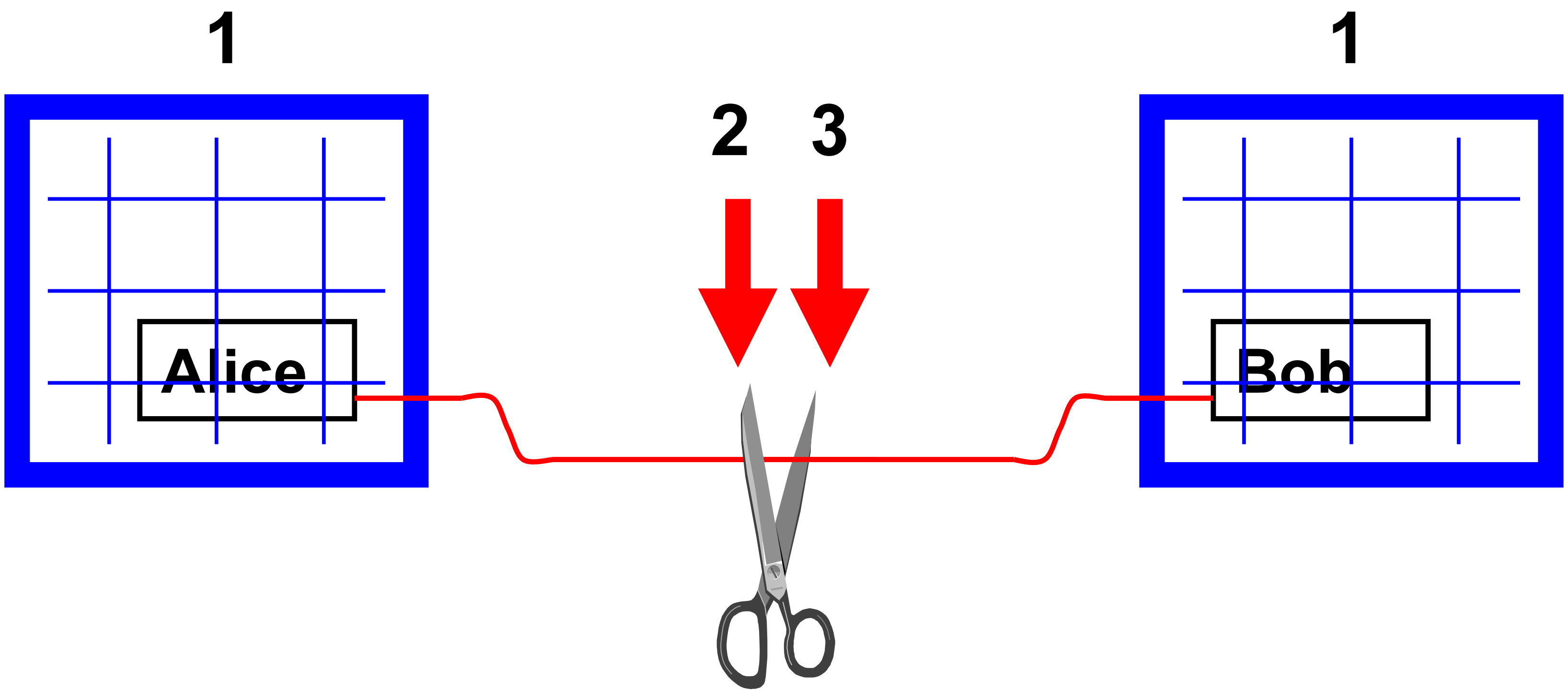
SECOQC QIT Workshop. Erlangen, September 13–17, 2004

Attacks via optical loopholes

Vadim Makarov

www.vad1.com/qcr/

Components of security

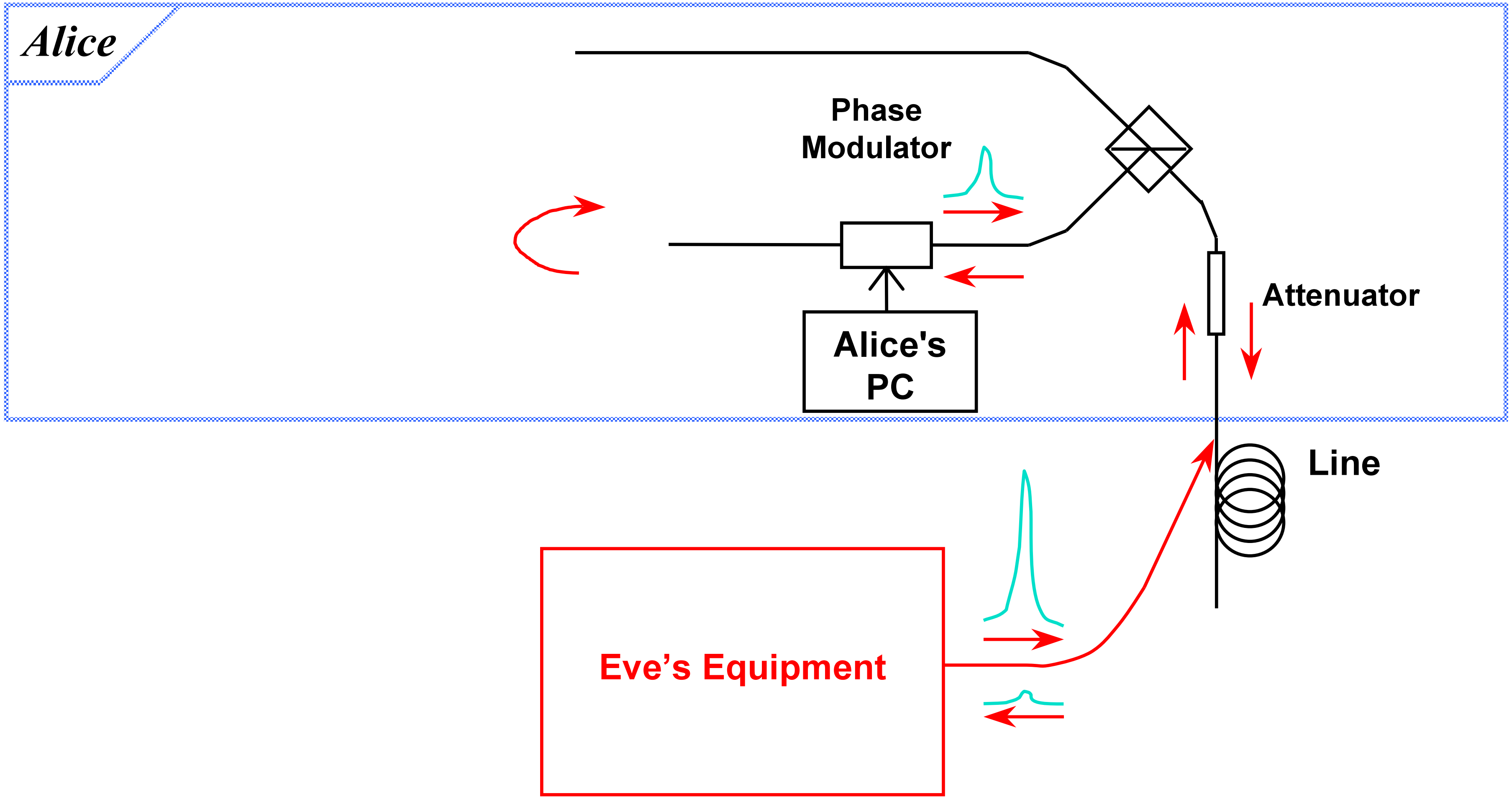


1. Conventional security; trusted equipment manufacturer
2. Security against quantum attacks
3. Loopholes in optical scheme

   – attacks that don't deal with quantum states, but use loopholes and imperfections in implementation

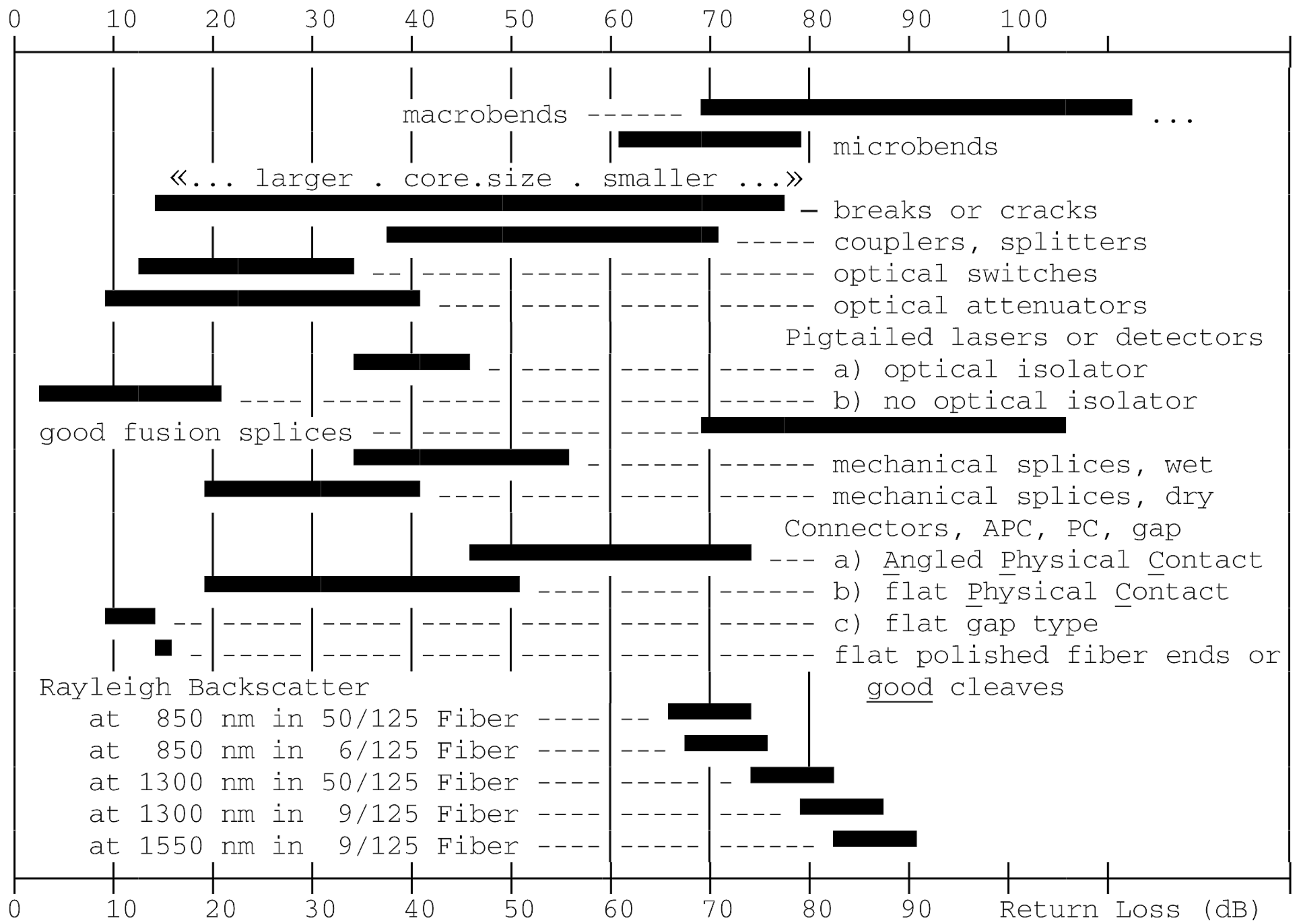
- **Large pulse attack**
- **Light emission from APDs**
- **Faked states attack – passive basis choice**
- **Faked states attack – active basis choice**

Large pulse attack



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

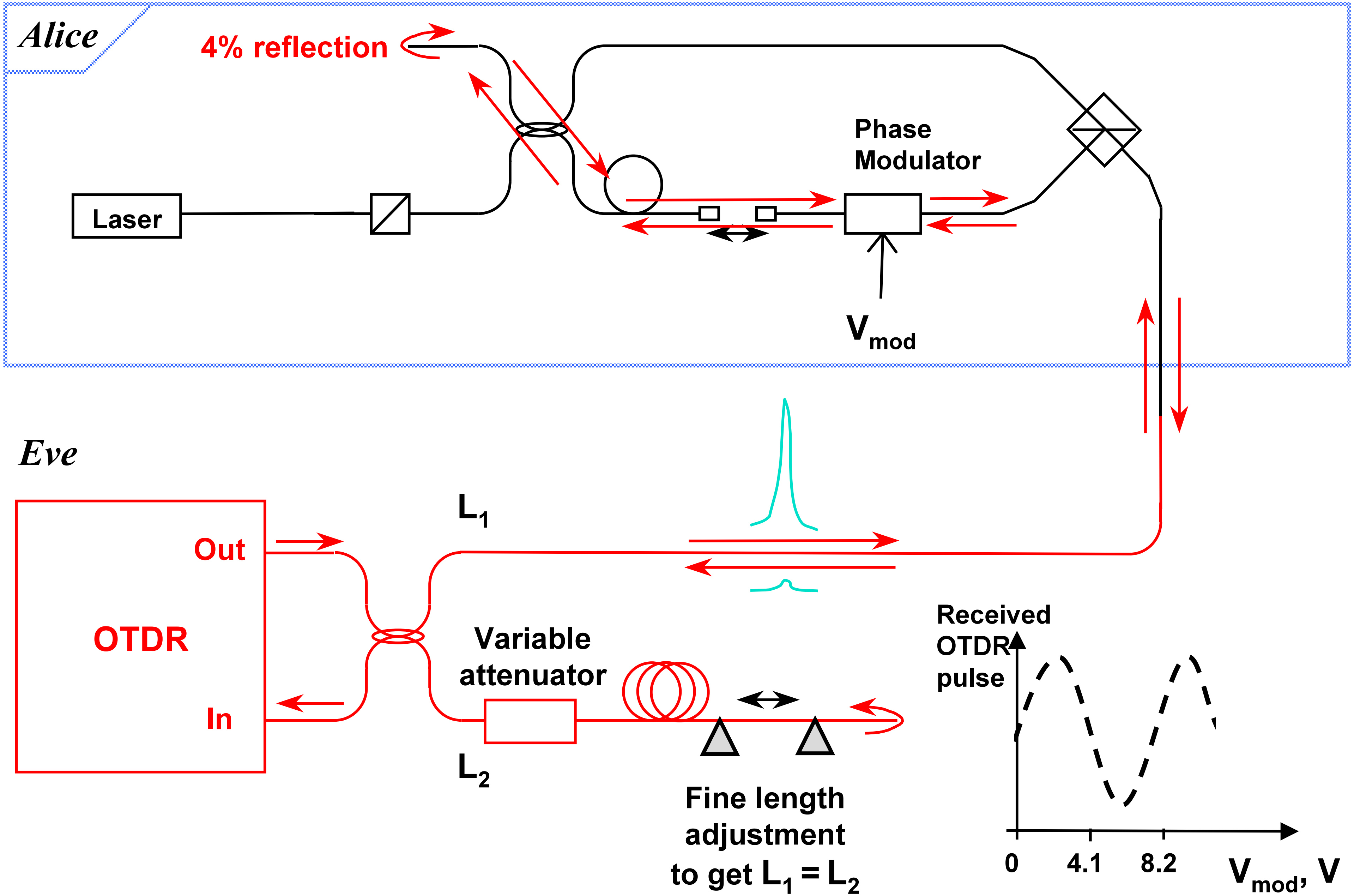
[A. Vakhitov, V. Makarov, and D.R. Hjelme, "Large pulse attack as a method of conventional optical eavesdropping in quantum cryptography," J. Mod. Opt. **48**, 2023-2038 (2001)].

