Defence for the degree *doktor ingeniør*
at the Norwegian University of Science and Technology, April 30, 2007

Quantum cryptography
and
quantum cryptanalysis

candidate: Vadim Makarov

NTNU
Norwegian University of Science and Technology

SPbSPU
St. Petersburg State Polytechnic University

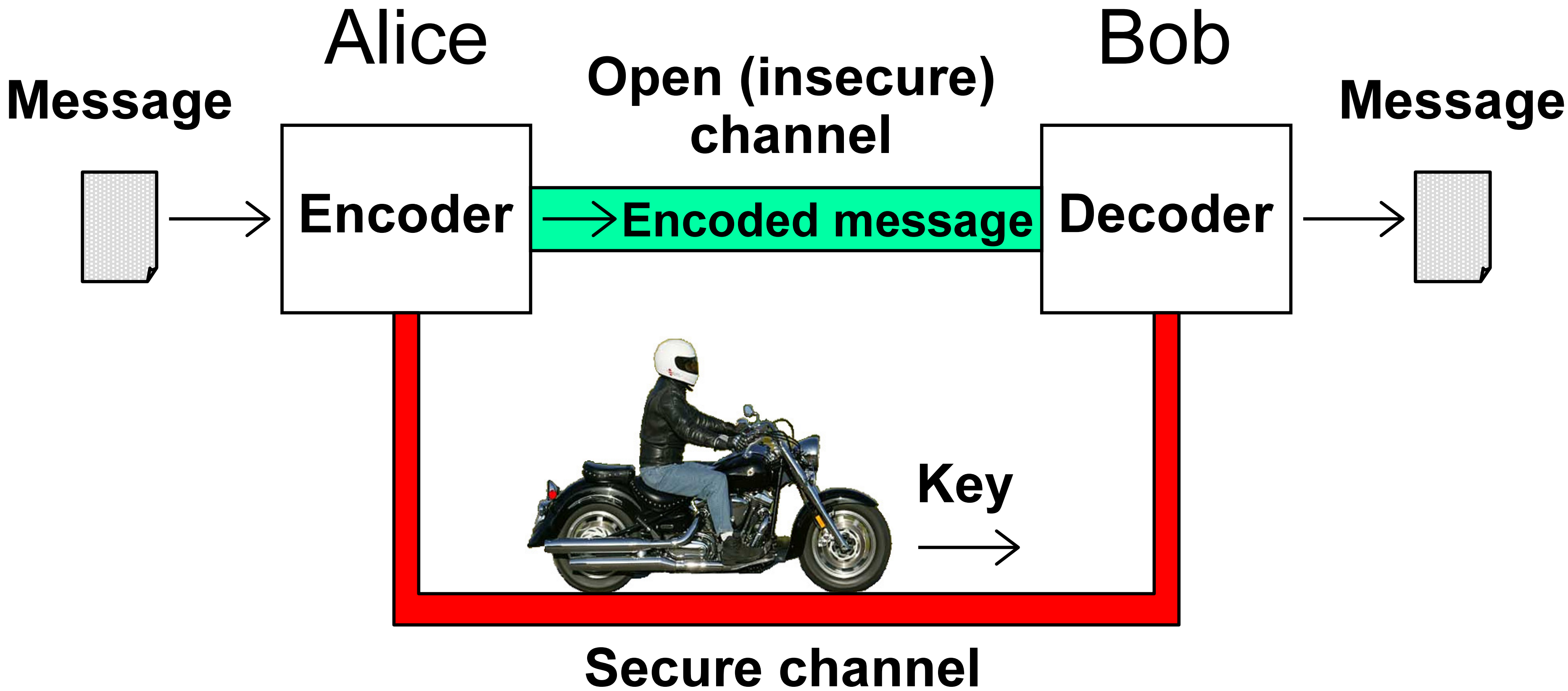
telenor R&D

SINTEF

Quantum cryptography timeline

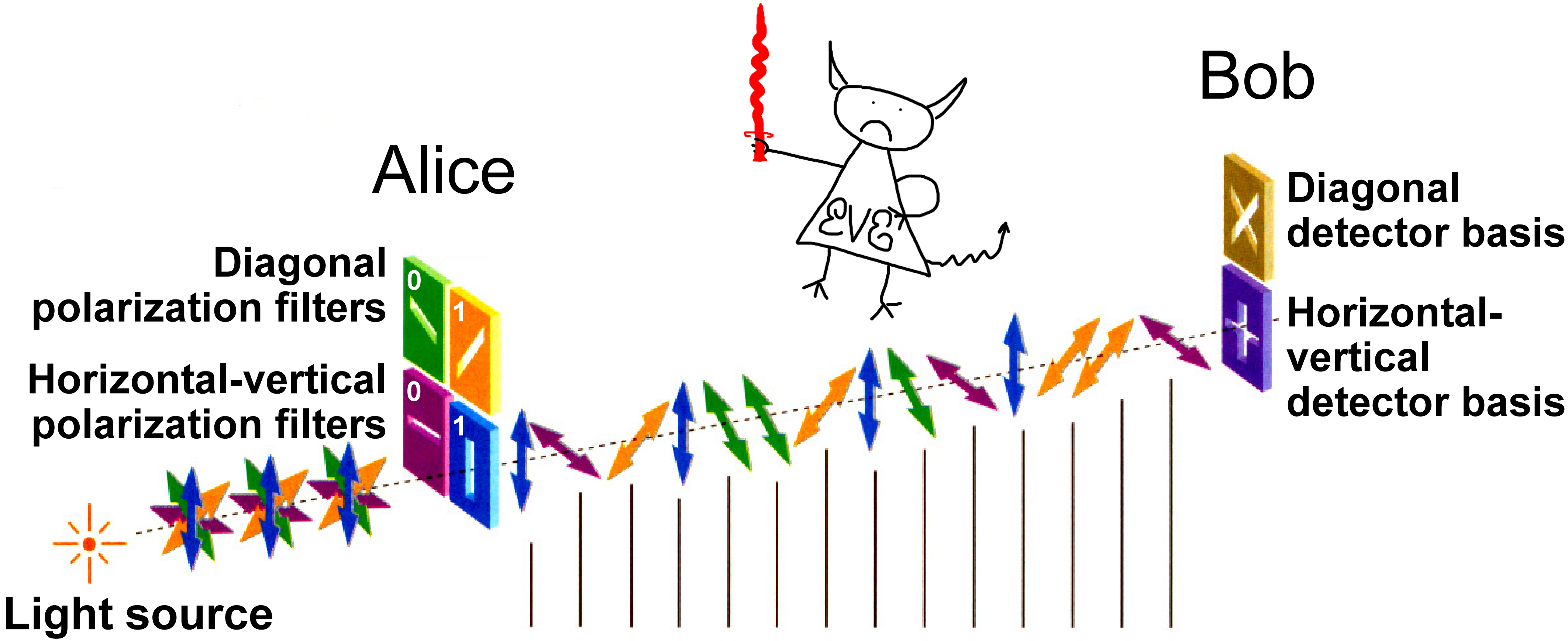
ca. **1970**	Concept ("money physically impossible to counterfeit")
1984	Key distribution protocol (BB84)
1989	Proof-of-the-principle experiment
1993	Key transmission over fiber optic link
2004	First commercial offers
...	Market?

Key distribution



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

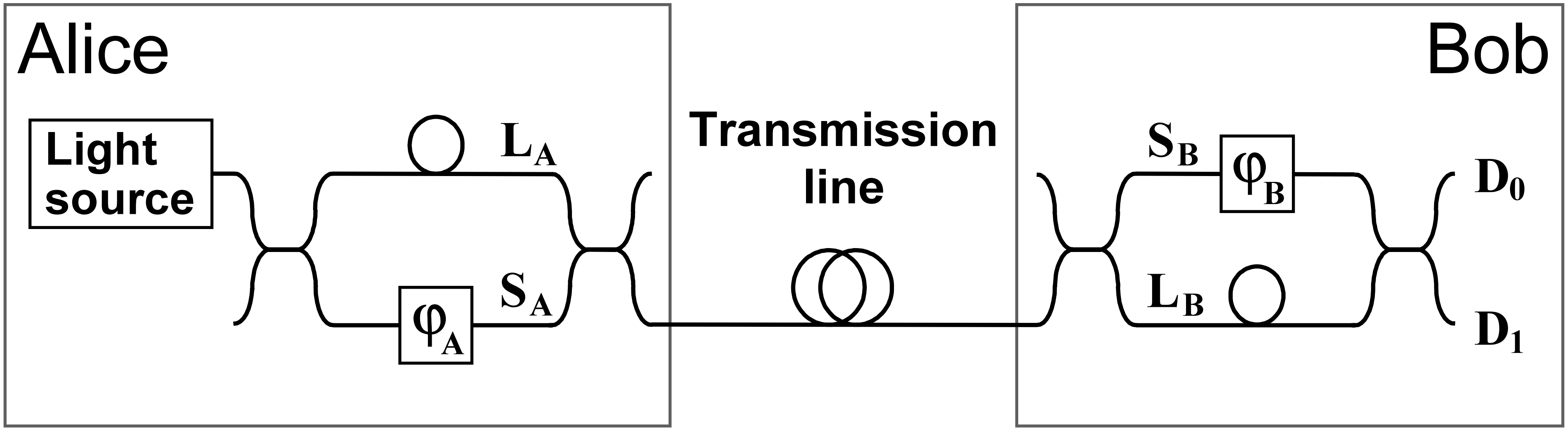
Quantum key distribution



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

Interferometric QKD channel



Detector bases:

$\varphi_A = -45°$ or $+45°$: 0

$\varphi_A = +135°$ or $-135°$: 1

$\varphi_B = -45°$: X

$\varphi_B = +45°$: Z

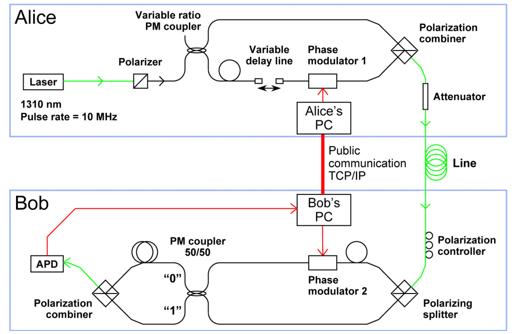
Quantum cryptography at NTNU

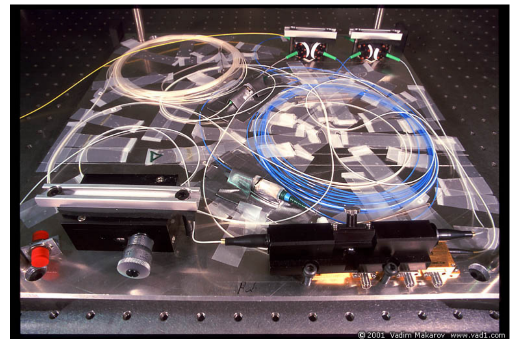
Fiber optic QKD setup

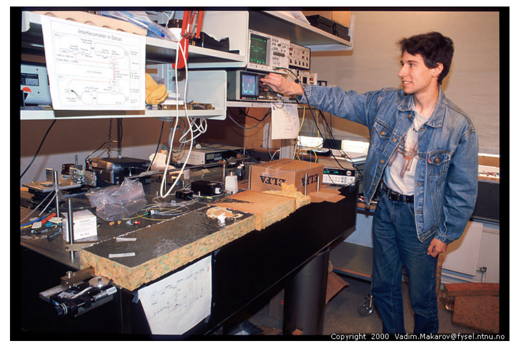
1. Optimal tracking of phase drift
2. Single photon detector with afterpulse blocking

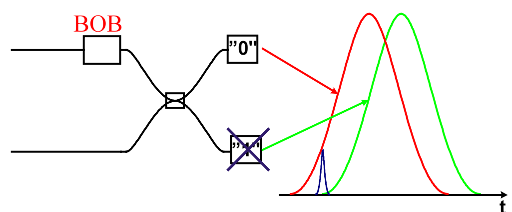
Security against practical attacks

3. Large pulse attack: experiment
4. Faked states attack
5. Detector efficiency mismatch

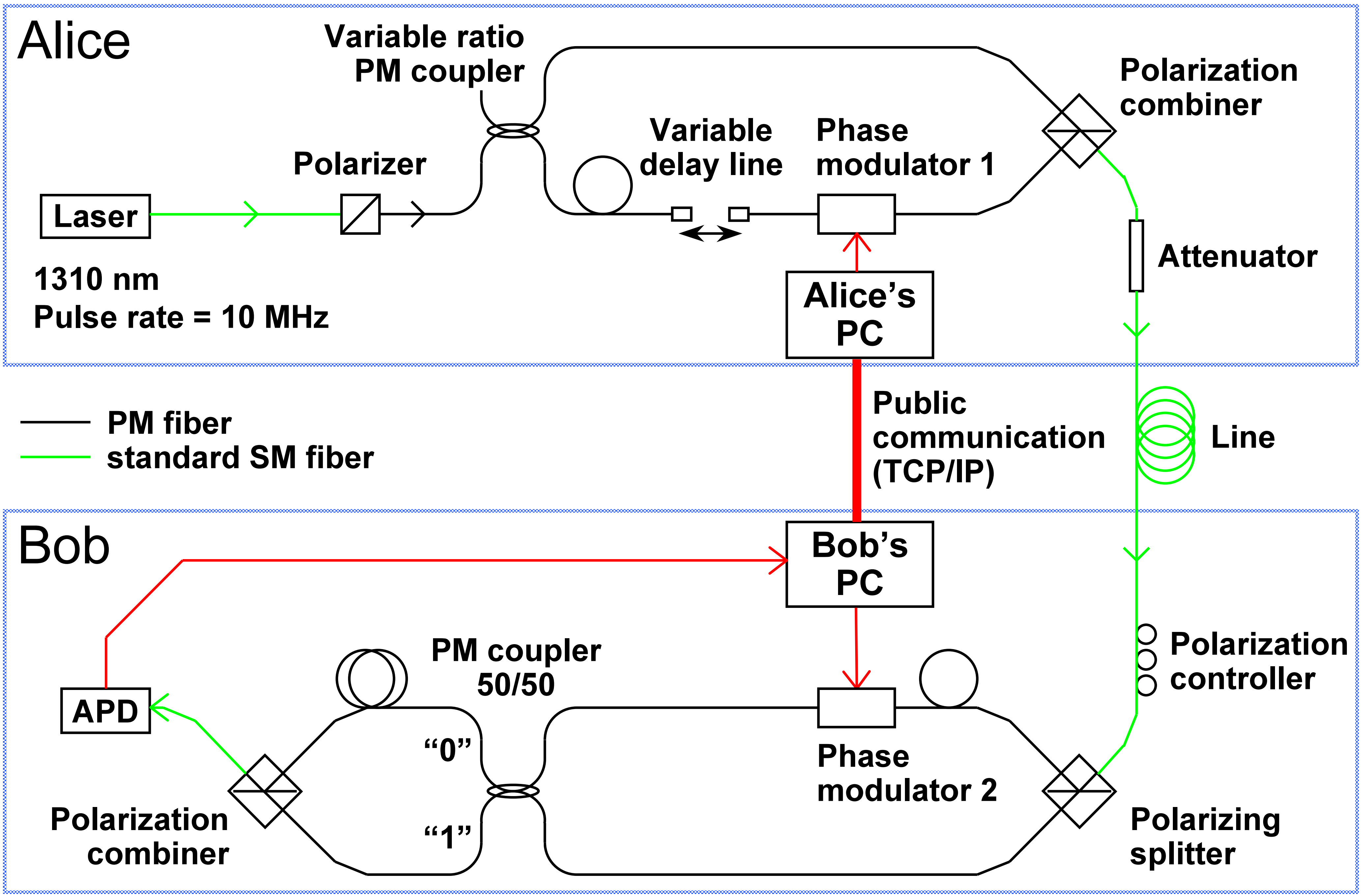








QKD setup


Alice
Variable ratio PM coupler
Polarization combiner
Variable delay line
Phase modulator 1
Polarizer
Laser
1310 nm
Pulse rate = 10 MHz
Attenuator
Alice's PC
PM fiber
standard SM fiber
Public communication (TCP/IP)
Line
Bob
Bob's PC
PM coupler 50/50
Polarization controller
APD
"0"
"1"
Phase modulator 2
Polarization combiner
Polarizing splitter

