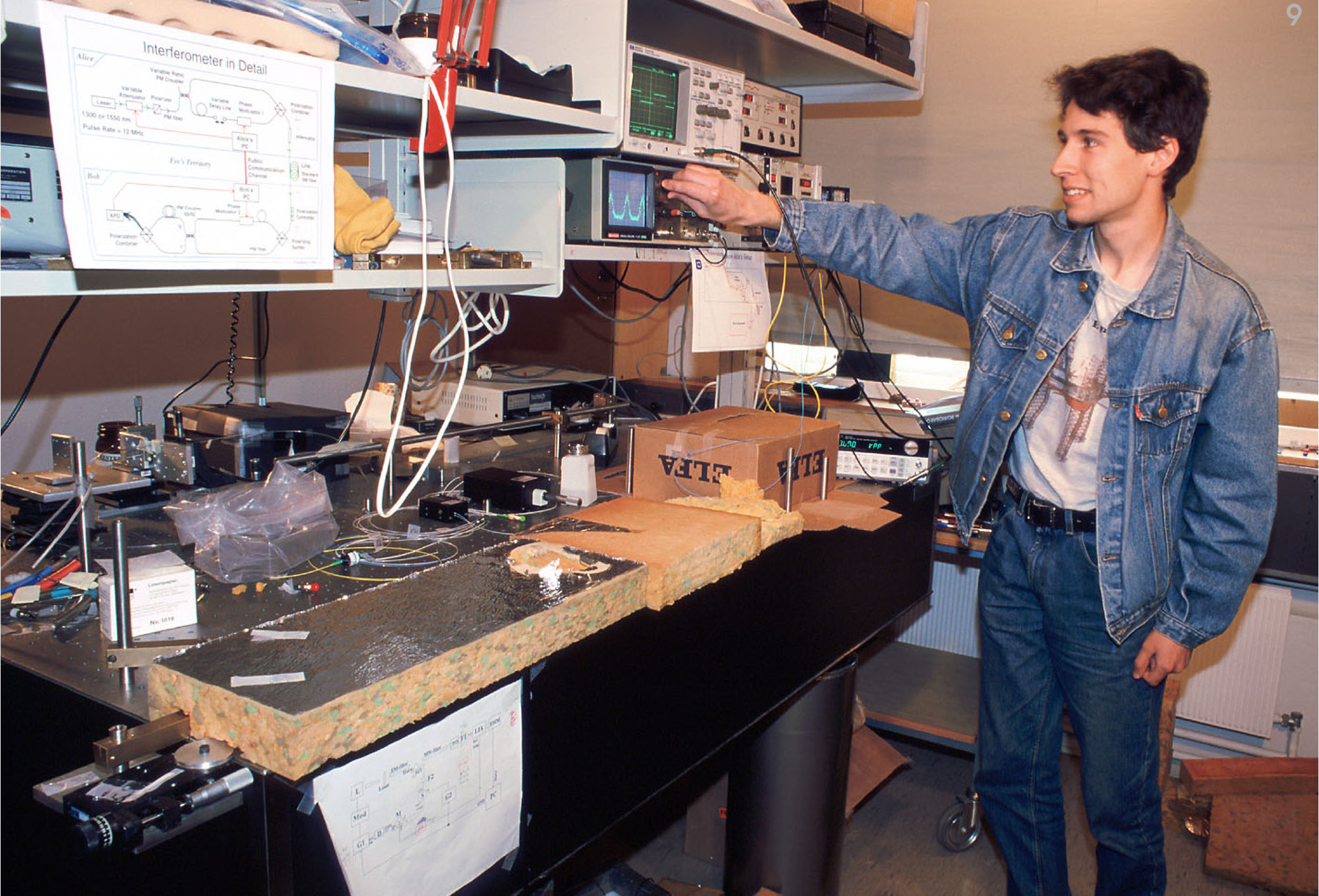


– interrogating Alice's phase modulator with powerful external pulses (can give Eve bit values directly)

Large pulse attack experiment

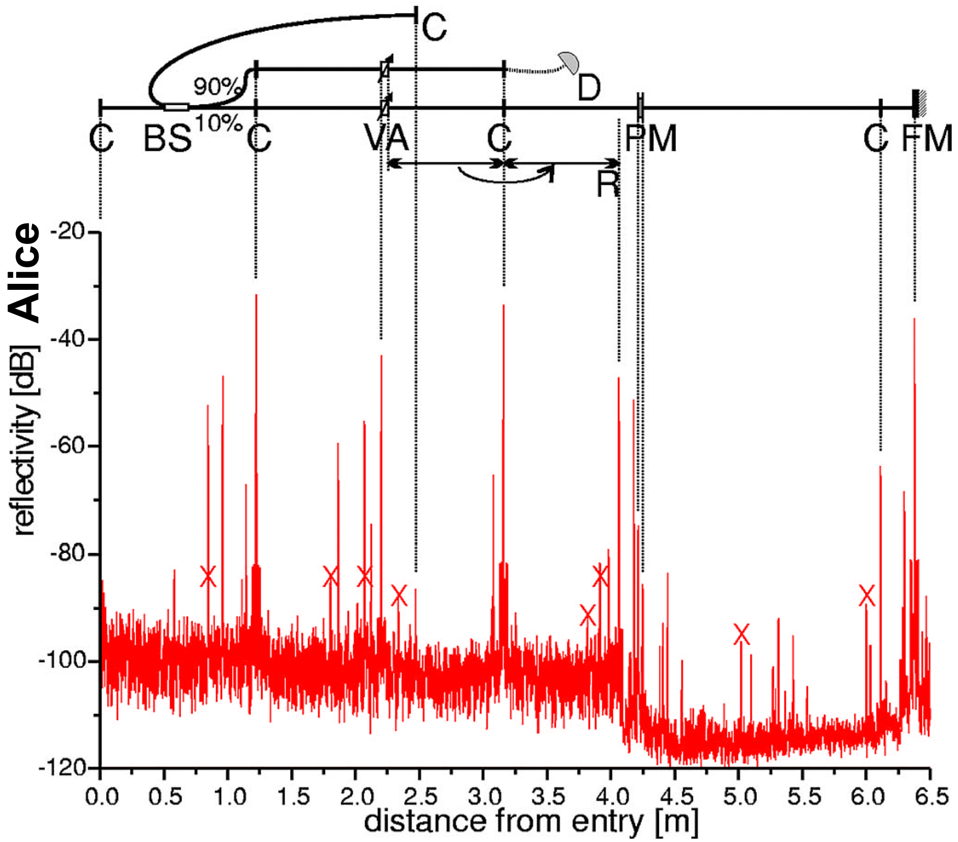


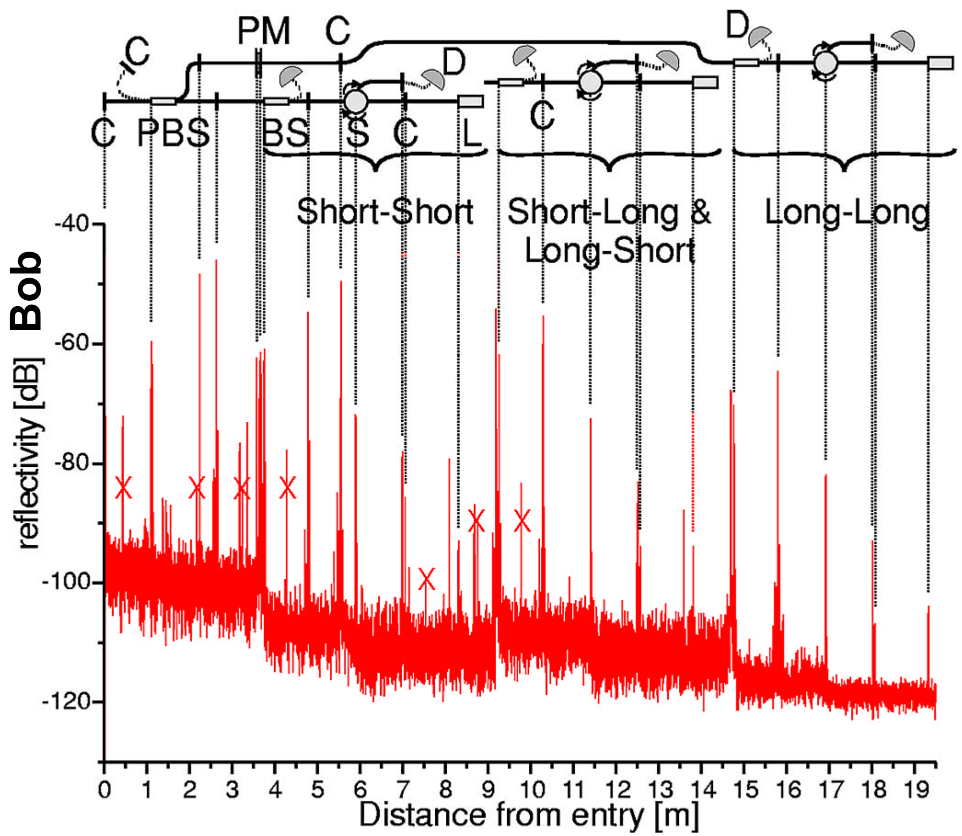
J. Mod. Opt. **48**, 2023 (2001)