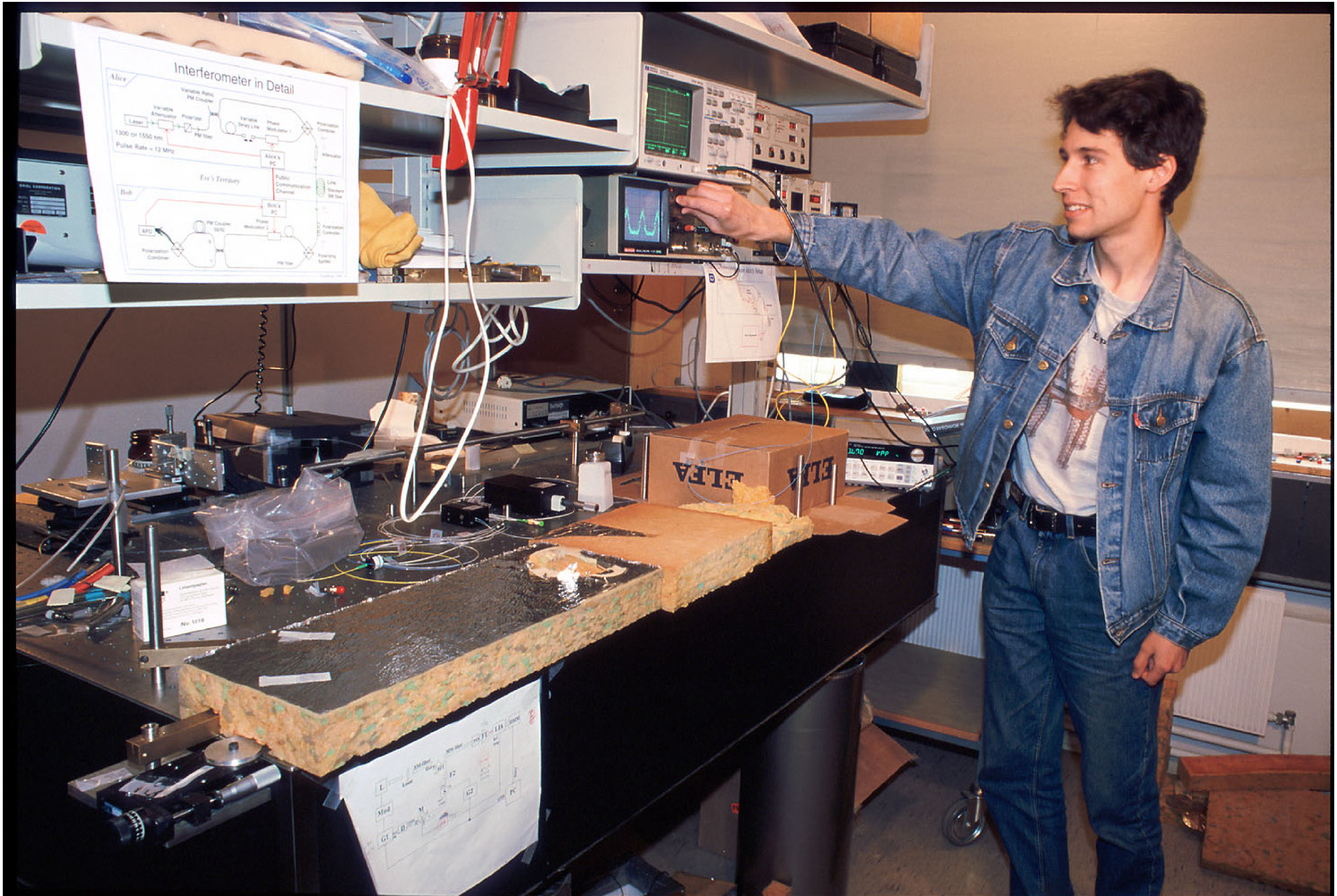


Typical values of reflection coefficients for different fiber-optic components

(courtesy Opto-Electronics, Inc.)

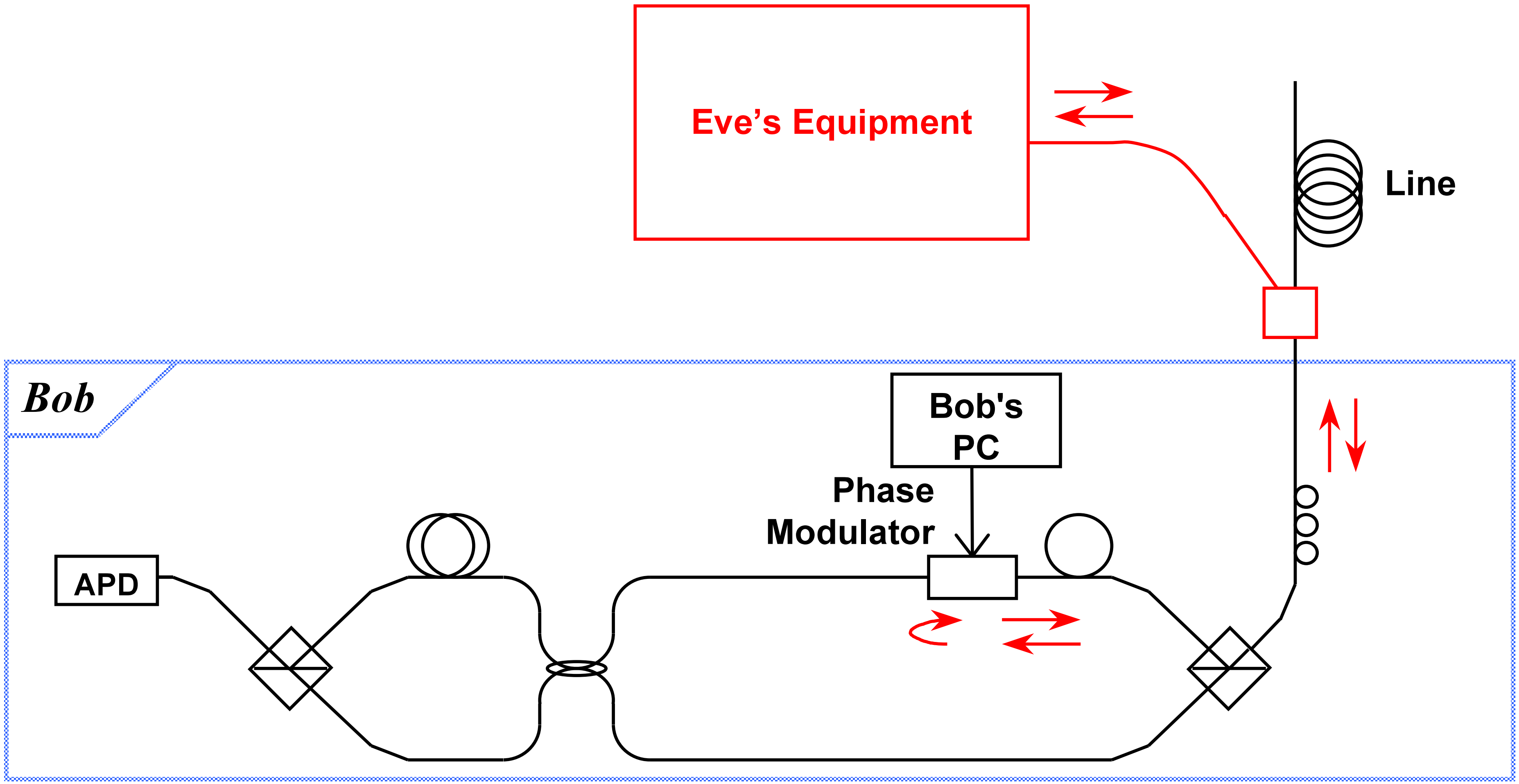
Large pulse attack: eavesdropping experiment



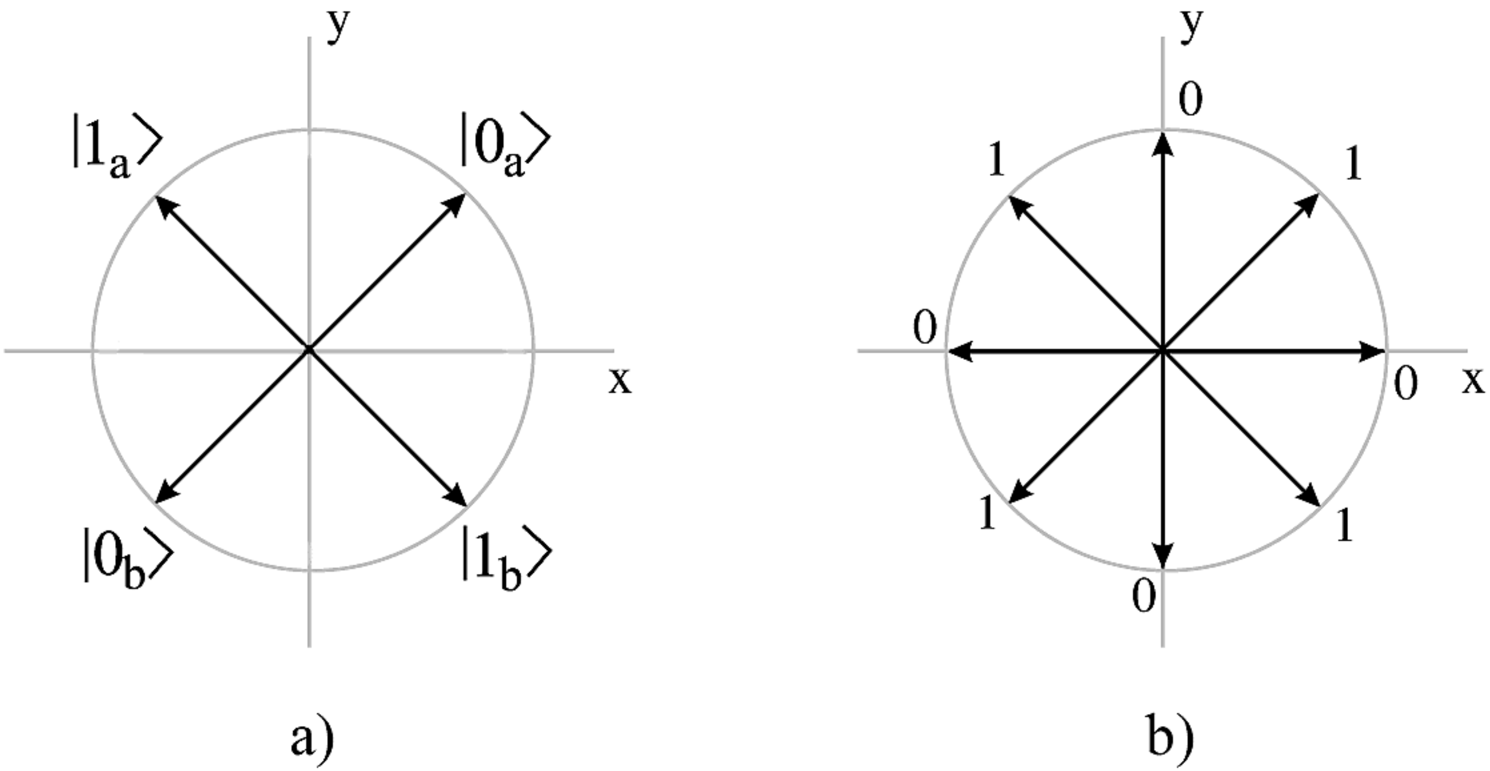


Artem Vakhitov tunes up Eve's setup (2000)

Interrogating Bob's modulator



PNS-resistant protocol and large pulse attack



States configuration for a QKD protocol robust to PNS attack (other name: "SARG protocol"): (a) two pairs of non-orthogonal states on the equator of the Poincare sphere, physically equivalent to the states used in the BB84 protocol; (b) bit encoding in a protocol using four bases [A. Acin, N. Gisin, and V. Scarani, "Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks," Phys. Rev. A **69**, 012309 (2004)].

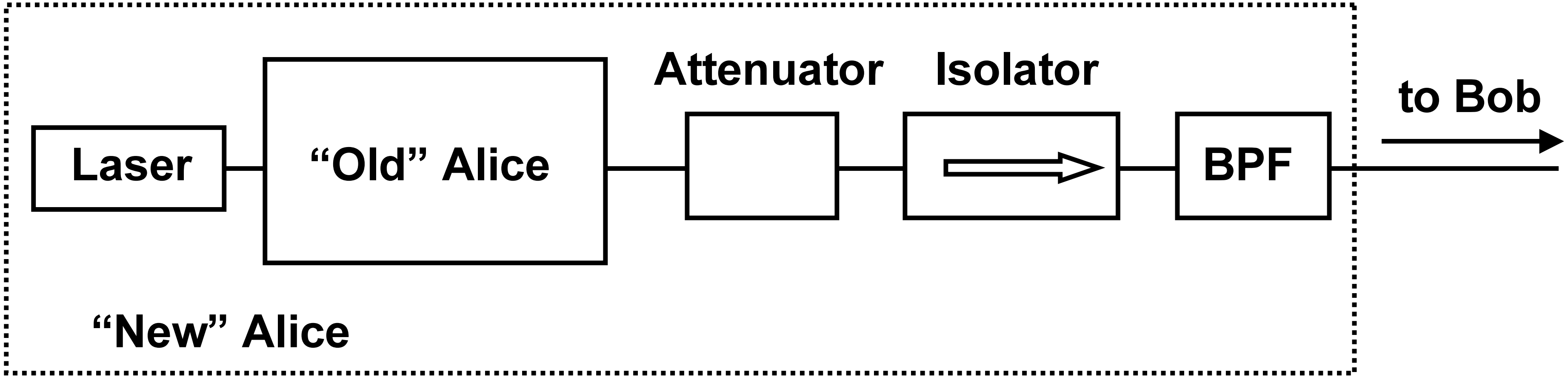
Unfortunately, measurement bases at Bob directly represent bit values.