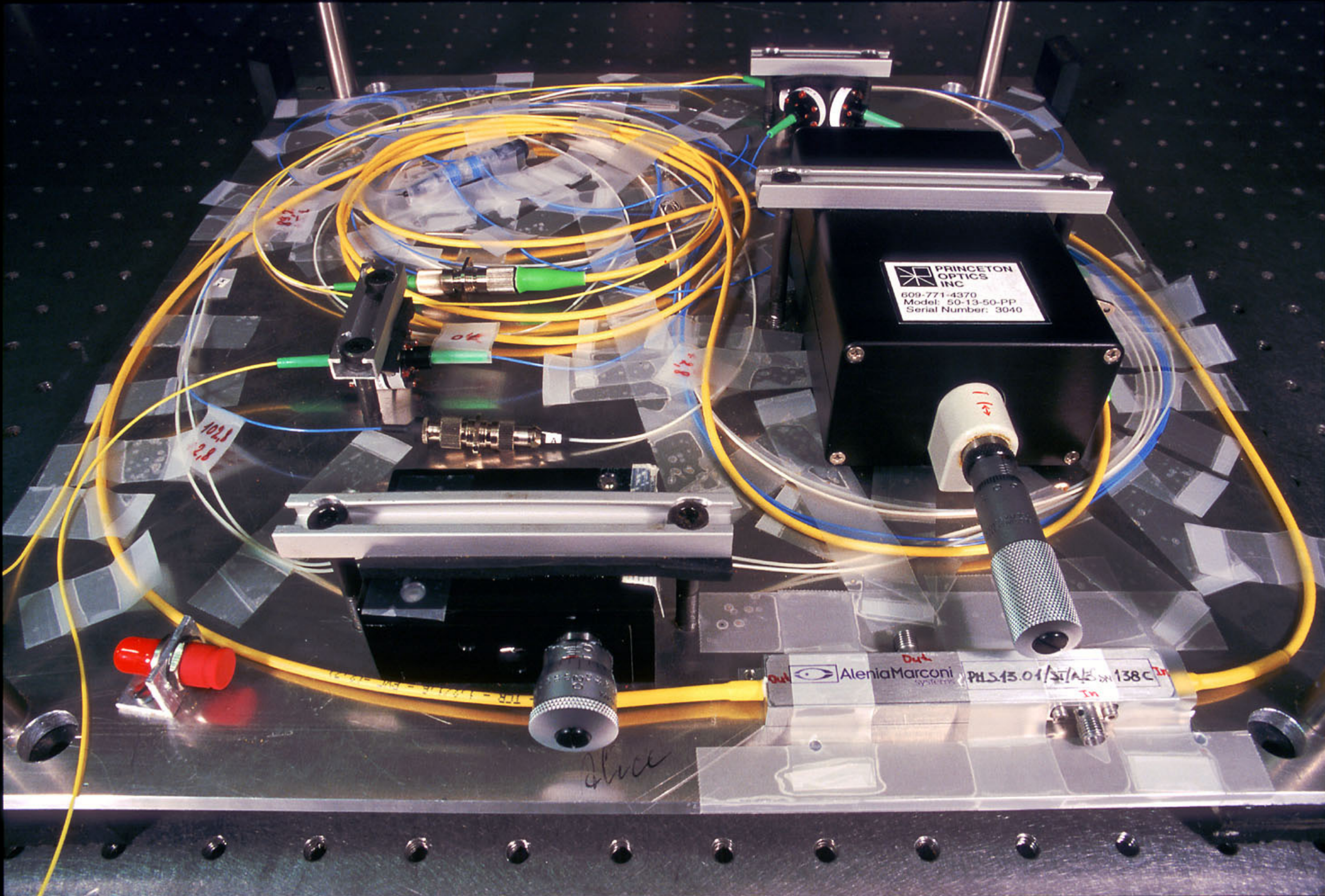


Photo 1. **Alice** (uncovered, no thermoisolation installed)

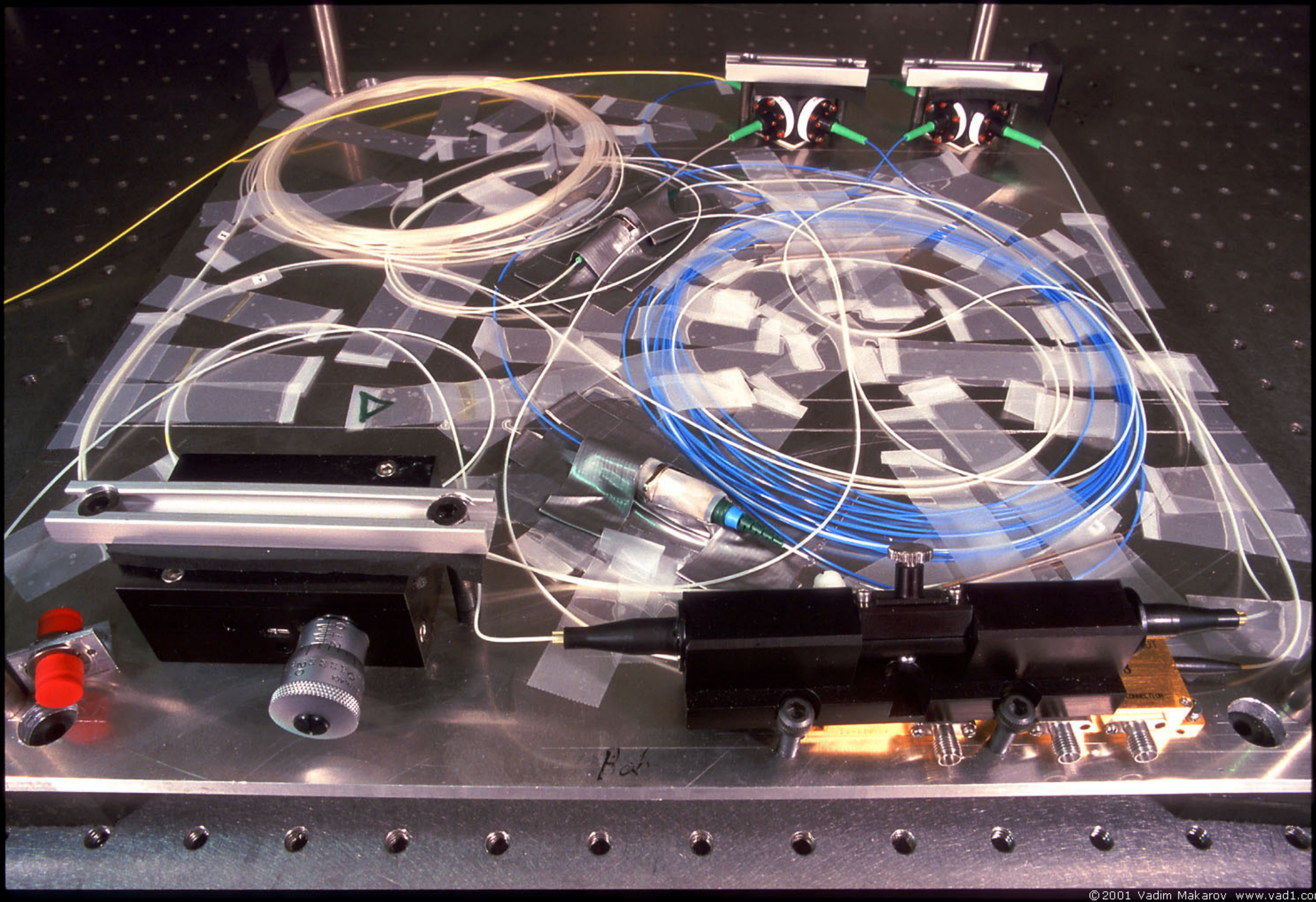


Photo 2. **Bob** (uncovered, no thermoisolation installed)

Tracking phase drift

To get phase accuracy $\Delta\varphi$ within ±10° ($\mathrm{QBER}_{\mathrm{opt}\,\Delta\varphi} < 1\%$), no more than N_a = ~200 detector counts per adjustment are required.

Optimally counted at ±90° points from the extreme of the interference curves. Exact required number of counts

$$N_a = \frac{2k^2}{\Delta\varphi^2}\left(\frac{1}{1-2(\mathrm{QBER})}\right)^2,$$

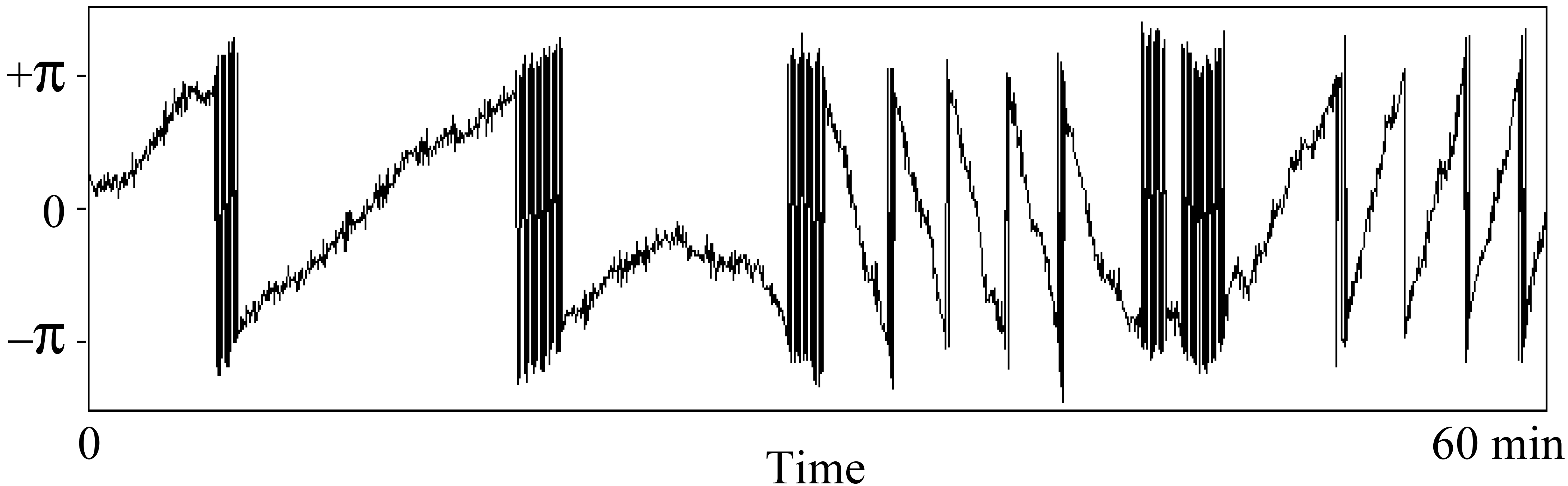
where *k* is the number of standard deviations of not exceeding $\Delta\varphi$.

J. Appl. Opt. **43**, 4385 (2004)

Tracking phase drift

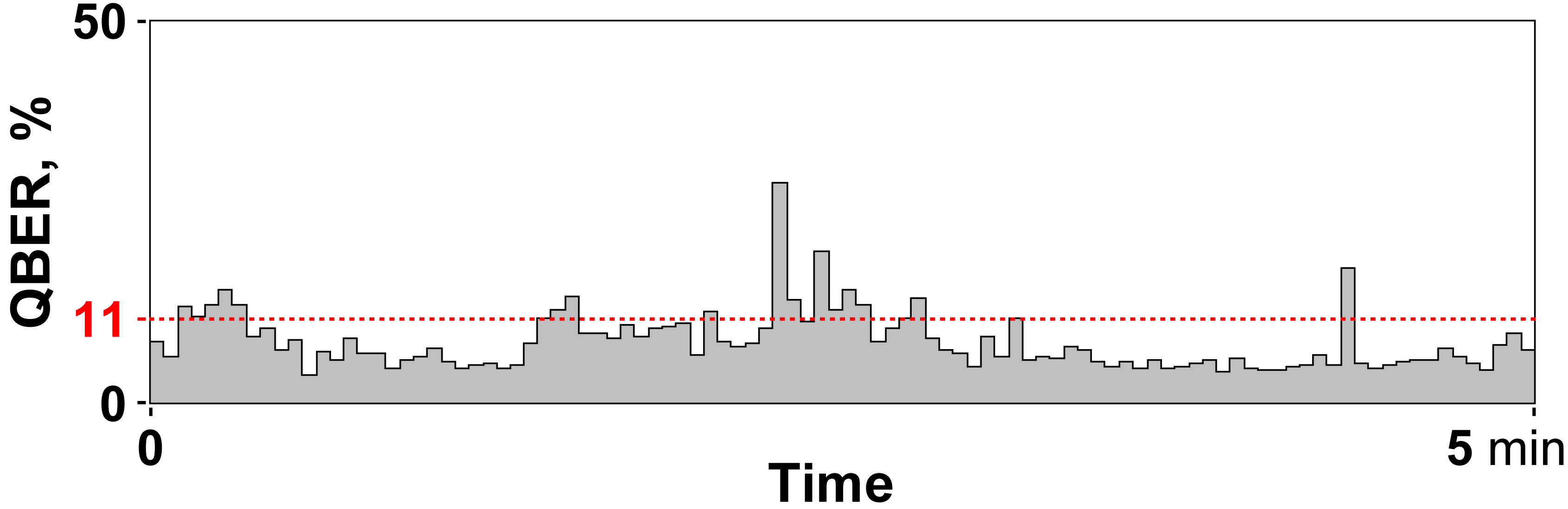
To get phase accuracy $\Delta\varphi$ within ±10° ($QBER_{opt\,\Delta\varphi} < 1\%$), no more than N_a = ~200 detector counts per adjustment are required.