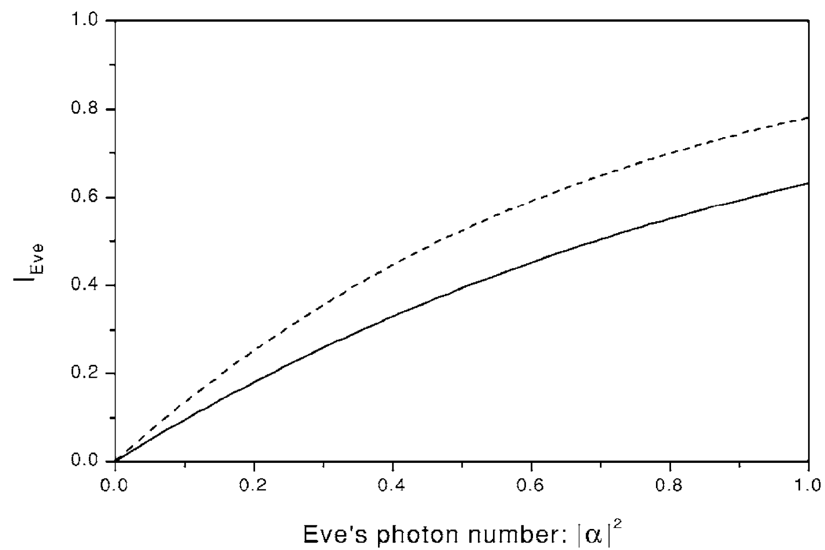


Artem Vakhitov tunes up Eve's setup

Example: plug-and-play system





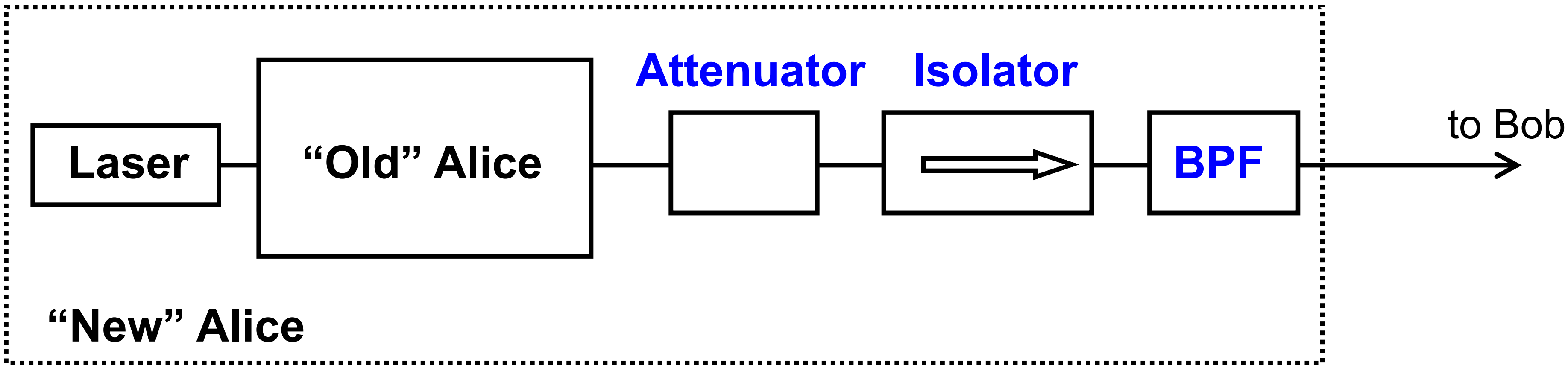


N. Gisin *et al.,* Phys. Rev. A **73**, 022320 (2006)

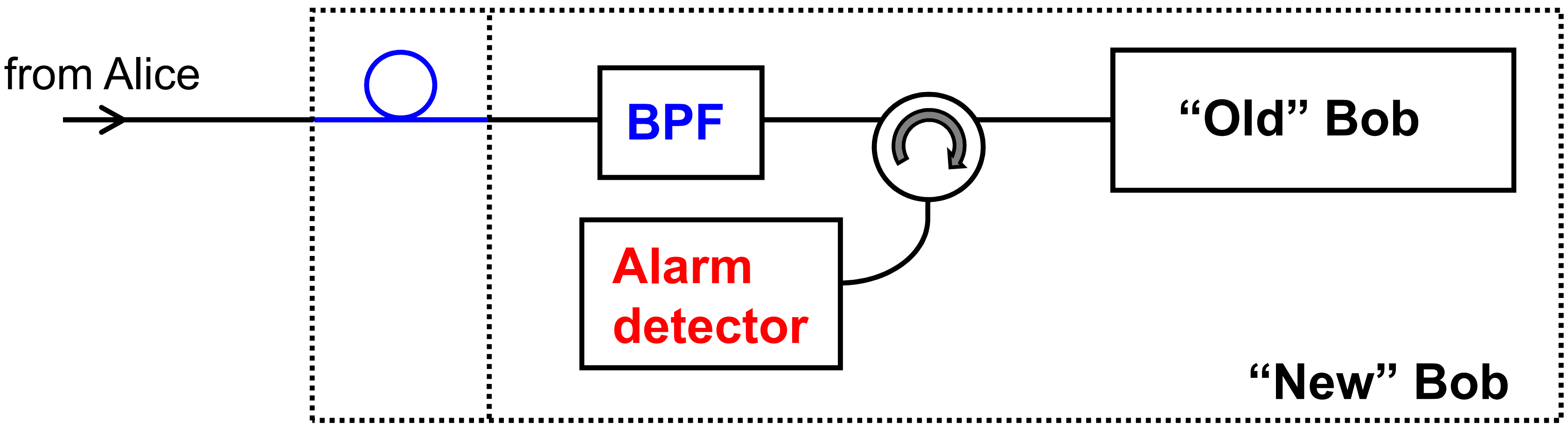
Protection against large pulse attack

1. Don’t use modulators

2. Passive (attenuator+isolator)

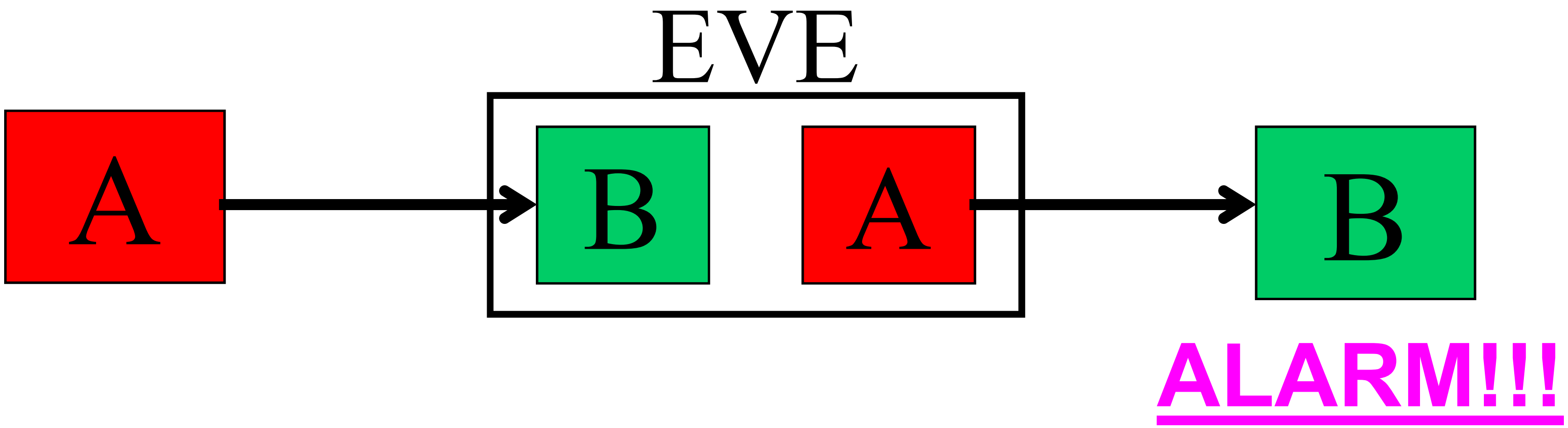


3. Active (detector)

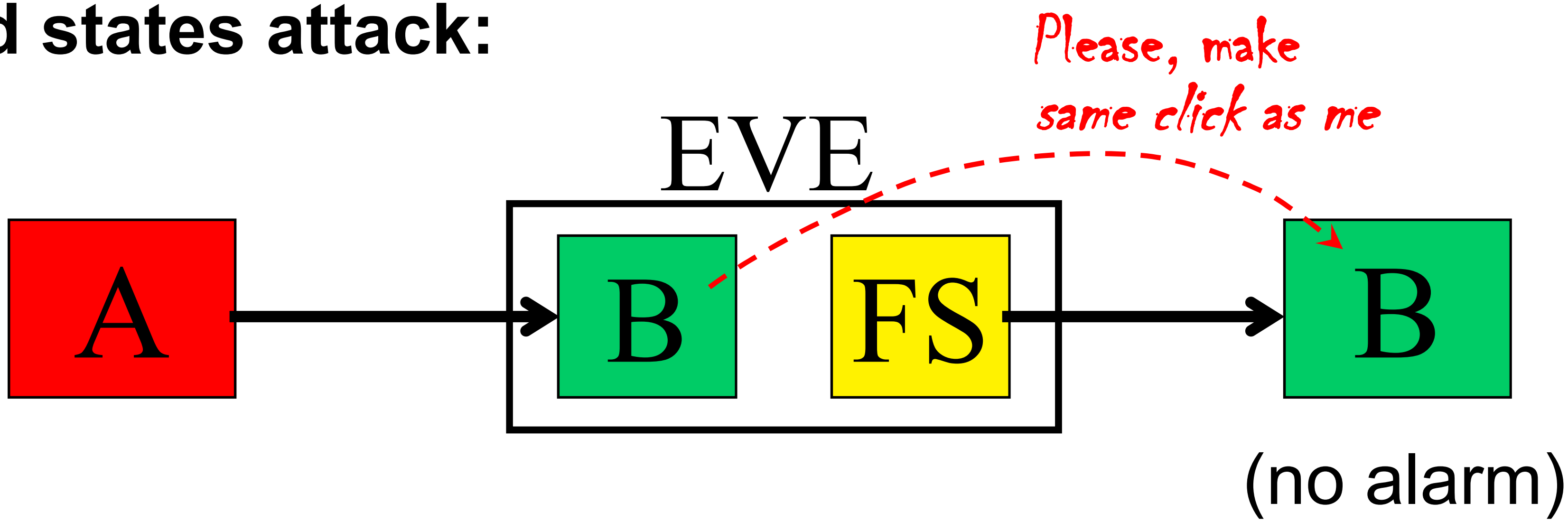


Faked states attack

Conventional intercept-resend:



Faked states attack:

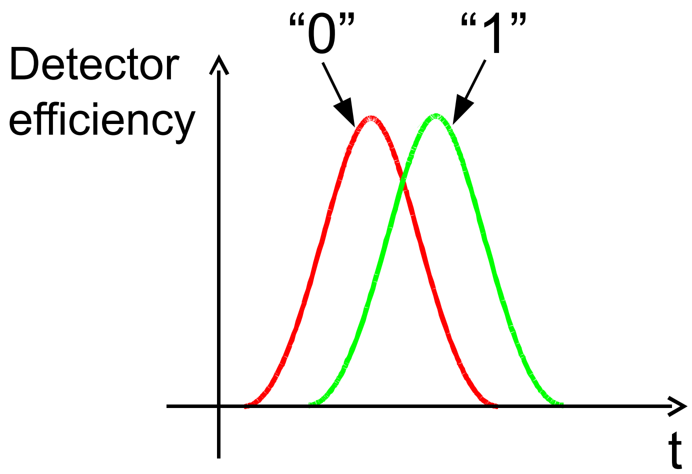


J. Mod. Opt. **52**, 691 (2005)

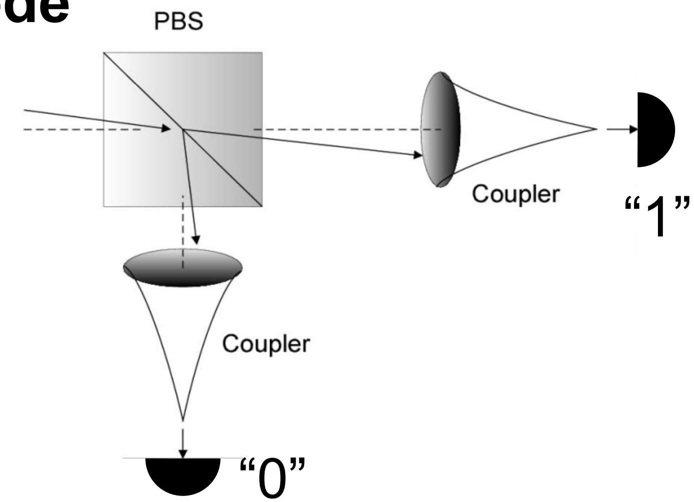
Detector efficiency mismatch

- **Most quantum cryptosystems need at least two detectors.**
- **Efficiency of detectors depends on external parameters and is *different* for two detectors, due to finite manufacturing and alignment precision.**
- External control parameters:

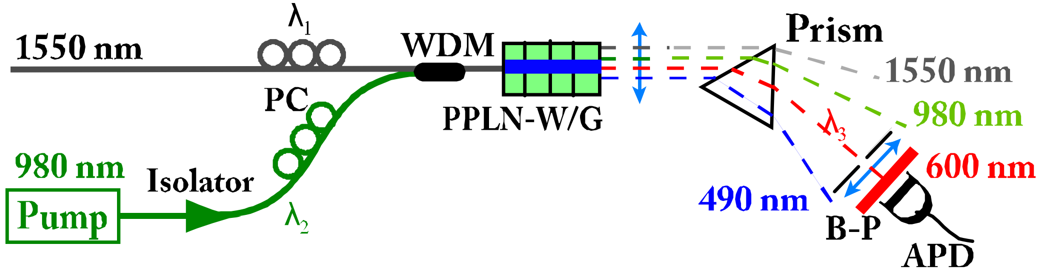
Timing



Spatial mode

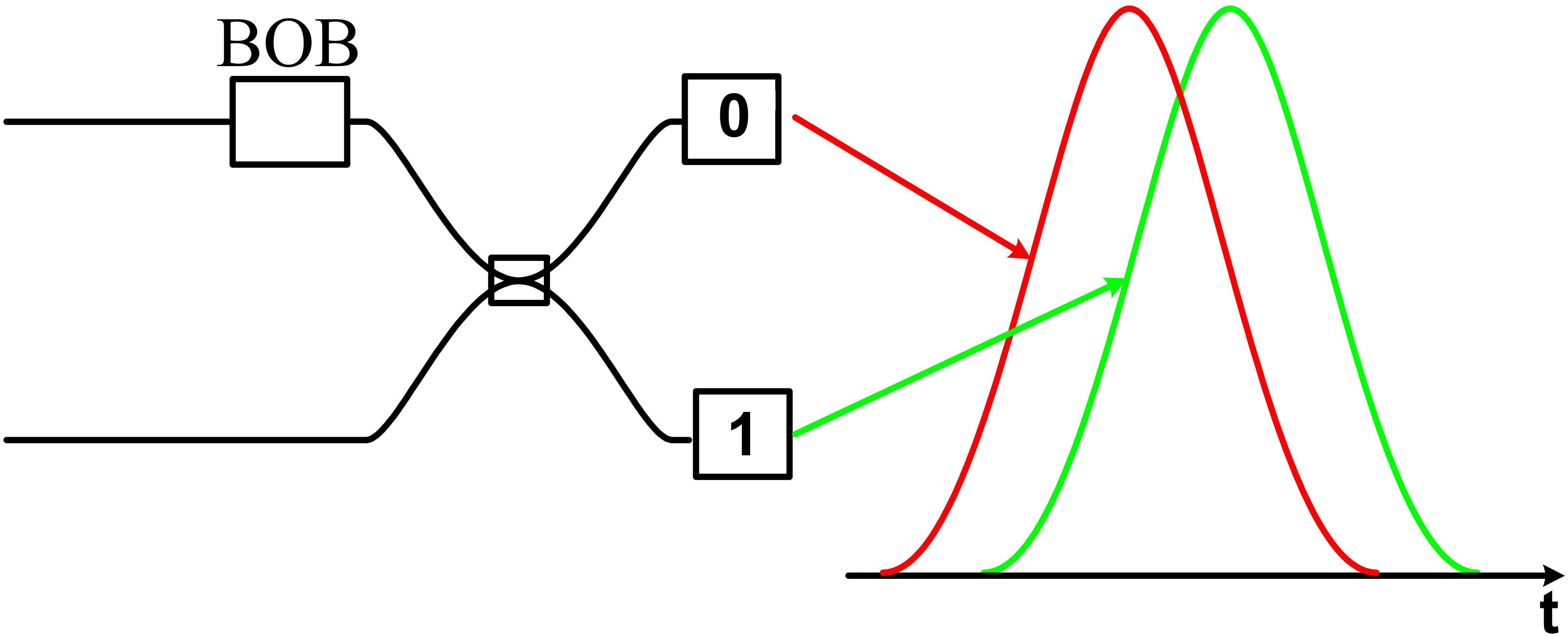


Wavelength



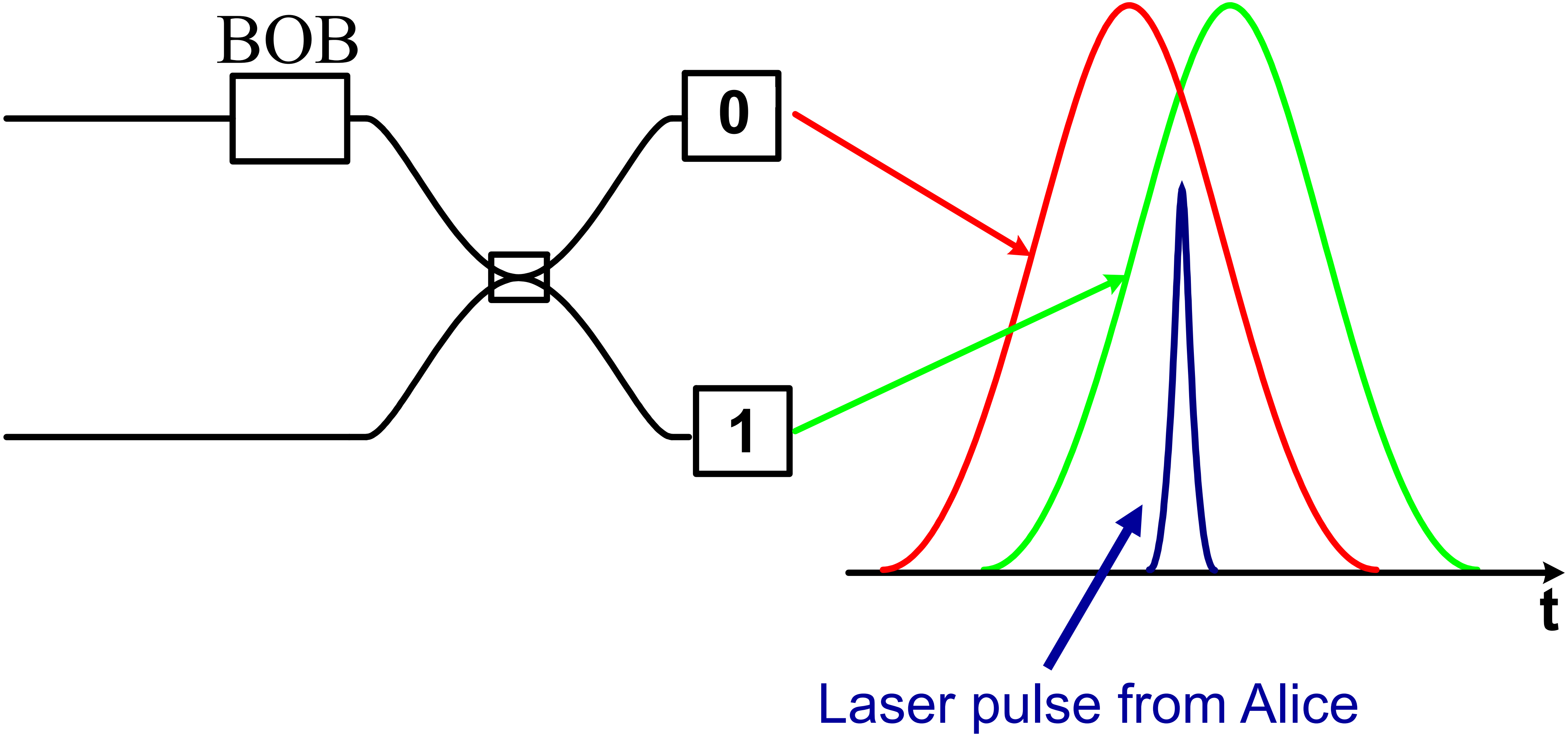
Polarization

Possible attack



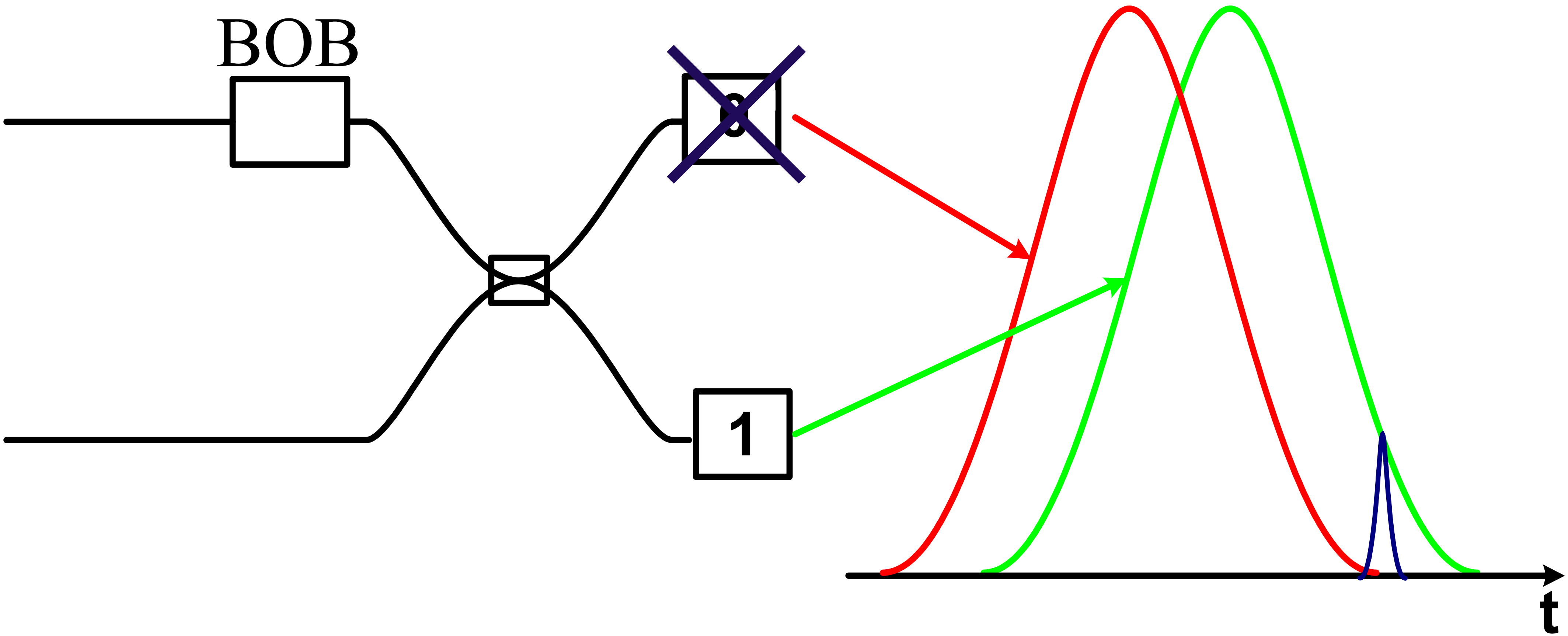
Phys. Rev. A **74**, 022313 (2006)