Protection measures

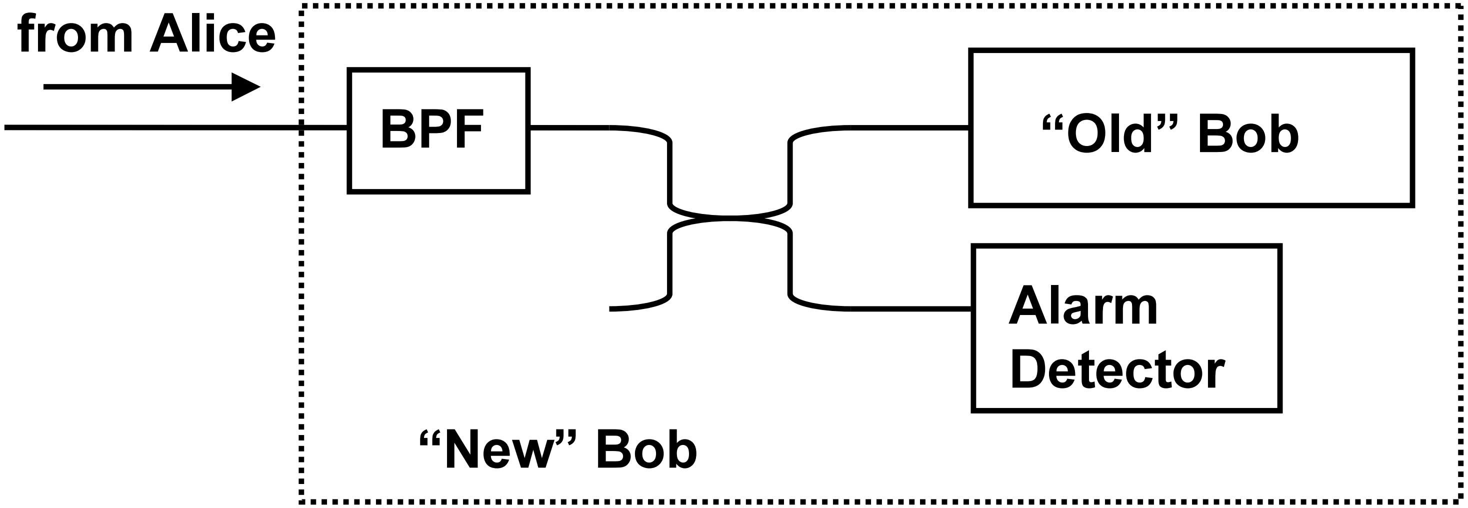
Scheme	Protocols	Protection		
		at Alice	*at Bob*	*
Townsend's	BB84	Passive (attenuator +isolator)	Passive (delay)	Yes
	B92, PNS-resistant		Active (detector)	
"Plug & Play"	BB84	Active (detector)	Passive (delay)	Yes
	B92, PNS-resistant		Active (detector)	

*Eve granted quantum memory (in reality she could use bases detection on Bob's side, not needing long storage)

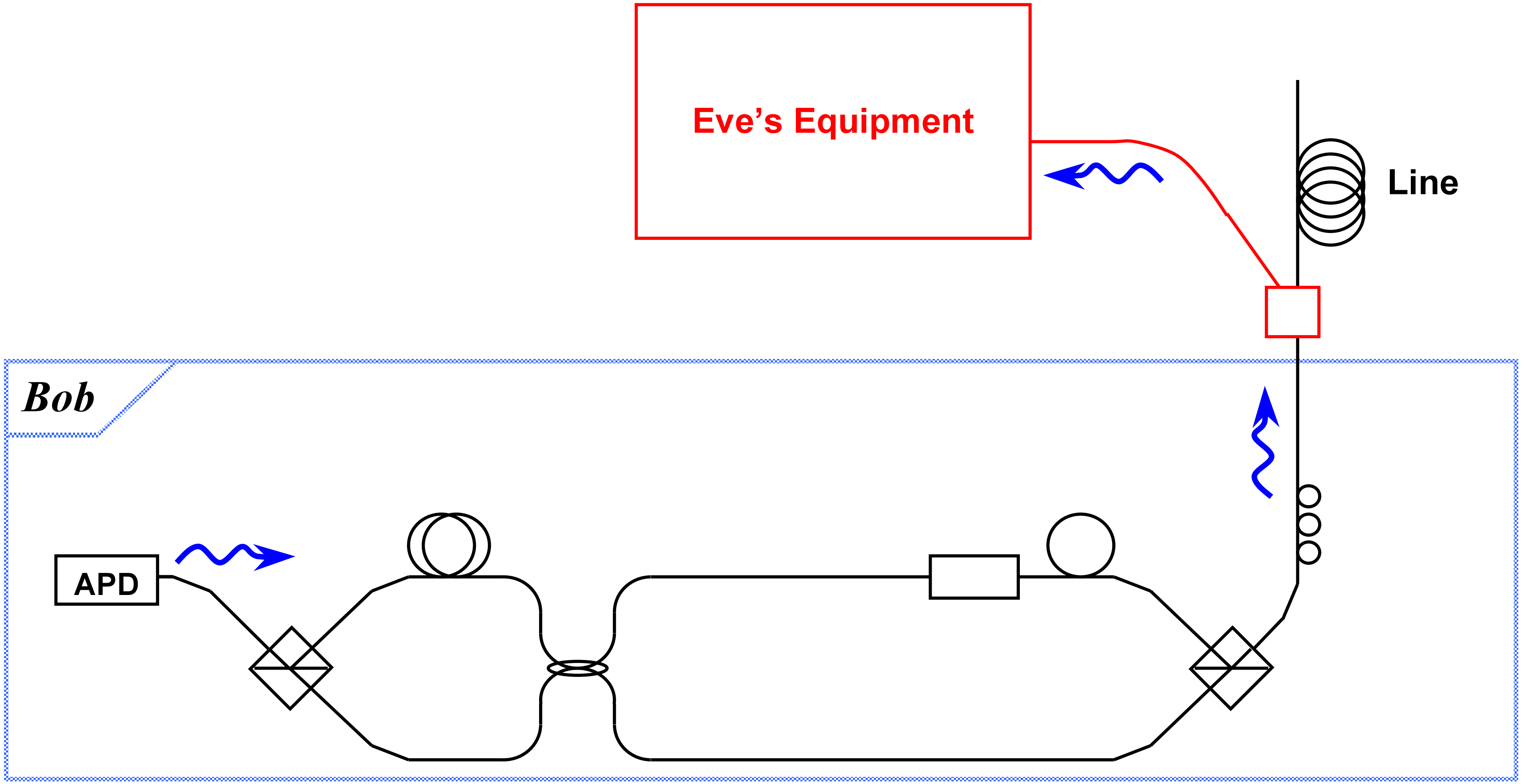
Passive (attenuator+isolator)



Active (detector)



Light emission from APD

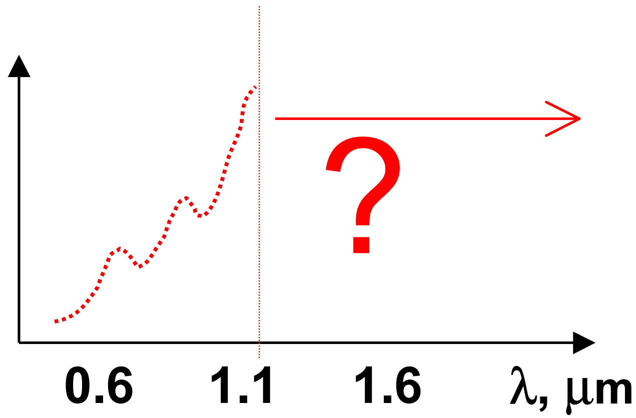


– Detect light emitted from single photon detector – avalanche photo diode (APD) – during avalanche, get bit value

Light emission from APDs

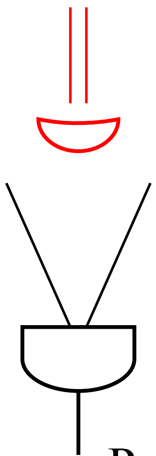
Hot-carrier luminescence in avalanching junction:

- **No single agreed-upon model of the process**
- **Studied only in Si devices, only down to 1.1 μm**



The only study in application to information leakage:

[C. Kurtsiefer, P. Zarda, S. Mayer, and H. Weinfurter, “The breakdown flash of silicon avalanche photodiodes – back door for eavesdropper attacks?” J. Mod. Opt. **48**, 2039-2047 (2001).]



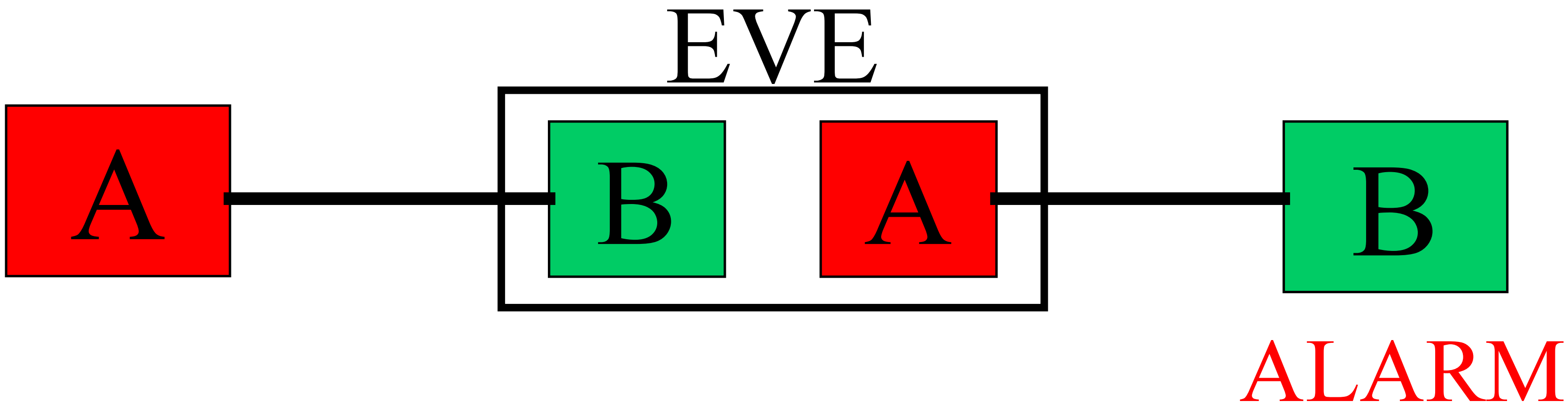
into SM fiber:
1.3E-3 photons

~11 photons/sr (700–1050 nm)

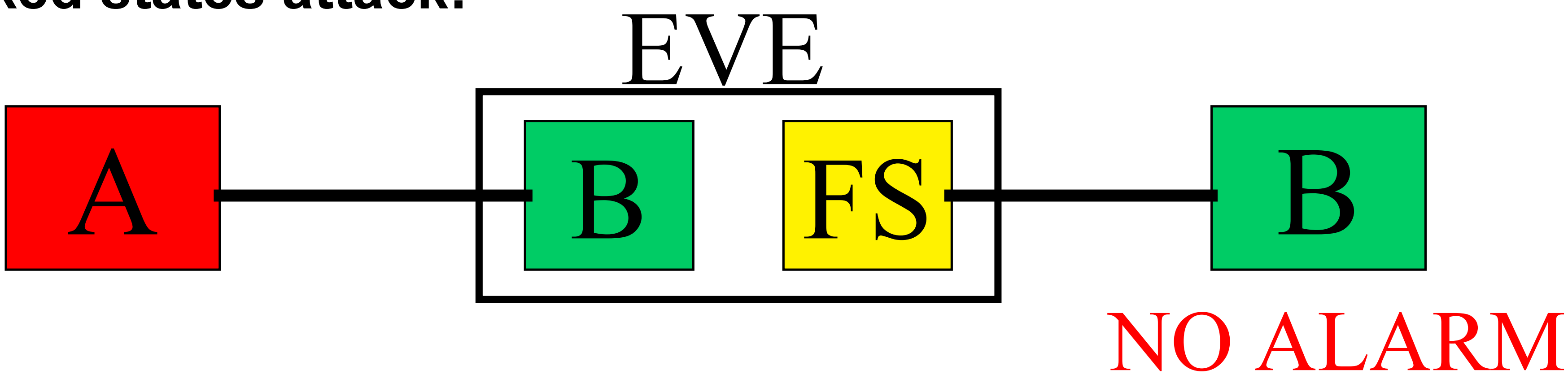
Perkin-Elmer C30902-SDTC (Si APD, d=0.5 mm)

Faked states attack

Conventional intercept/resend:



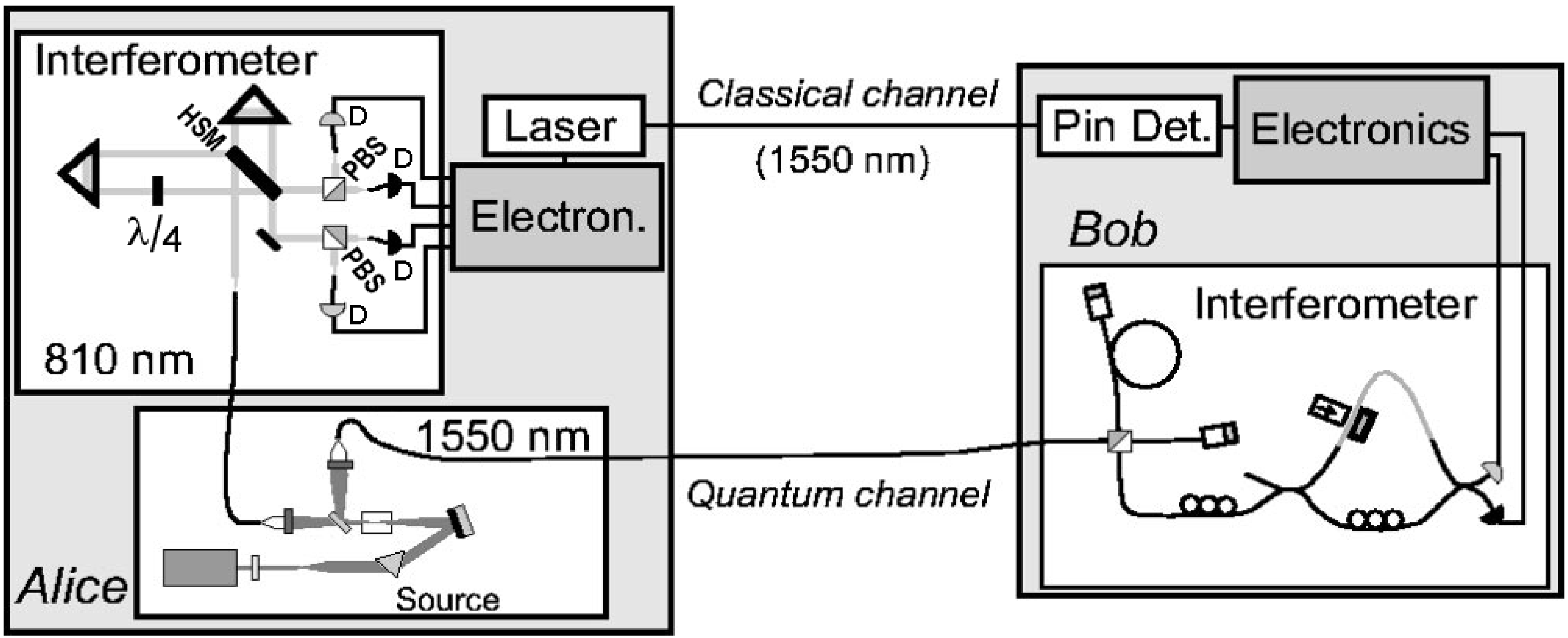
Faked states attack:

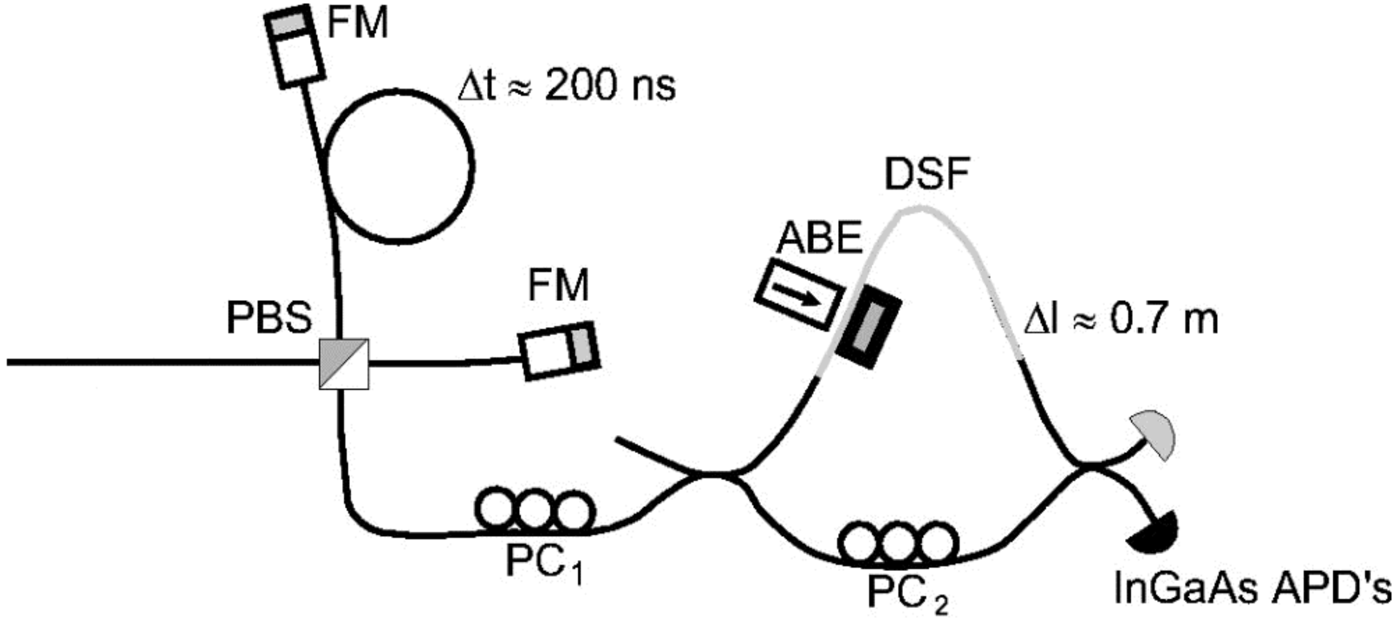


Faked states attacks...