Experiment: adjustment every 3 s, N_a = 230:



J. Appl. Opt. **43**, 4385 (2004)

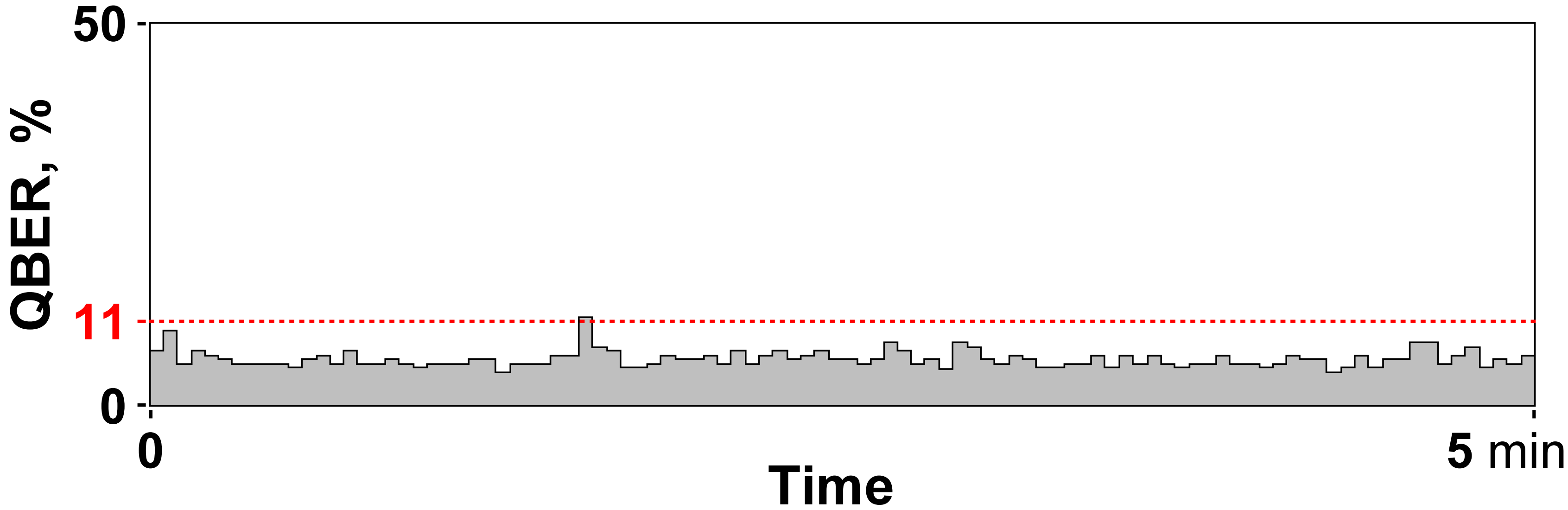
Test of QKD in laboratory conditions



Test run No. 1

best QBER

~ 4%

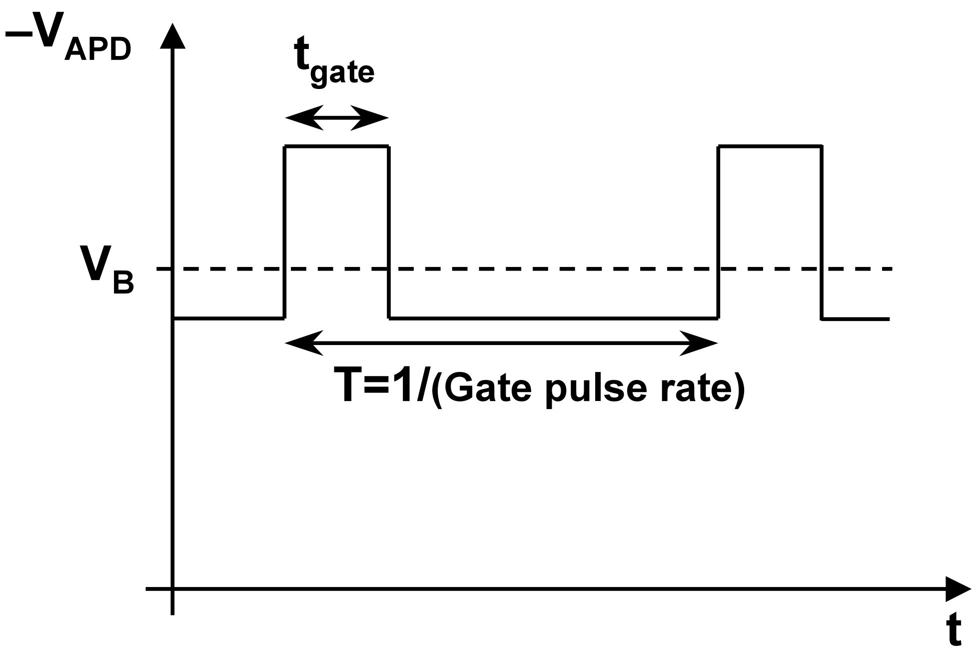


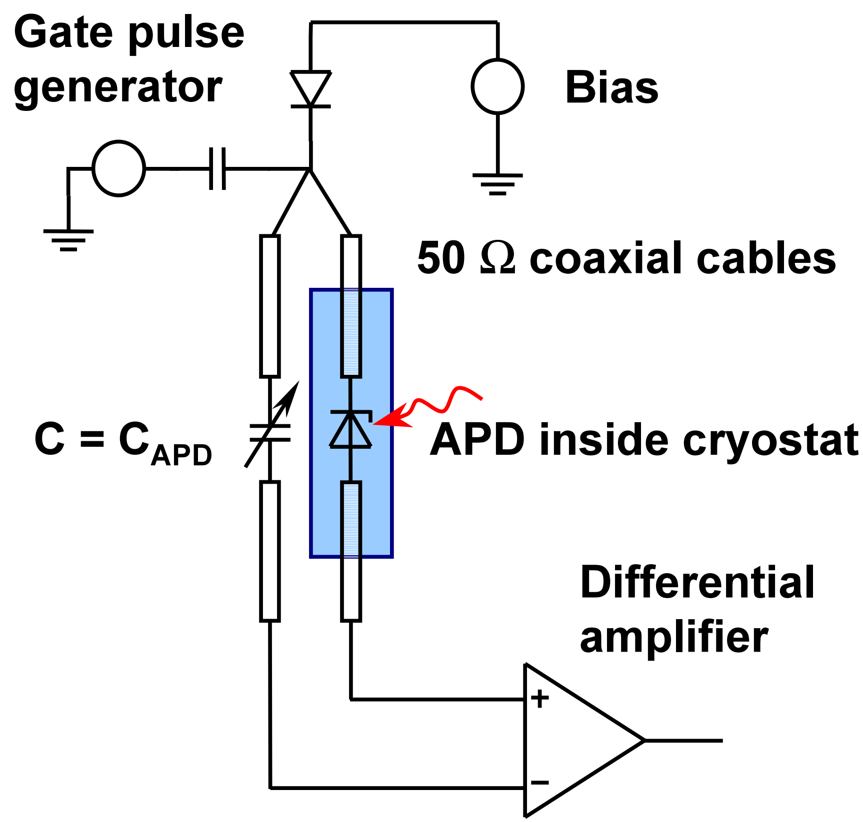
Test run No. 2

QBER =

5.7% average

Single photon detector: avalanche photodiode in Geiger mode





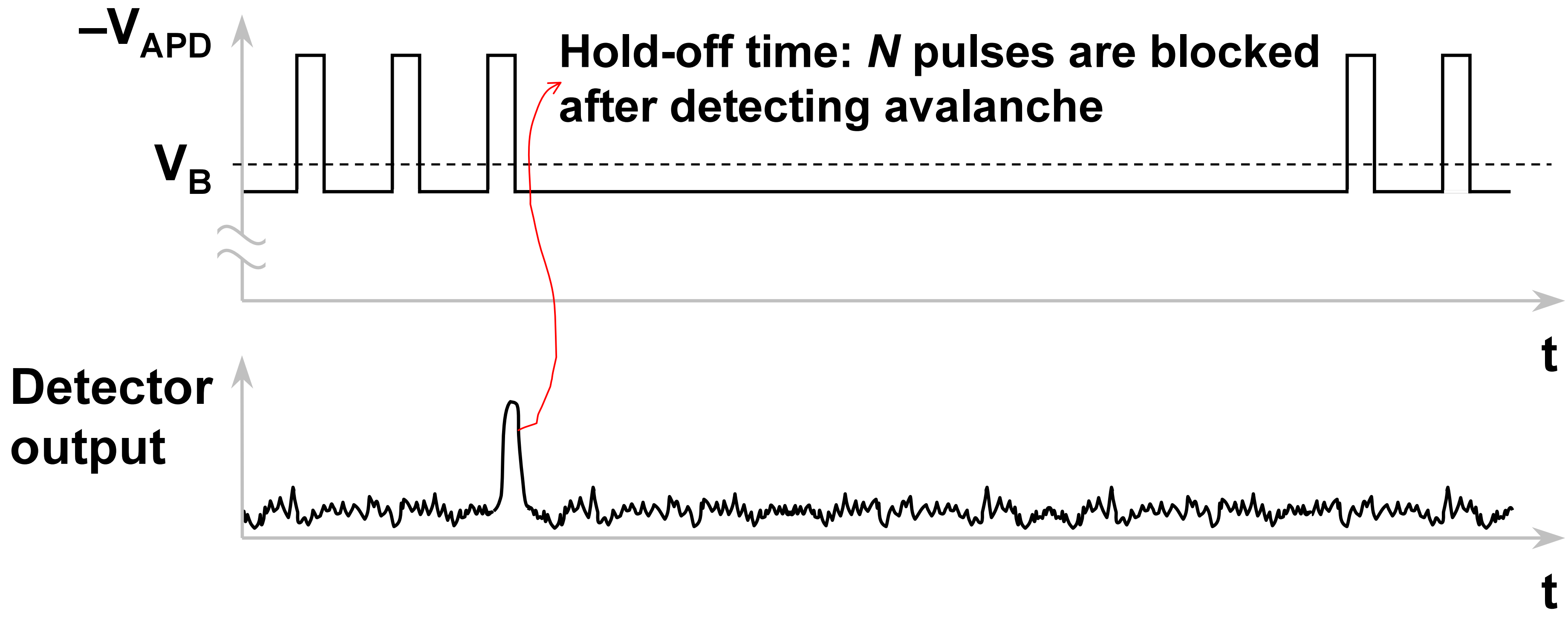
t_{gate} down to 1ns

Gate pulse rate = 20 MHz

APD: Ge FD312L

T=77K, QE=16%, DC=$5 \cdot 10^{-5}$

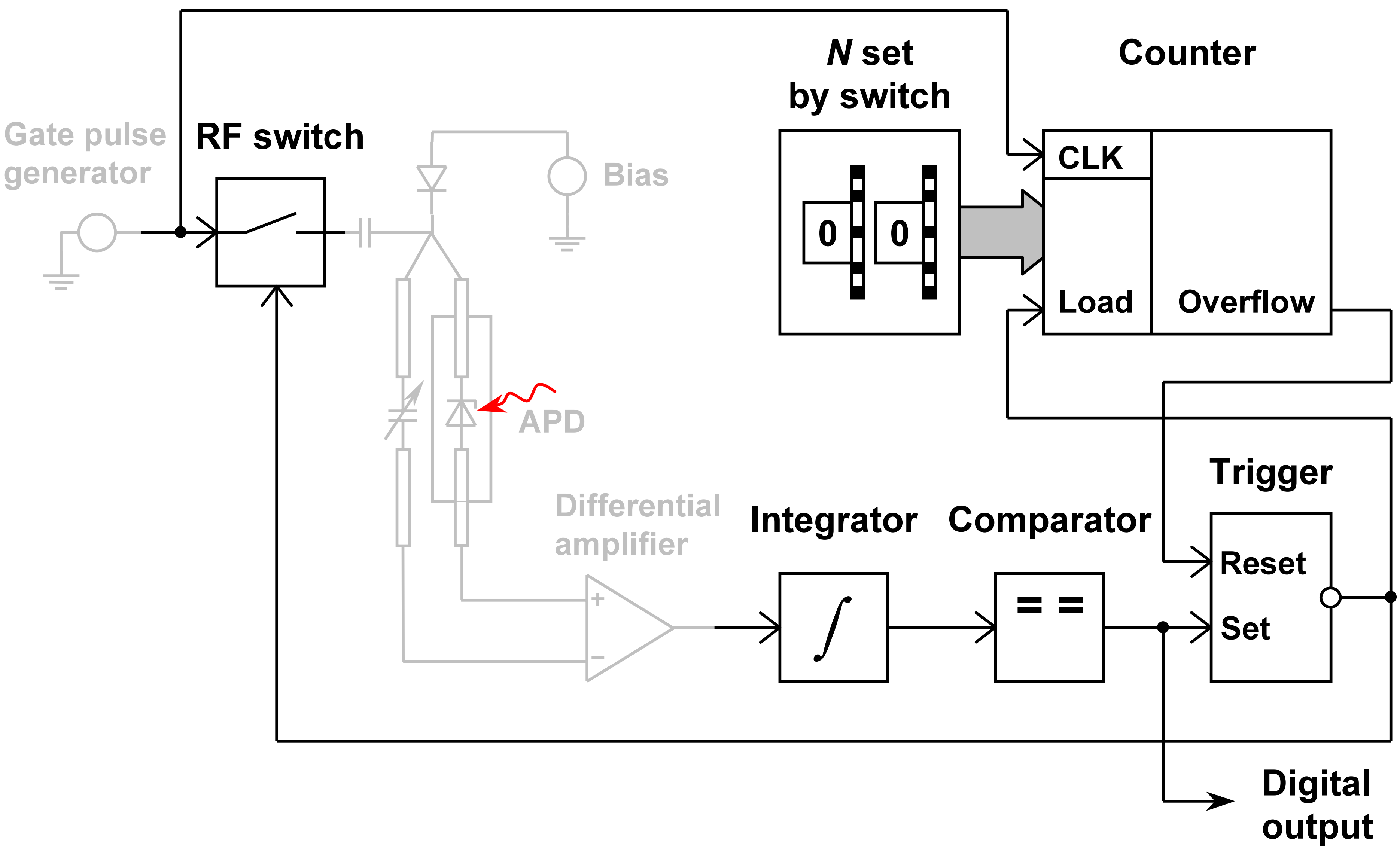
Afterpulse blocking



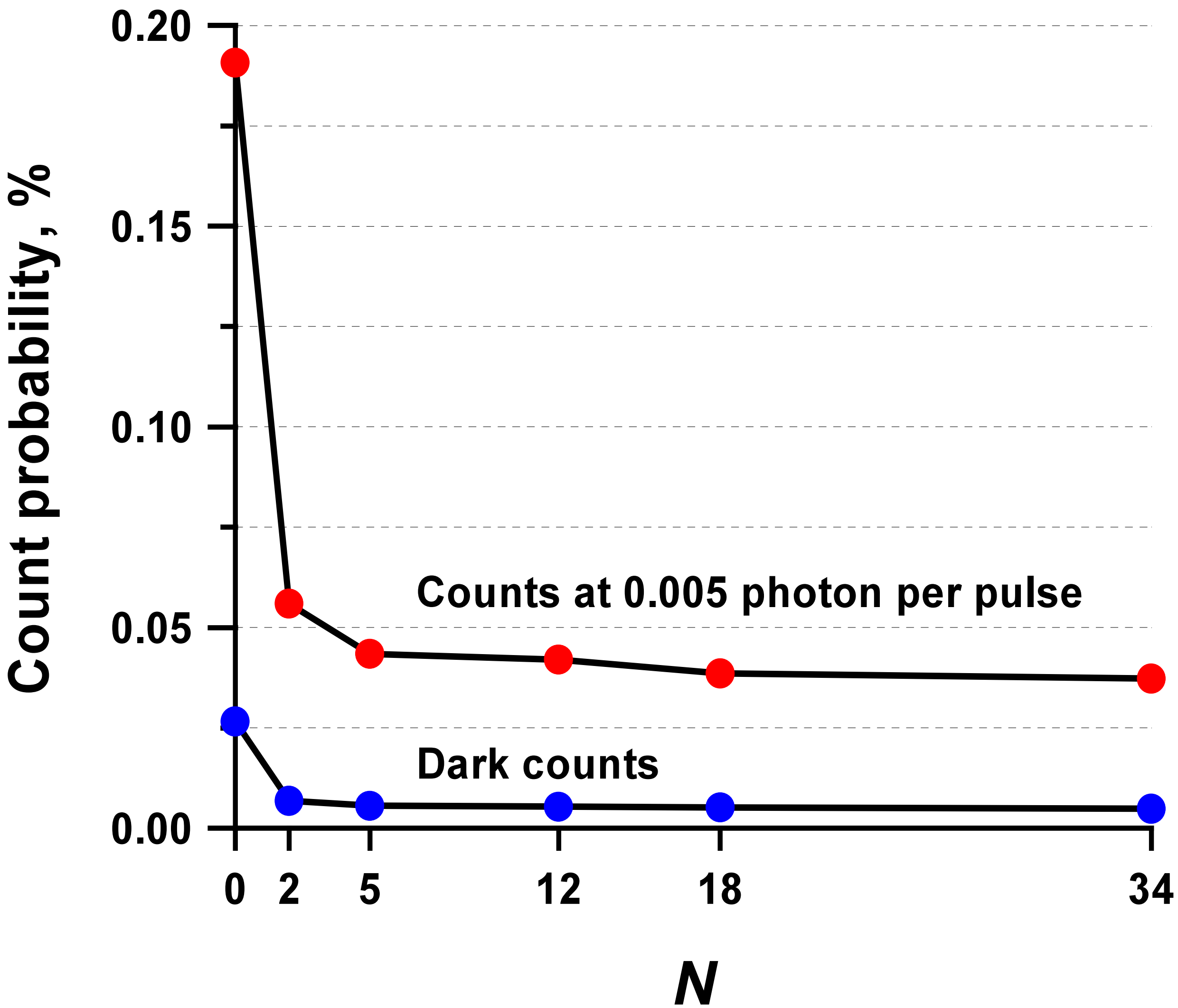
In QKD systems, probability of detecting a photon per pulse is always much lower than 1 (e.g., ~1/1000). This makes afterpulse blocking efficient, allowing without much loss in detection probability:

- **In our QKD system: 20 MHz gate pulse rate**
- **In principle: a few orders of magnitude faster gate pulse rate**

Hardware implementation of afterpulse blocking



Test of afterpulse blocking



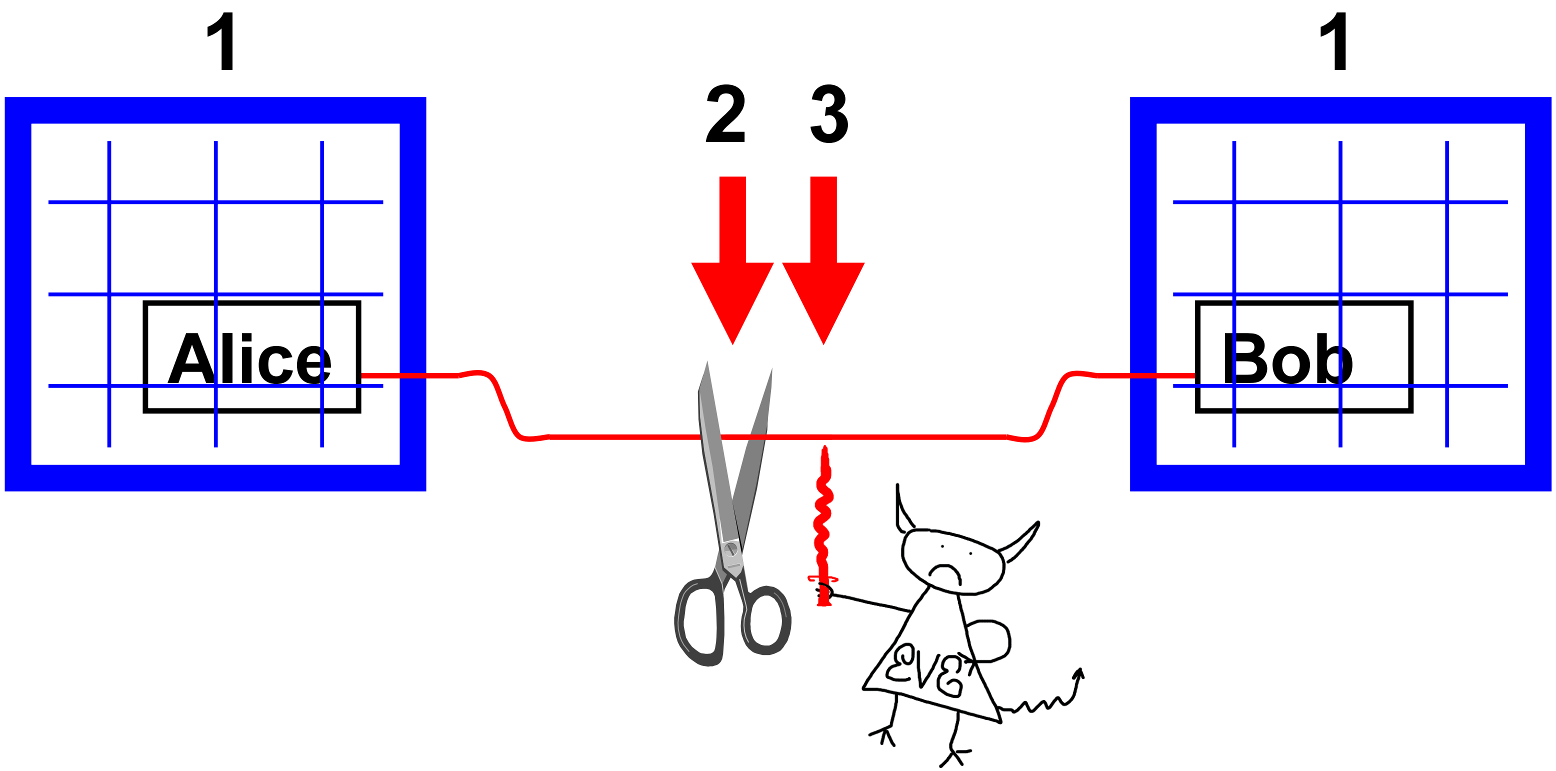
APD: Ge FD312L

Gate pulse rate = 12 MHz

QE = 7%

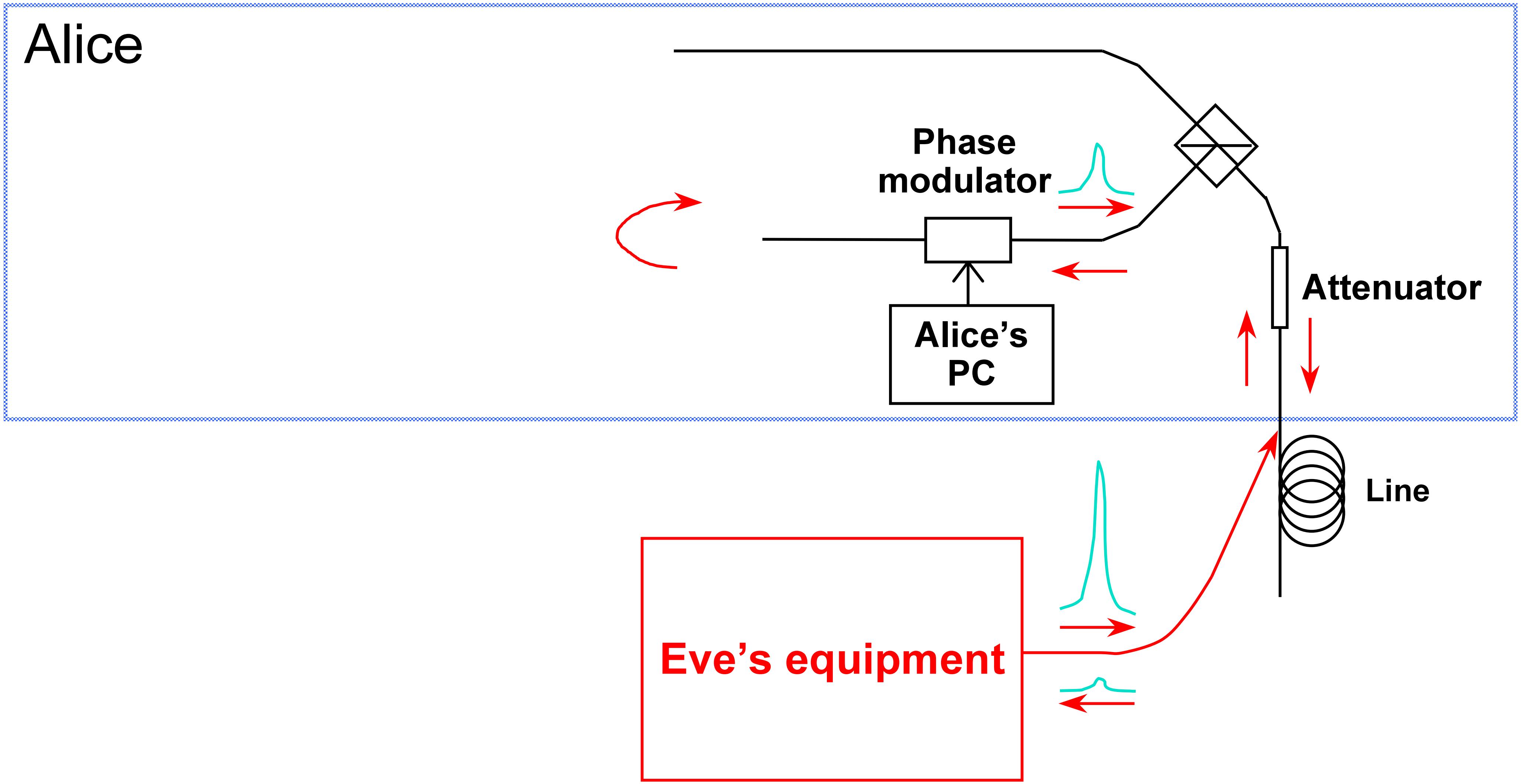
T = 77K

Quantum key distribution: components of security



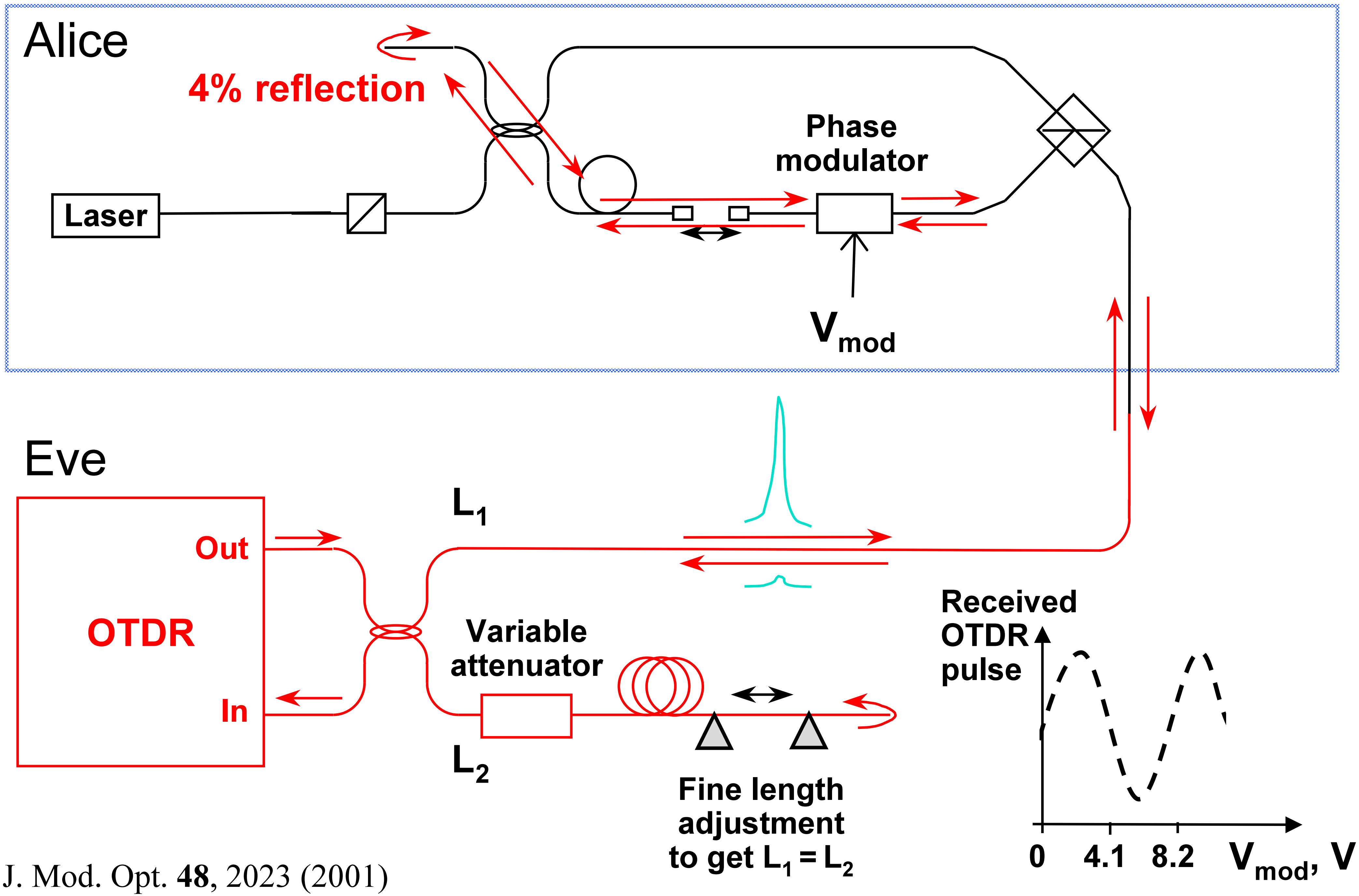
1. Conventional security; trusted equipment manufacturer
2. Security against quantum attacks
   – security proofs for idealized model of equipment
3. Loopholes in optical scheme
   – imperfections not yet accounted in the proof

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)