Possible attack



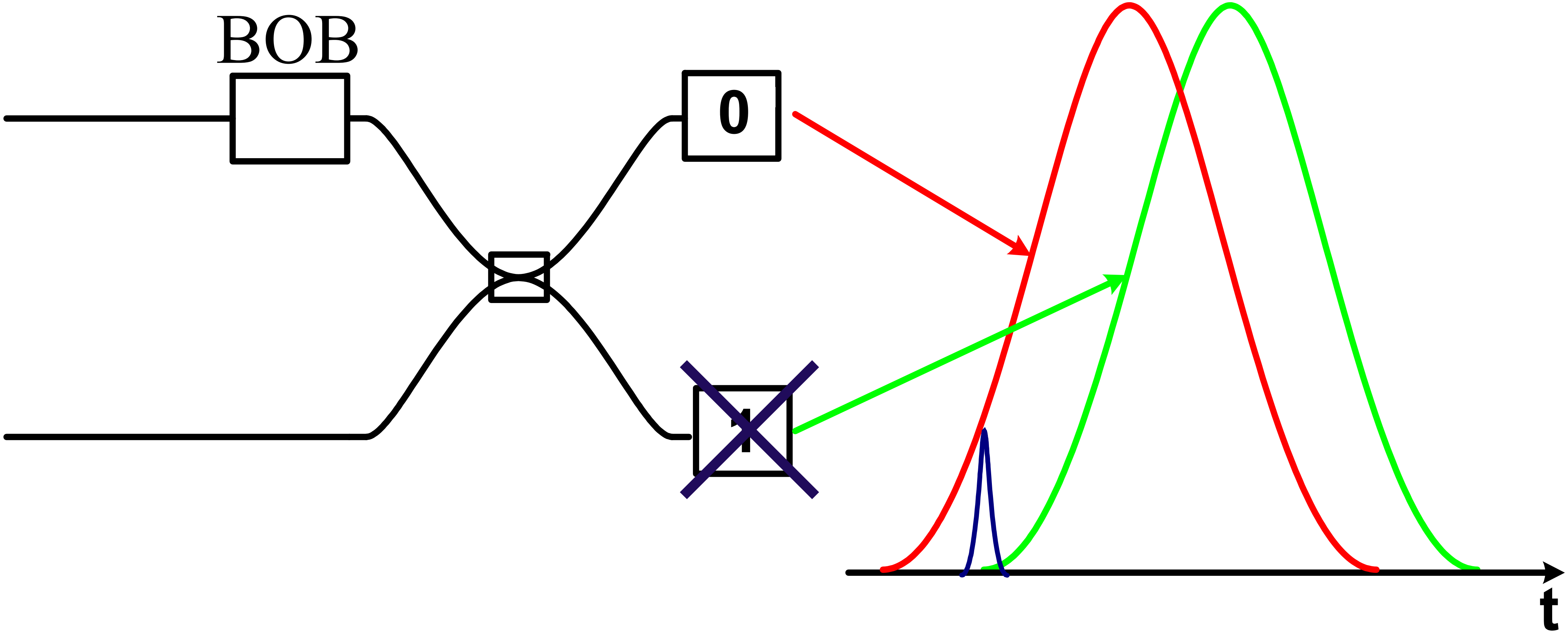
Phys. Rev. A **74**, 022313 (2006)

Possible attack



Phys. Rev. A **74**, 022313 (2006)

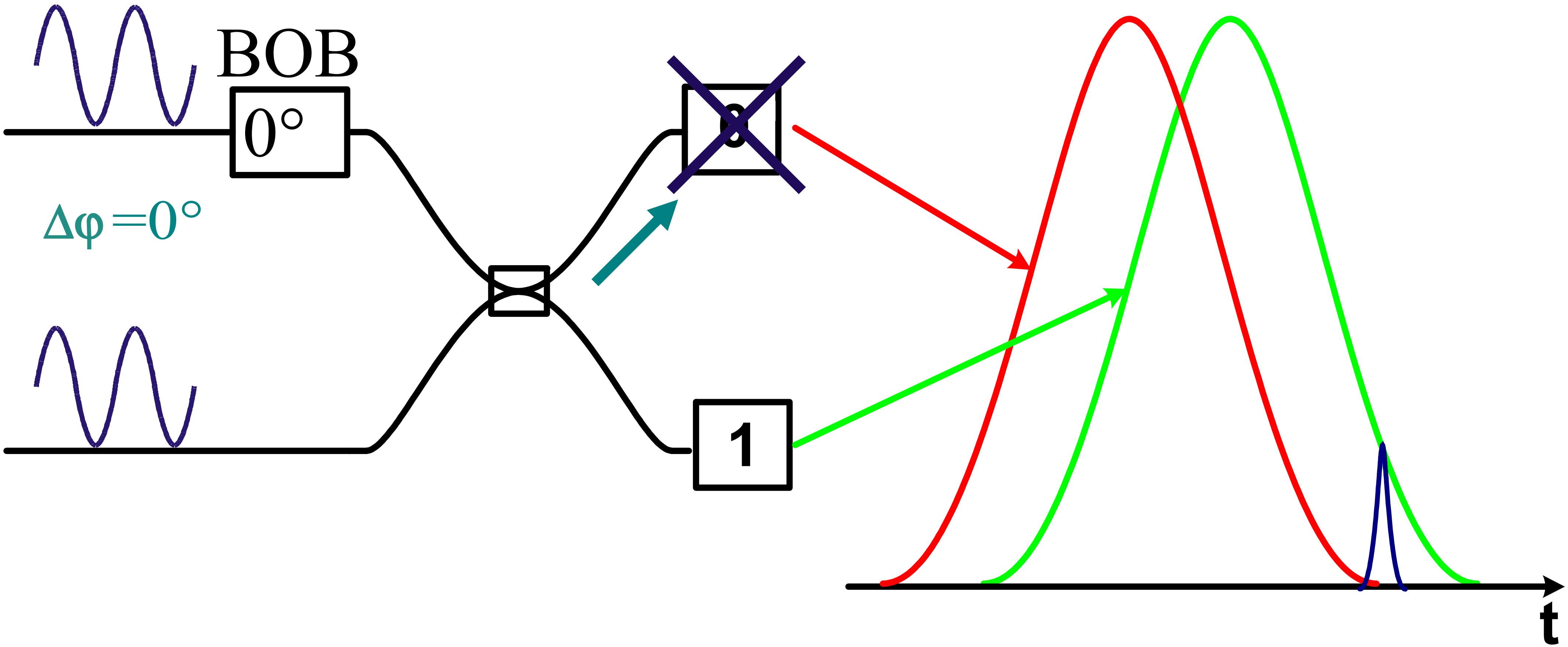
Possible attack



Phys. Rev. A **74**, 022313 (2006)

Possible attack

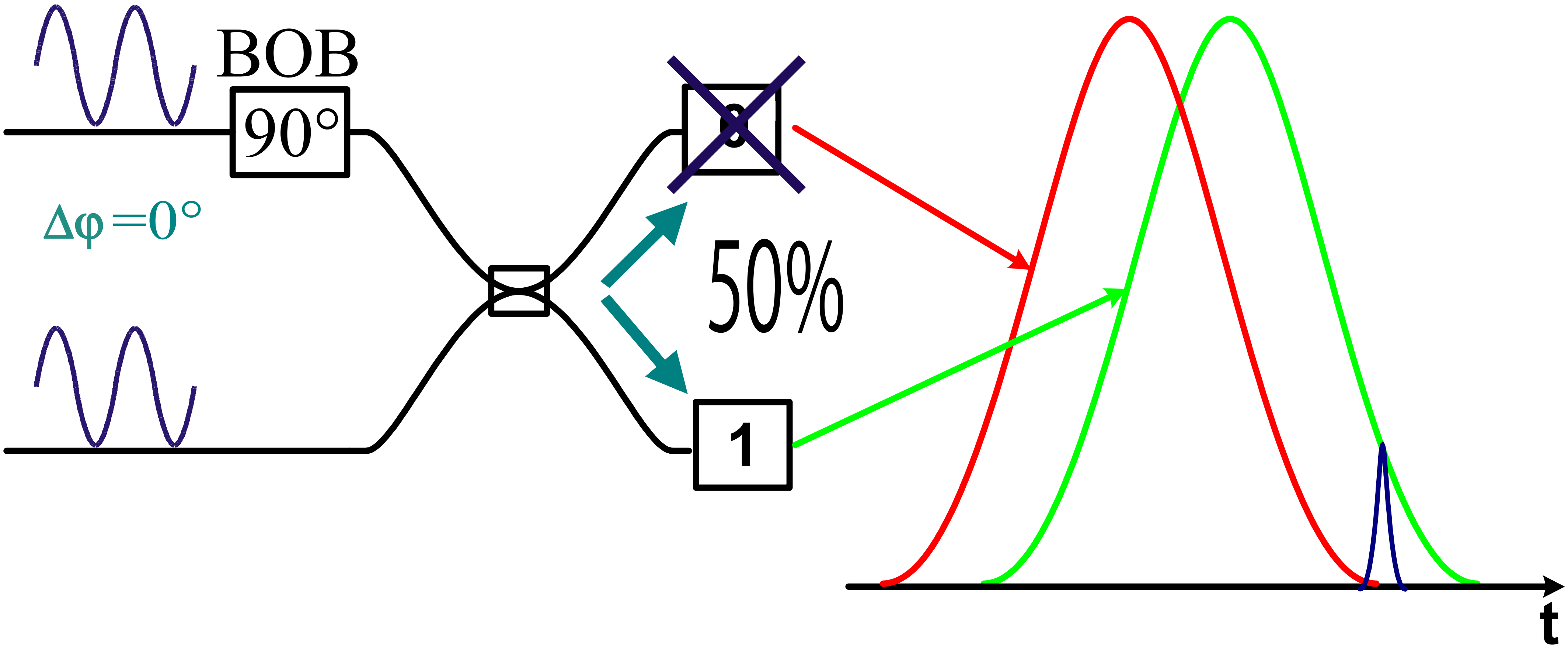
Example: Eve measured with basis Z (90°), obtained bit 1



(Eve resends the opposite bit 0 in the opposite basis X, shifted in time)