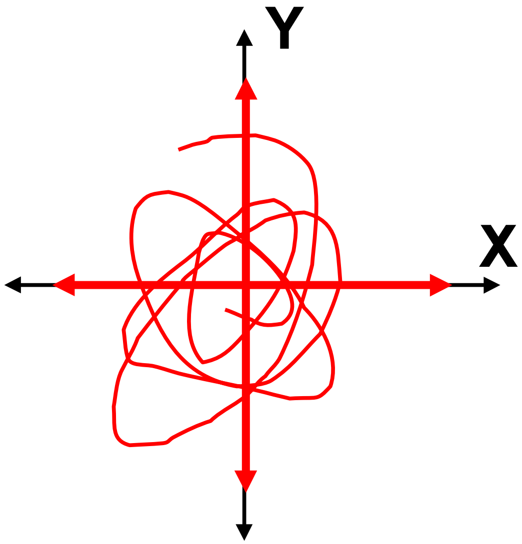
are described in [Vadim Makarov and Dag R. Hjelme, "Faked states attack on quantum cryptosystems," Journal of Modern Optics (to be published, 2004)]

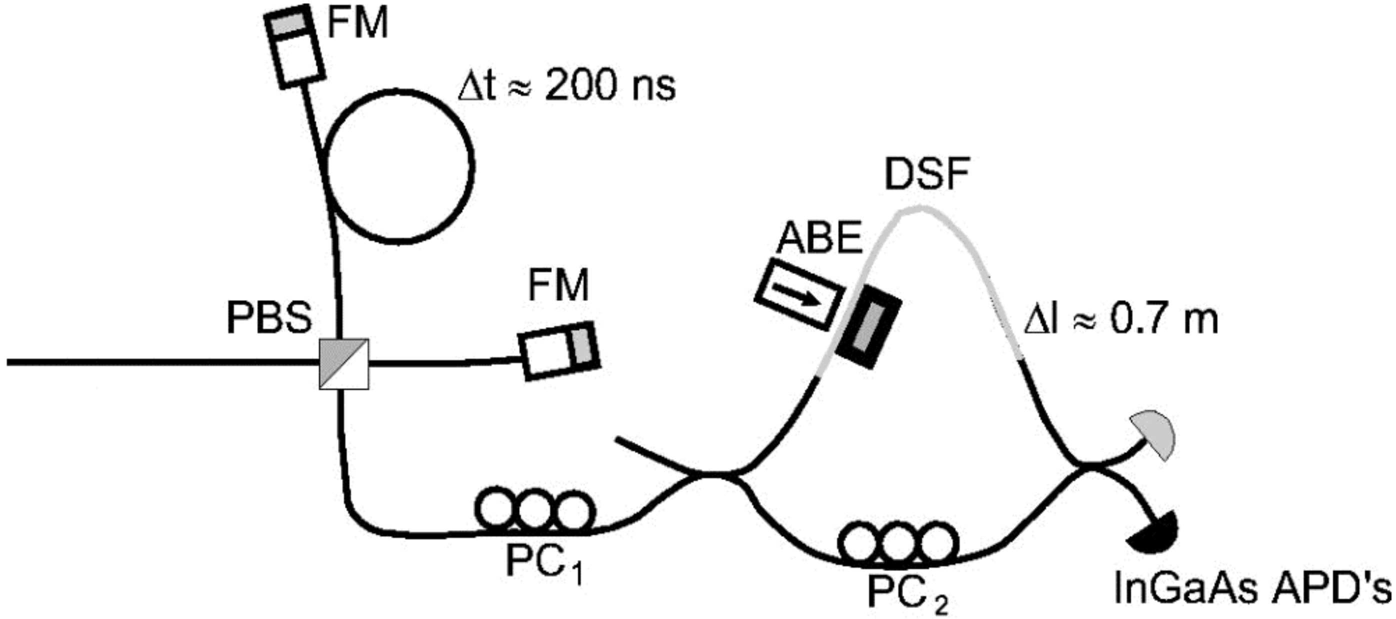
on the example of Geneva group's entanglement-based QKD system
[G. Ribordy, J. Brendel, J.-D. Gautier, N. Gisin, and H. Zbinden, "Long-distance entanglement-based quantum key distribution," Phys. Rev. A **63**, 012309 (2001)].



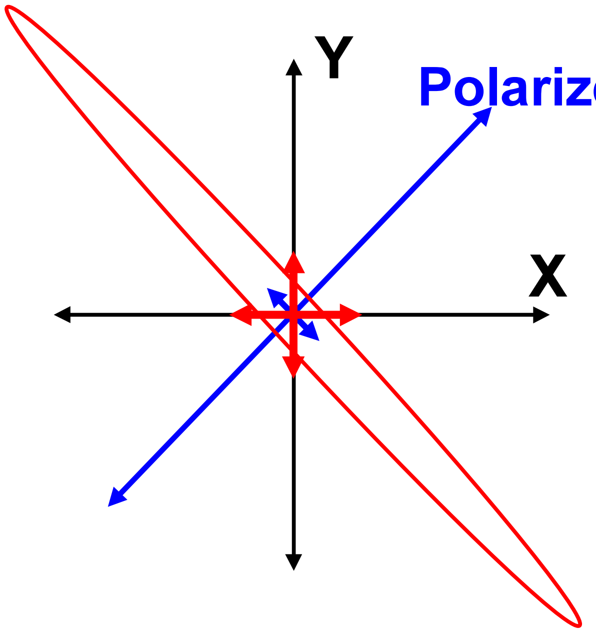

FM
Δt ≈ 200 ns
DSF
ABE
FM
PBS
Δl ≈ 0.7 m
PC1
PC2
InGaAs APD's

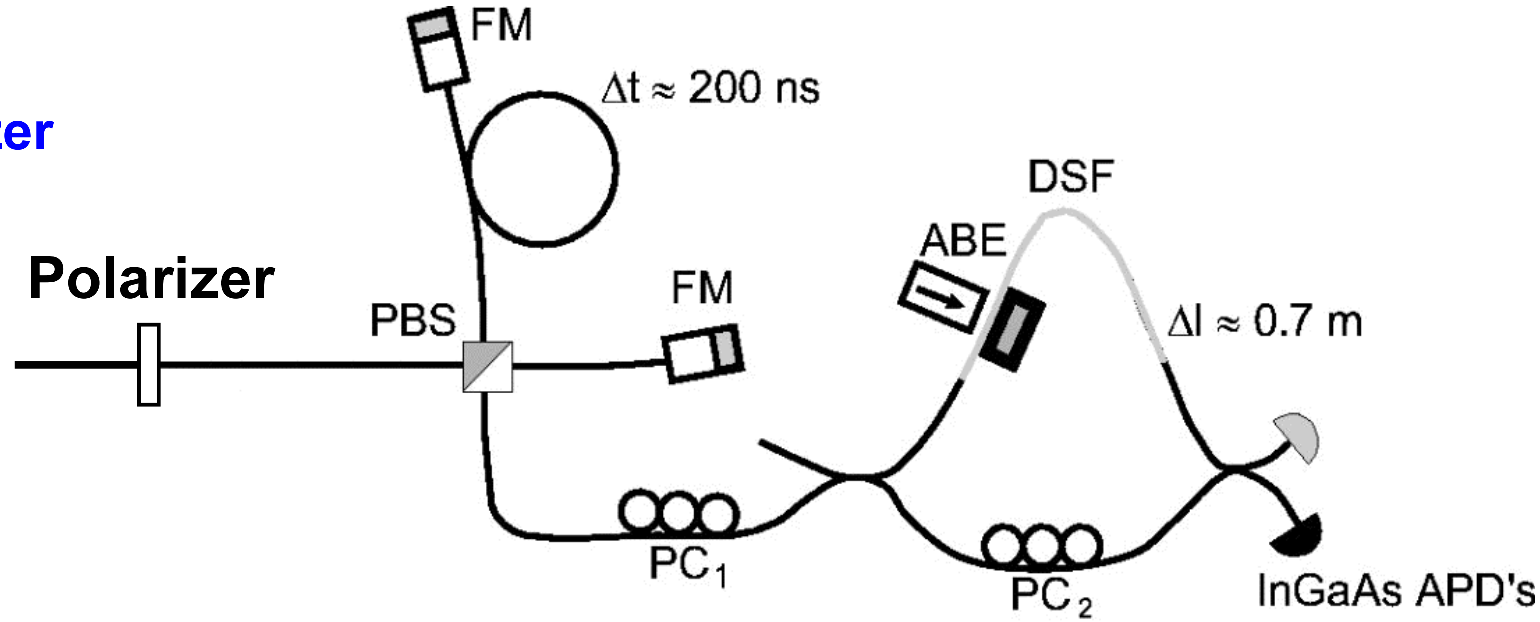
1. Basis choice via polarization





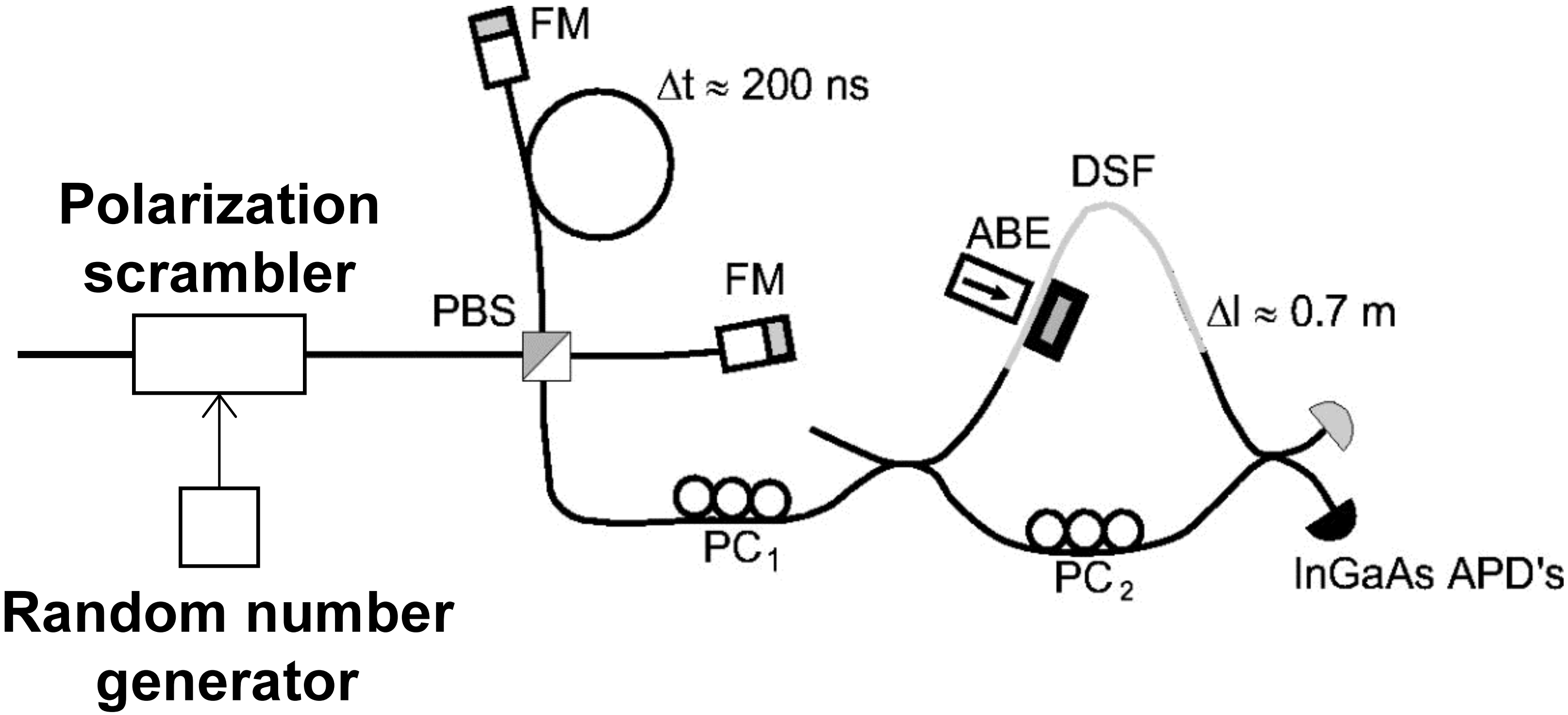
1. Basis choice via polarization





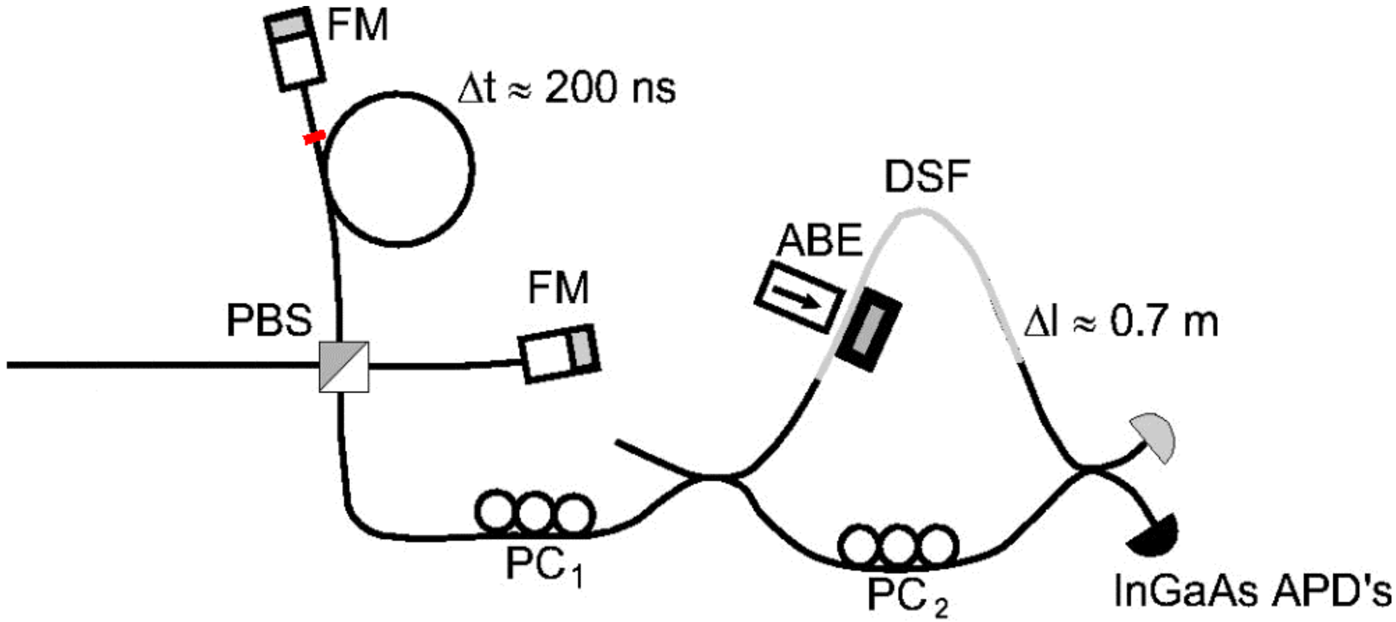
‘Eve could devise a strategy where she could benefit from forcing detection of a given qubit in a particular basis, [so] we must introduce a polarizer aligned at 45° or a polarization scrambler in front of the PBS.’