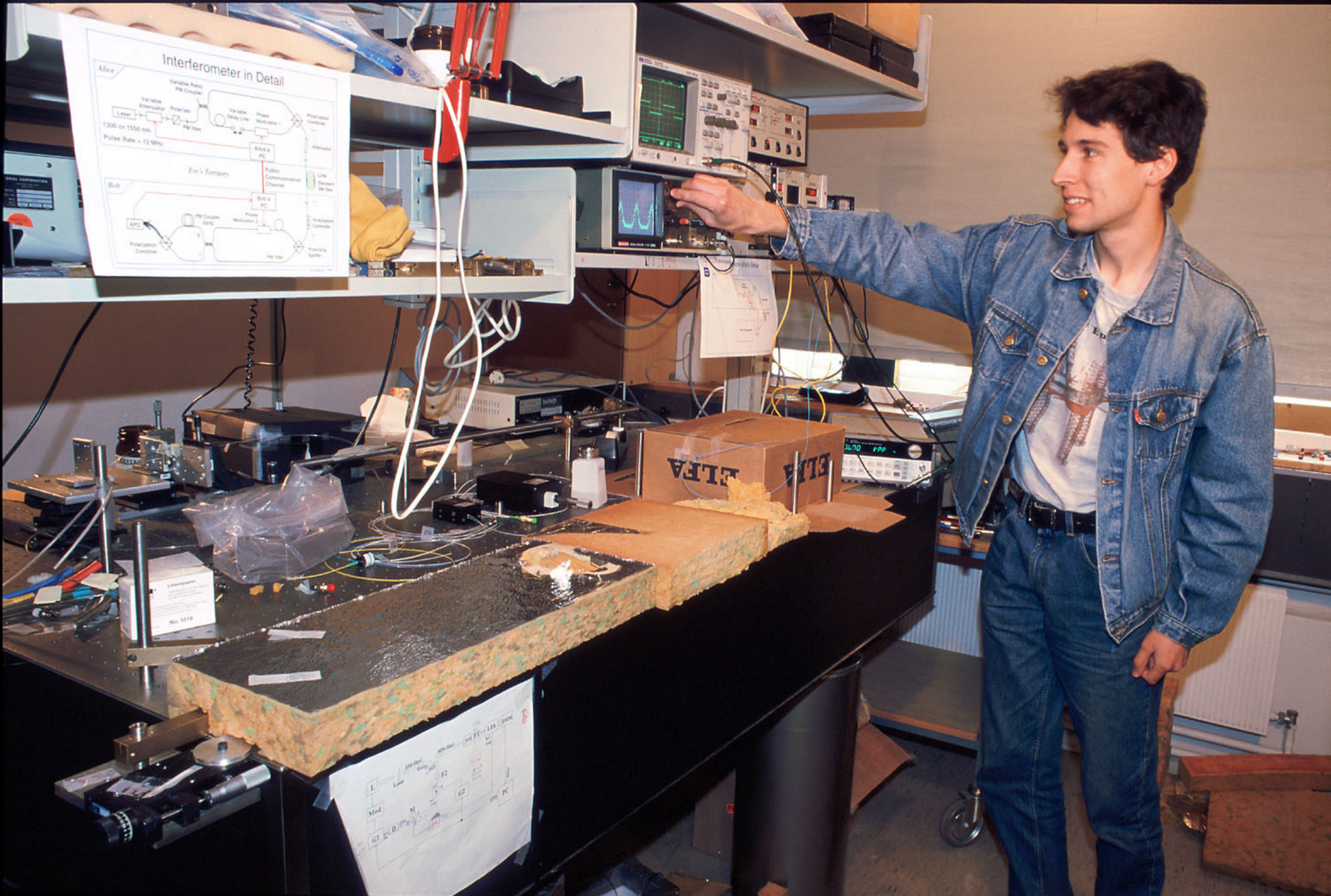
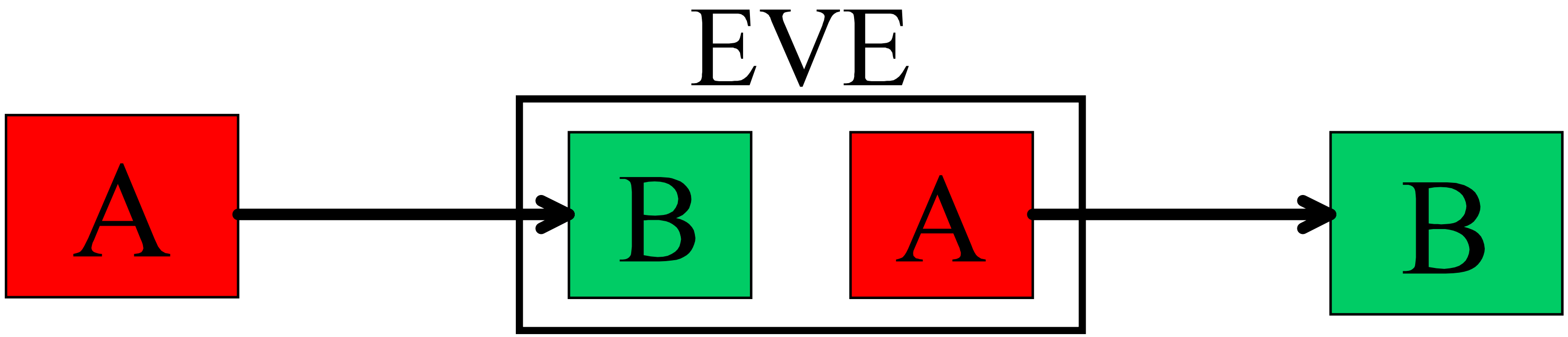


Photo 3. **Artem Vakhitov tunes up Eve's setup**

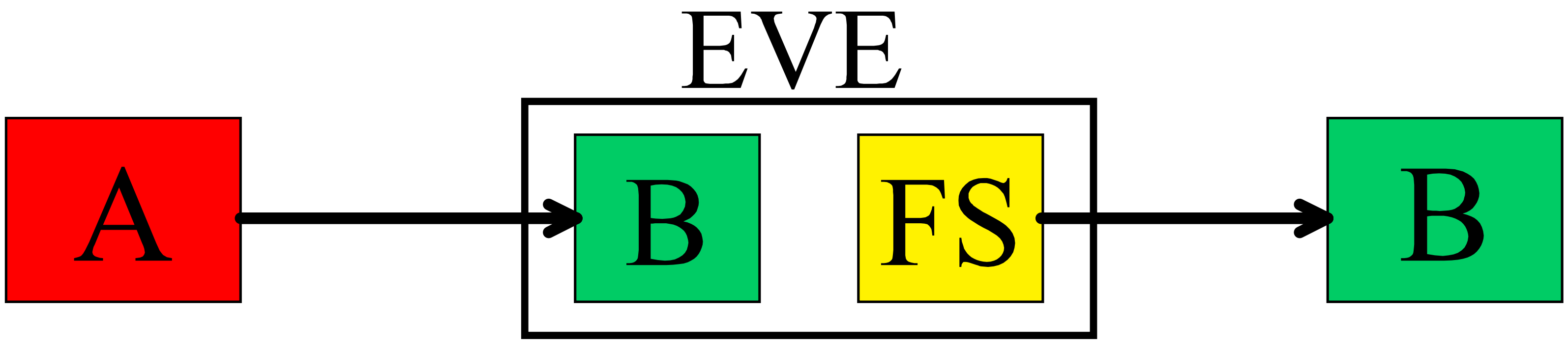
Faked states attack

Conventional intercept-resend:



ALARM!!!

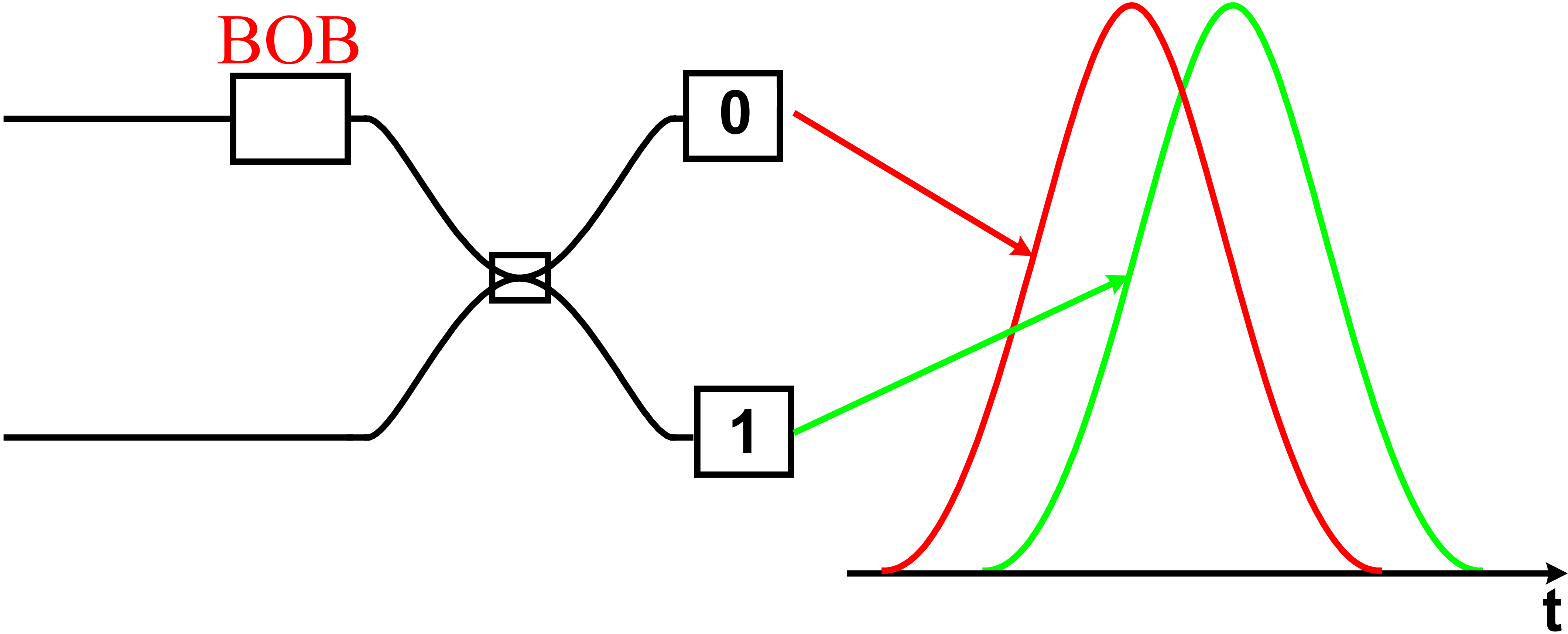
Faked states attack:



(no alarm)

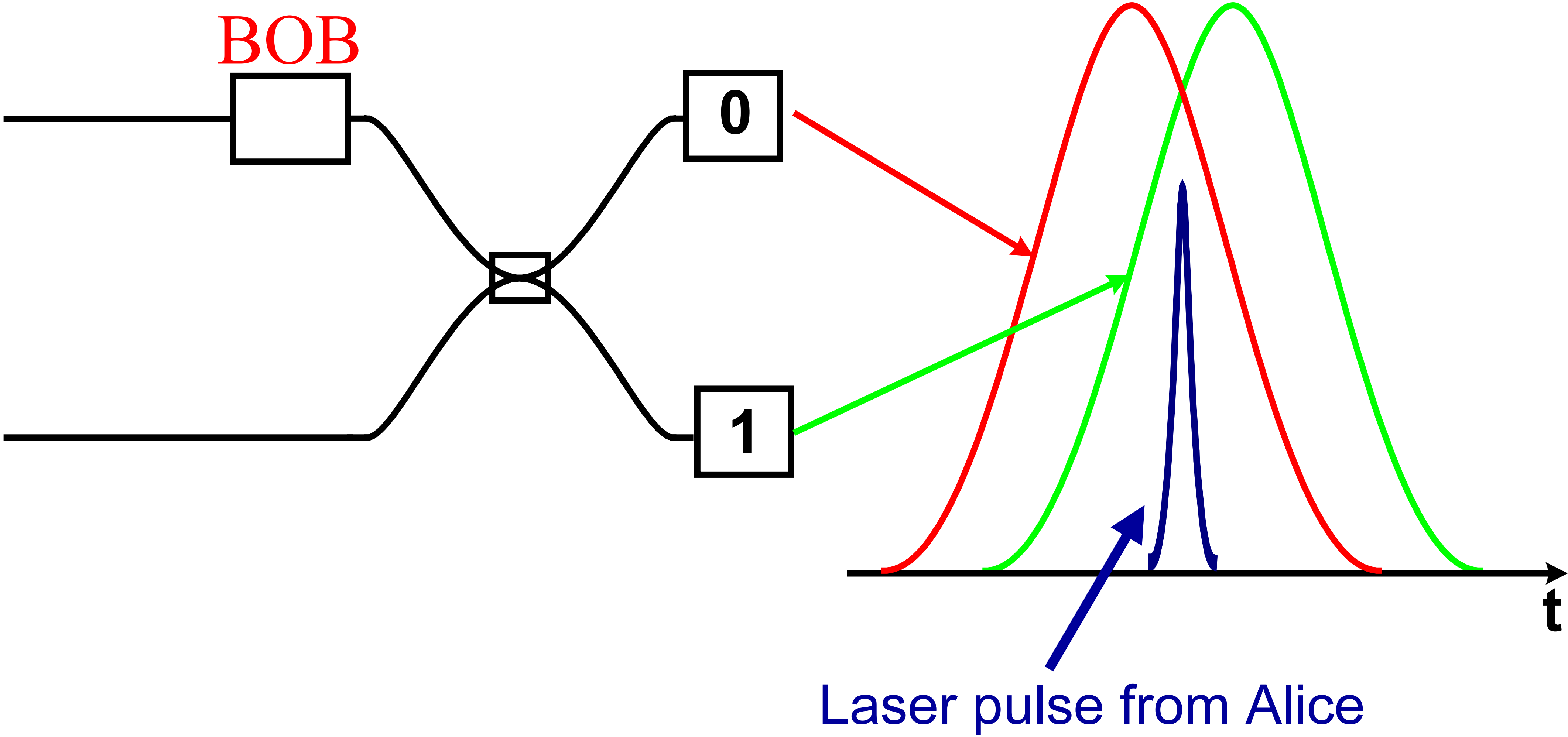
J. Mod. Opt. **52**, 691 (2005)

Exploiting common imperfection: detector gate misalignment



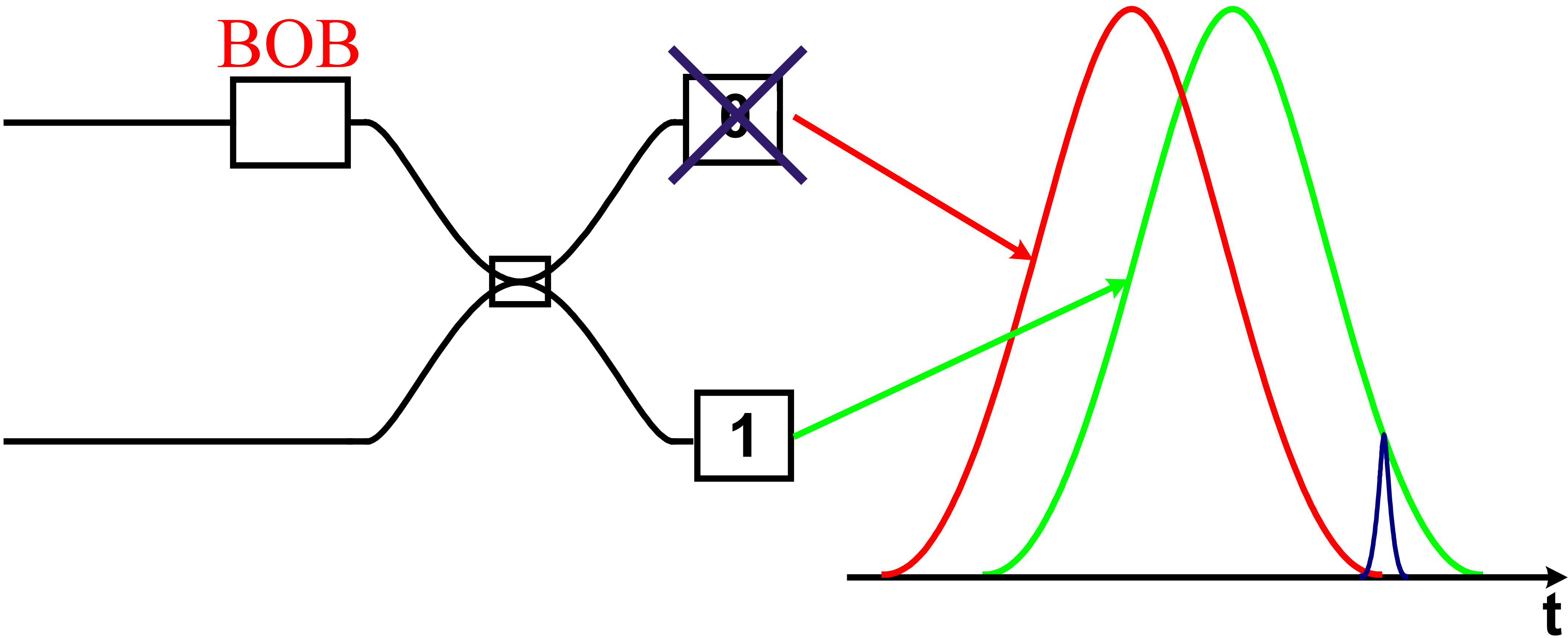
Phys. Rev. A **74**, 022313 (2006)