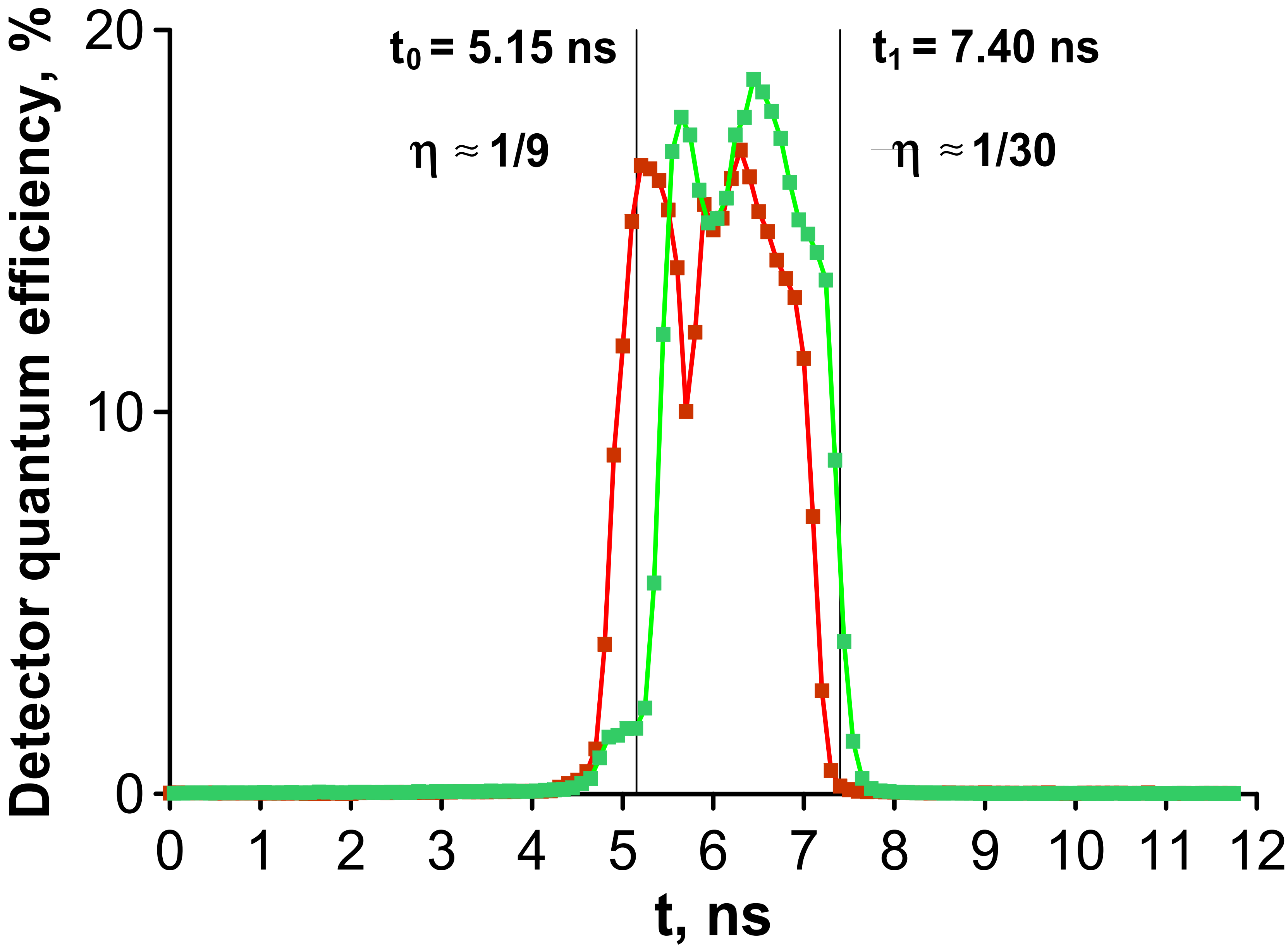
Possible attack

Example: Eve measured with basis Z (90°), obtained bit 1

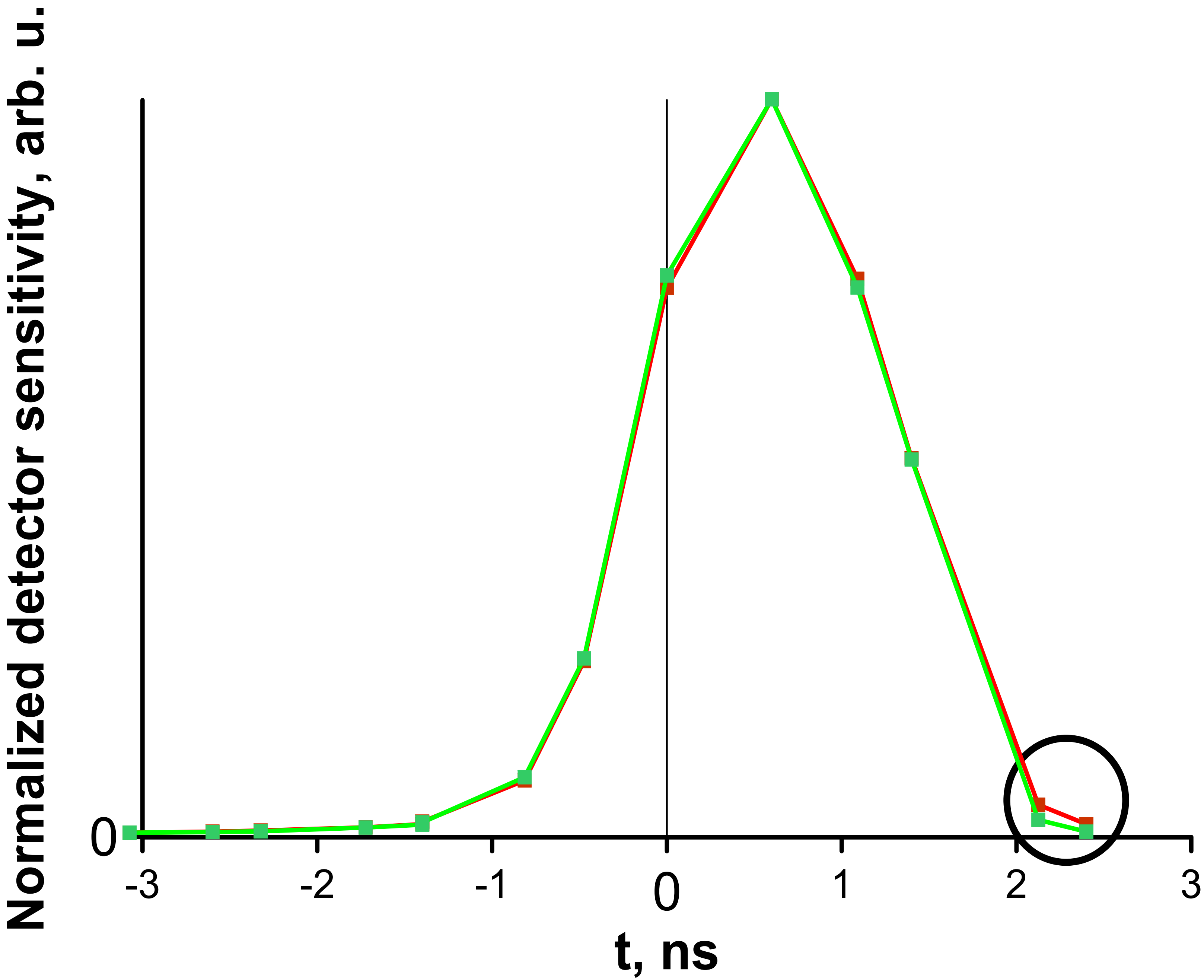


- ✓ Eve's attack is not detected
- ✓ Eve obtains 100% information of the key

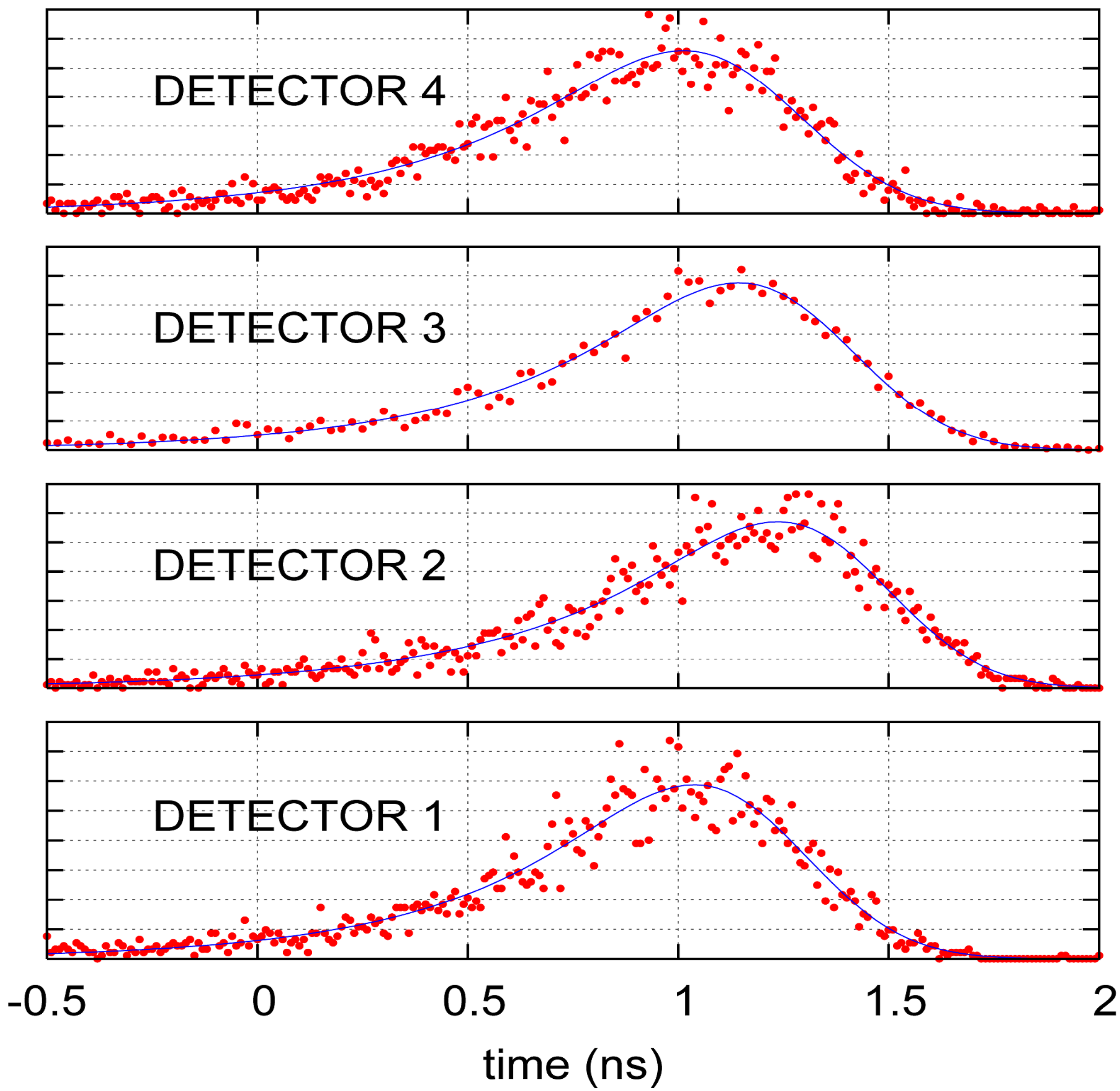
Example: pair of detectors for QKD



Example: time-multiplexed detector

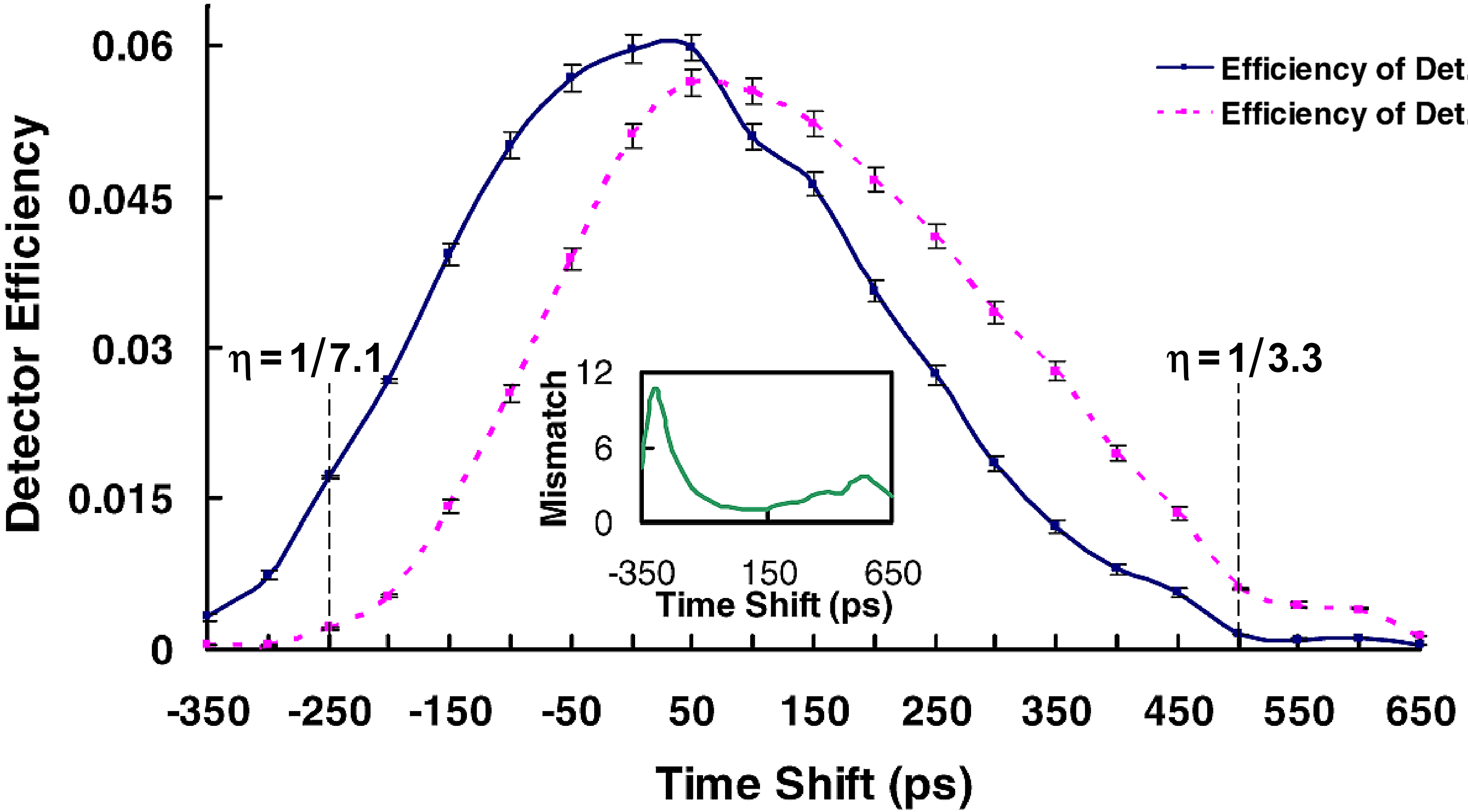


Example: 144 km free-space experiment



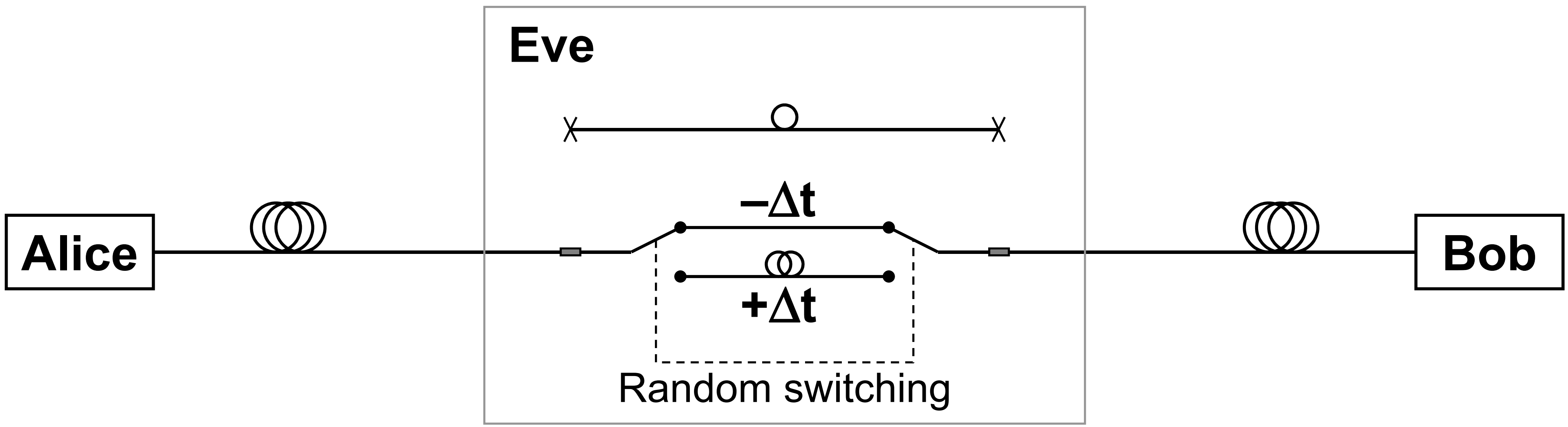
A. Lamas-Linares, C. Kurtsiefer, Opt. Express **15**, 9388 (2007)

Example: *id Quantique ID-500* commercial QKD system in worst 4% of automatic line length measurement cycles



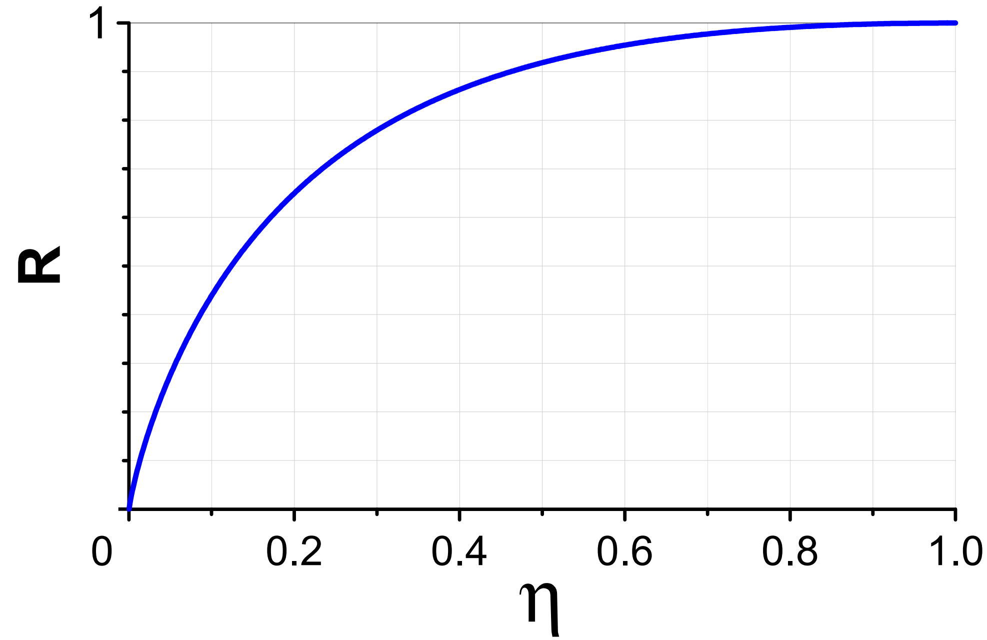
Y. Zhao *et al.,* arXiv:0704.3253

Time-shift attack



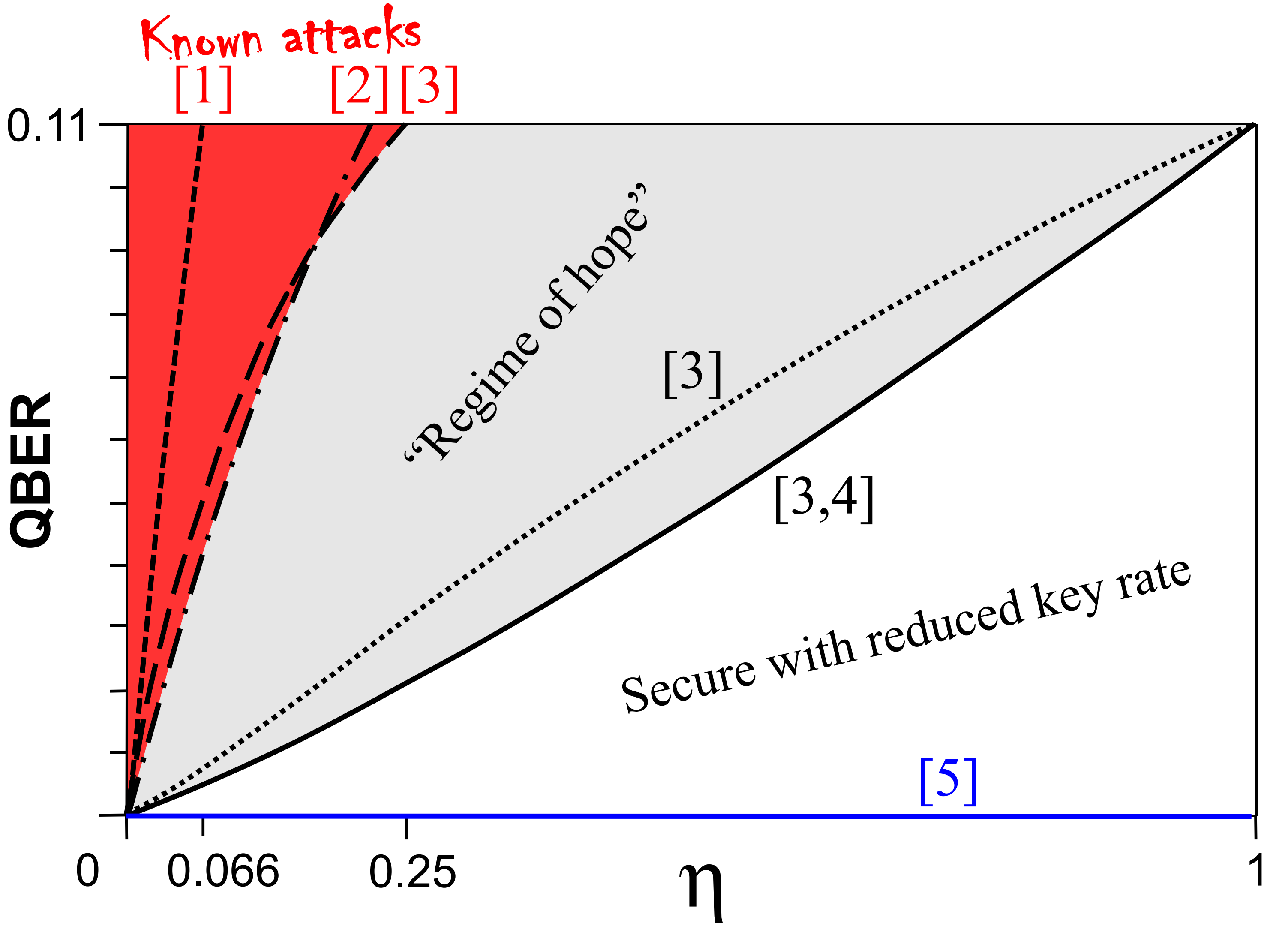
Available bit rate at QBER=0,
in symmetric case:

$$R = I(A:B|E) = h(\eta/(\eta+1))$$



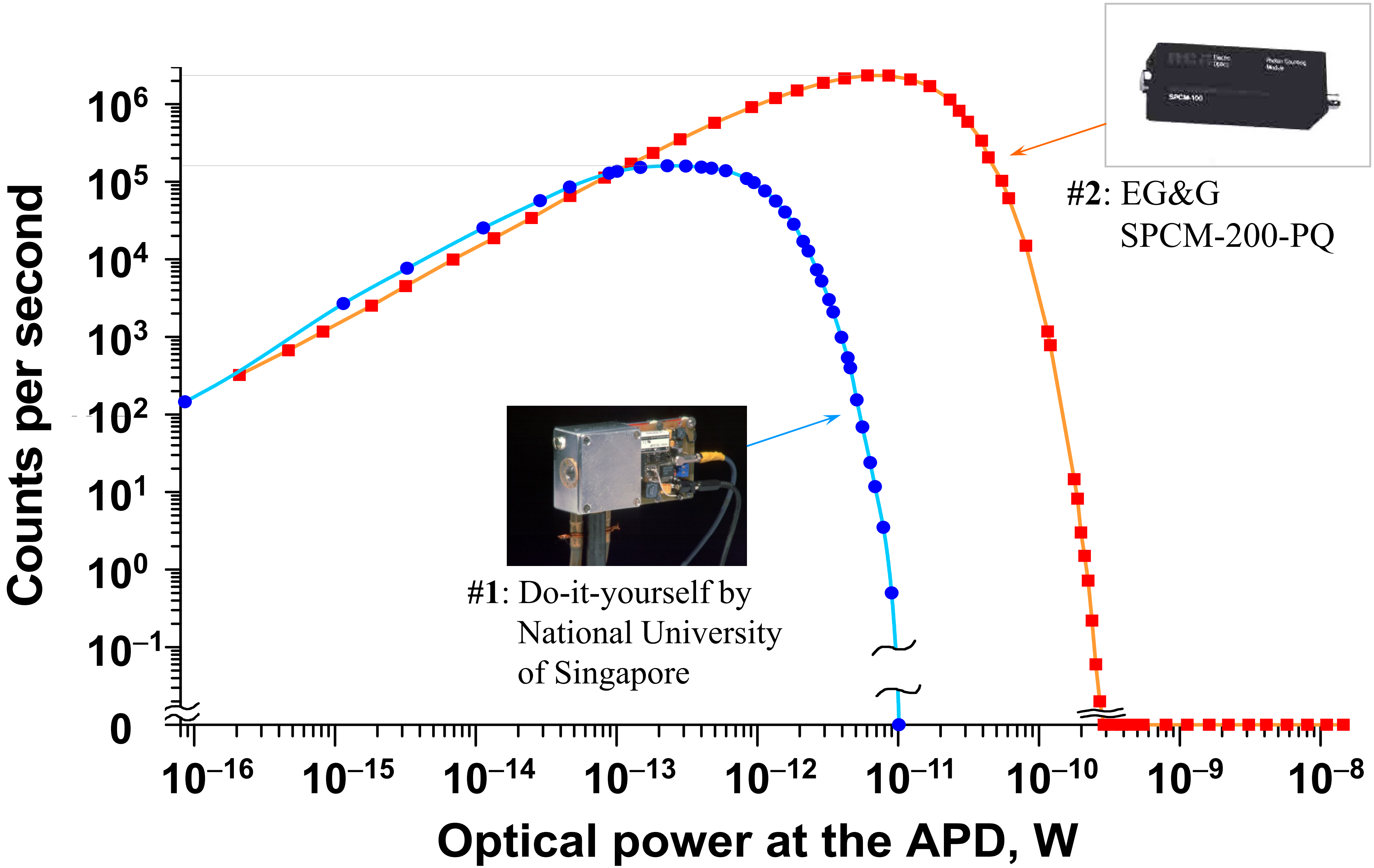
B. Qi *et al.*, Quant. Inf. Comp. **7**, 73 (2007)

Solution: develop security proof *for a quantified η*

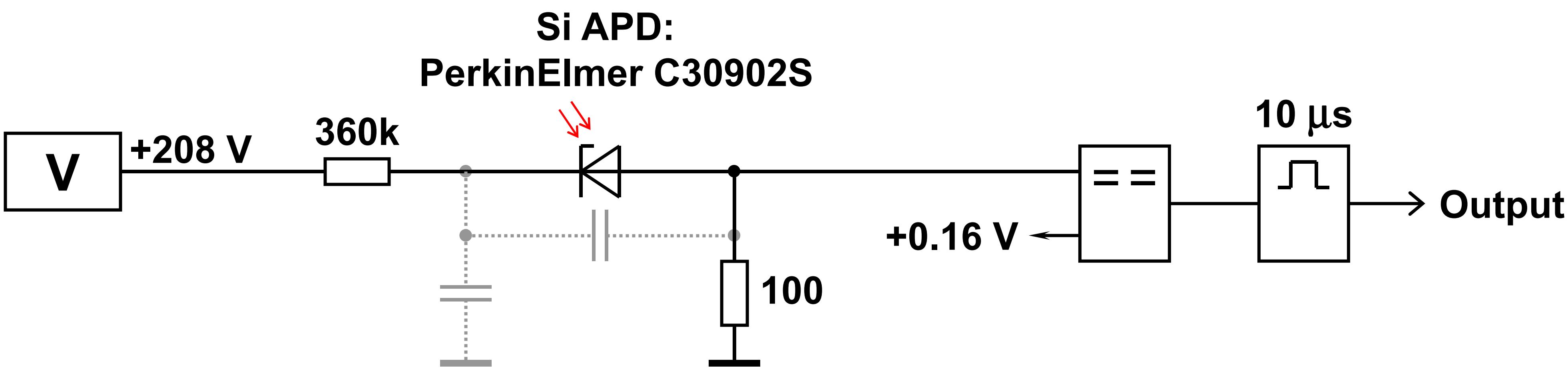


[1] V. Makarov *et al.,* Phys. Rev. A **74**, 022313 (2006)
[2] L. Lydersen, private communication
[3] L. Lydersen, J. Skaar, arXiv:0807.0767
[4] C.-H. F. Fung *et al.,* arXiv:0802.3788
[5] B. Qi *et al.,* Quant. Inf. Comp. **7**, 73 (2007)
Other protocols (DPSK, SARG04, Ekert): V. Makarov, J. Skaar, Quant. Inf. Comp. **8**, 0622 (2008)

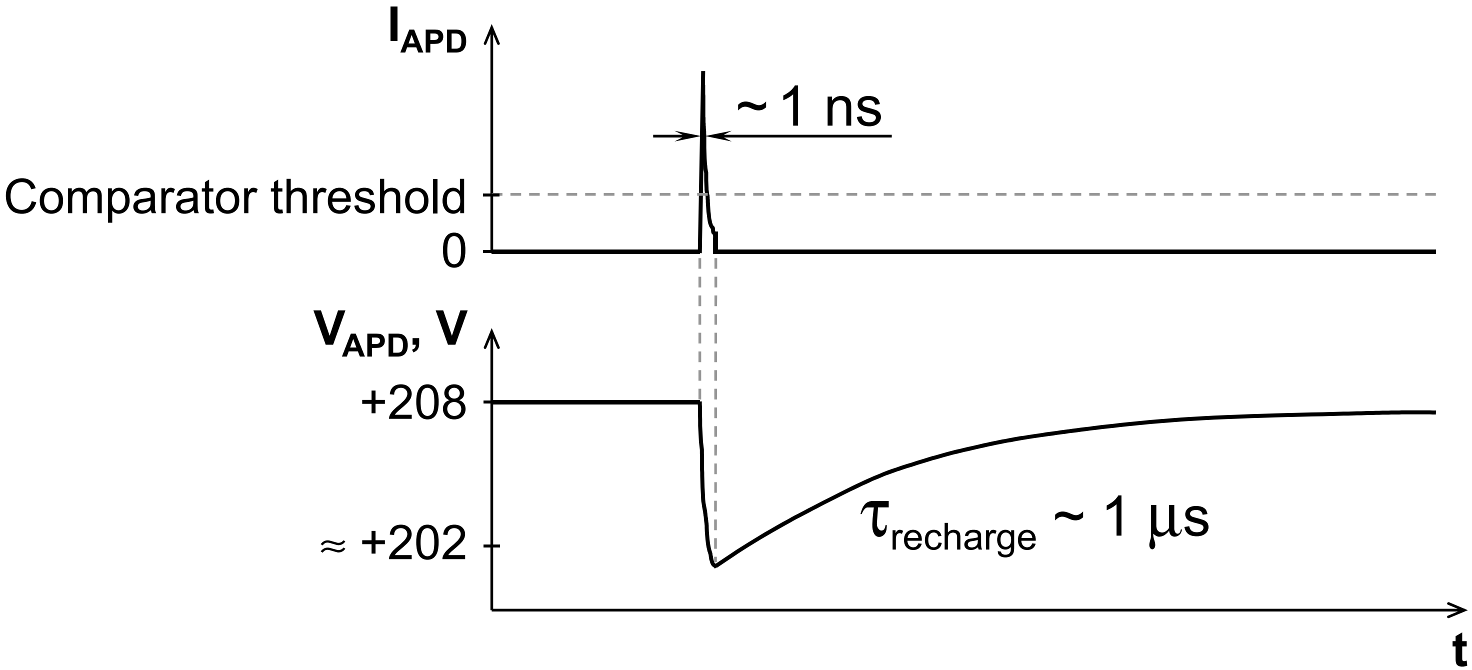
Control of passively-quenched detector. Detector saturation curves



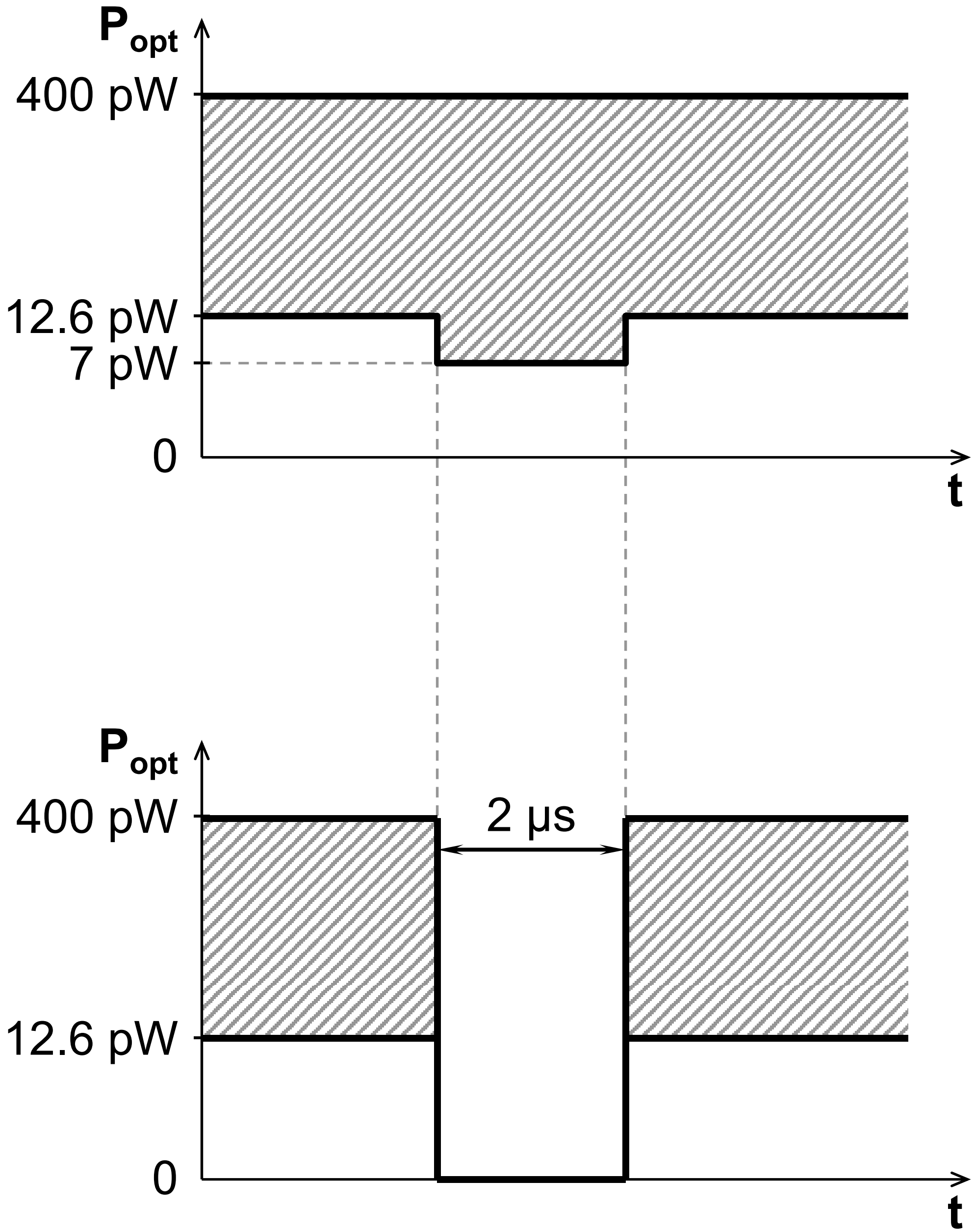
Detector #1

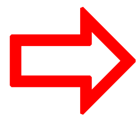


Single-photon response:

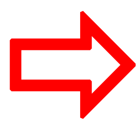


Control intensity diagrams (for detector #1):