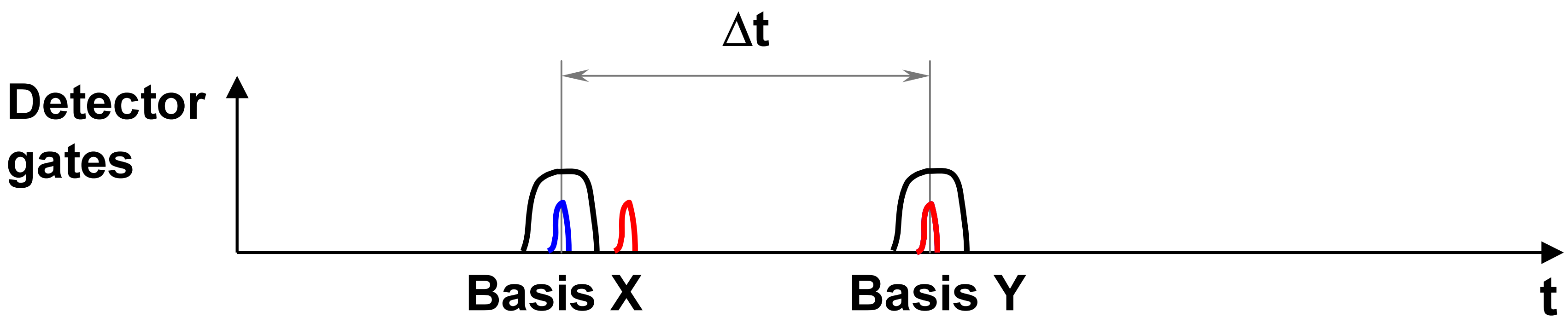
1. Basis choice via polarization



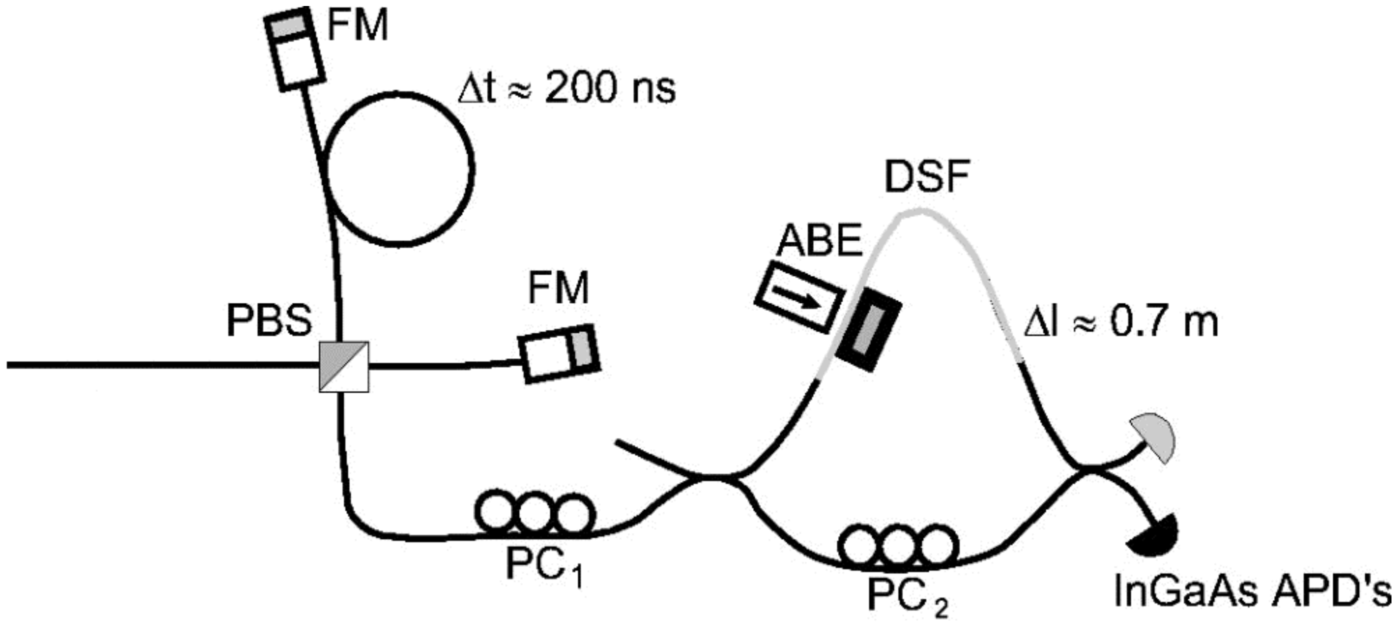
'Eve could devise a strategy where she could benefit from forcing detection of a given qubit in a particular basis, [so] we must introduce a polarizer aligned at 45° or a polarization scrambler in front of the PBS.'

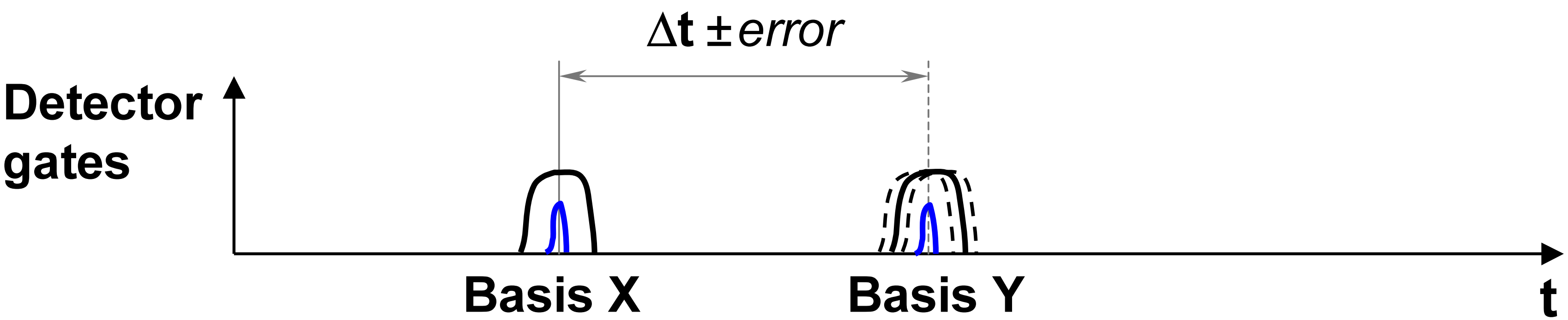
2. Basis choice via timing using reflections off optical interfaces



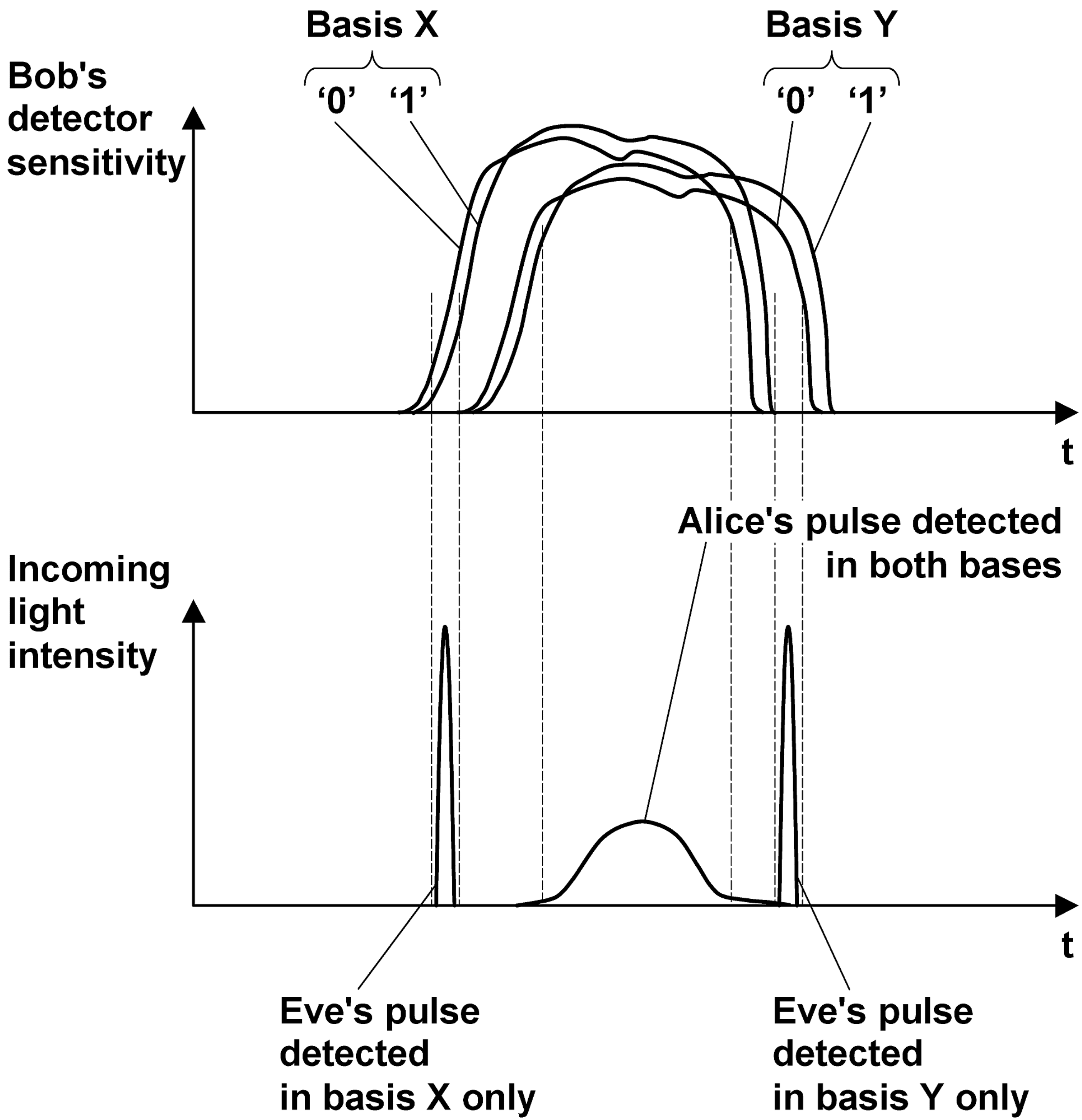


3. Basis choice via timing using non-overlapping parts of detection window



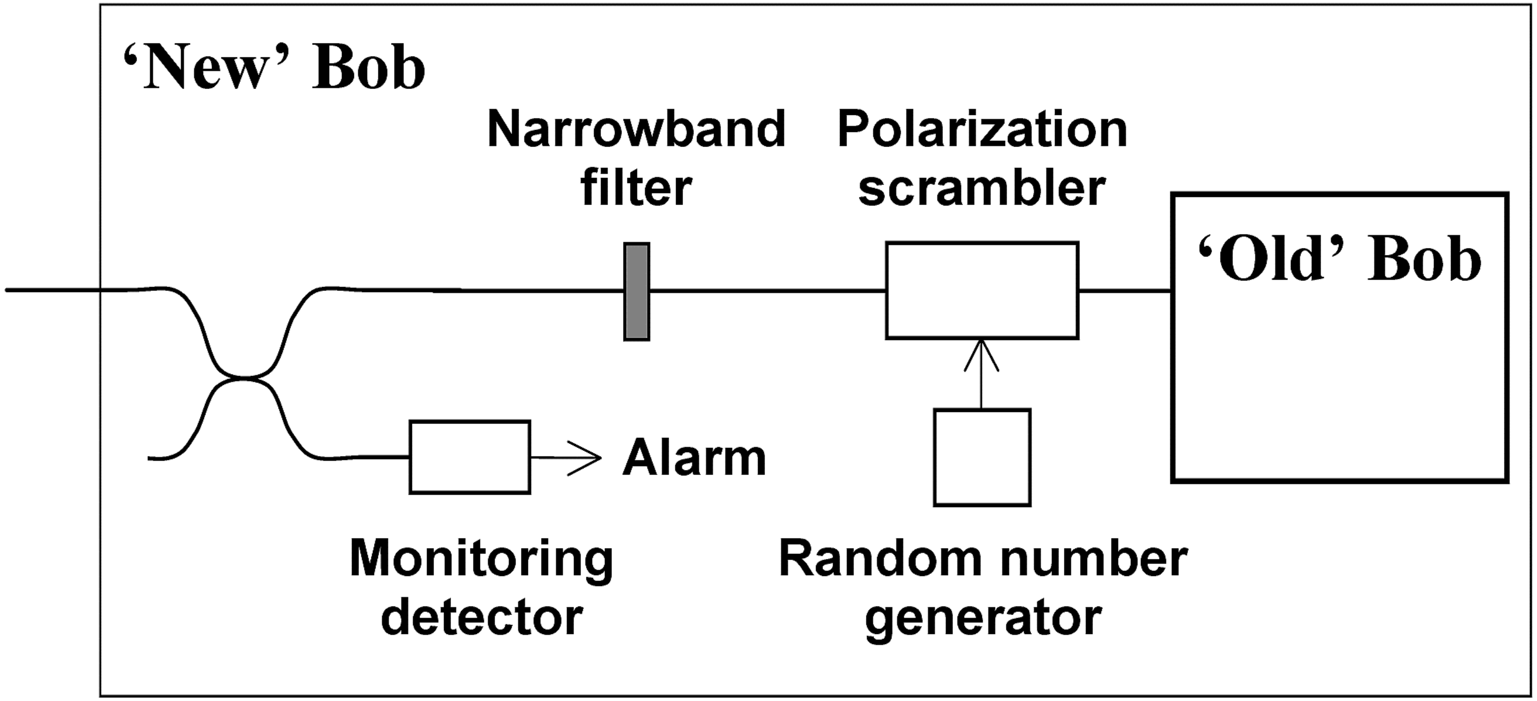


NTNU

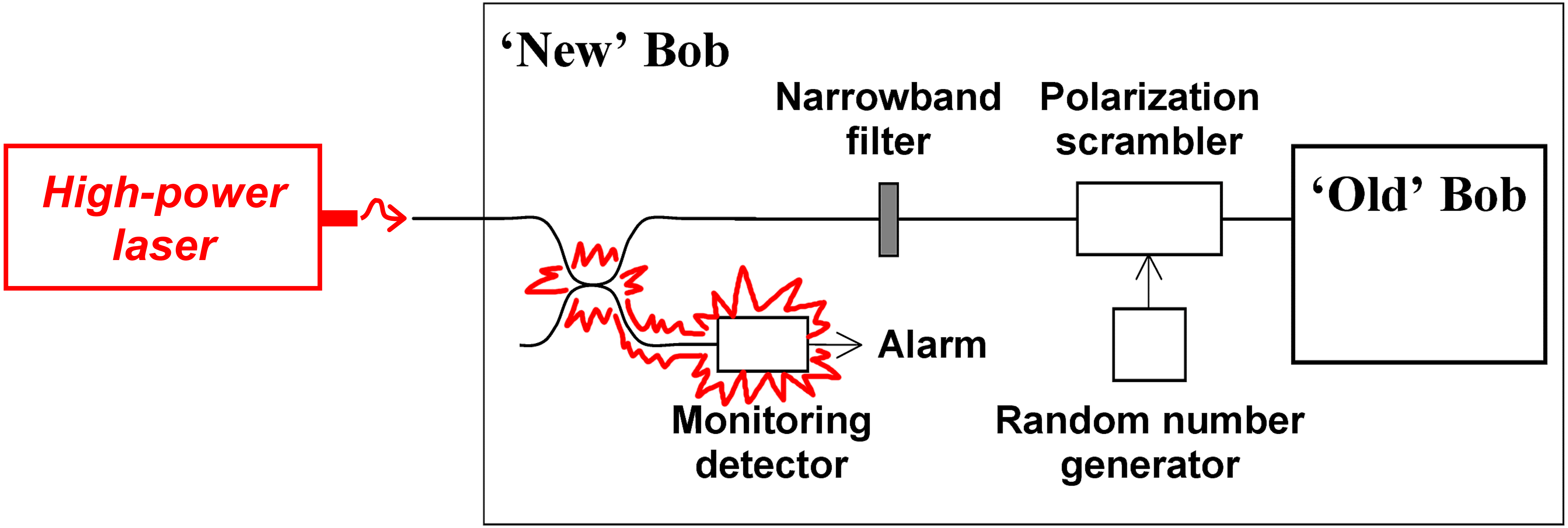

Basis X
Basis Y
Bob's detector sensitivity
'0' '1'
'0' '1'
t
Alice's pulse detected in both bases
Incoming light intensity
t
Eve's pulse detected in basis X only
Eve's pulse detected in basis Y only

NTNU

Protection measures against attacks 1–3



4. Incapacitation of monitoring detector



Modern classical cryptography:

"Security depends on key, not on algorithm."