Detector gate misalignment



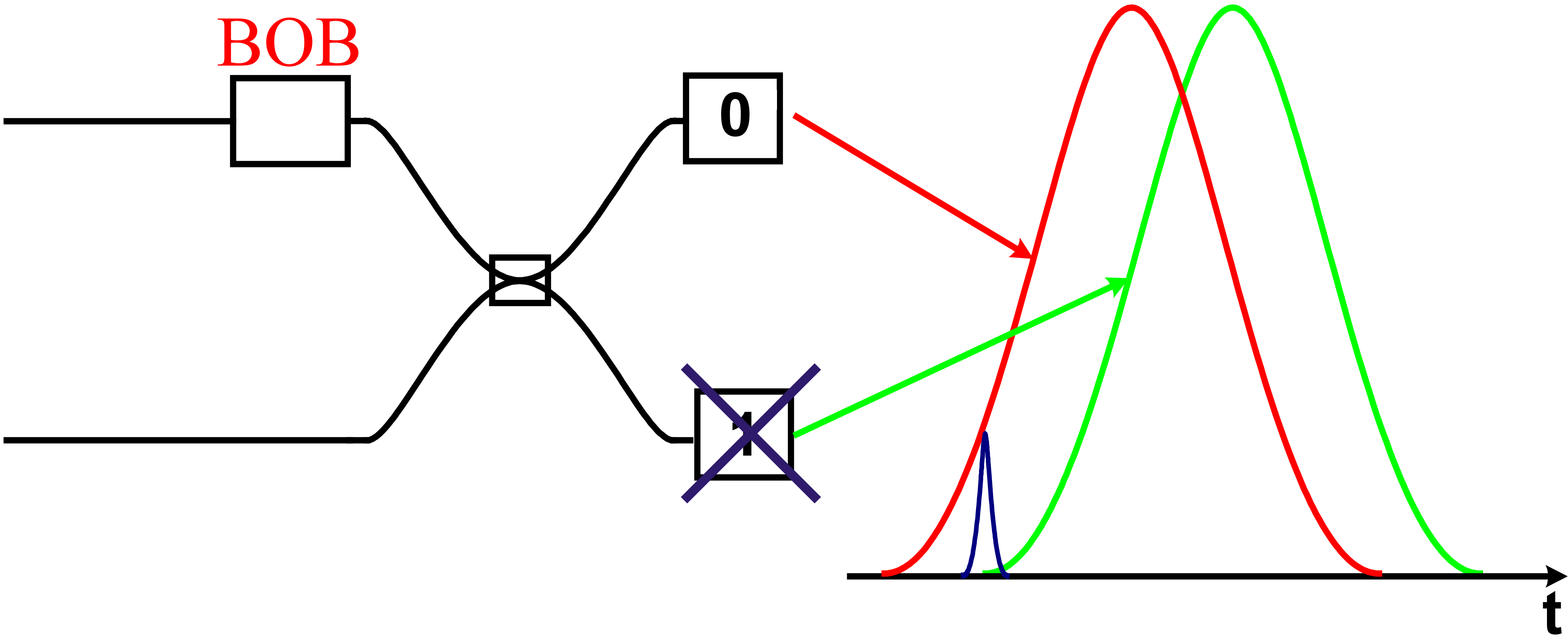
Phys. Rev. A **74**, 022313 (2006)

Detector gate misalignment



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

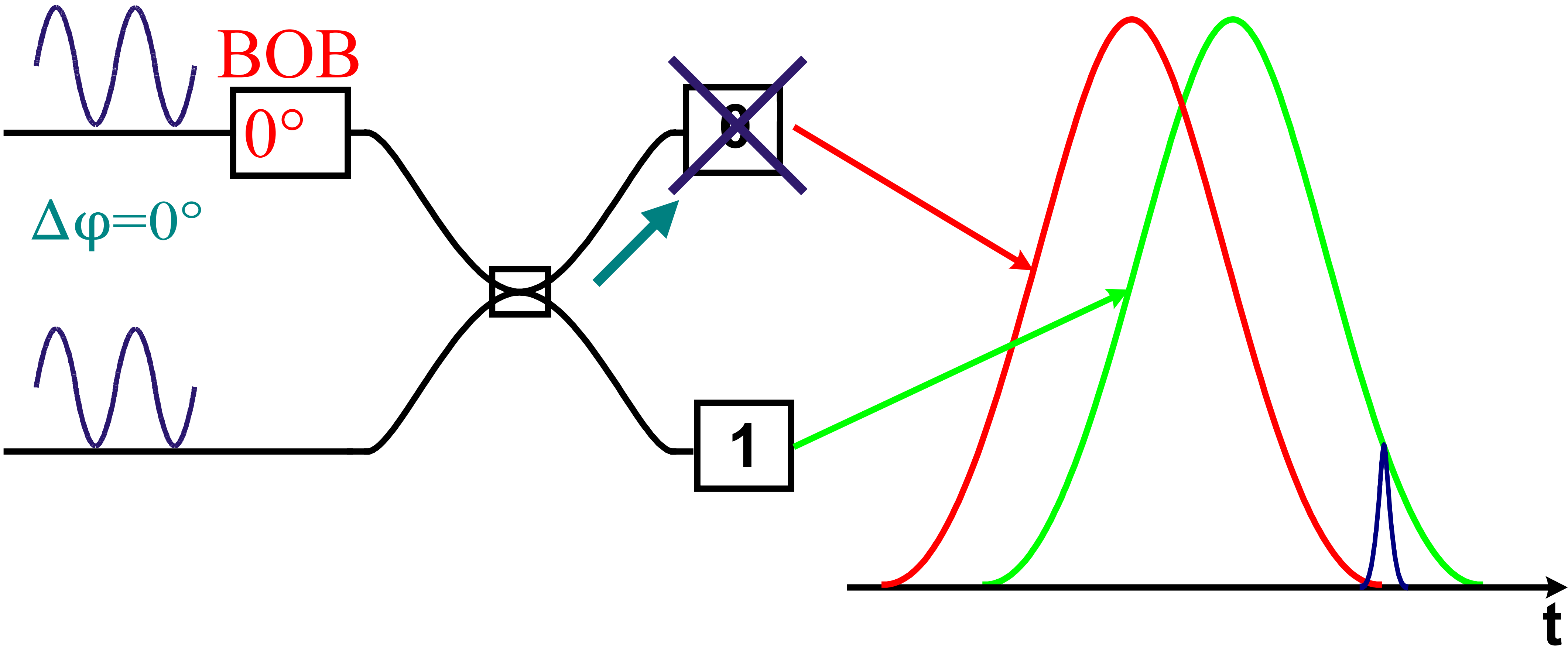
Detector gate misalignment



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

Detector gate misalignment

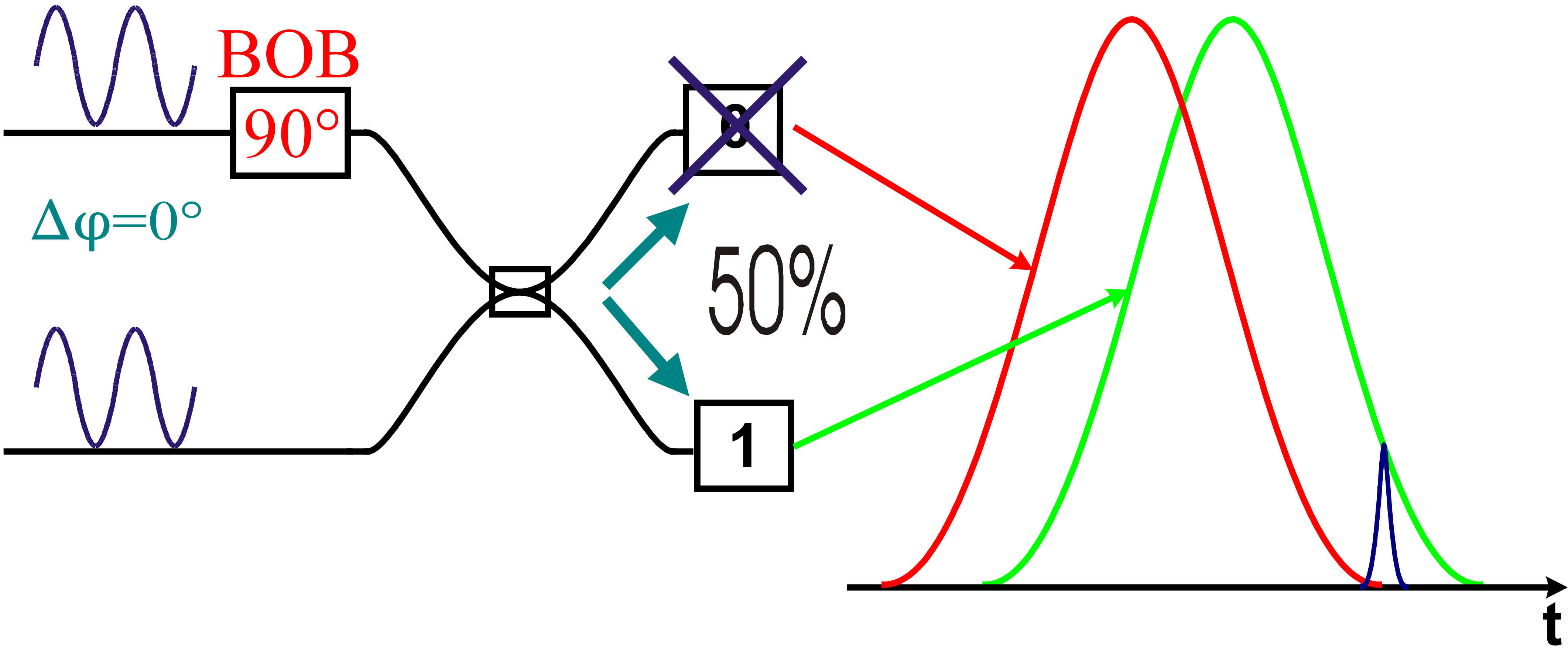
Example: Eve measured with basis Z (90°), obtained bit 1



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

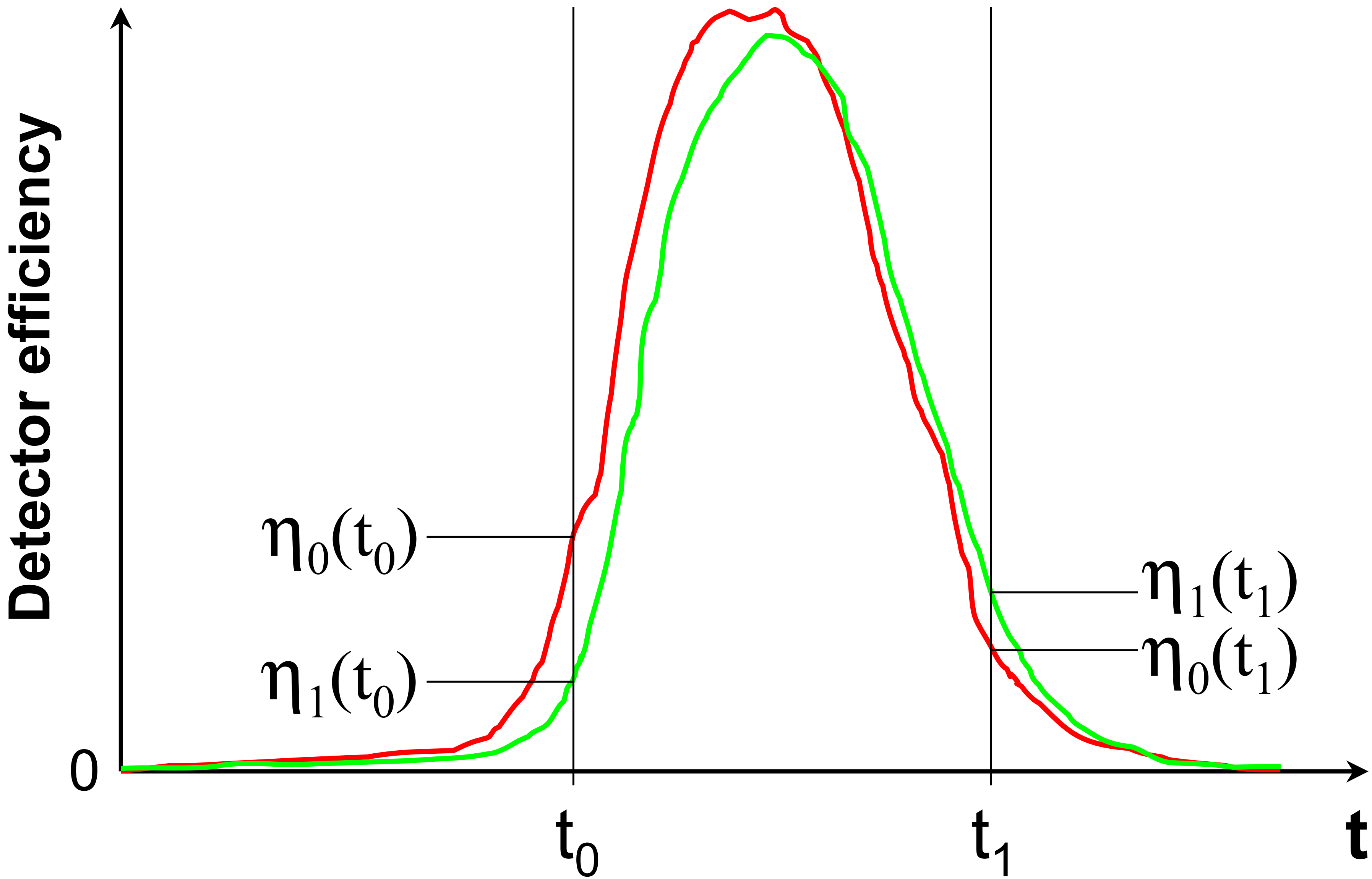
Detector gate misalignment

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



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

Partial efficiency mismatch



Partial efficiency mismatch

A. Practical faked states attack:

$$\mathrm{QBER} = \frac{P(\text{error})}{P(\text{arrive})} = \frac{2\eta_0(t_1) + 2\eta_1(t_0)}{\eta_0(t_0) + 3\eta_0(t_1) + 3\eta_1(t_0) + \eta_1(t_1)}$$

$\Rightarrow$ In the symmetric case (when $\eta_1(t_0)/\eta_0(t_0) = \eta_0(t_1)/\eta_1(t_1)$),
Eve causes less than 11% QBER if mismatch is larger than 1:15

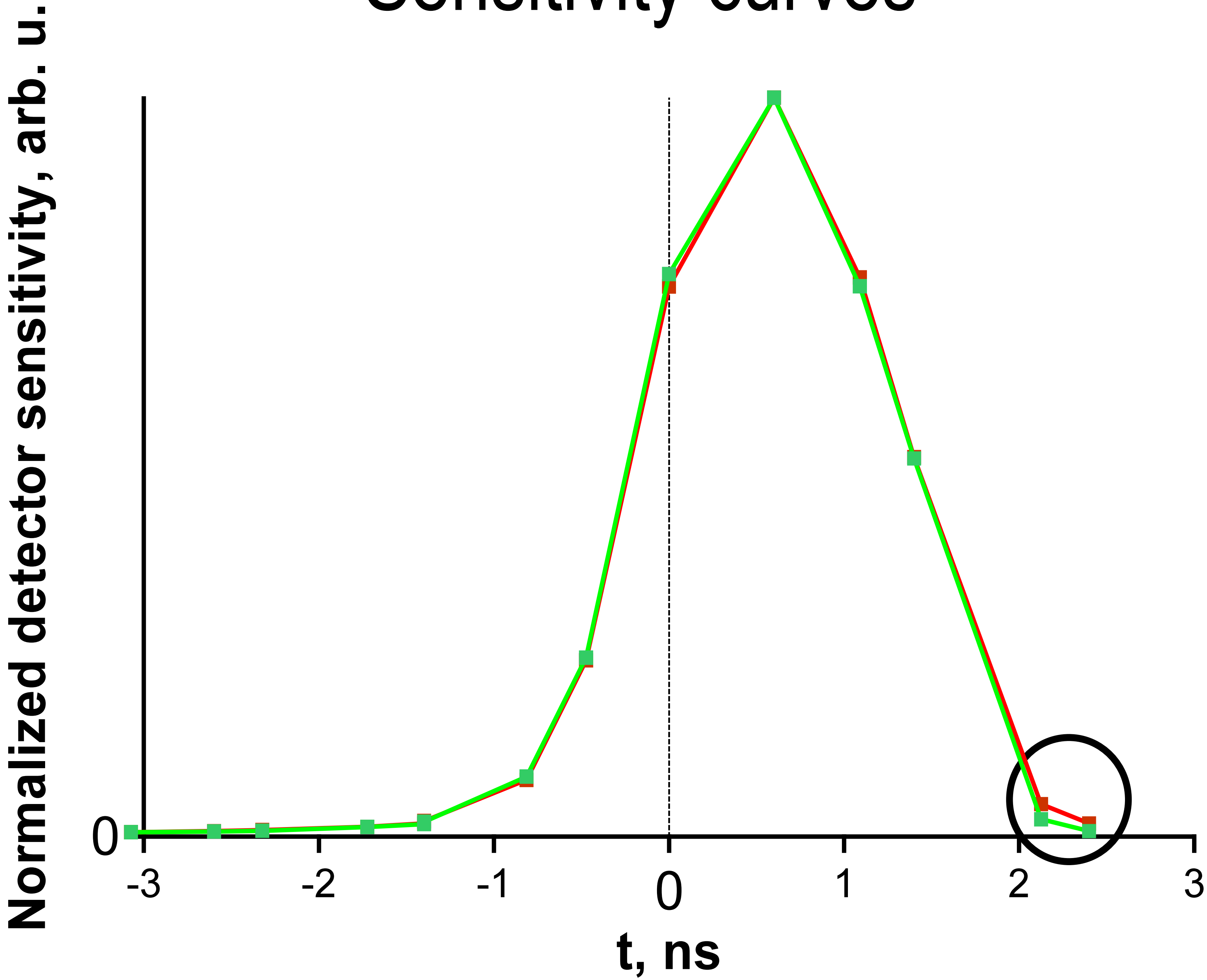
B. General security bound (incomplete):

$$\mathrm{QBER} = \frac{\eta\delta}{1 + \eta\delta - \delta} \approx \eta\delta,$$

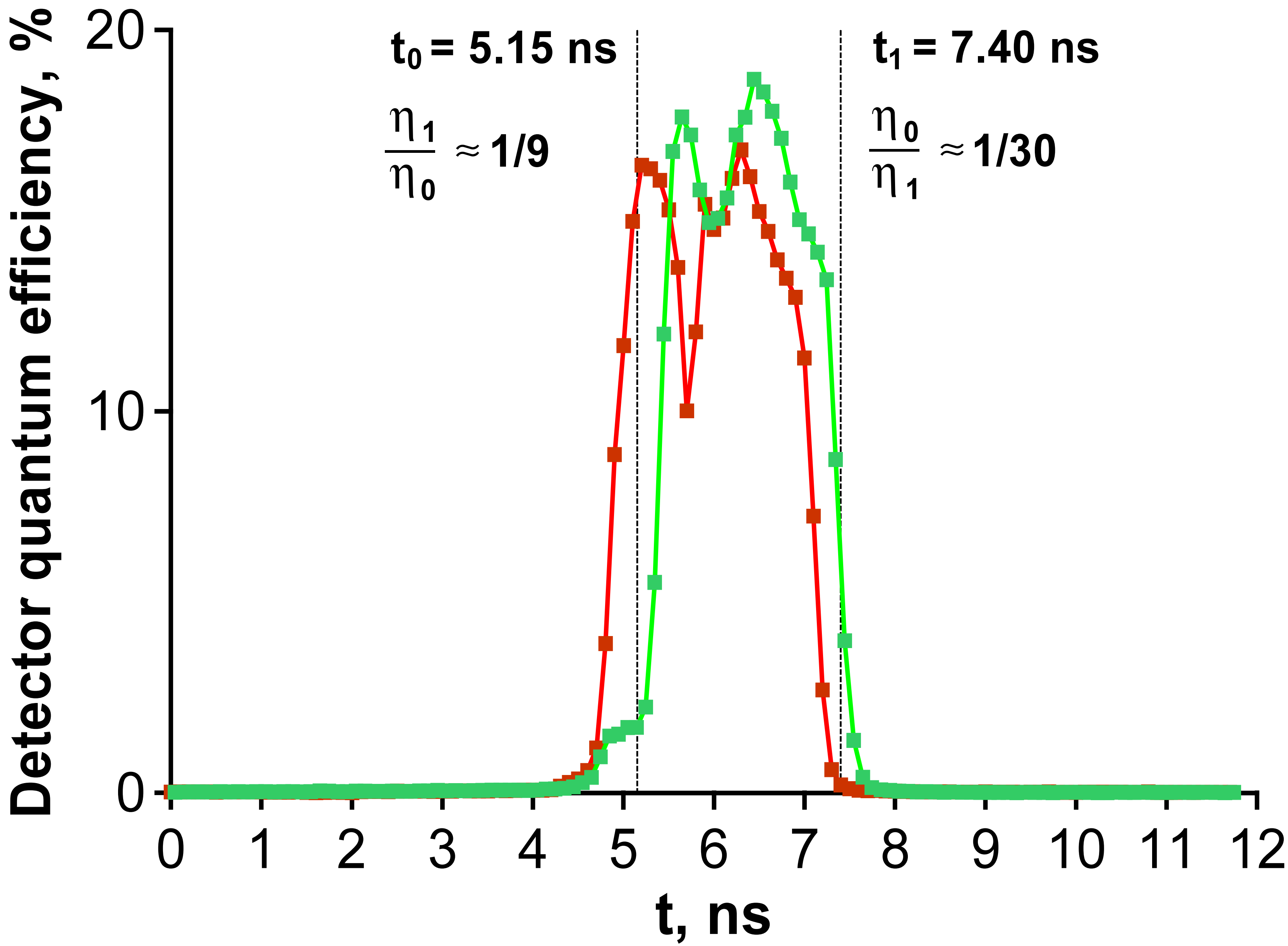
where

$$\eta = \min\left\{ \min_t \frac{\eta_1(t)}{\eta_0(t)}, \min_t \frac{\eta_0(t)}{\eta_1(t)} \right\}$$

Detector model 1.
Sensitivity curves



Detector model 2.
Sensitivity curves at low photon number μ=0.5



Detector efficiency mismatch

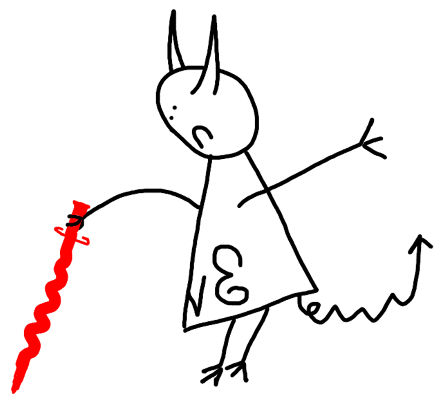
- **Detector efficiency mismatch is a problem for many protocols and encodings: BB84 (considered above), SARG04, phase-time, DPSK and Ekert protocols.**
  [quant-ph/0702262]

- **Control parameter *t* that changes detector efficiencies shall not be necessarily timing; it can be, e.g., wavelength or polarization.**

- **The worst-case mismatch, no matter how small, must be characterized and accounted for during privacy amplification.**

Conclusion

- **A phase tracking technique and detector with afterpulse blocking were successfully developed. (QKD was demonstrated with a very limited success.)**



- **Our group has built *unique expertise* in quantum cryptanalysis of attacks via optical loopholes. Several attacks have been proposed, studied in detail, and protection measures suggested.**

Possible future research

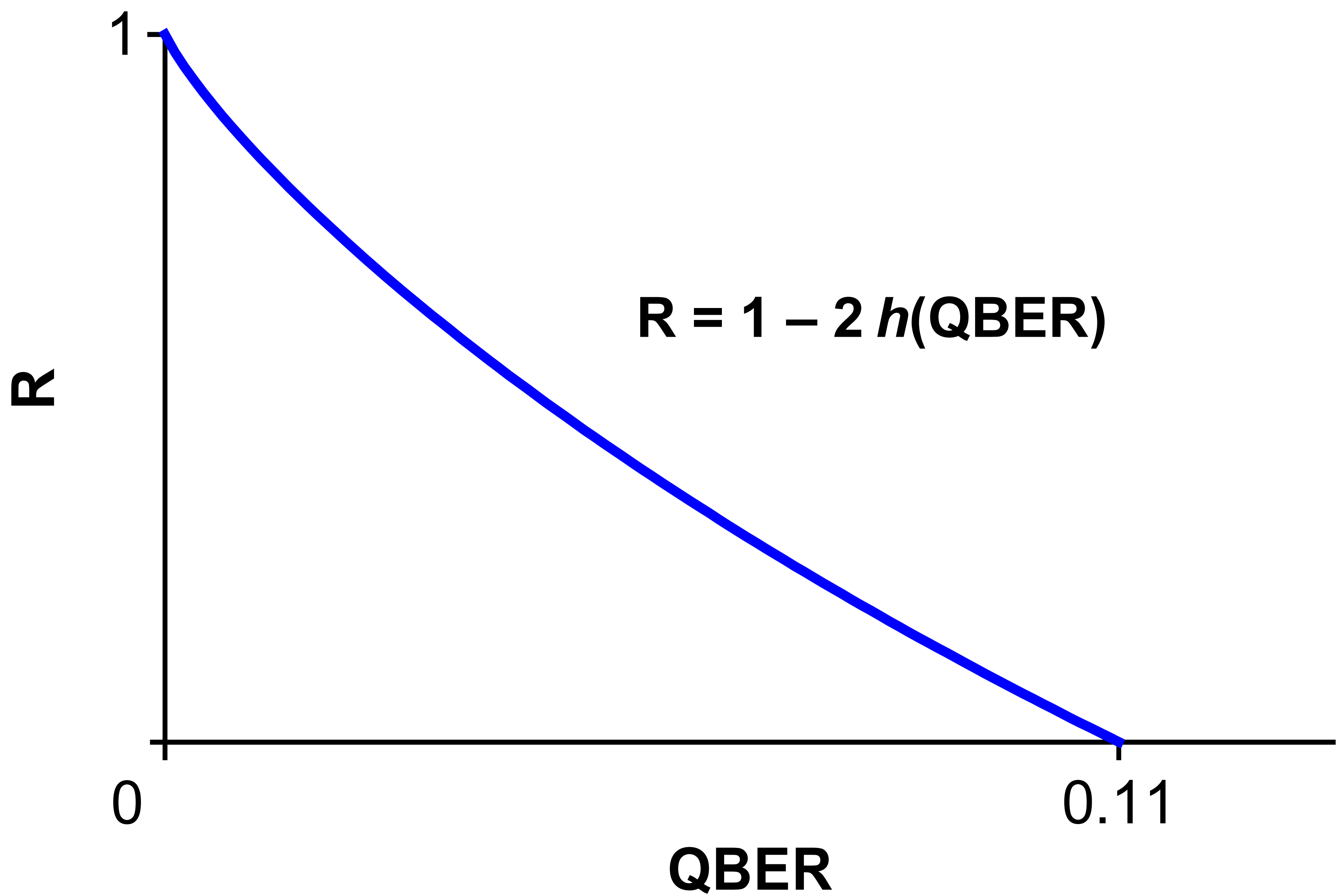
- **Continuing security studies beyond those presented in the thesis; we have experimented with passively-quenched Si APD; we are trying to incorporate detector efficiency mismatch into general proof... With sufficient financing, a study of high-power damage can be attempted.**

- **Improving the QKD experiment, demonstrating it over at least ~20 km distance. Performance of detector and phase tracking can be more accurately characterized.**

- **The QKD field is abound with novel ideas that can be tried...**

Optional slides

Handling errors in raw key



Commercial offers (as of late 2006)