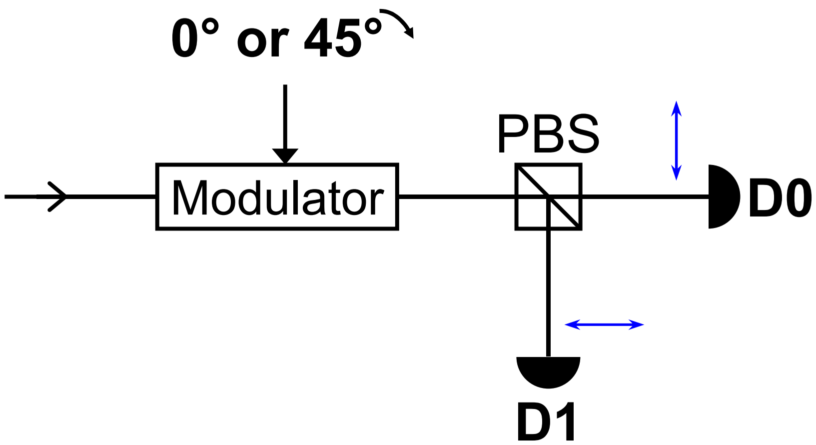
No click

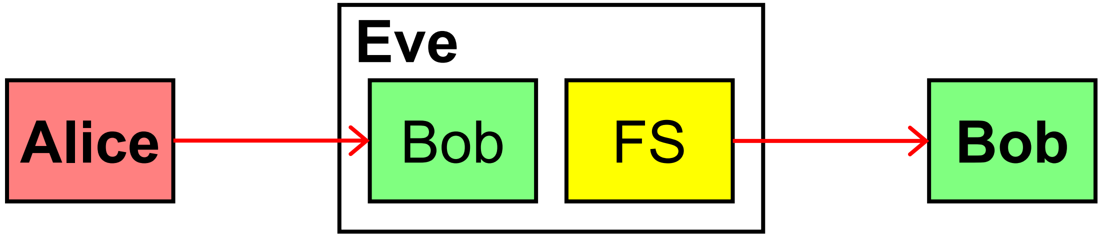


Single "click"
with probability ≥ 0.8

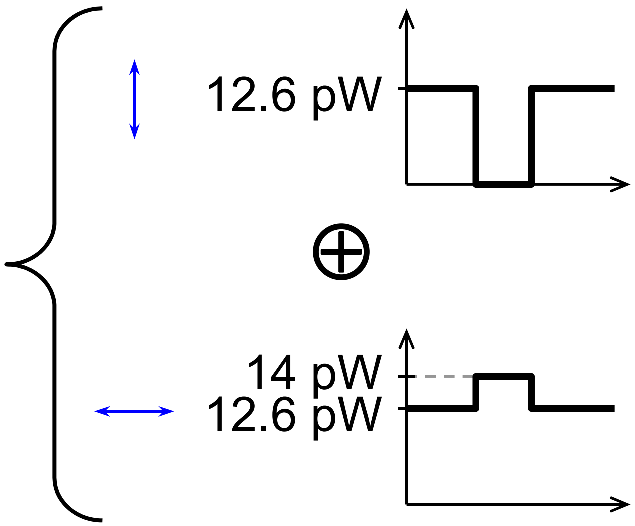
arXiv:0707.3987

Proposed attack

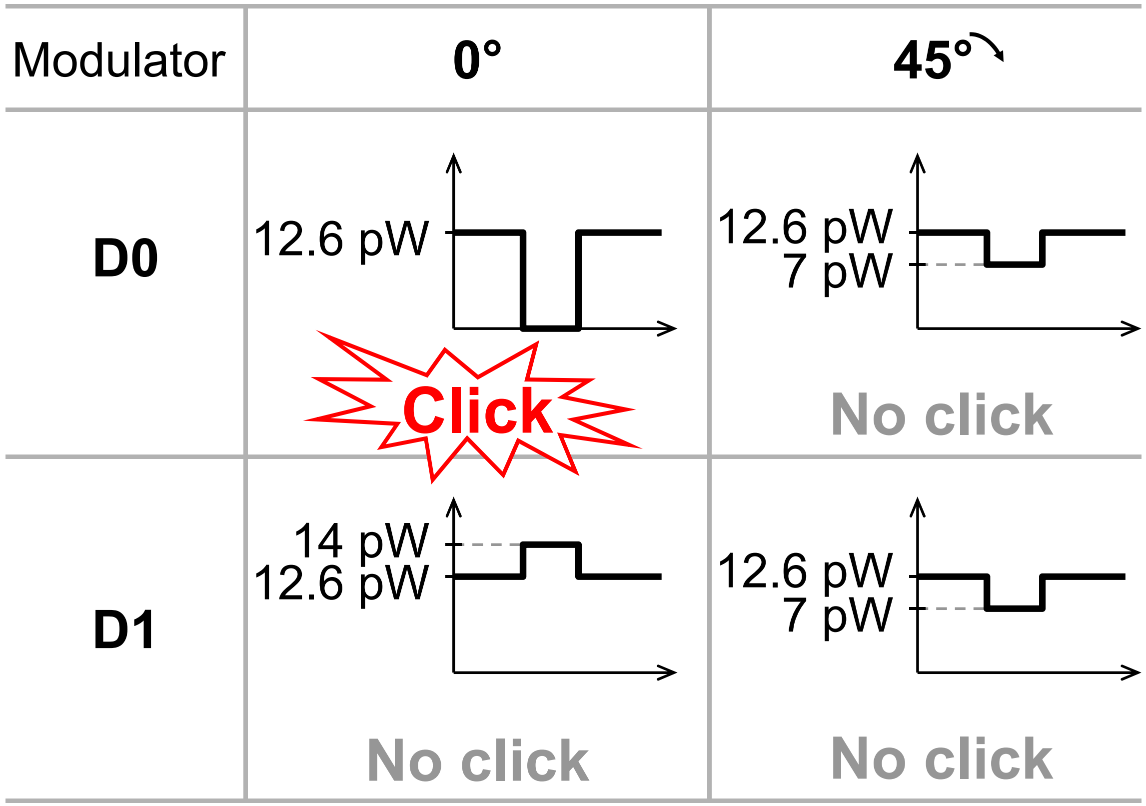




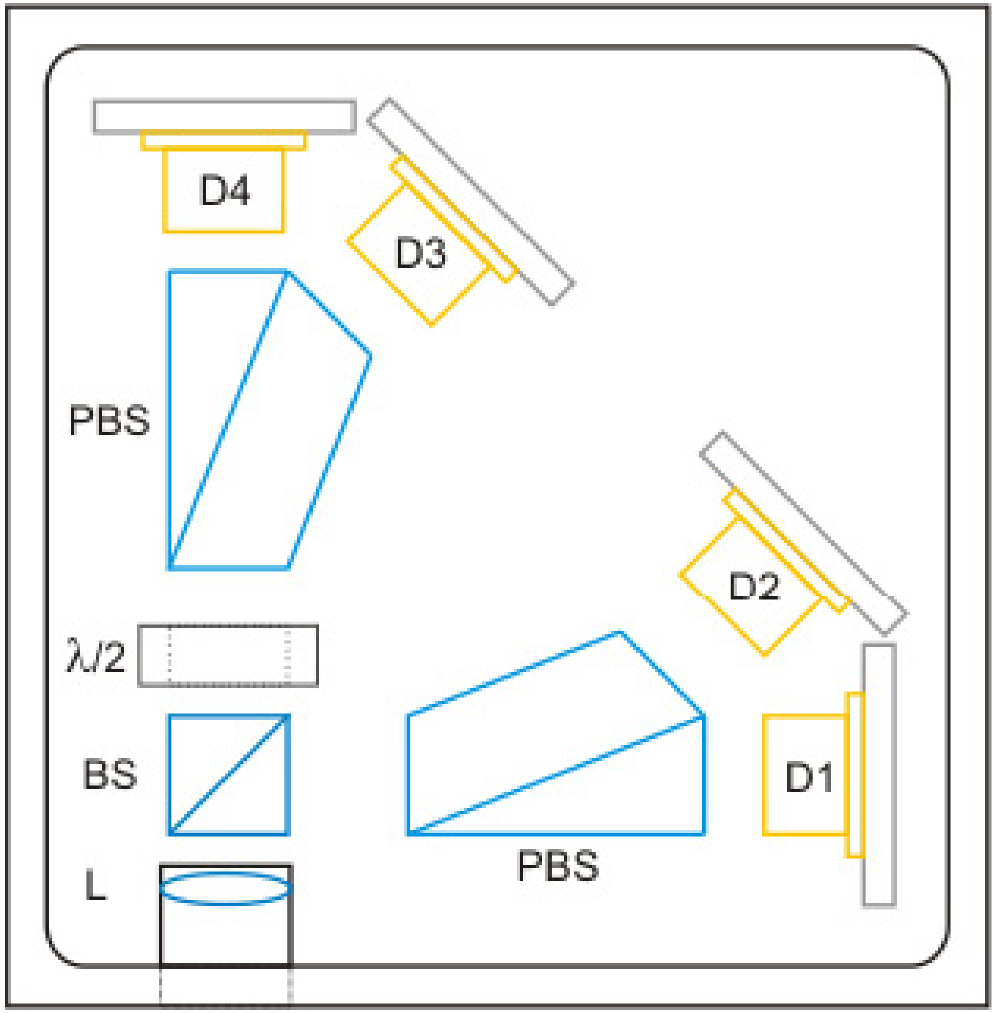
Eve detects, obtains: 0°, D0.
Eve resends faked state:



Bob:

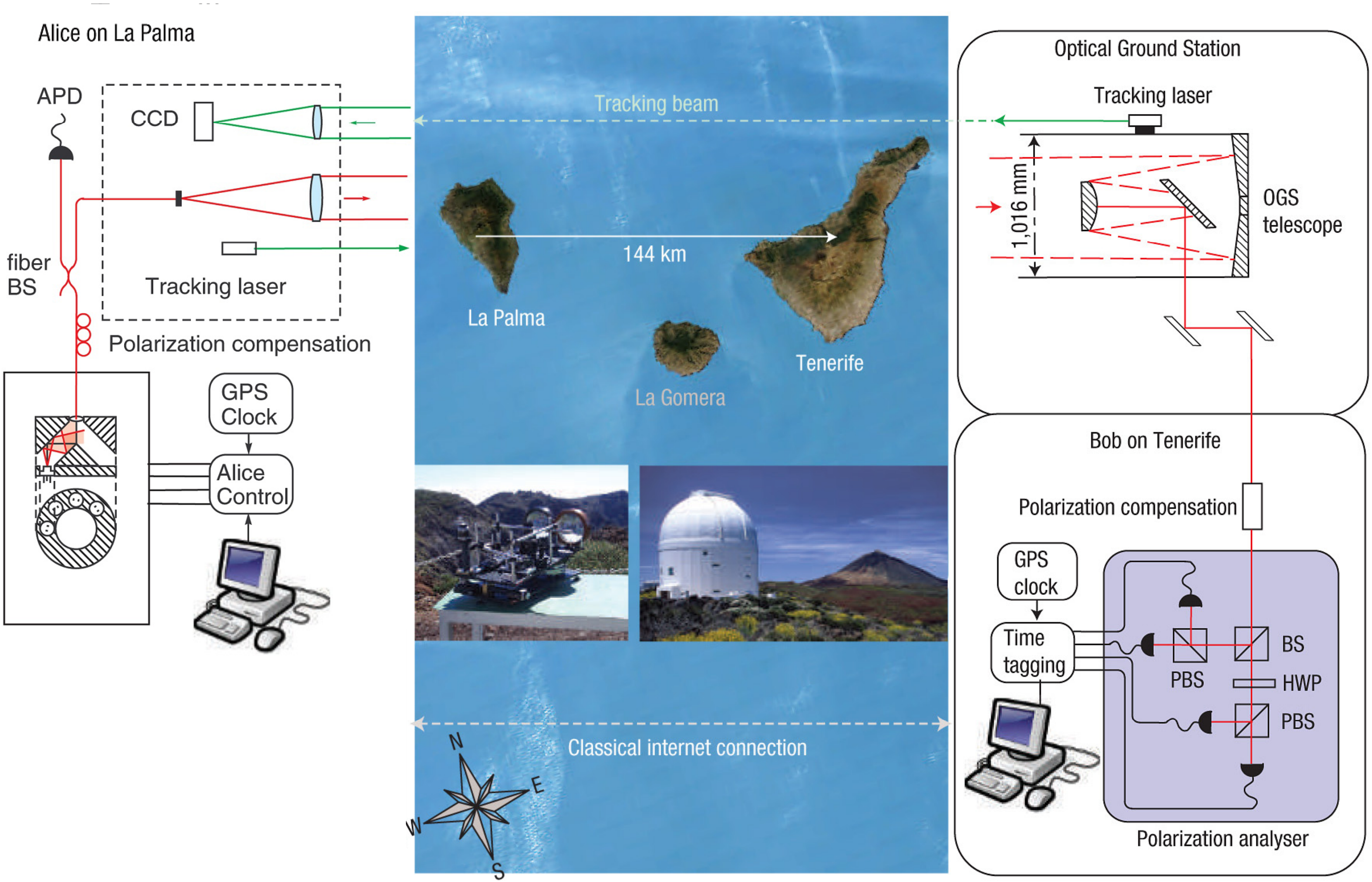


Example: ultrashort range QKD system



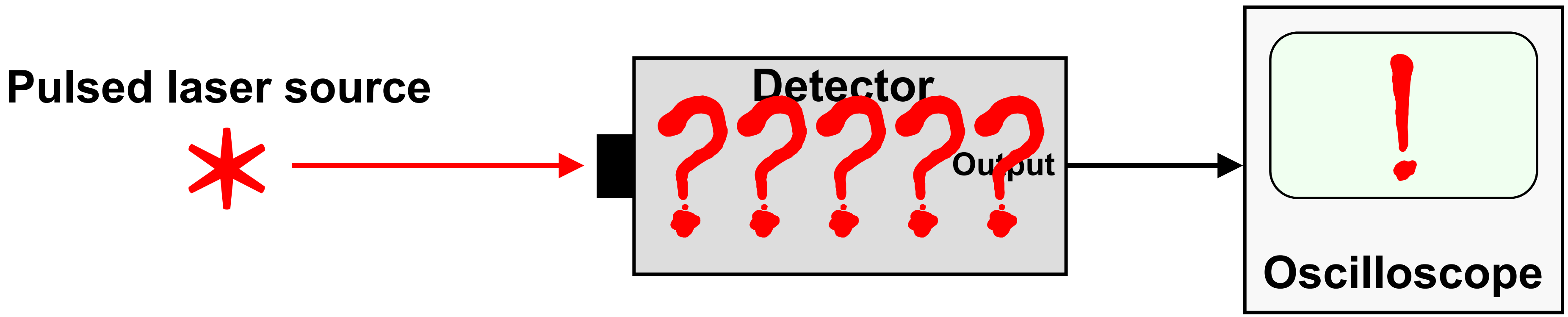
J. Duligall *et al.,* "Quantum key distribution for consumer applications" (LPHYS08, July 2008)

Example: 144 km free-space experiment

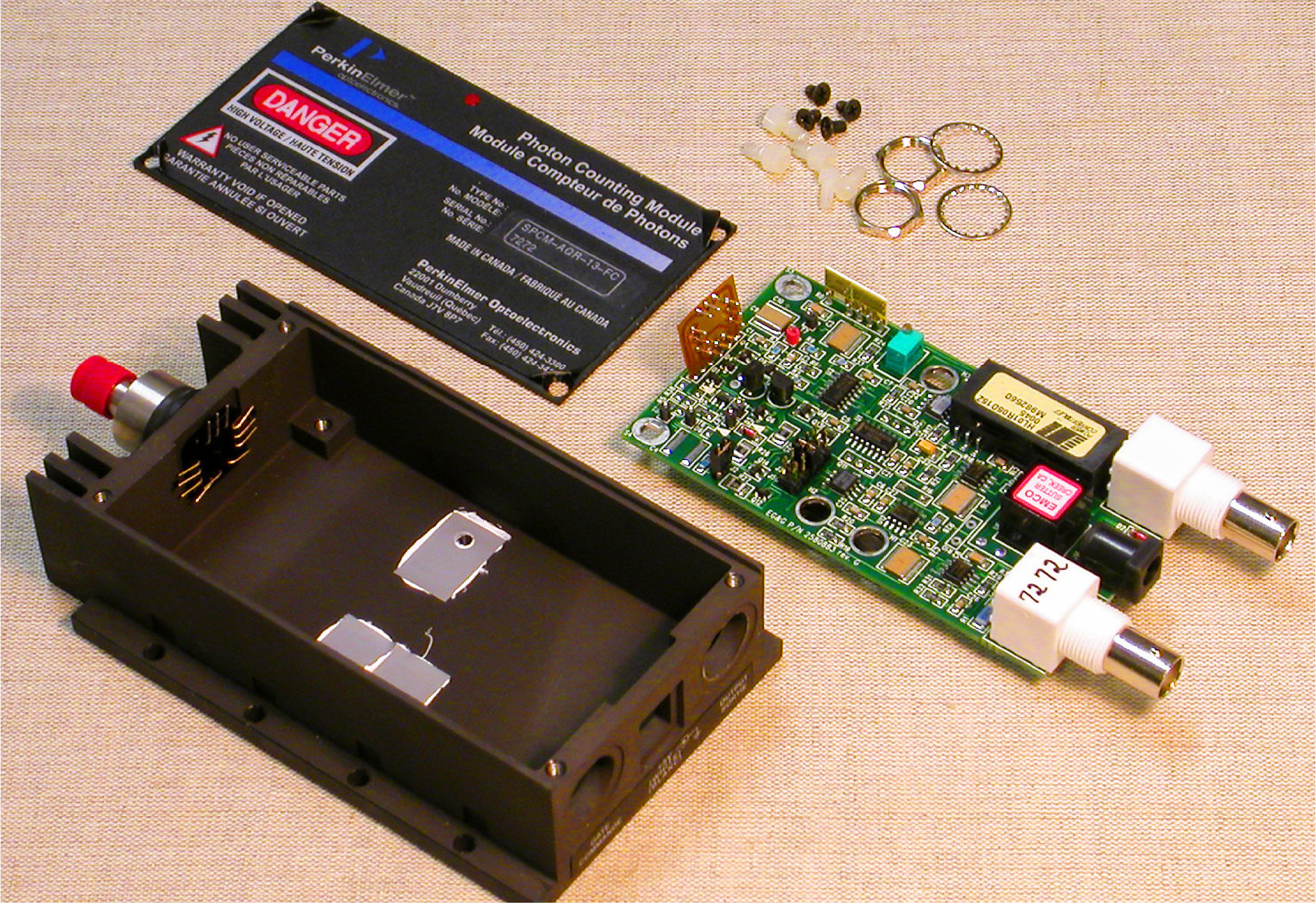


R. Ursin *et al.*, Nature Physics **3**, 481 (2007); Phys. Rev. Lett **98**, 010504 (2007)

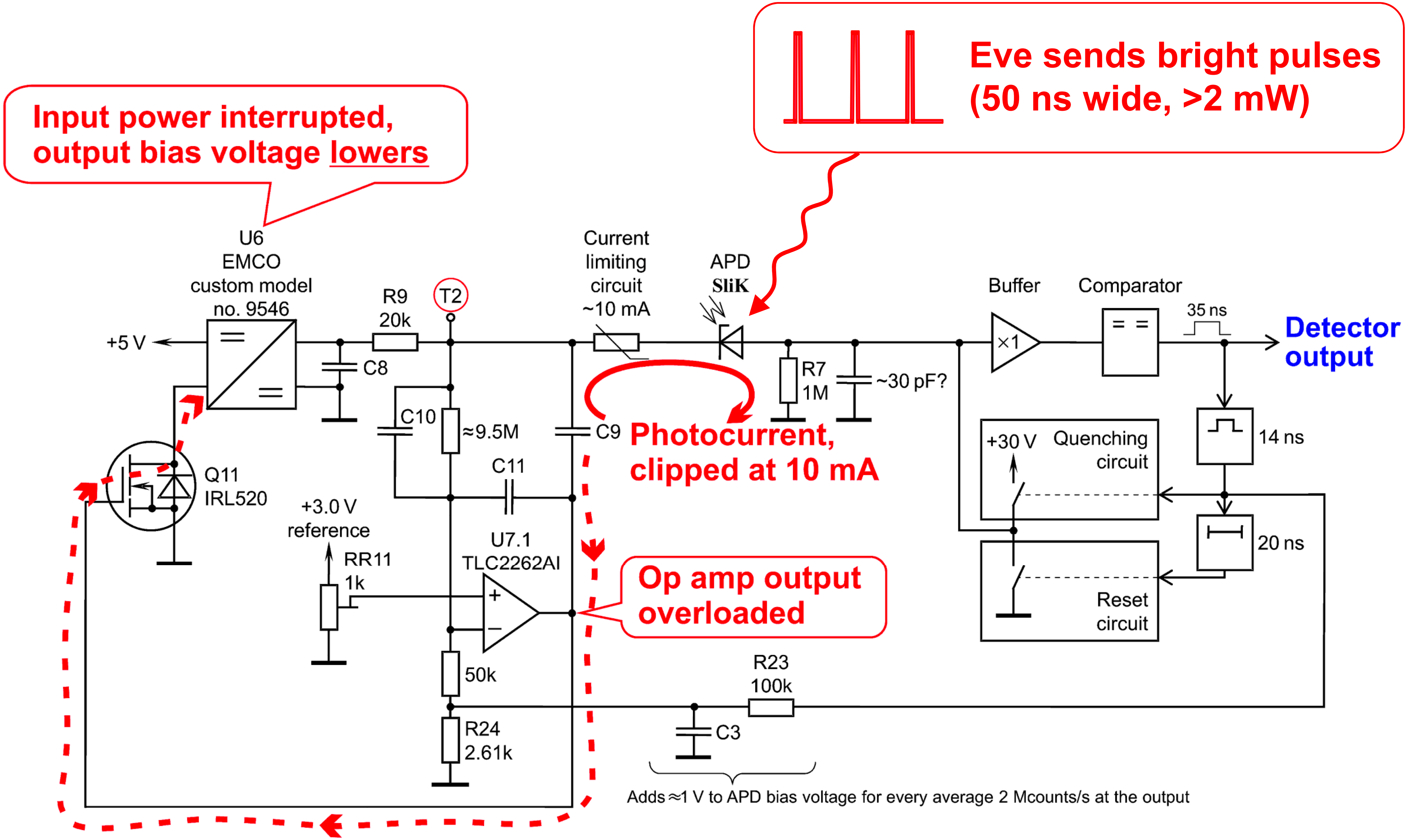
Control of PerkinElmer actively-quenched detector