Quantum cryptography:

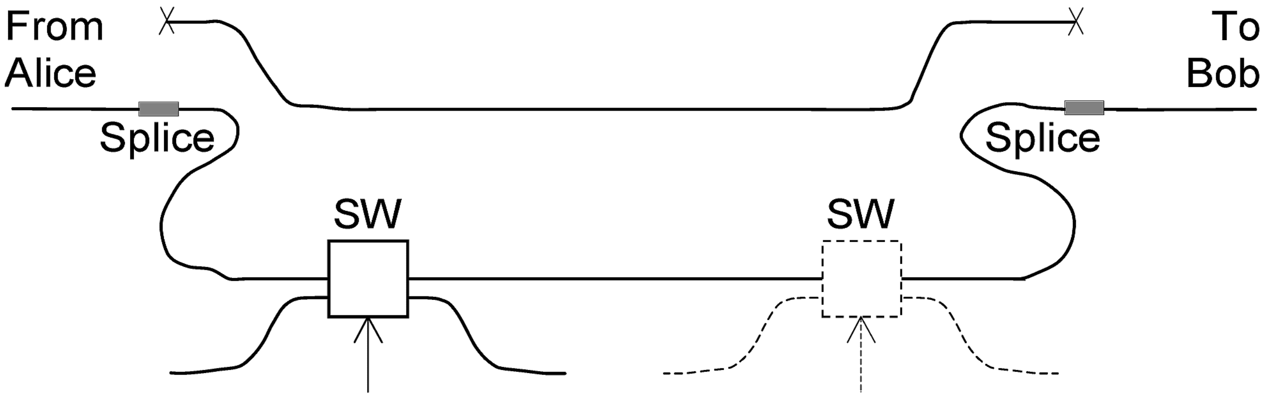
"Security depends on physics, not on equipment."

⬇

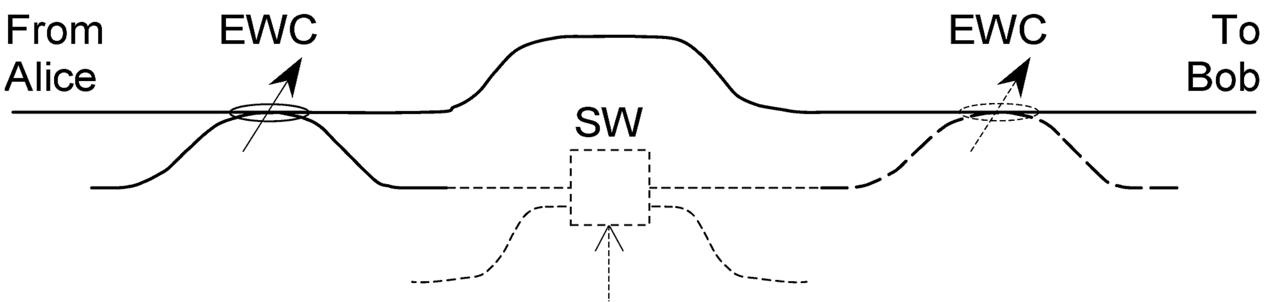
Assume equipment is known and accessible to Eve?..

A. Establishing optical connection

Link not in use:

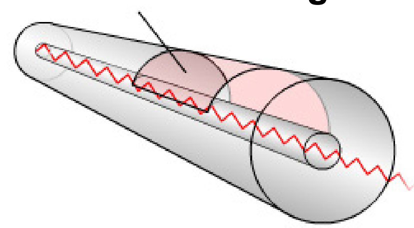


Running link:

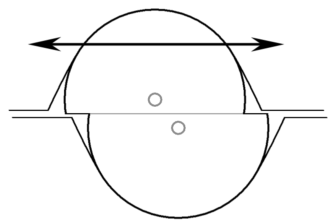


Evanescent wave technology:

Removed cladding



Variable coupler



B. Finding the right attack parameters

Before attack:

- **Study commercially available samples of equipment**

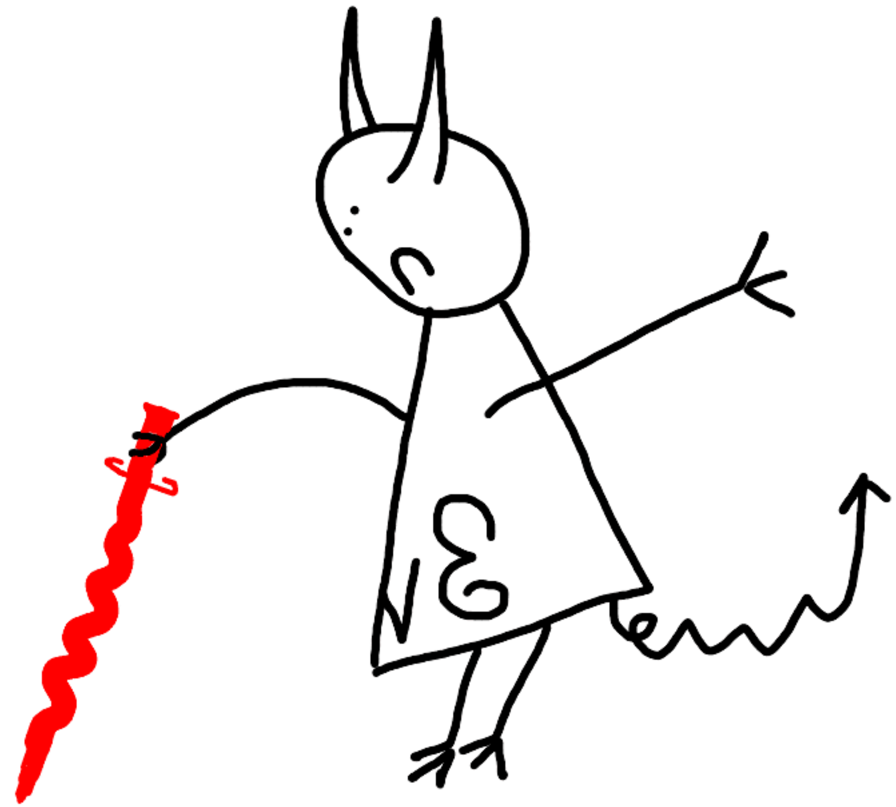
After connecting to line:

- **OTDR**
- **Probe the parameters of equipment by substituting *few* Alice's pulses with faked states at first. Watch the public discussion for those bits substituted. Accumulate statistics.**

⬇

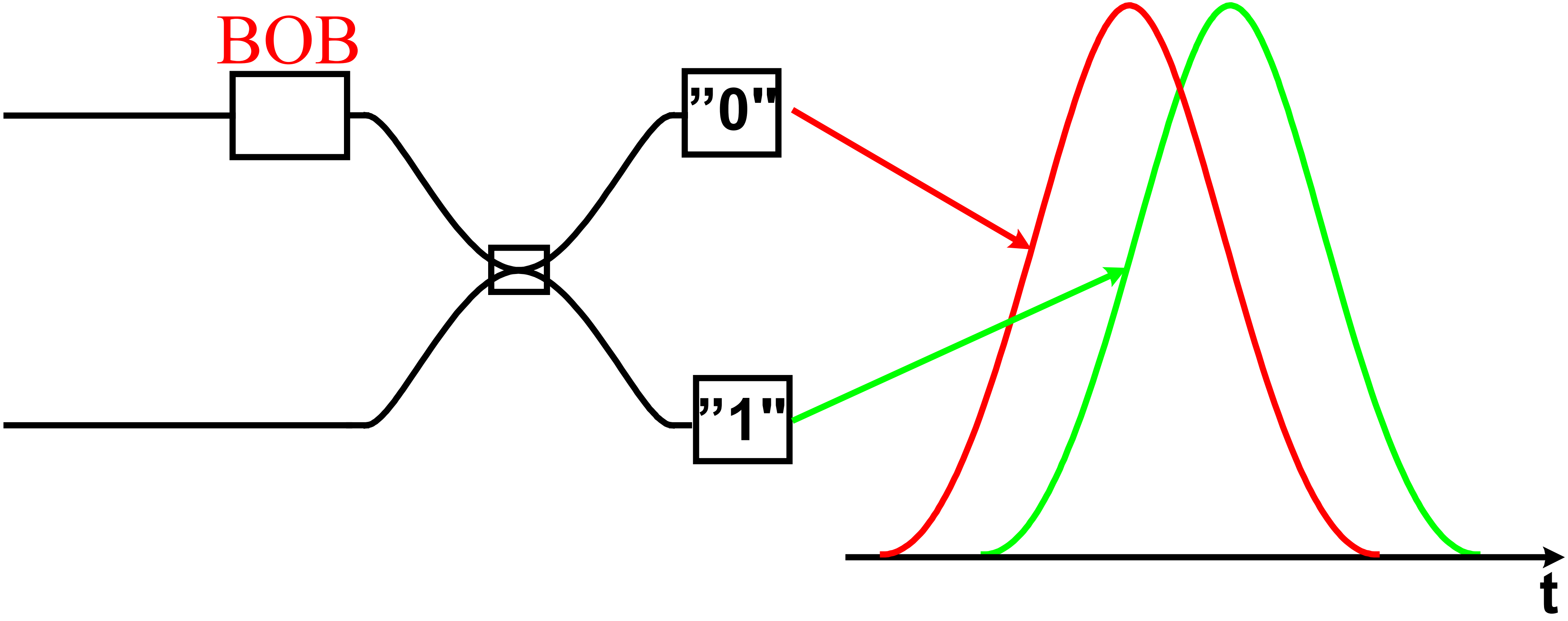
Then, switch to substituting *every* pulse.

- Large pulse attack
- Light emission from APDs
- Faked states attack – passive basis choice