MagiQ Tecnologies

USA

id Quantique

Switzerland

Standard VPN router + QKD equipment for frequent key changes

Several other companies also have the QKD technology, but are not selling yet

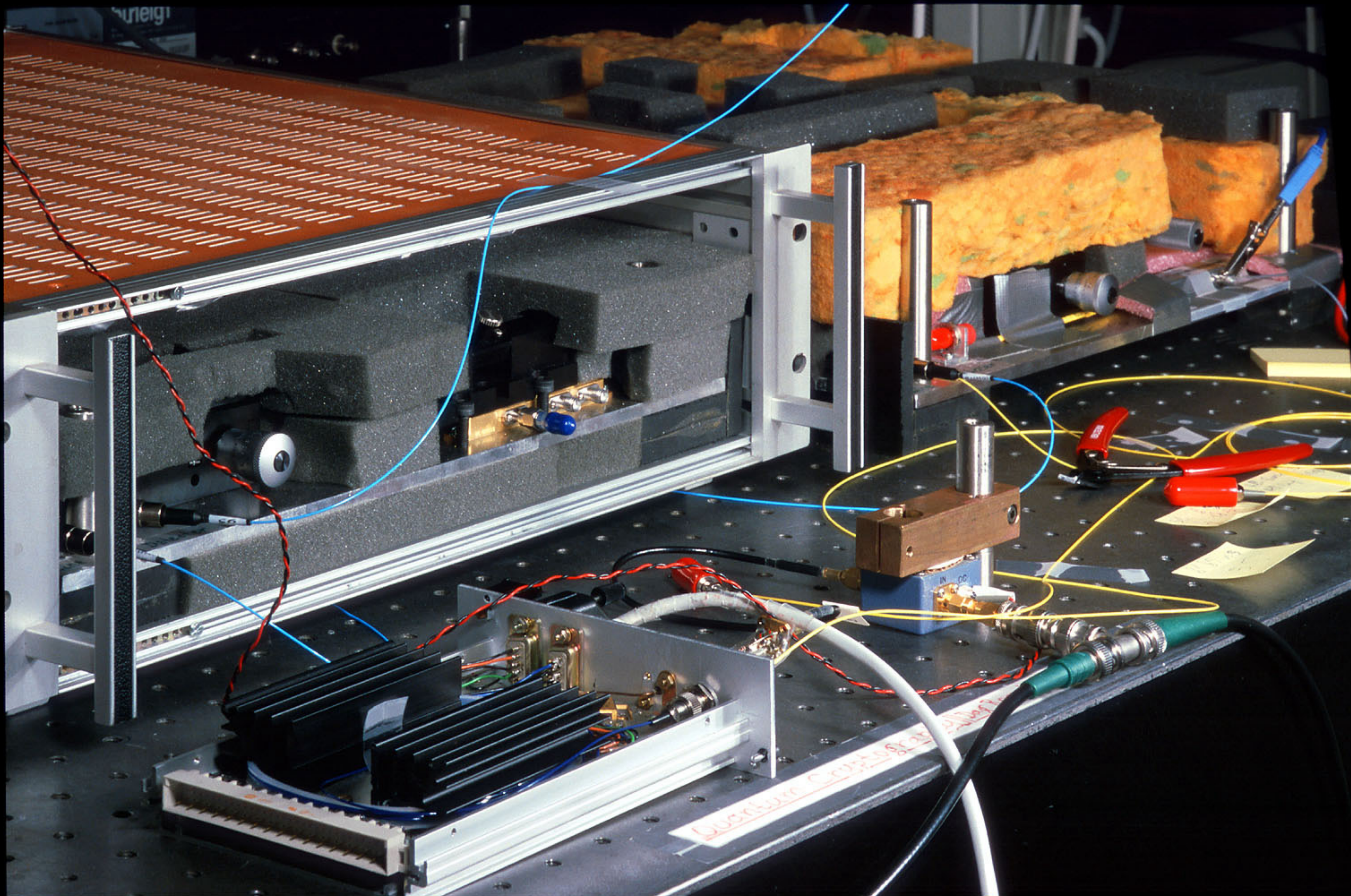
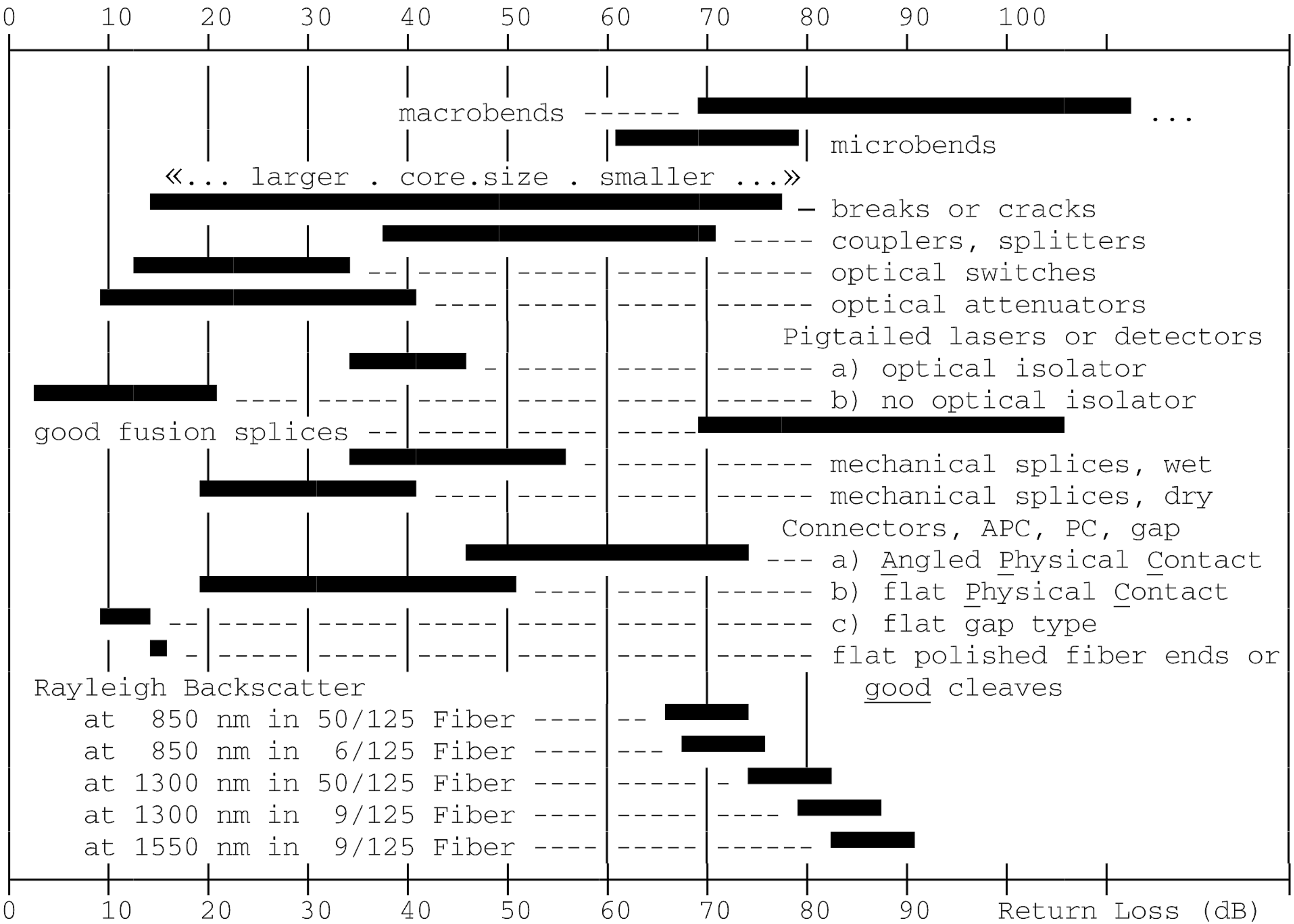


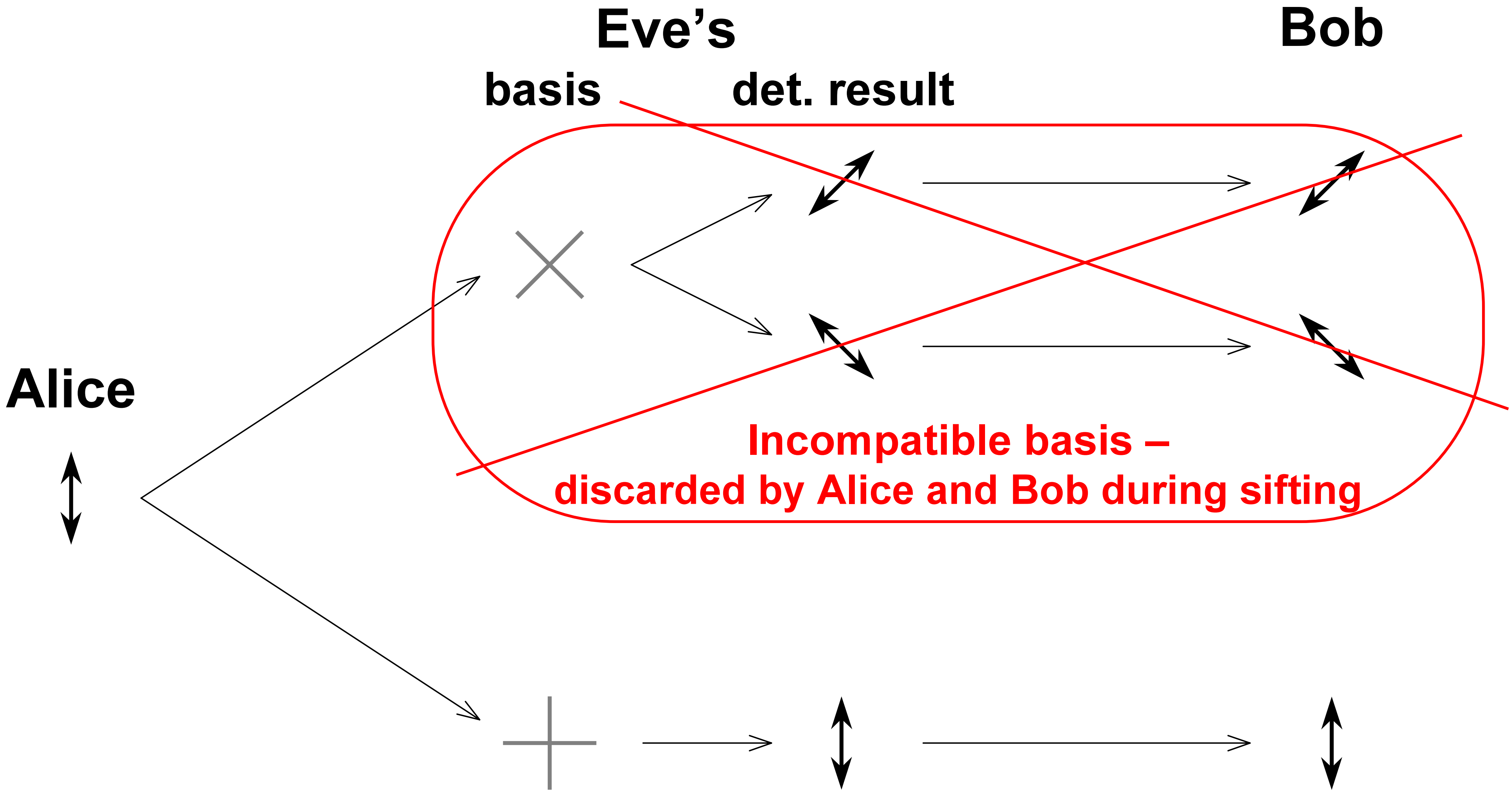
Photo 4. **Bob** (left) and **Alice** (right), thermoisolation partially installed



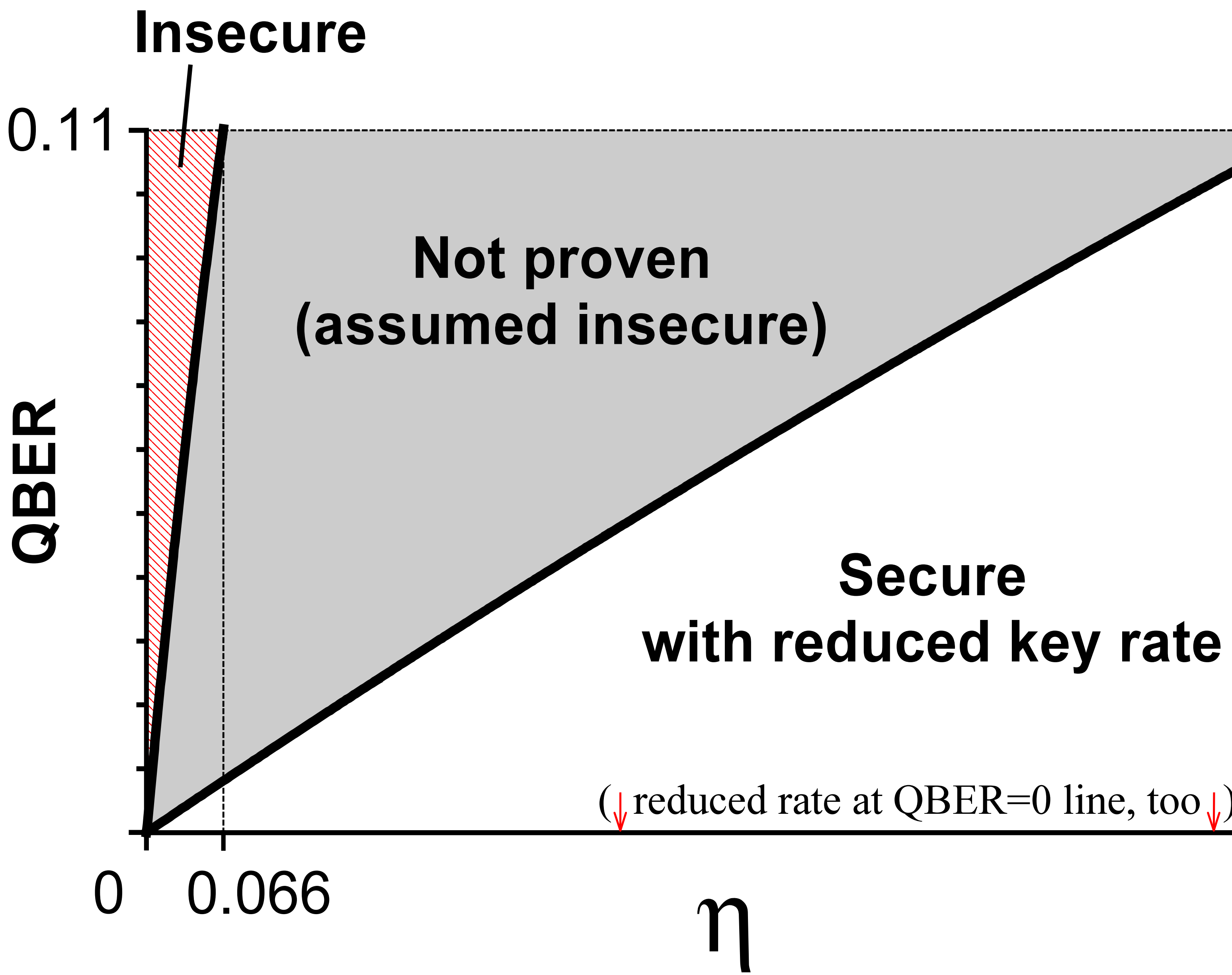
Typical values of reflection coefficients for different fiber-optic components

(courtesy Opto-Electronics, Inc.)

(Eve's basis = Bob's basis) is sufficient for eavesdropping



Security state of QKD system




Trondheim
St. Petersburg
Norway
Sweden
Finland
Denmark
Estonia
Latvia
Lithuania
Russia
Byelarus
North Cape
Hammerfest
ICE HOTEL
Kiruna
Narvik
Kemi
Oulu
Oslo
Bergen
Stockholm
Helsinki
Tallinn
Riga
Vilnius
Copenhagen
Geiranger
Gothenburg
Oskarshamn
Uppsala
Gotland
Oland
Bornholm
Kaliningrad
Gdansk