Control of PerkinElmer actively-quenched detector

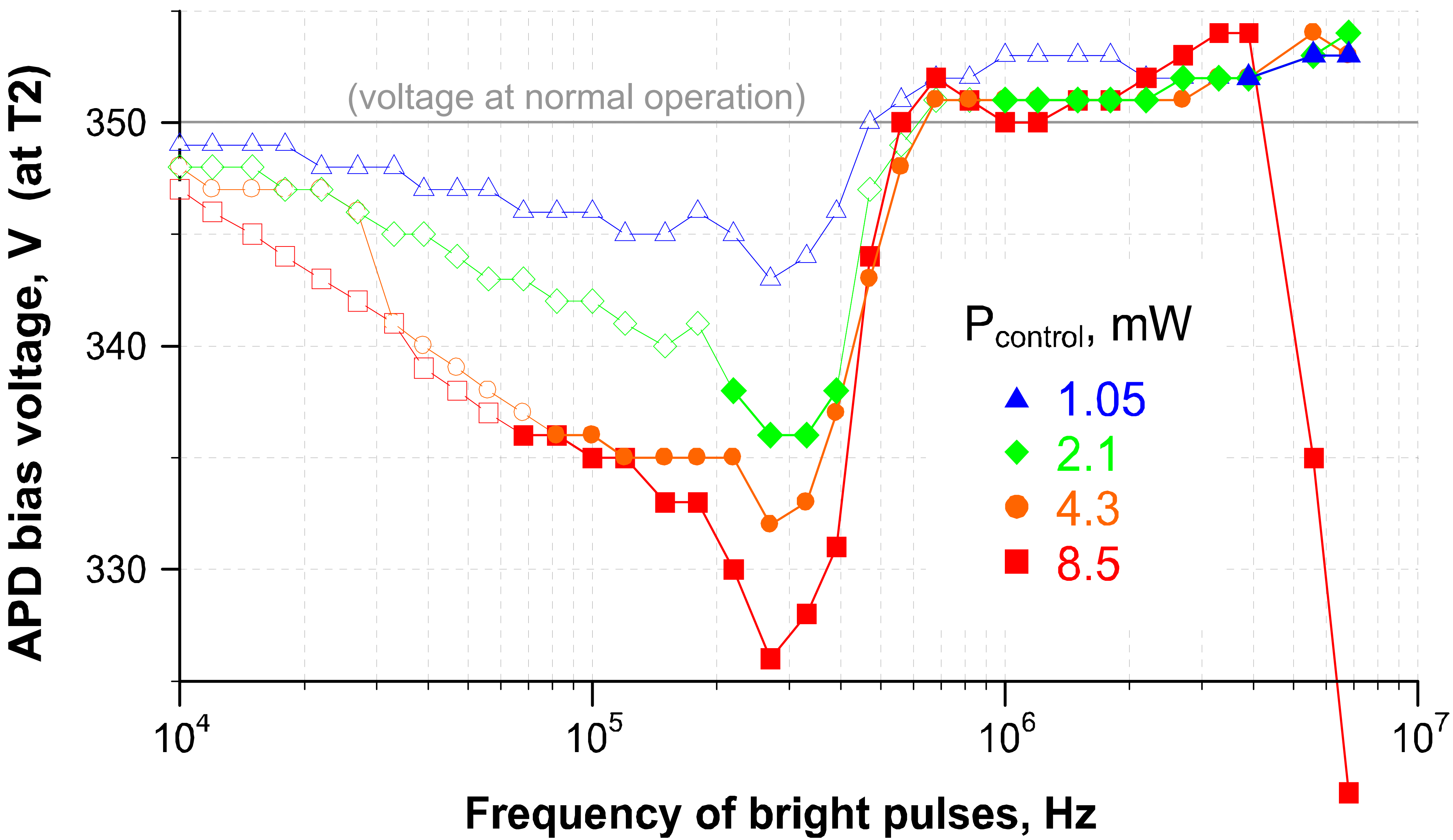


PerkinElmer detector reverse-engineered. Control method №4



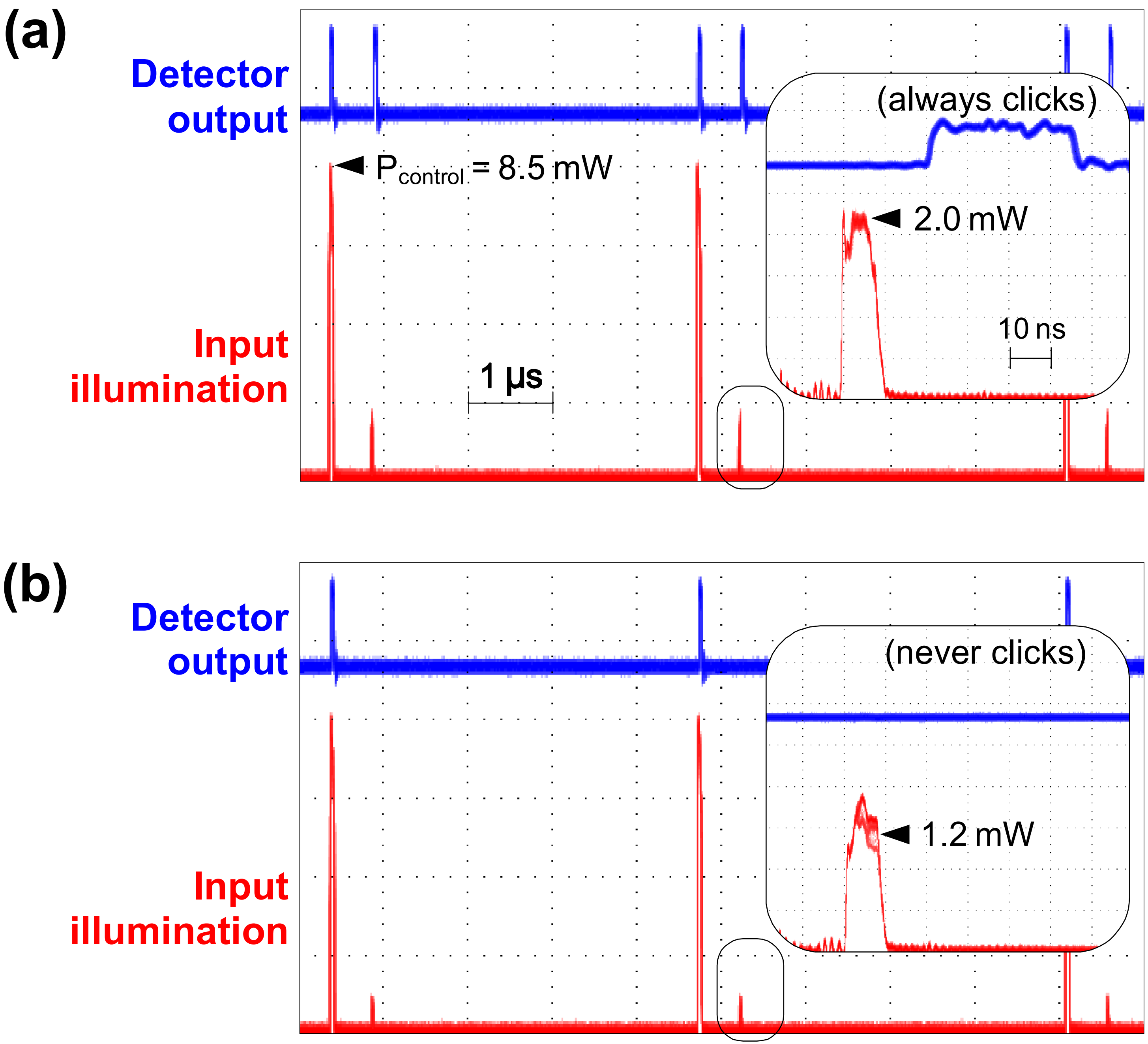
arXiv:0809.3408

Bias voltage vs. parameters of bright pulses

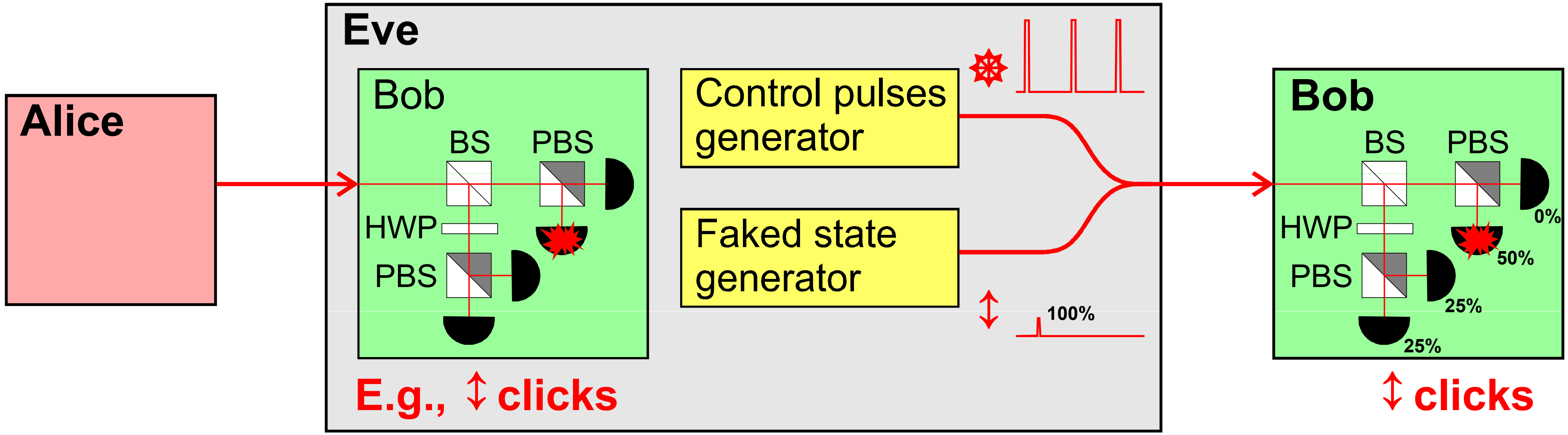


Filled symbols: full control over detector

Control intensity diagrams



Proposed attack



Side effect: simultaneous clicks from control pulses, >70 kHz

[1] C. Erven *et al.*, arXiv:0807.2289

[2] V. Fernandez *et al.*, IEEE J. Quantum Electron. **43**, 130 (2007);
K. J. Gordon *et al.*, Opt. Express **13**, 3015 (2005); IEEE J. Quantum Electron. **40**, 900 (2004)

[3] X. Shan *et al.*, Appl. Phys. Lett. **89**, 191121 (2006)

[4] K. J. Resch *et al.*, Opt. Express **13**, 202 (2005)

[5] W. T. Buttler *et al.*, Phys. Rev. Lett. **84**, 5652 (2000); *ibid.* **81**, 3283 (1998); Phys. Rev. A **57**, 2379 (1998)

NewScientistTech

Laser cracks 'unbreakable' quantum communications

Quantum cryptography is supposed to be unbreakable. But a flaw in a common type of equipment used makes it possible to intercept messages without detection.

adressa.no | trondheim

Bryter seg inn i fremtidens krypteringsmetode

Fra et laboratorium på Gløshaugen bryter Vadim Makarov seg inn i fremtidens kommunikasjonskryptering.

Foto: KIM NYGÅRD

Med offentlig støtte og velsignelse forsøker Vadim Makarov og de fire kollegene hans å bryte seg gjennom datamurer som i teorien skal være ugjennomtrengelige.

the physics arXiv blog

Loophole found in quantum cryptography photon detectors

If you're hoping to secure your data using quantum cryptography, you might want to find a shoulder to cry on.

HACK A DAY BETA

quantum cryptography in-band attack

quantum cryptography is an emerging field, but low install base hasn't kept researchers from exploring attacks against it.

BBC RADIO

Loopholes, and their patching status

- Large pulse attack
  – not much yet done to protect in practice
- Detector efficiency mismatch
  – have proofs, but not yet detectors with guaranteed η
- Control of passively-quenched detectors
  – have vague ideas, not yet hack-proof detectors/Bob
- Control of PerkinElmer actively-quenched detector
  – just discovered

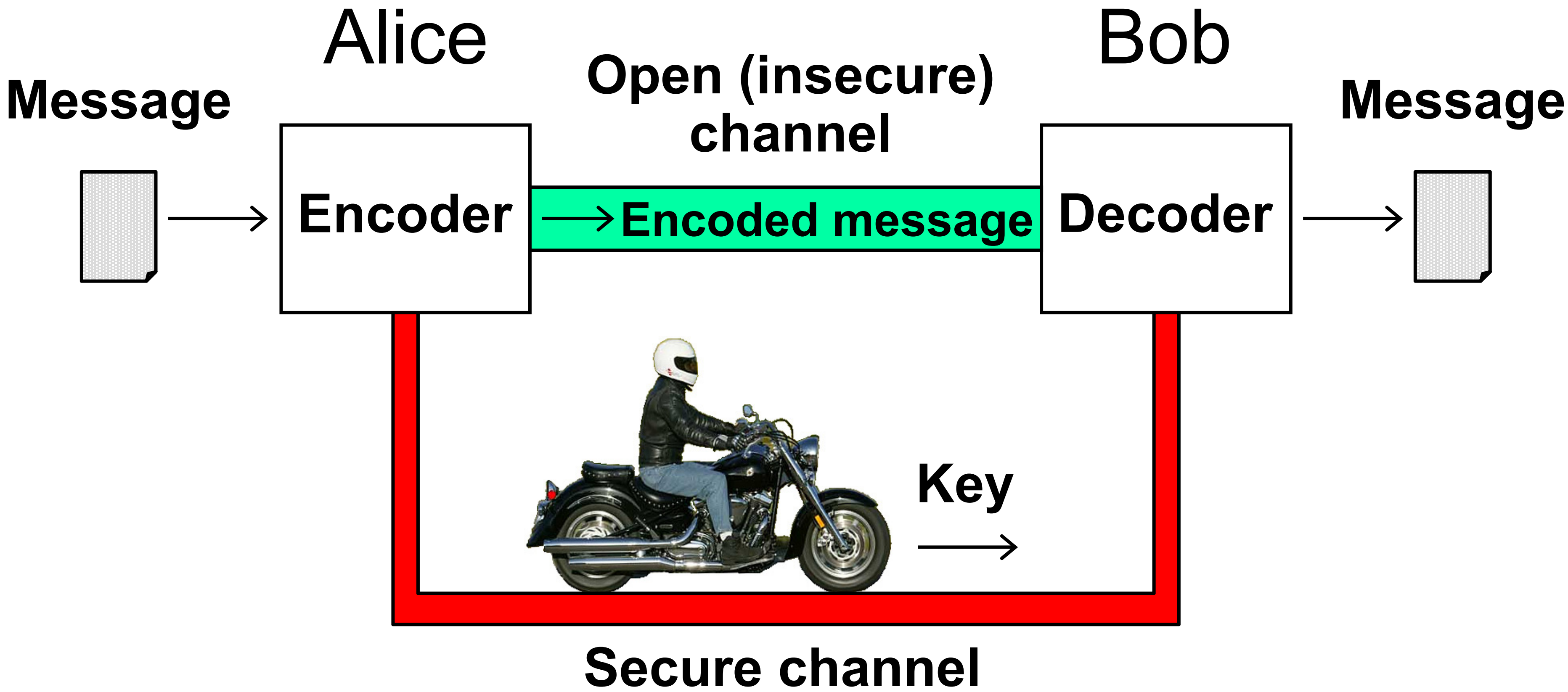
Is quantum cryptography secure?

Yes.

Testing for loopholes is normal, necessary practice.