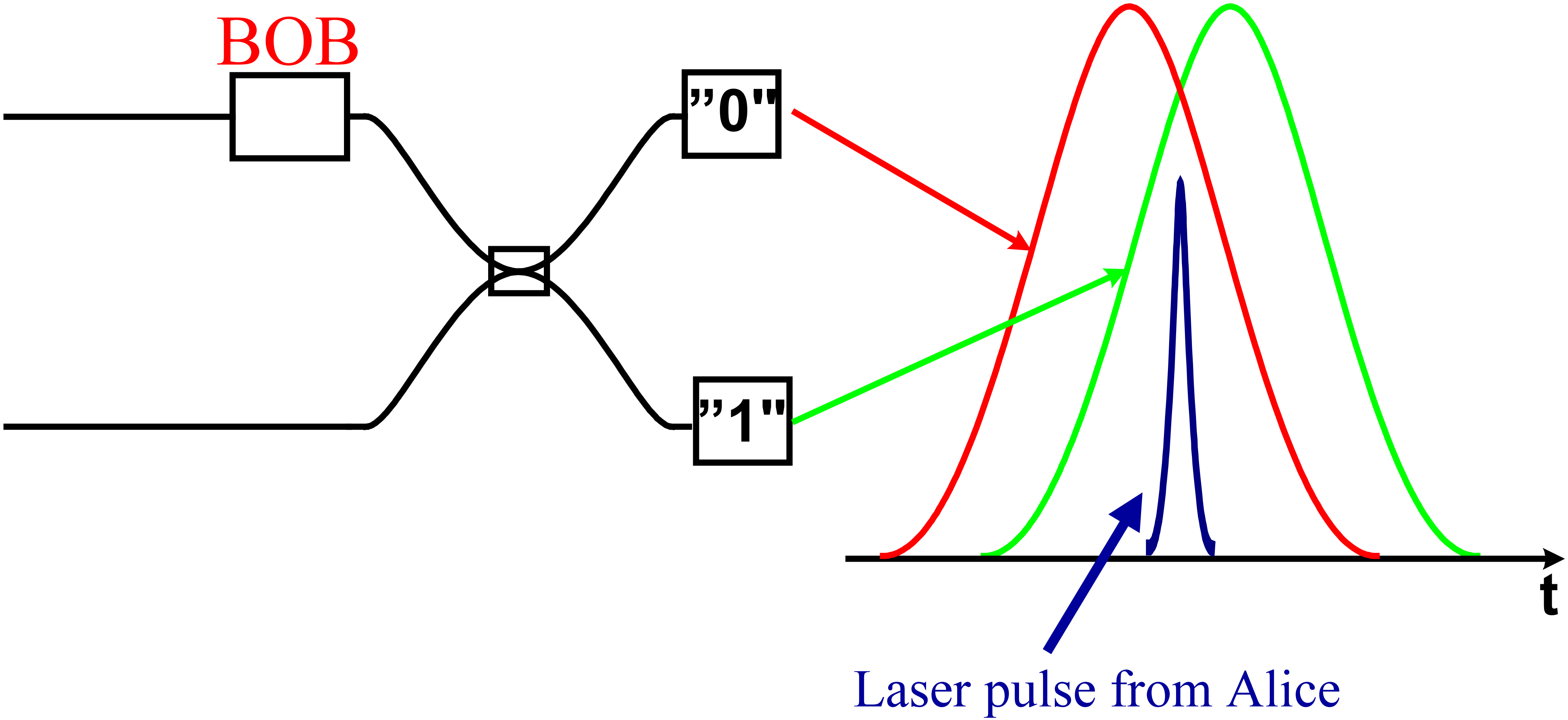


- **Faked states attack – active basis choice**

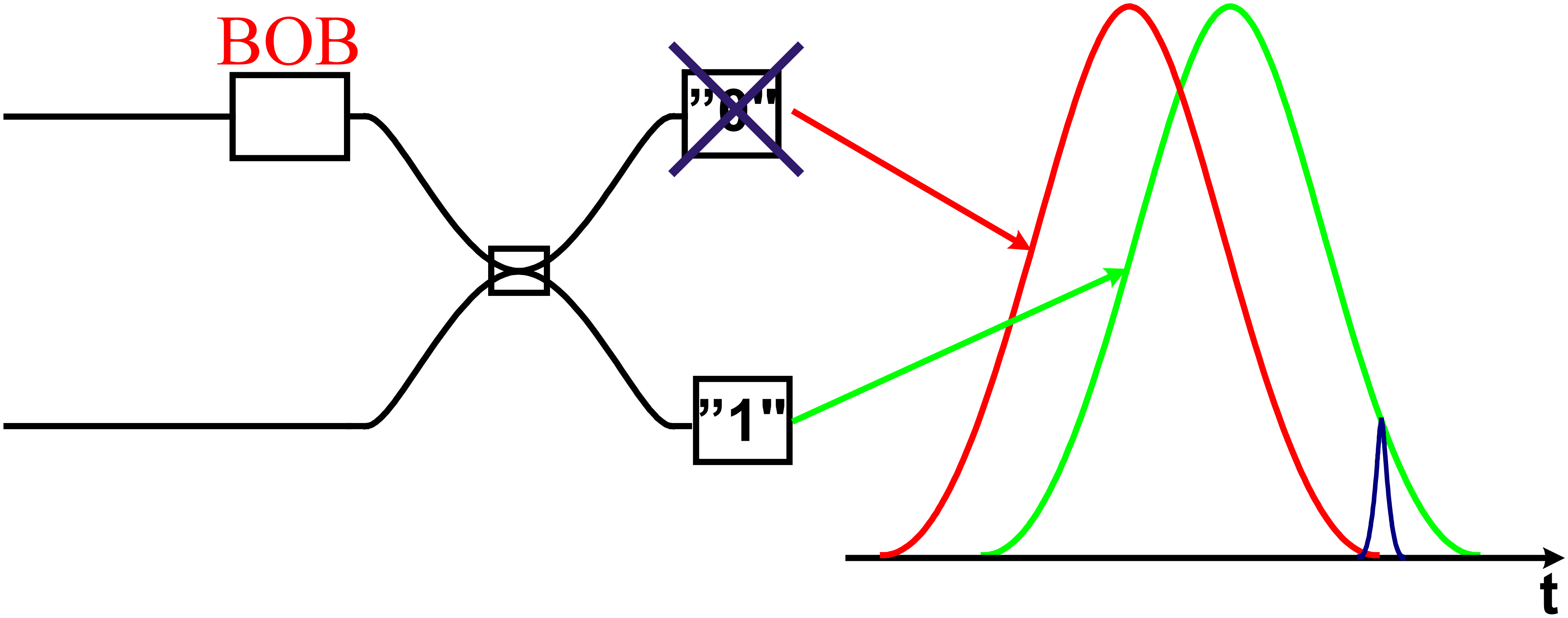
Detector gate misalignment



Detector gate misalignment

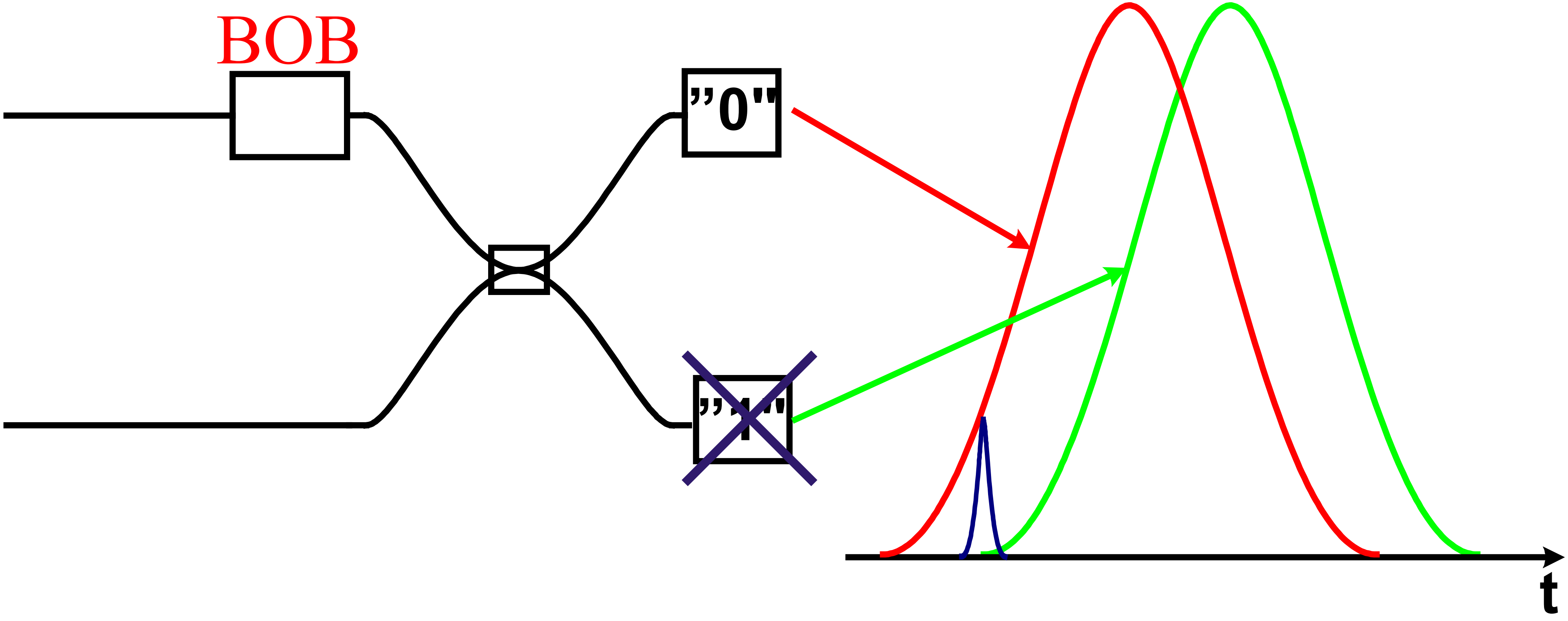


Detector gate misalignment



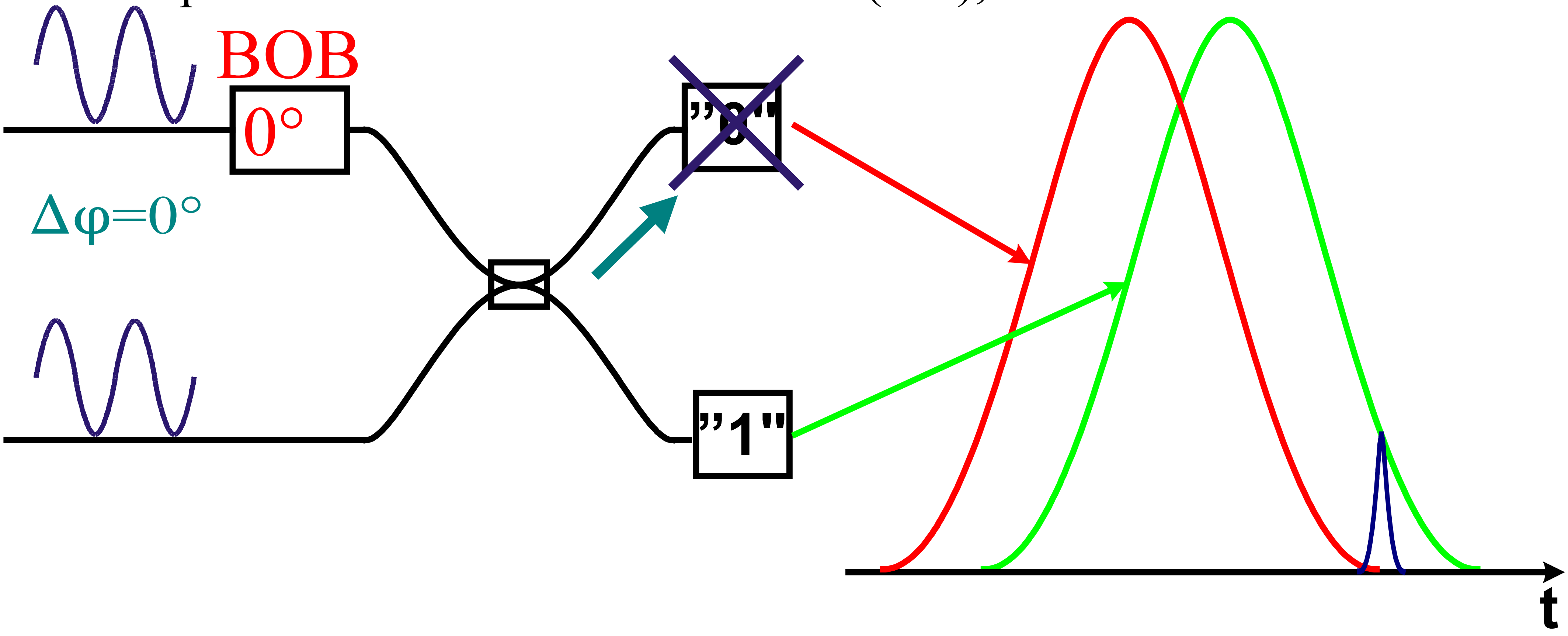
NTNU

Detector gate misalignment



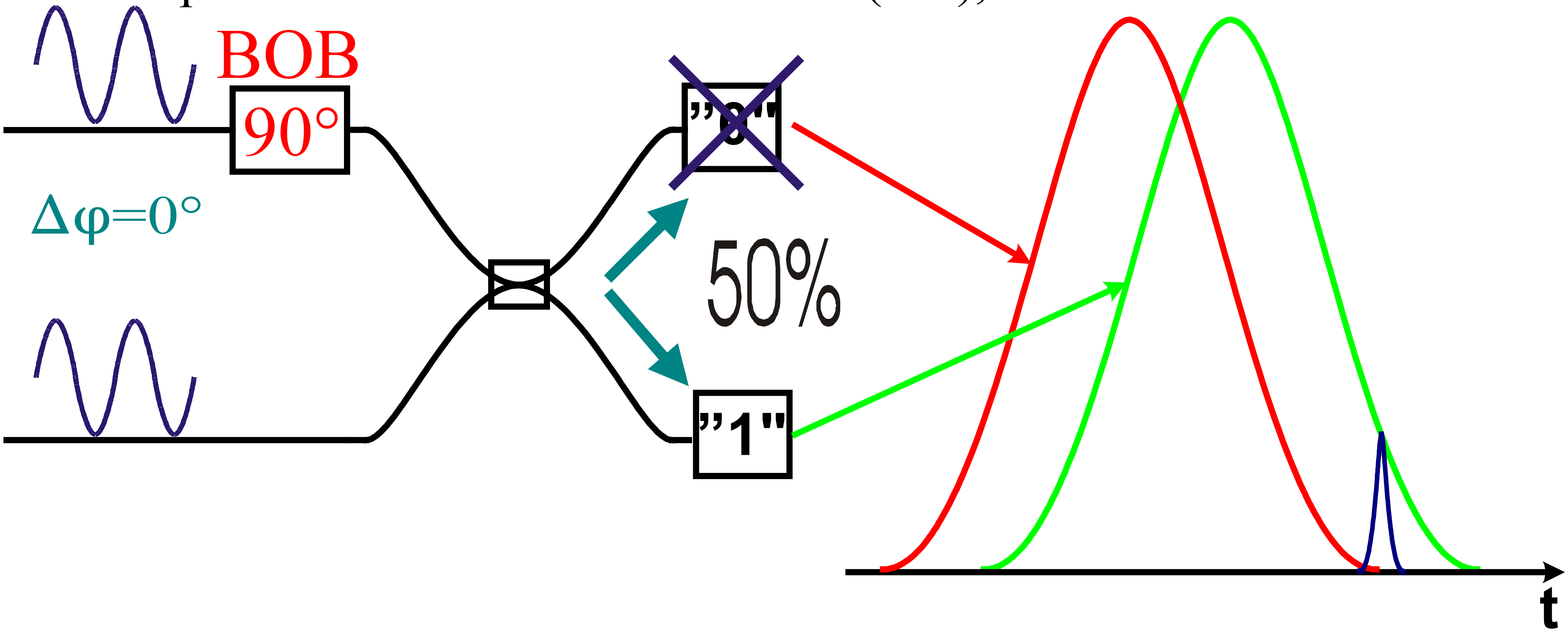
Detector gate misalignment

Example: Eve measured with basis Y (90°), obtains bit "1"



Detector gate misalignment

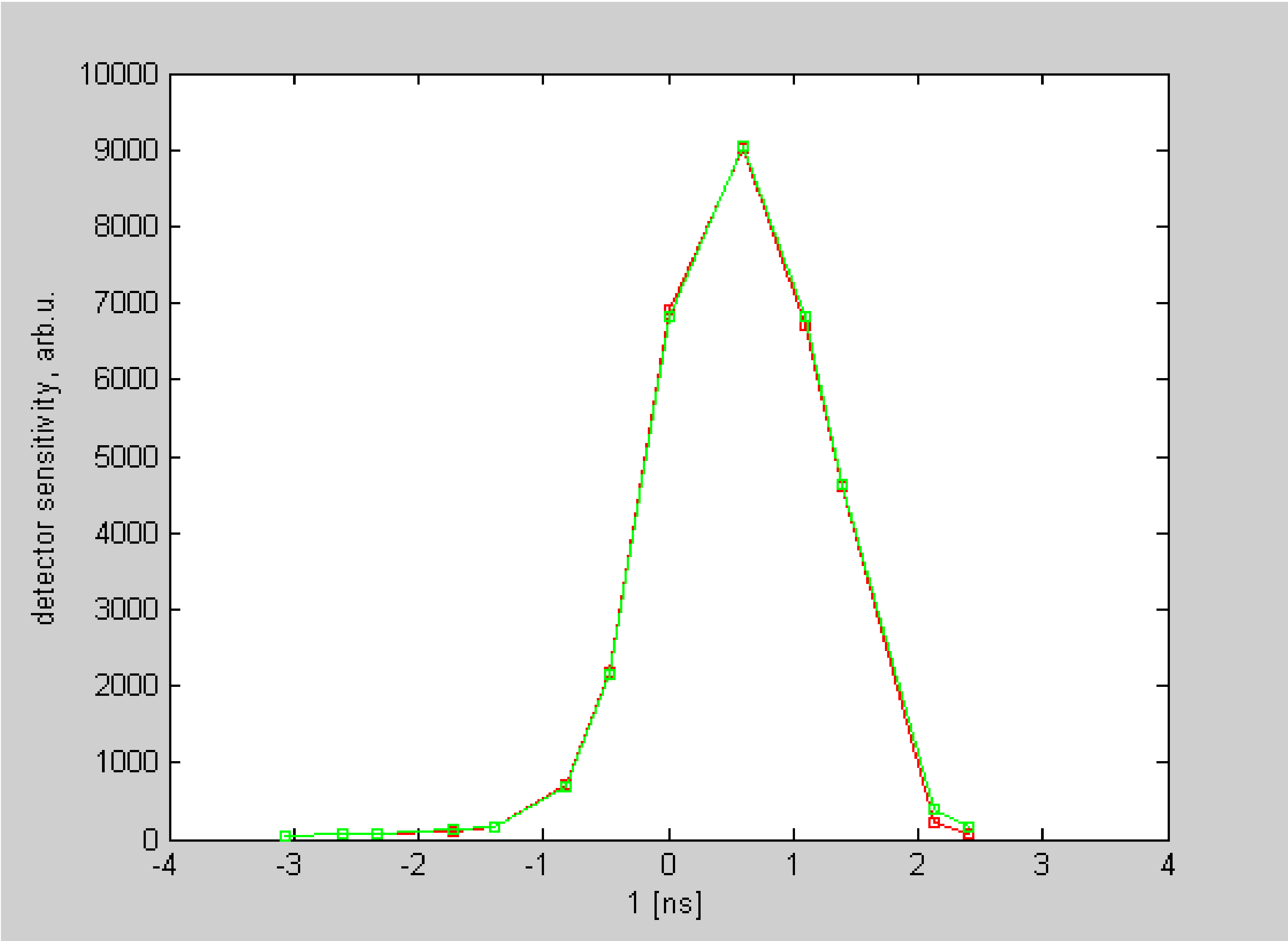
Example: Eve measured with basis Y (90°), obtains bit “1”



✓Eve’s attack is not detected

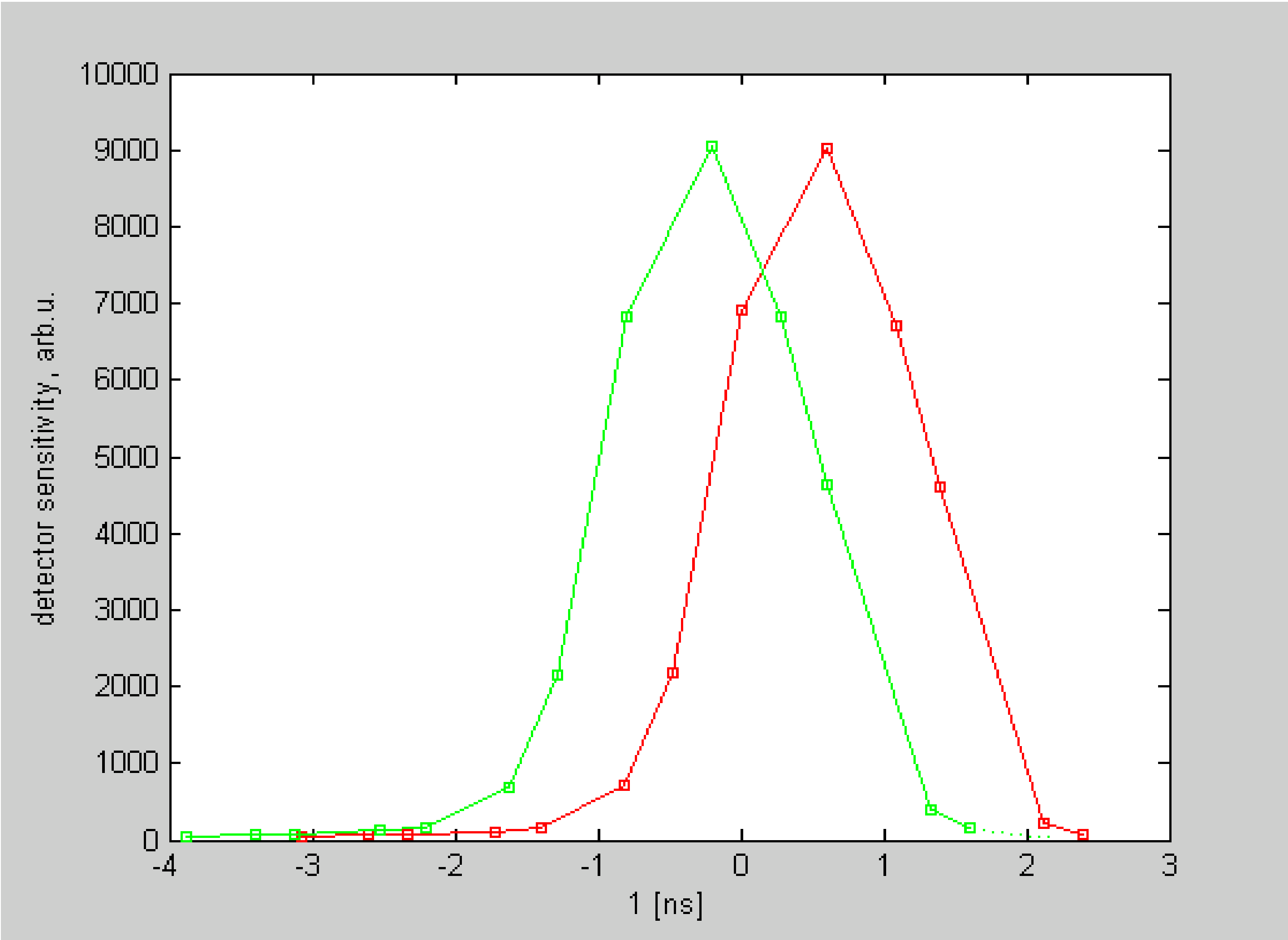
✓Eve obtains 100% information of the key

QKD setup in Trondheim

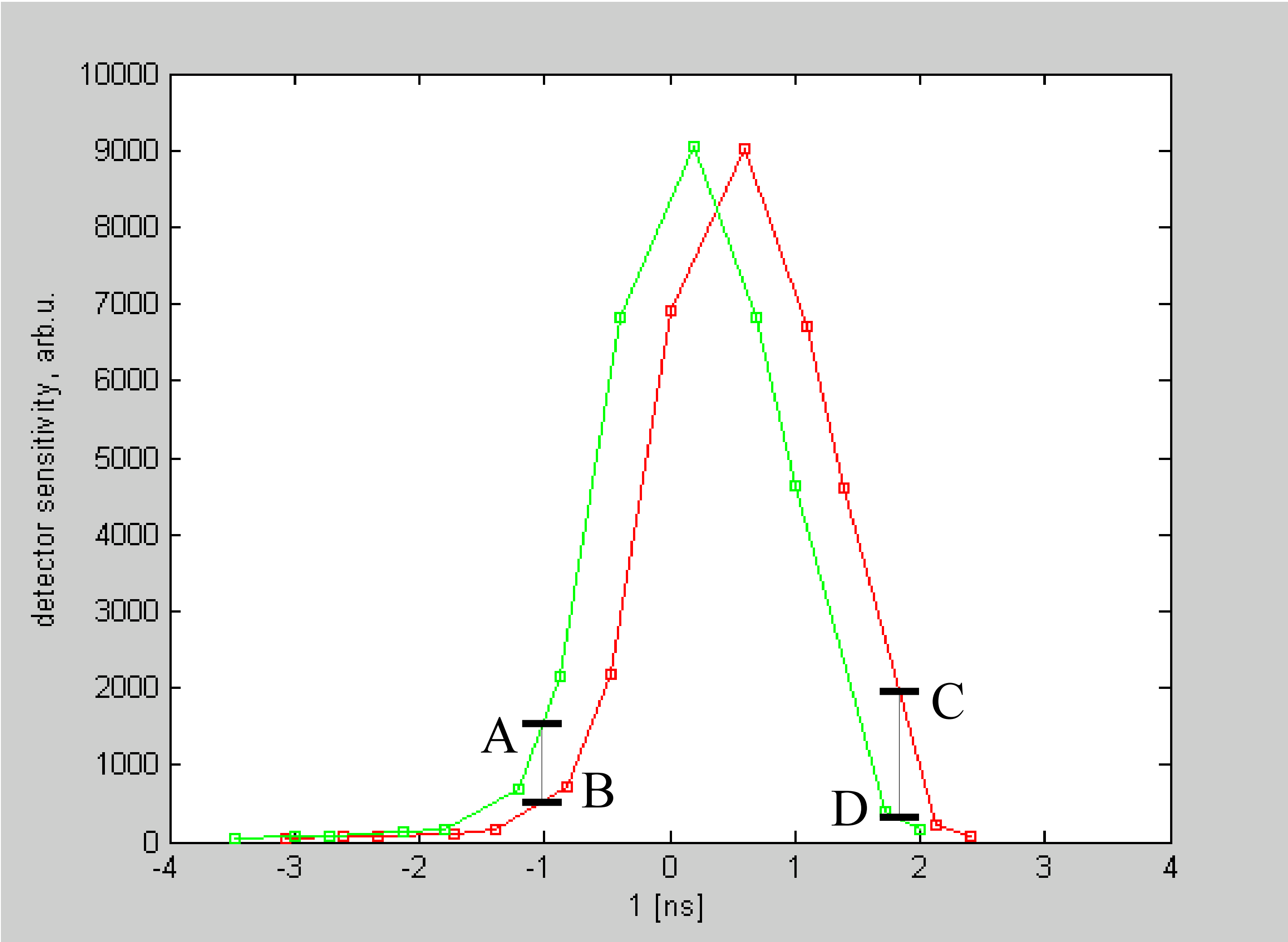


Detector sensitivity curves. Probing pulse 100 ps FWHM

(Possible) ideal case



Non-ideal case

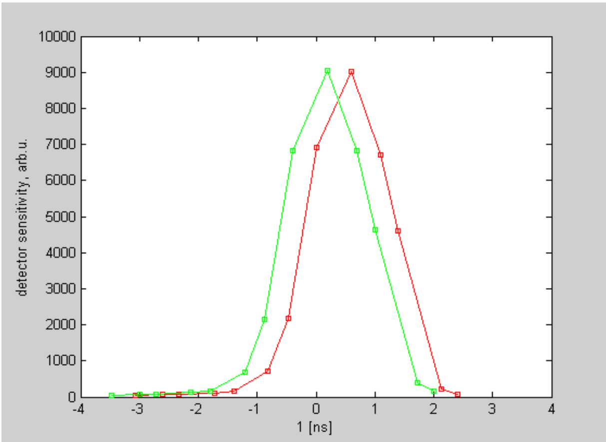


$$QBER = f\left(A/B, C/D \right)$$

NTNU

We want detector data from other setups!

- Measurements of detector sensitivity curves from other QKD setups will help understand and quantify the problem
- This is a very simple measurement: **count rate** vs. **time of incoming pulse**



- The probing pulse <u>preferably</u> need be as short as possible, down to <30 ps
- Use small time increments; measure tails

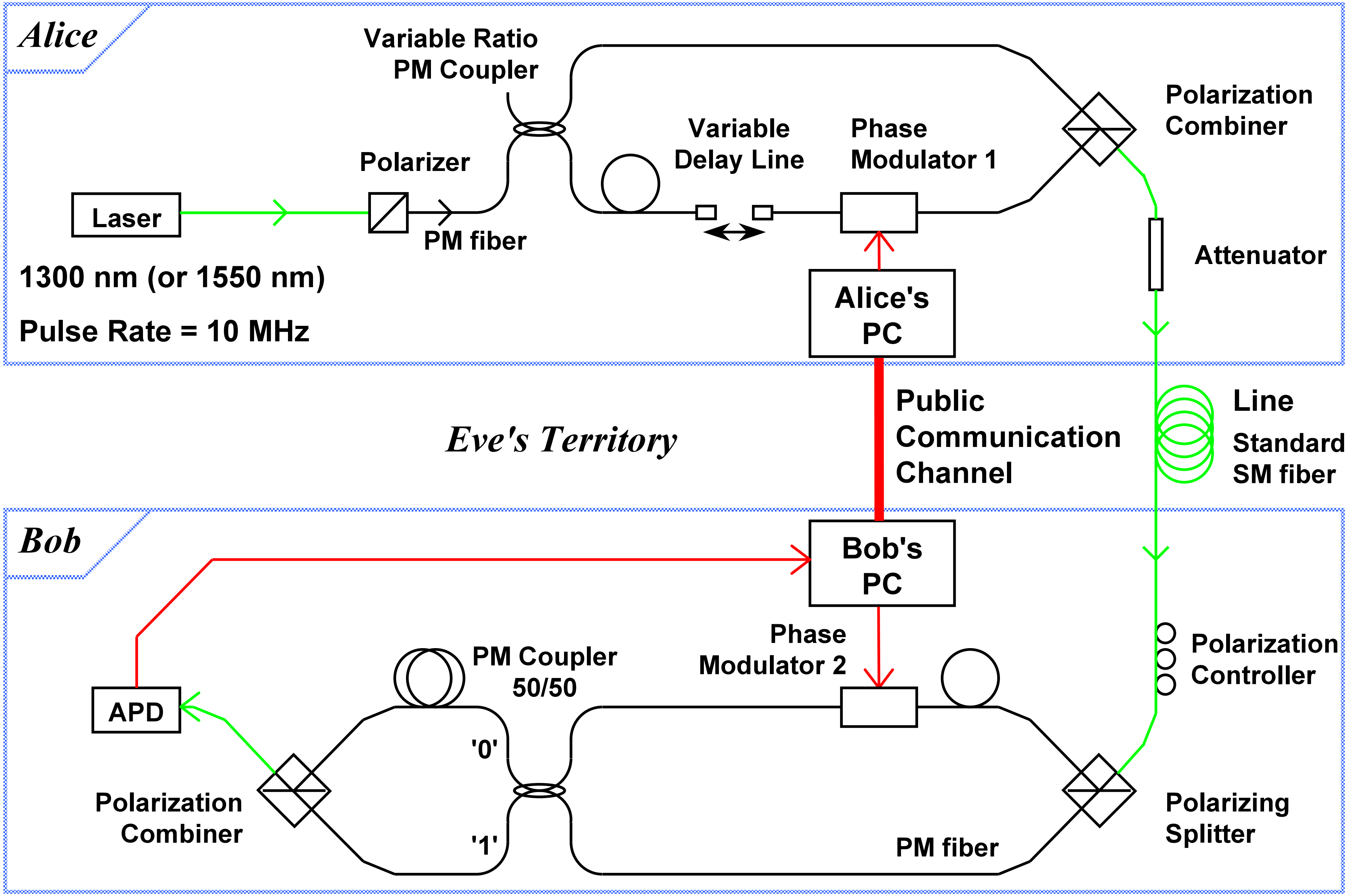
NTNU

- Large pulse attack
- Light emission from APDs
- Faked states attack – passive basis choice
- Faked states attack – active basis choice

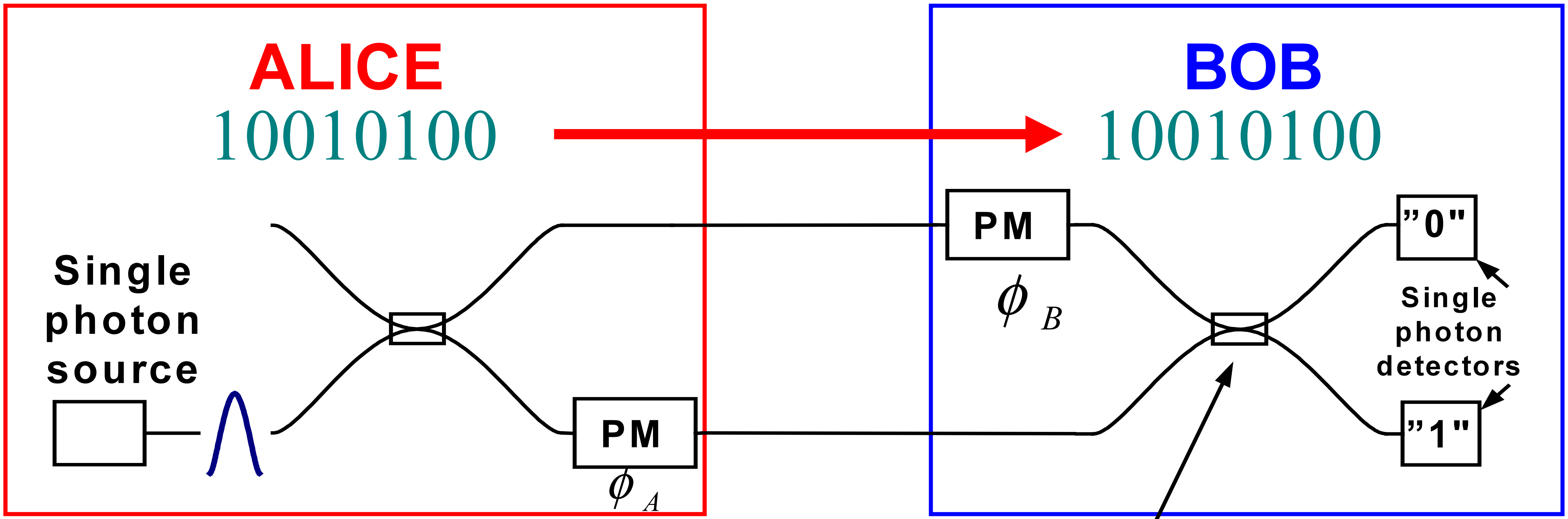
ВСЁ!

Optional slides

Interferometer structure (setup in Trondheim)



Quantum key distribution: phase coding



Φ_A:

	X	Y
"0"	0^o	90^o
"1"	180^o	270^o

Φ_B:

X	Y
0^o	90^o

$$P(0) \sim \cos^2\left(\frac{\phi_A - \phi_B}{2}\right)$$