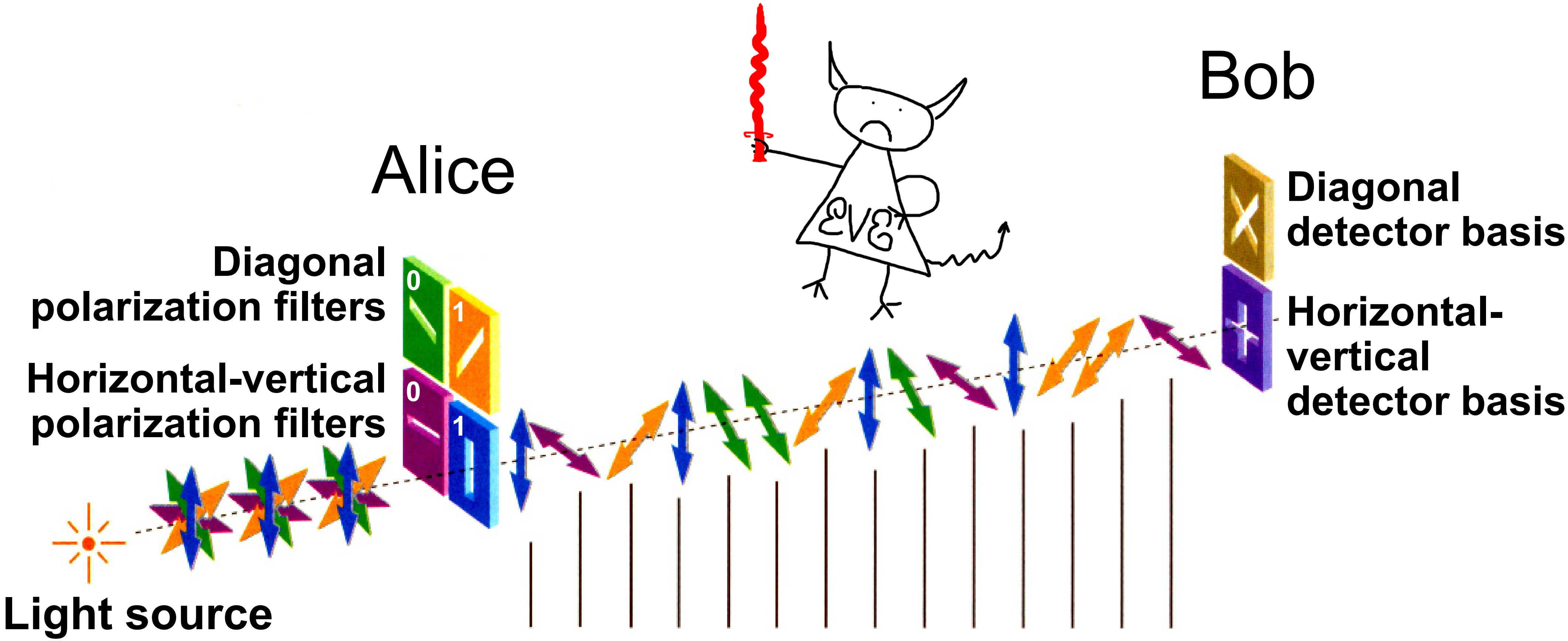
Optional slides

Key distribution



- Secret key cryptography requires secure channel for key distribution.
- Quantum cryptography distributes the key by transmitting quantum states in *open channel*.

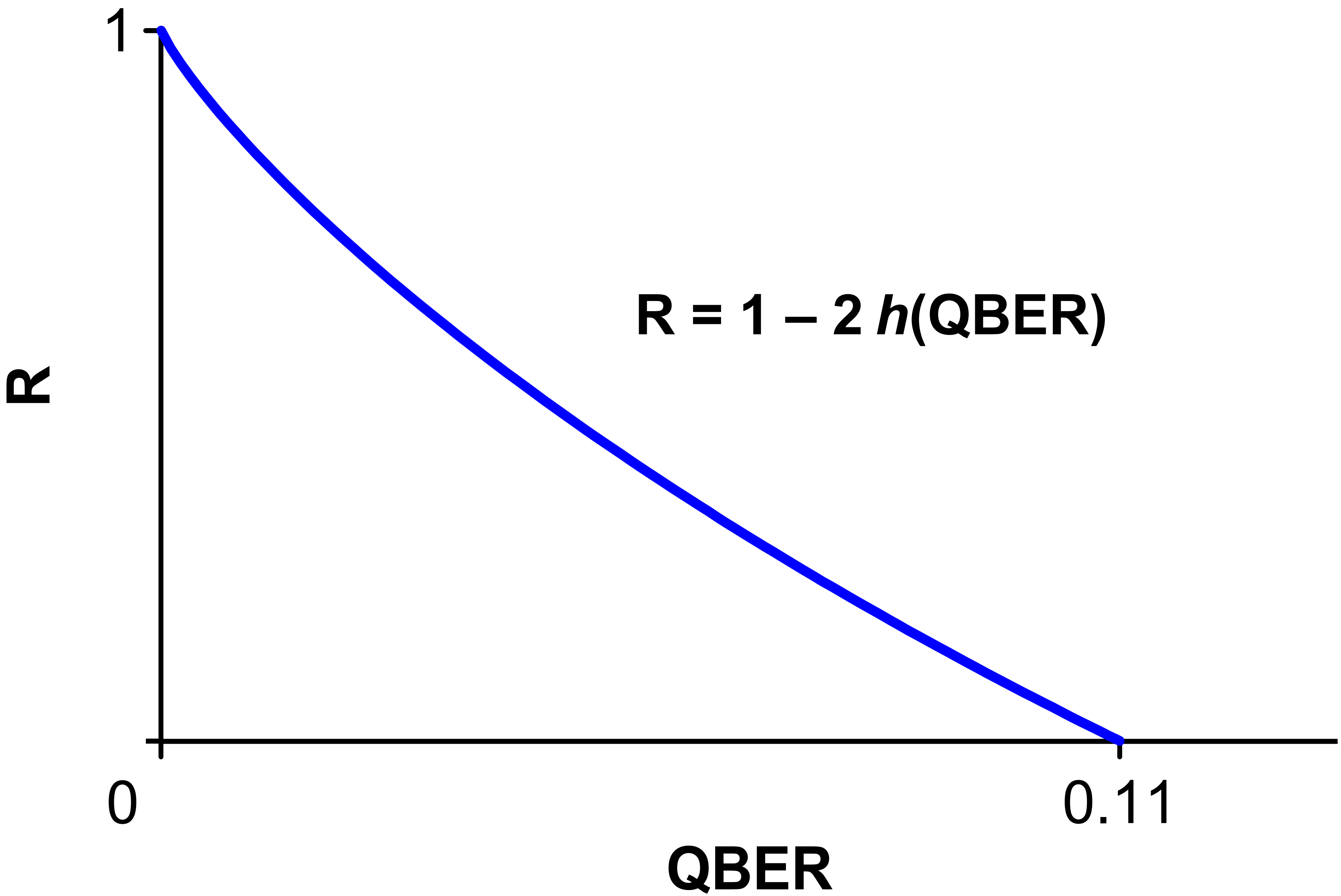
Quantum key distribution

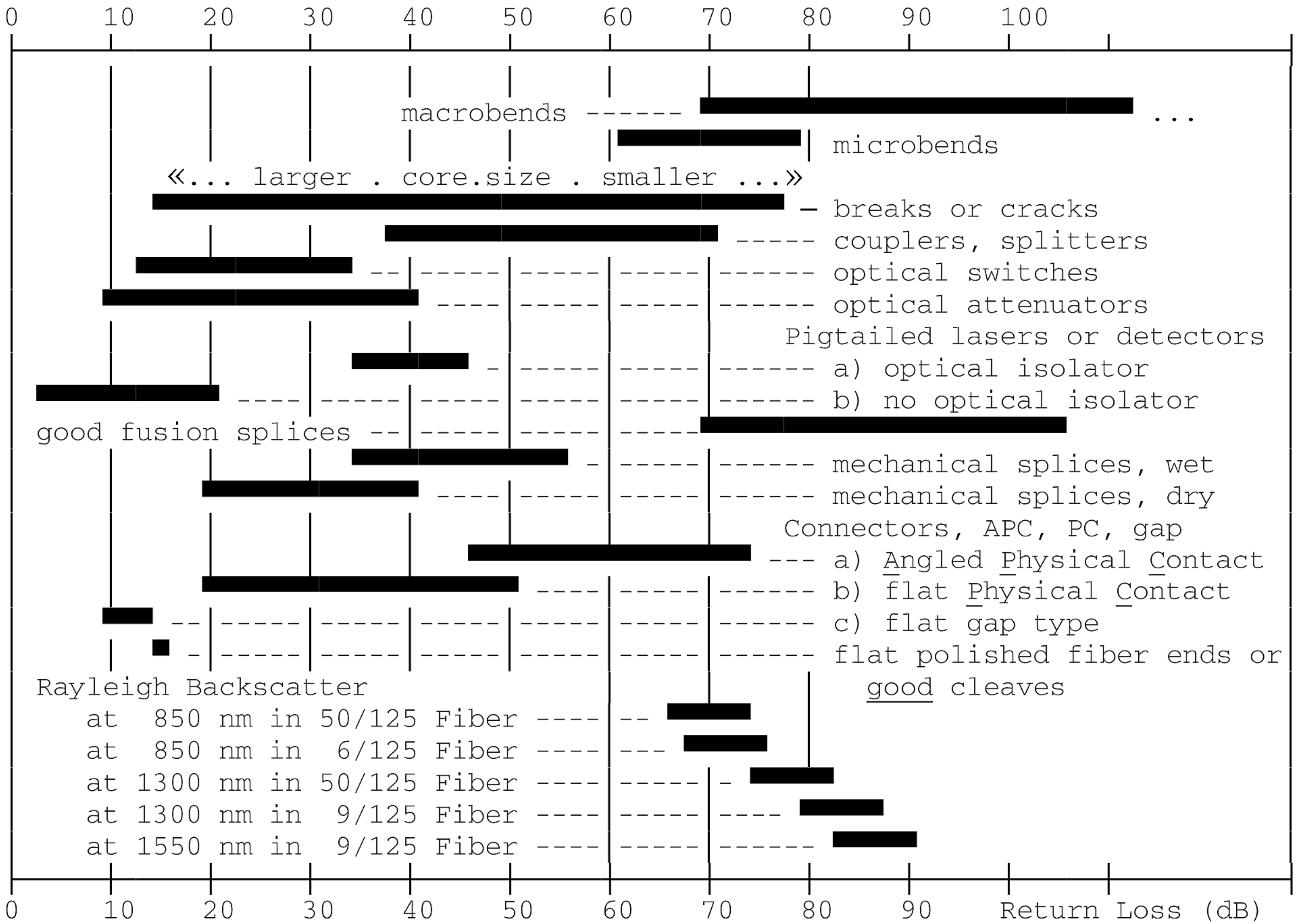


Alice's bit sequence	1	0	1	1	0	0	1	1	0	0	1	1	1	0
Bob's detection basis	+	×	+	+	×	×	+	+	×	+	×	×	+	+
Bob's measurement	1	0	0	1	0	0	1	1	0	0	0	1	0	0
Retained bit sequence	1	–	–	1	0	0	–	1	0	0	–	1	–	0

Image reprinted from article: W. Tittel, G. Ribordy, and N. Gisin, "Quantum cryptography," Physics World, March 1998

Handling errors in raw key



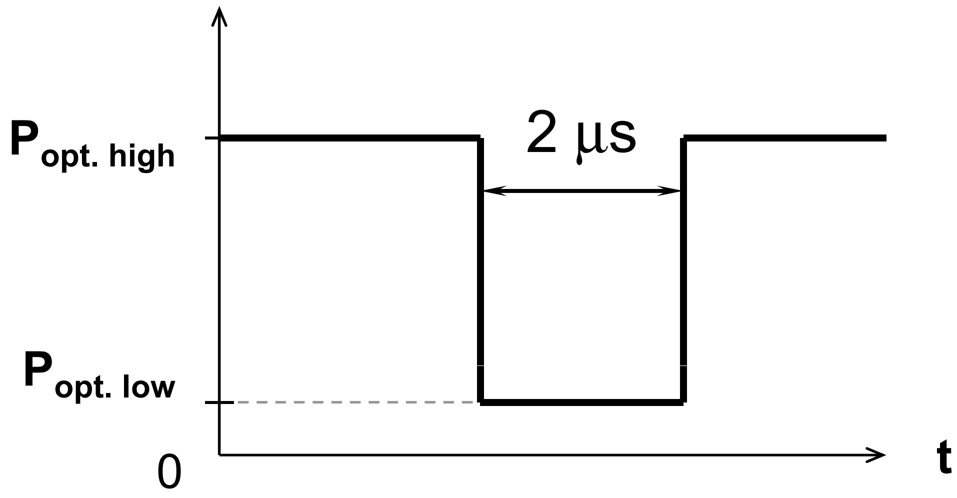


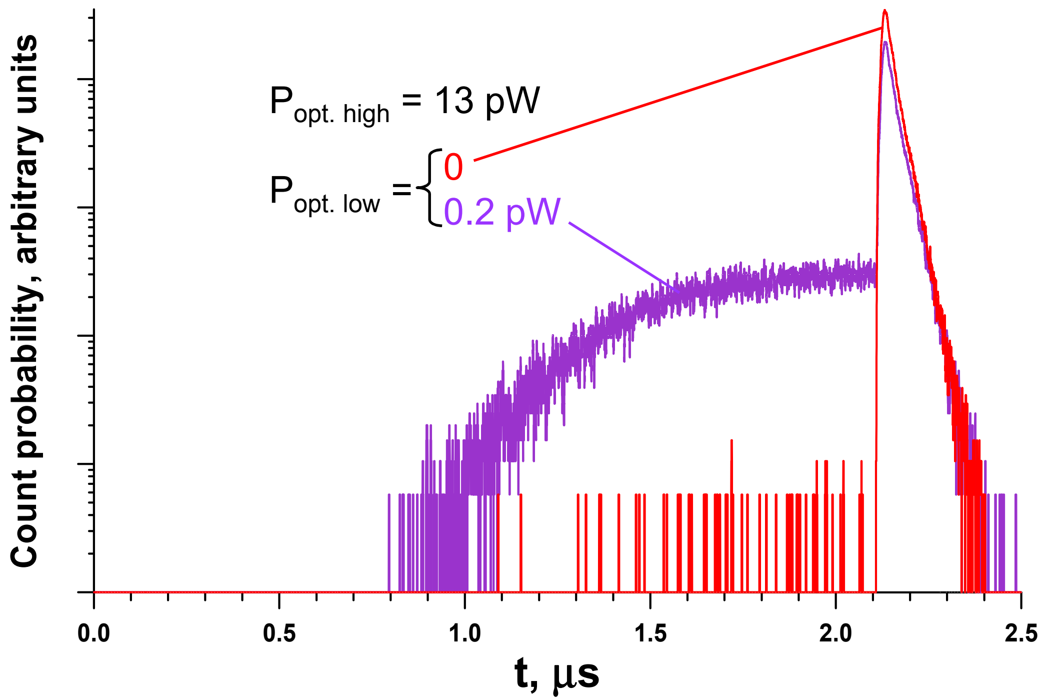
Typical values of reflection coefficients for different fiber-optic components

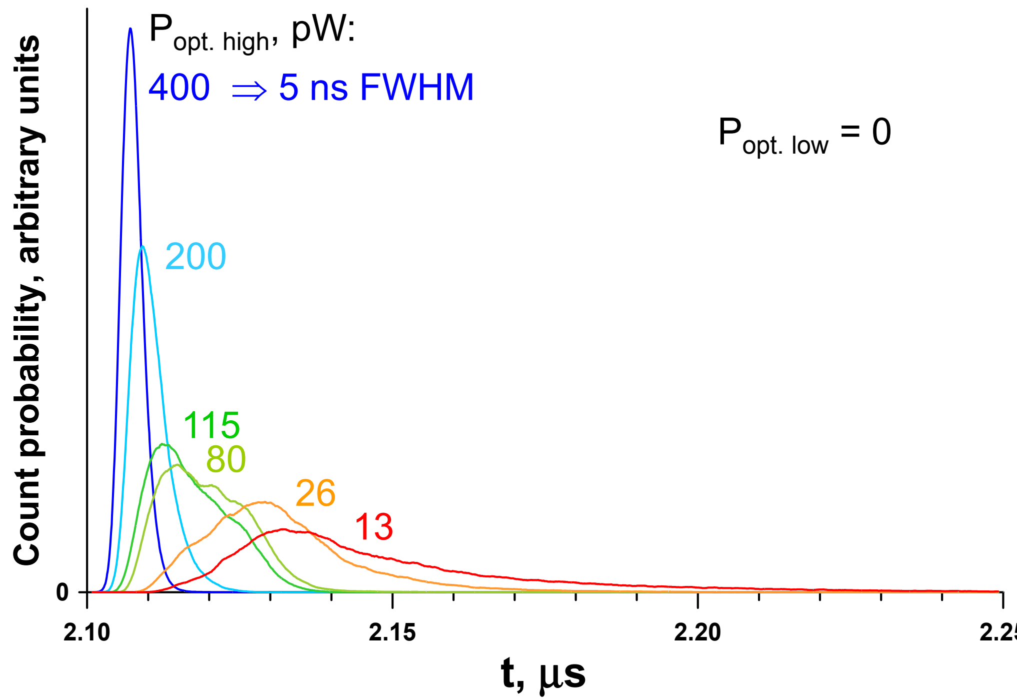
(courtesy Opto-Electronics, Inc.)

Quality of control (detector #1)

Control intensity diagram:







arXiv:0707.3987

Quality of control (detector #2)

Control intensity diagram: