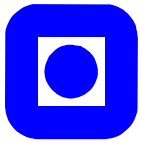
Lecture in "Fiberkomponenter" course, November 13, 2003

NTNU



Quantum Cryptography

Kvantekryptering

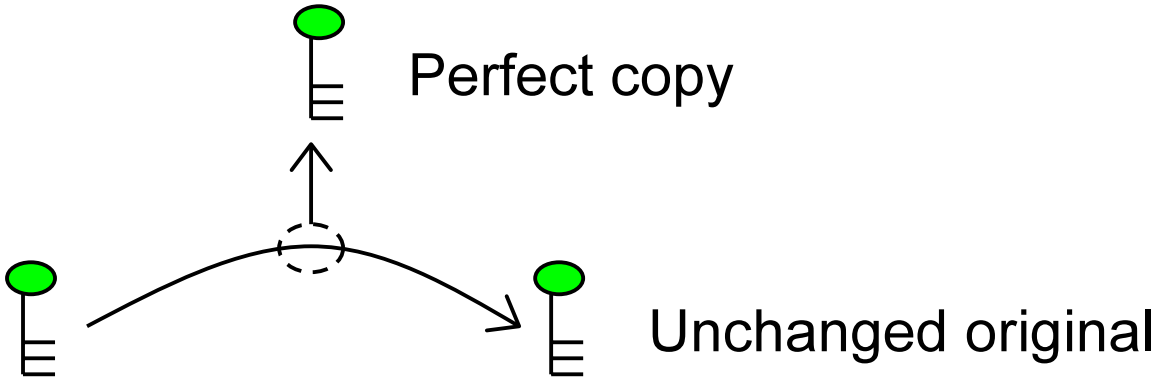
Vadim Makarov

www.vad1.com/qcr/

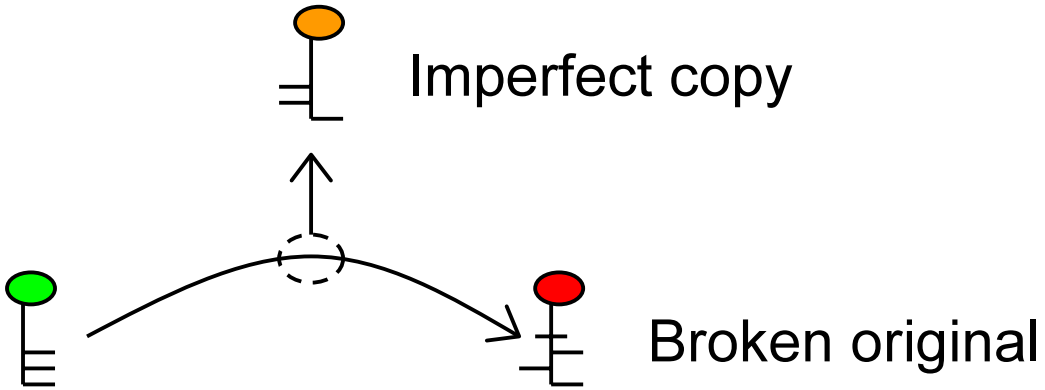
Classical vs. quantum information

NTNU

- **Classical information**

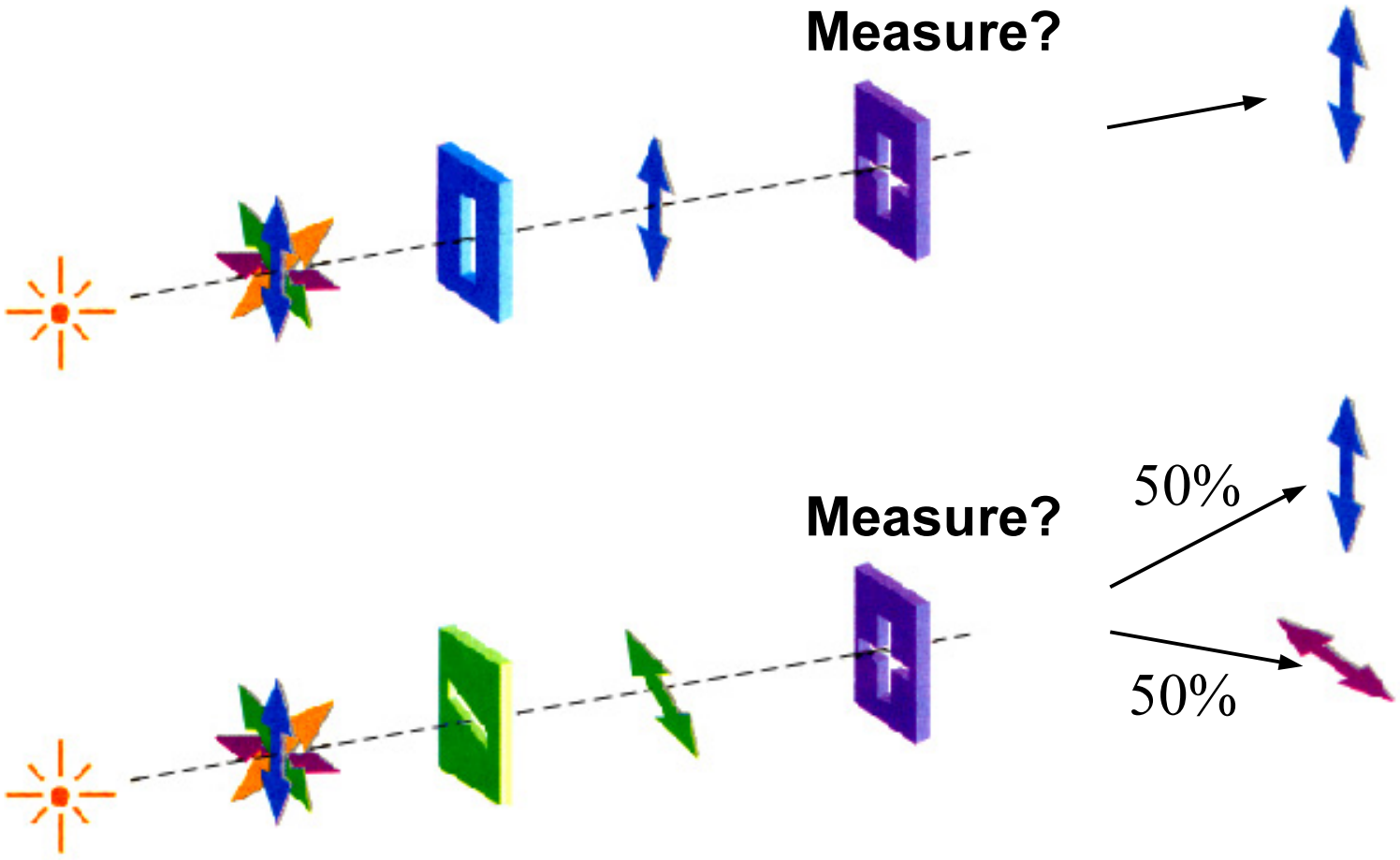


- **Quantum information**

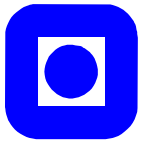


Qubit: polarization state of a single photon

NTNU



NTNU

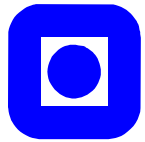


What is the problem with classical cryptography?

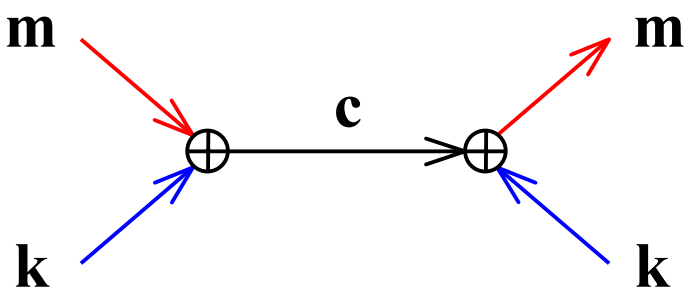
- **Secret key cryptography**
  - **Requires secure channel for key distribution**
  - ***In principle* every classical channel can be monitored passively**
  - **Security is mostly based on complicated non-proven algorithms**
- **Public key cryptography**
  - **Security is based on non-proven mathematical assumptions (e.g. in RSA cipher, difficulty of factoring large numbers)**
  - **We DO know how to factorize in polynomial time! Shor's algorithm for quantum computers. Just wait until one is built.**
  - **Breakthrough renders messages insecure *retroactively***

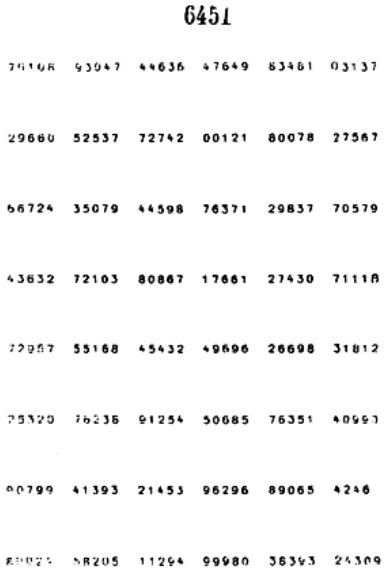
The holy grail: One-time pad

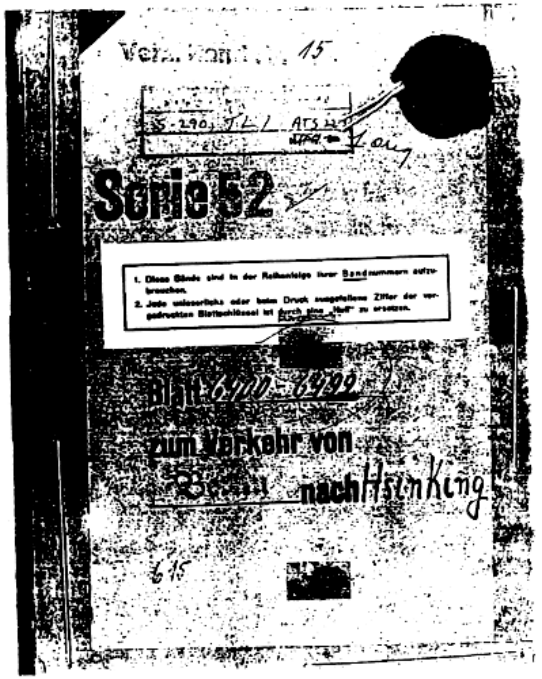
NTNU



- **The only cipher mathematically proven**
- **Requires massive amounts of key material**
  (key of same length as message, used only once)

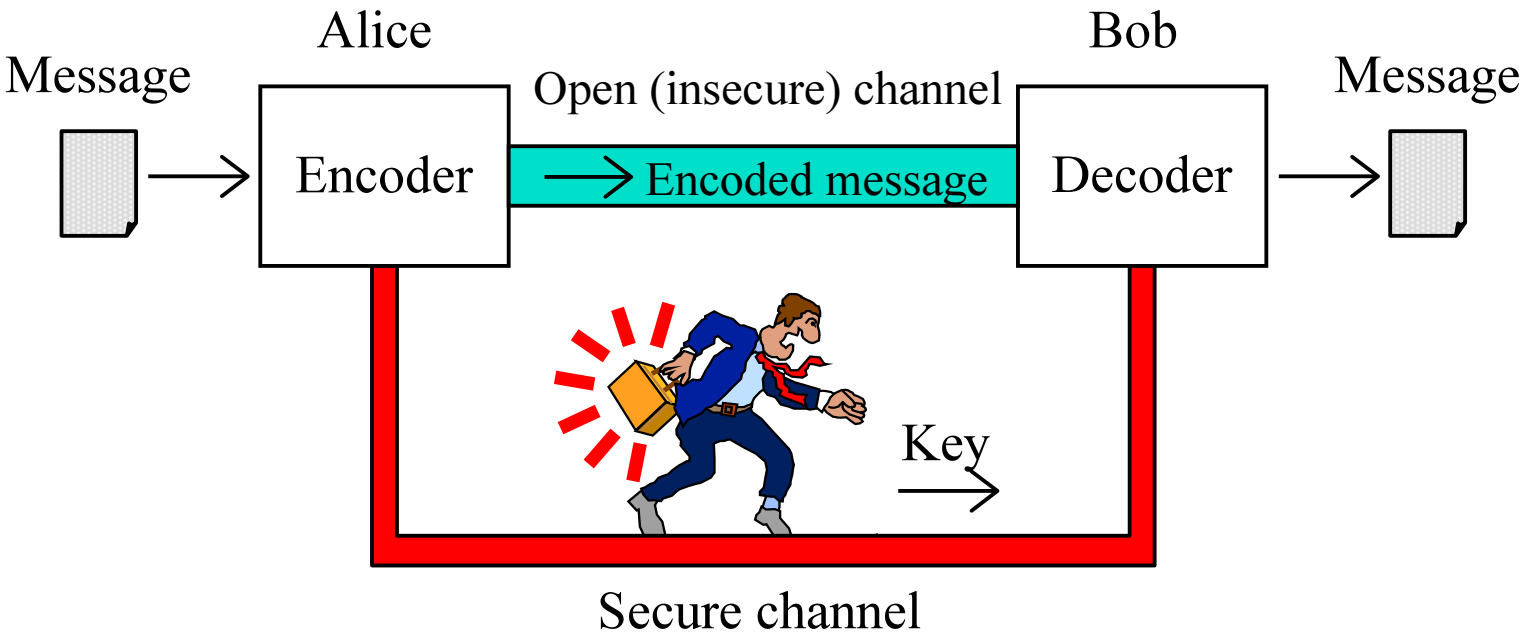






Key distribution

NTNU



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

Quantum key distribution

NTNU

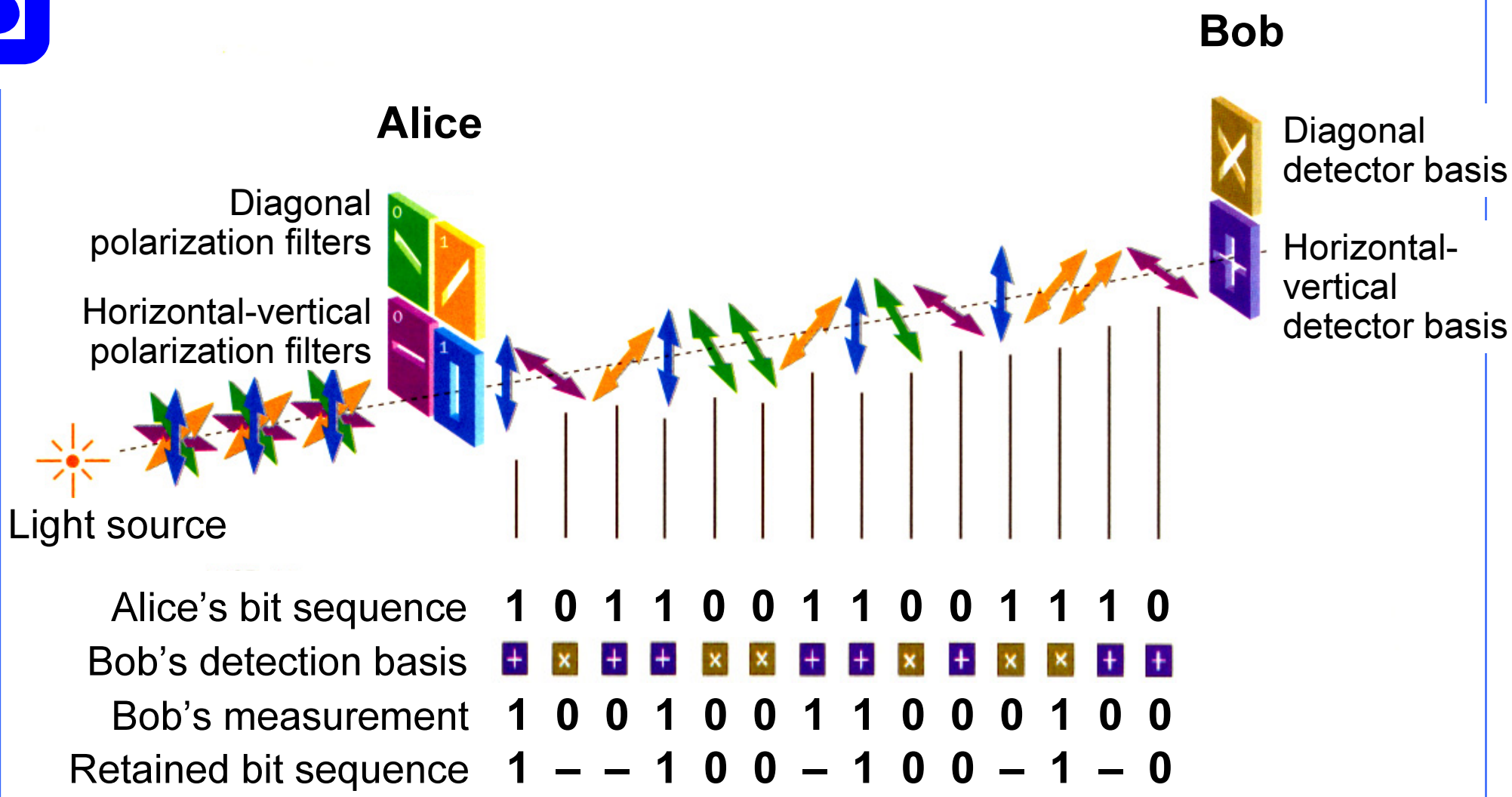
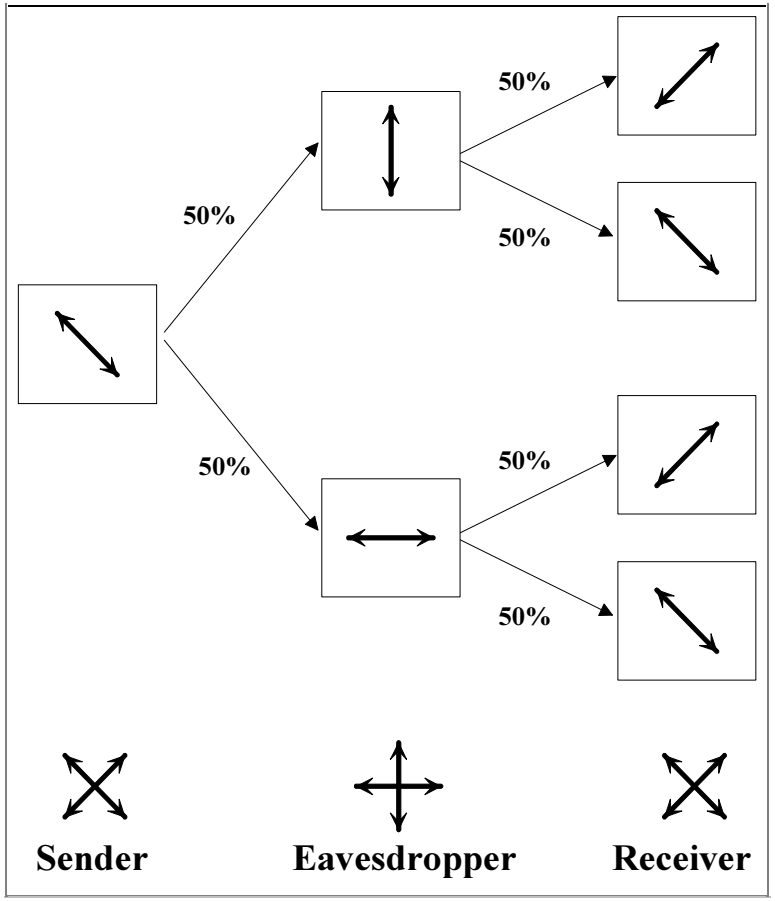


Image reprinted from article: W. Tittel, G. Ribordy, and N. Gisin, "Quantum cryptography," Physics World, March 1998

Eavesdropping with wrong reference system

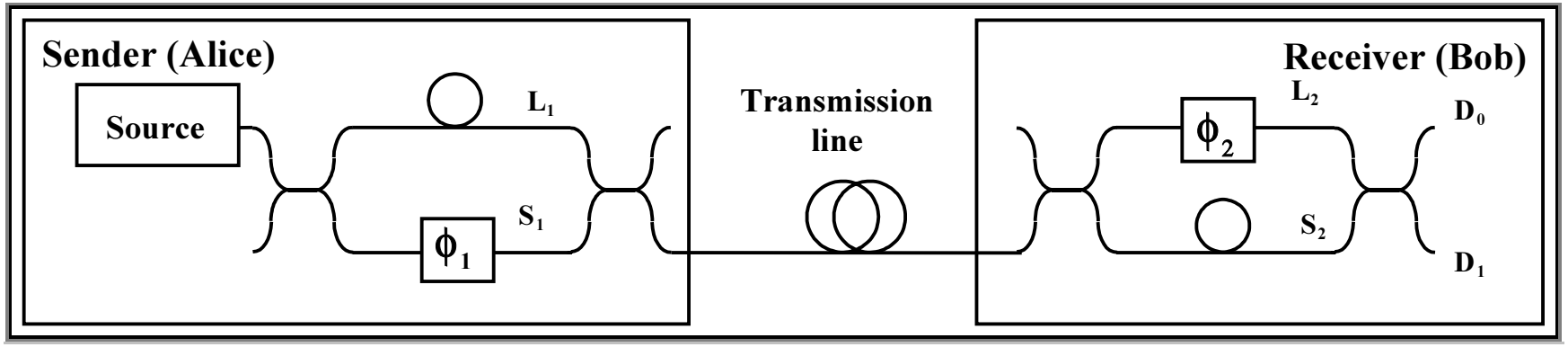
NTNU



Sender	Tyvlytter			Mottaker
	Referanse	Resultat av måling		
"0"	Rett	"0"	Rett	Rett
	Galt	"0"	Rett	Rett
		"1"	Galt	Galt
"1"	Rett	"1"	Rett	Rett
	Galt	"0"	Galt	Rett
		"1"	Rett	Galt
"0"	Rett	"0"	Rett	Rett
	Galt	"1"	Galt	Rett
		"0"	Rett	Galt
"1"	Rett	"1"	Rett	Rett
	Galt	"1"	Rett	Rett
		"0"	Galt	Galt

Interferometric QKD channel

NTNU



$\phi_1 =$ 0° or 90° - "1"

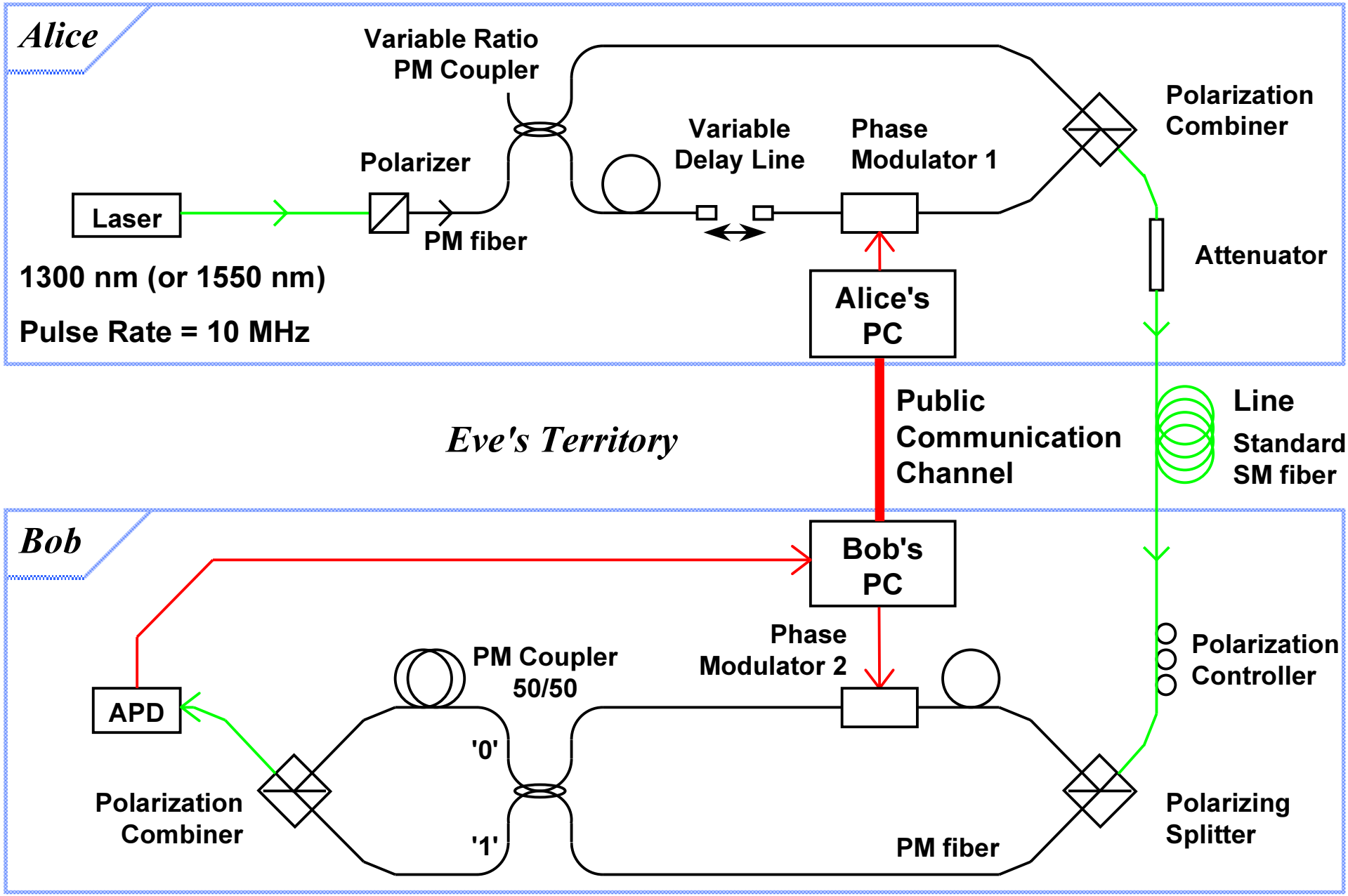
$\phi_1 =$ 180° or 270° - "0"

Reference systems:

$\phi_2 =$ 0°

$\phi_2 =$ 90°

Implementation: interferometer structure



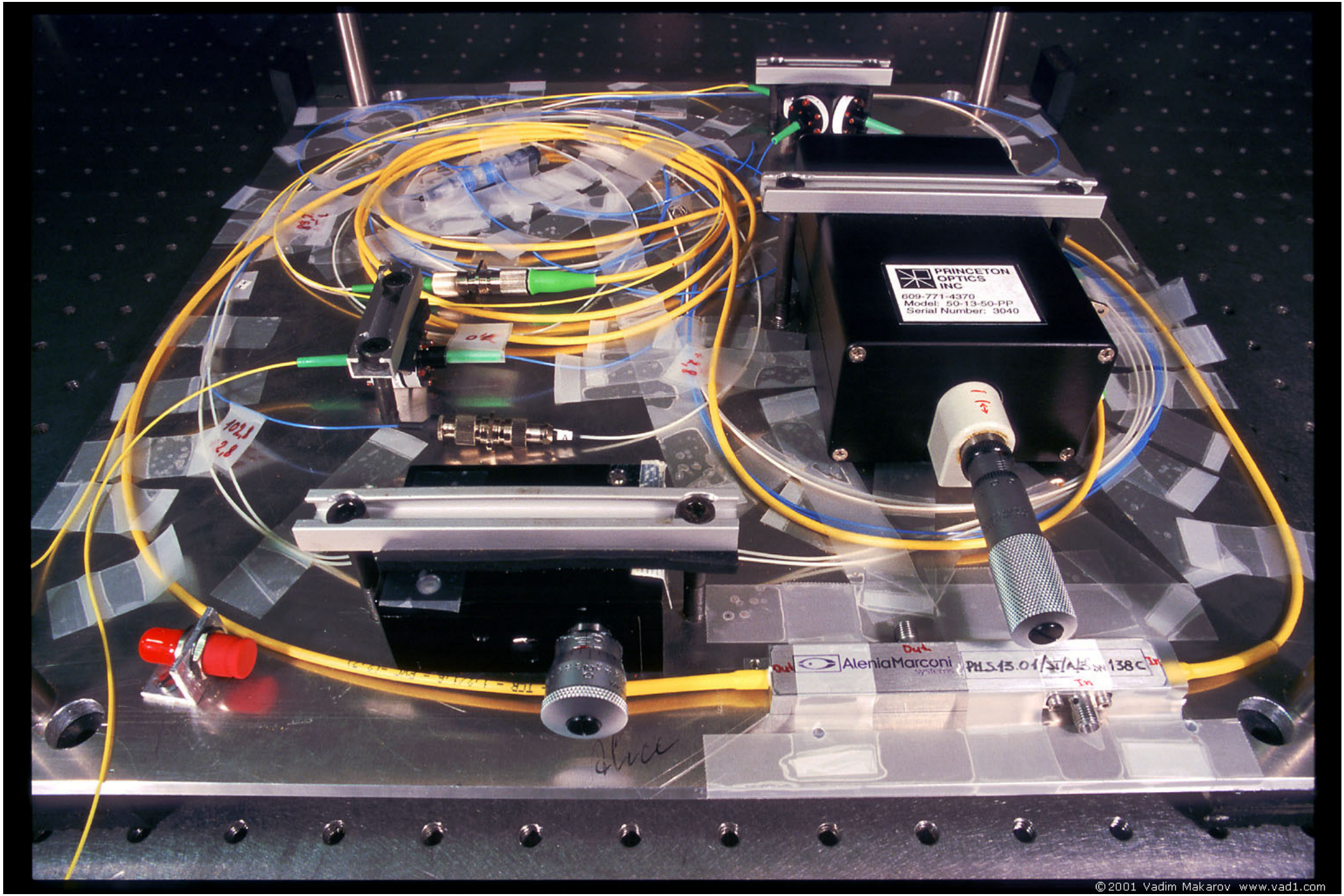


Photo 1. **Alice** (uncovered, no thermoisolation installed)

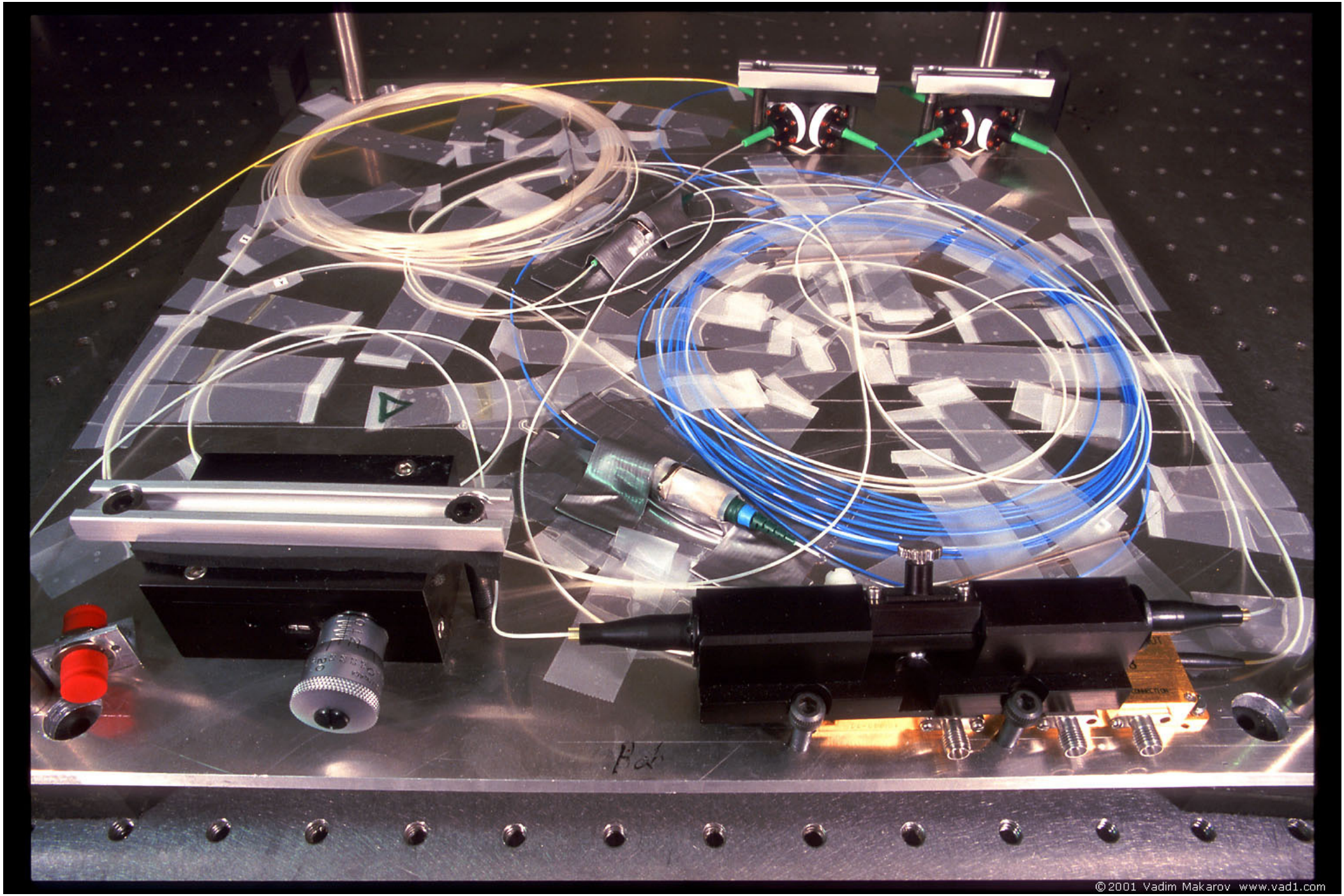
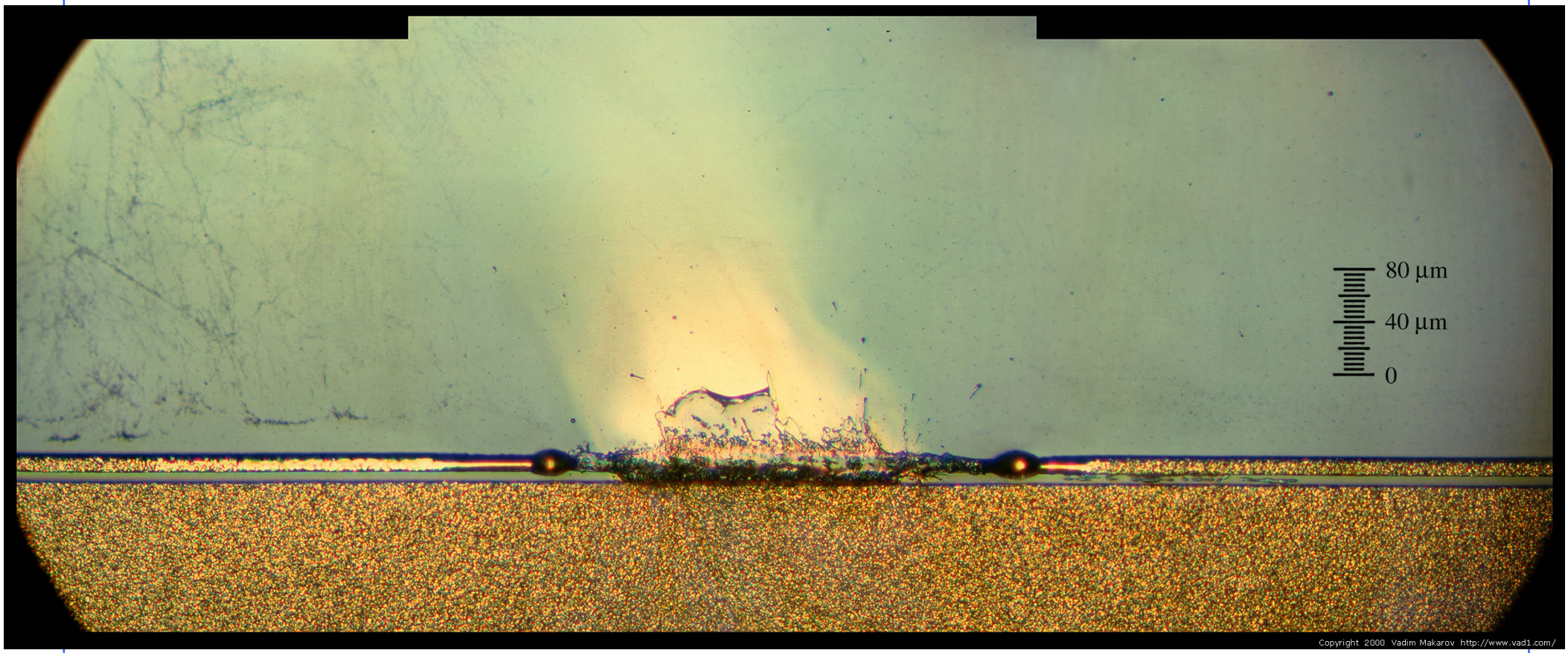


Photo 2. **Bob** (uncovered, no thermoisolation installed)

20 GHz travelling-wave phase modulator, 1300 nm

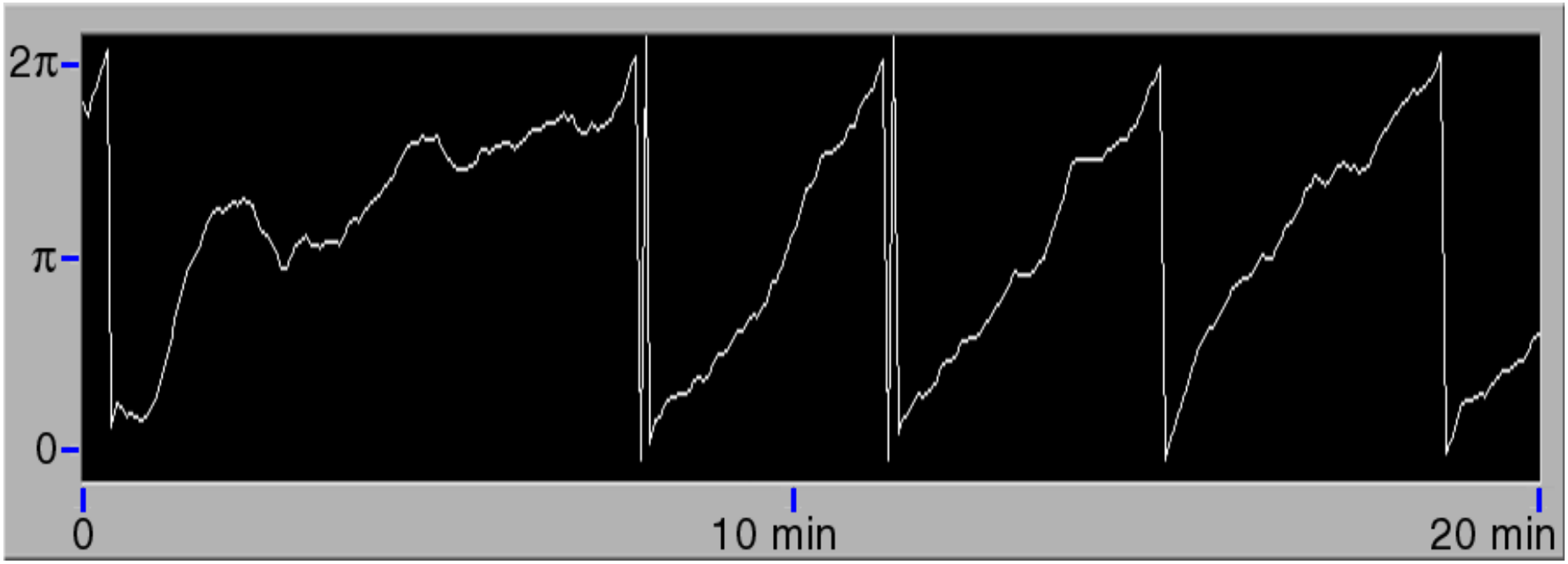
(manufacturer: Uniphase)



Results of electrical breakdown in the waveguide (microphotograph)

Real-time phase tracking in the interferometer

NTNU



Due to thermal drift, interferometer needs automatic phase adjustment every few seconds.

Phase adjustment takes ≈0.3 s and requires no additional components, e.g. no variable attenuator.

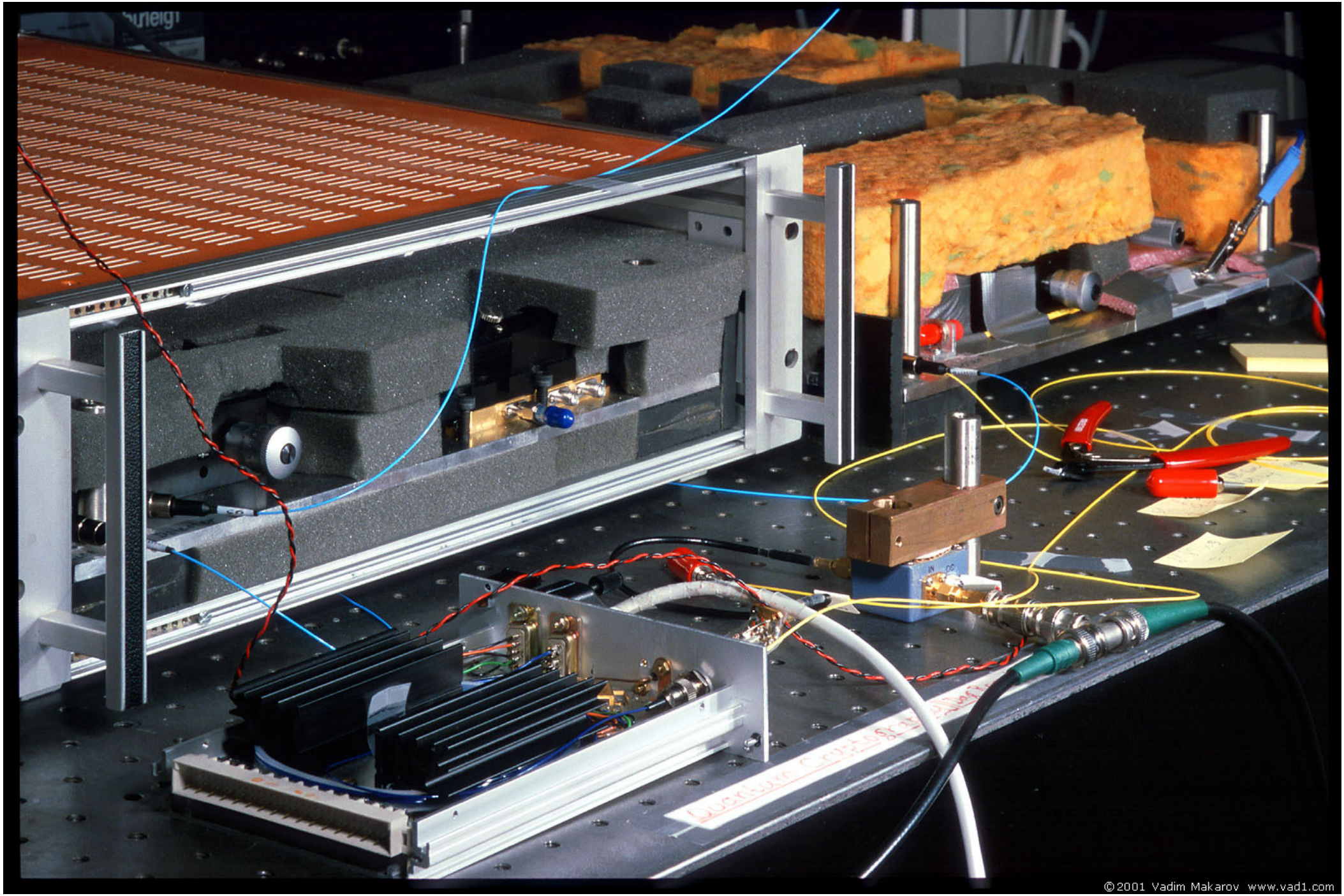
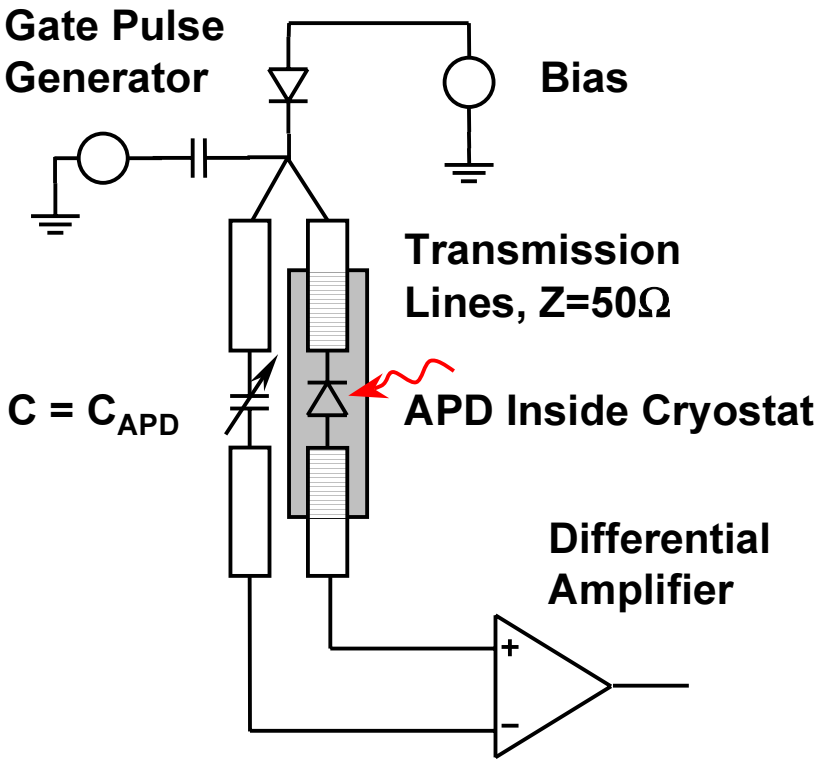
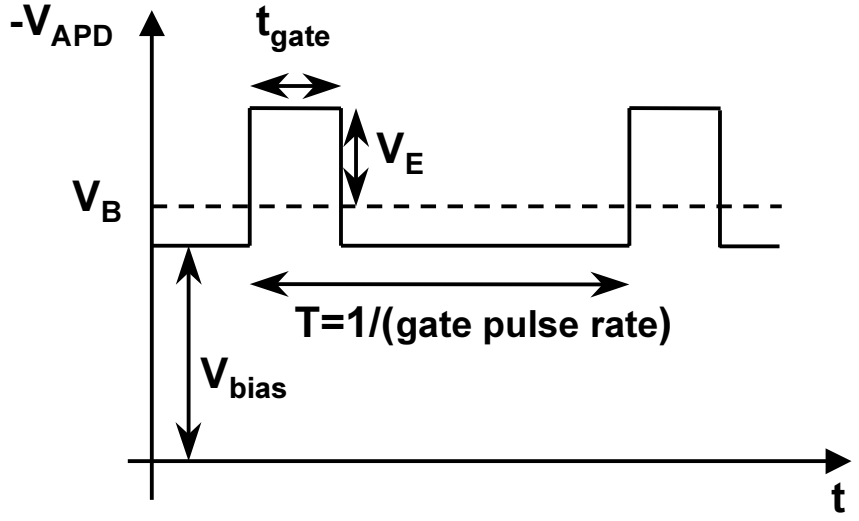


Photo 4. Bob (left) and Alice (right), thermoisolation partially installed

Single-photon detector: APD in Geiger mode

NTNU



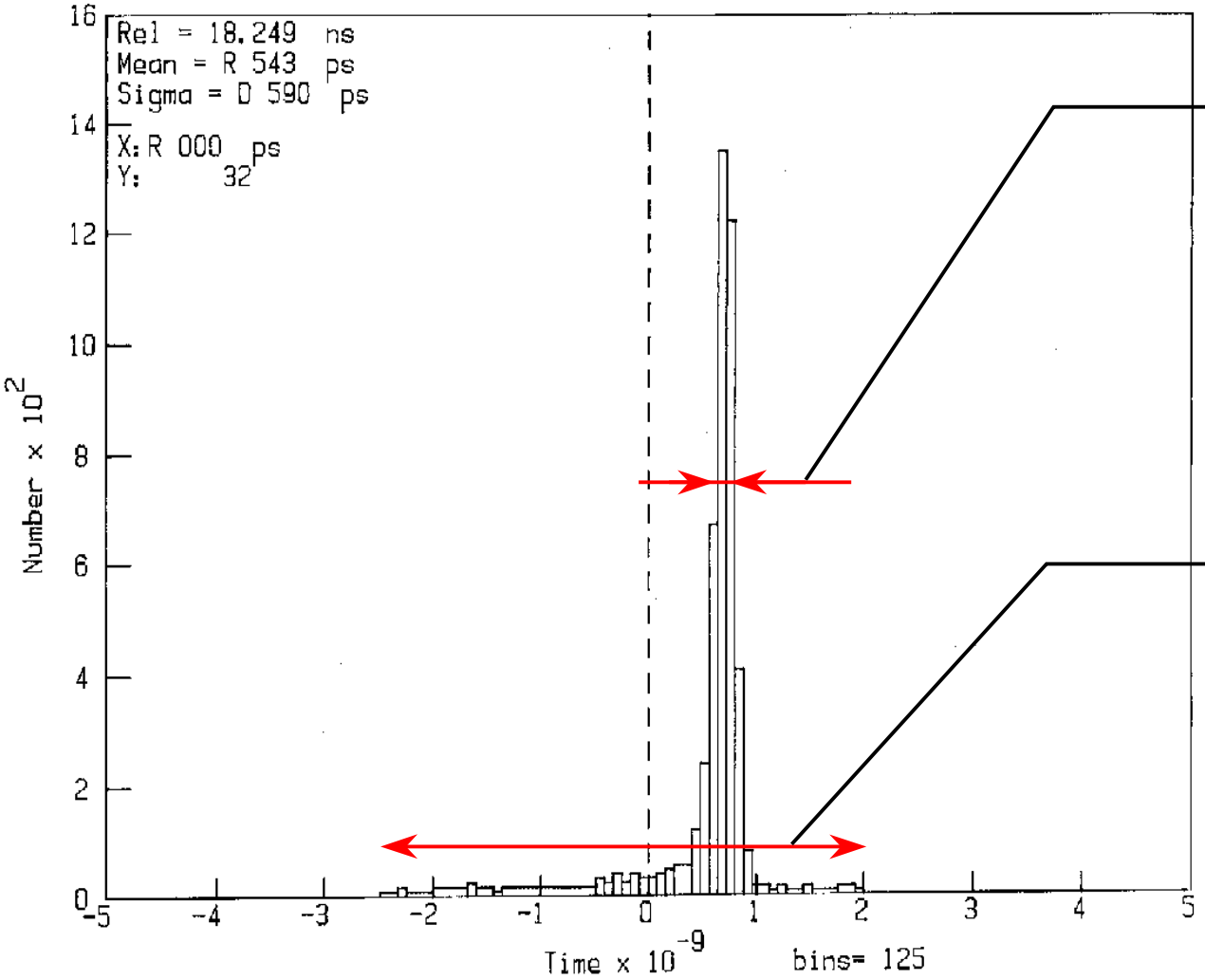


t_{gate} down to 1ns

gate pulse rate = 20 MHz

Timing resolution of photon detection

NTNU



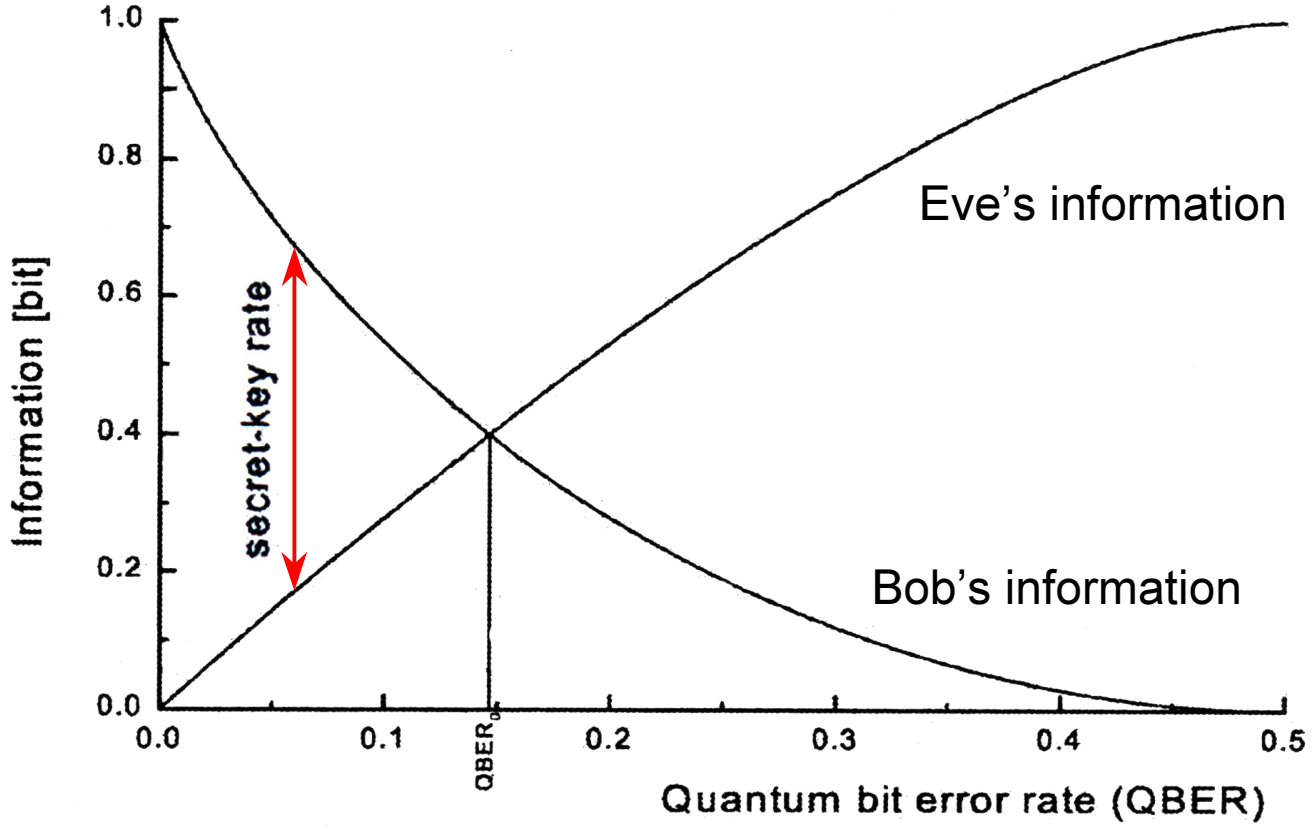
Photon counts due to 75 ps laser pulse

FWHM ~ 200 ps

Dark counts within 5ns gate

Recovery from errors

NTNU

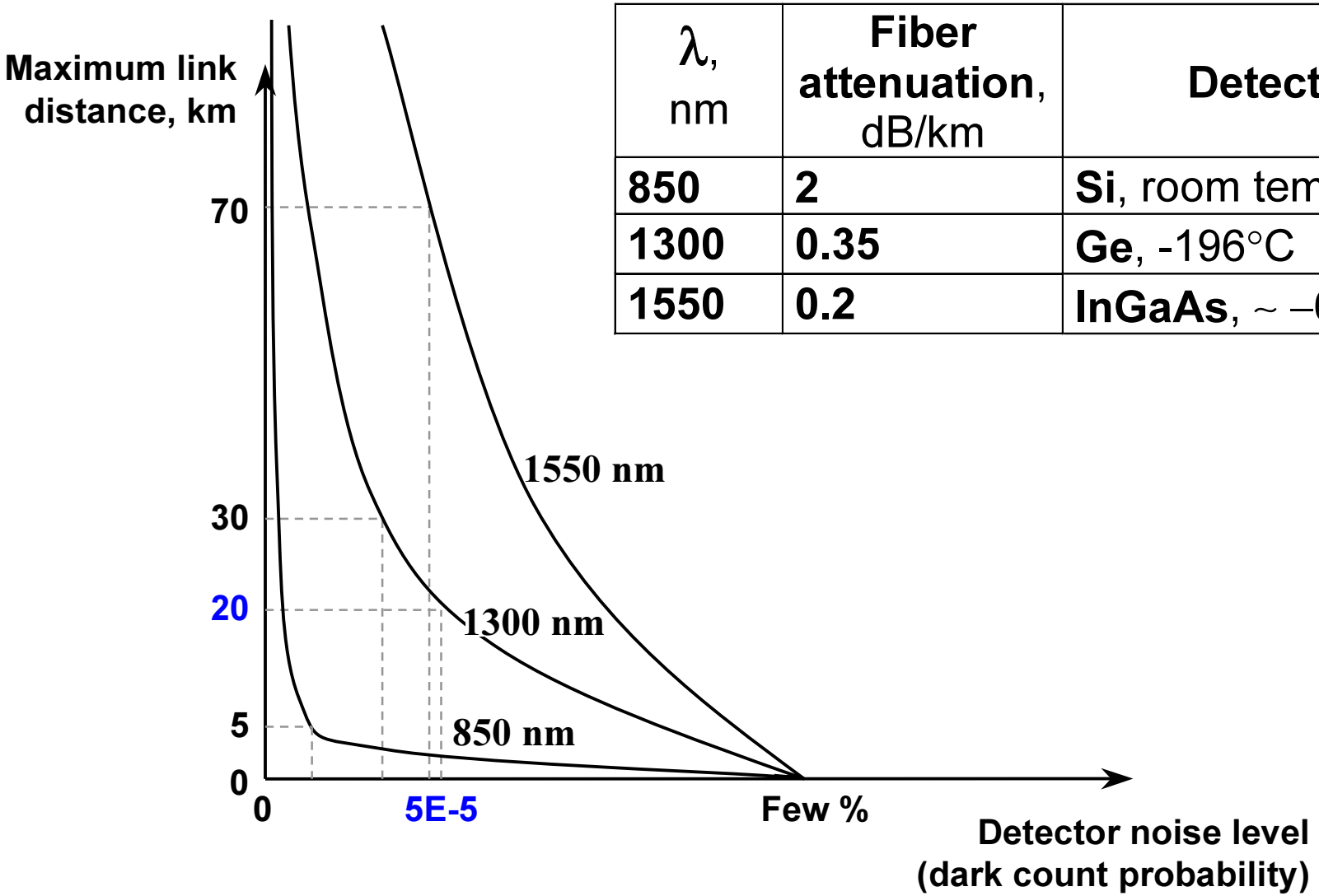


QBER limit:

- **Individual attacks: 15%**
- **All theoretically possible attacks: 11%(?)**

Distance limitation

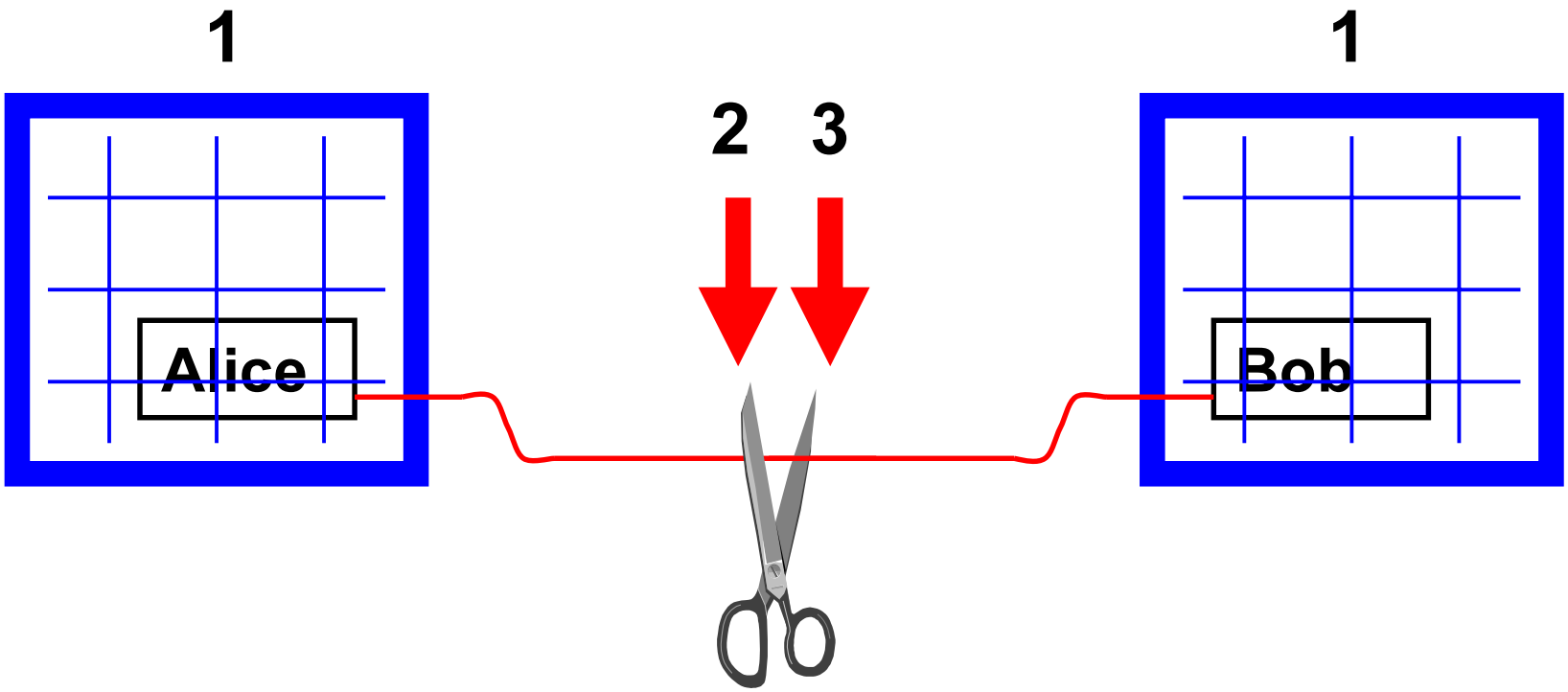
NTNU



λ, nm	**Fiber attenuation**, dB/km	**Detectors**
850	**2**	**Si**, room temperature
1300	**0.35**	**Ge**, -196°C
1550	**0.2**	**InGaAs**, ~ –60°C

Components of security

NTNU

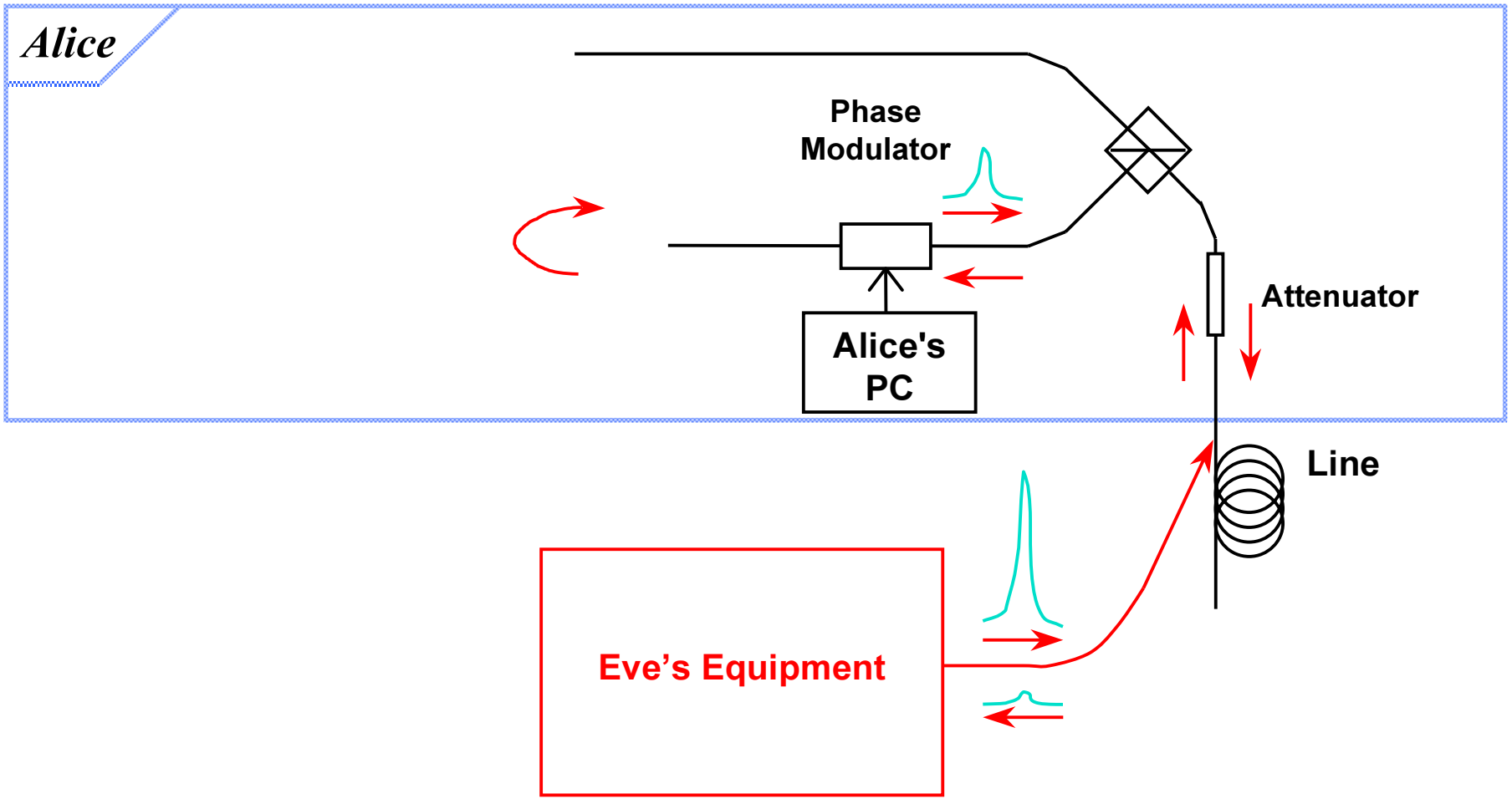


1. **Conventional security**
2. **Security against quantum attacks**
3. **Security against Trojan horse attacks**

   - ones that don't deal with quantum states, but use loopholes in optical scheme

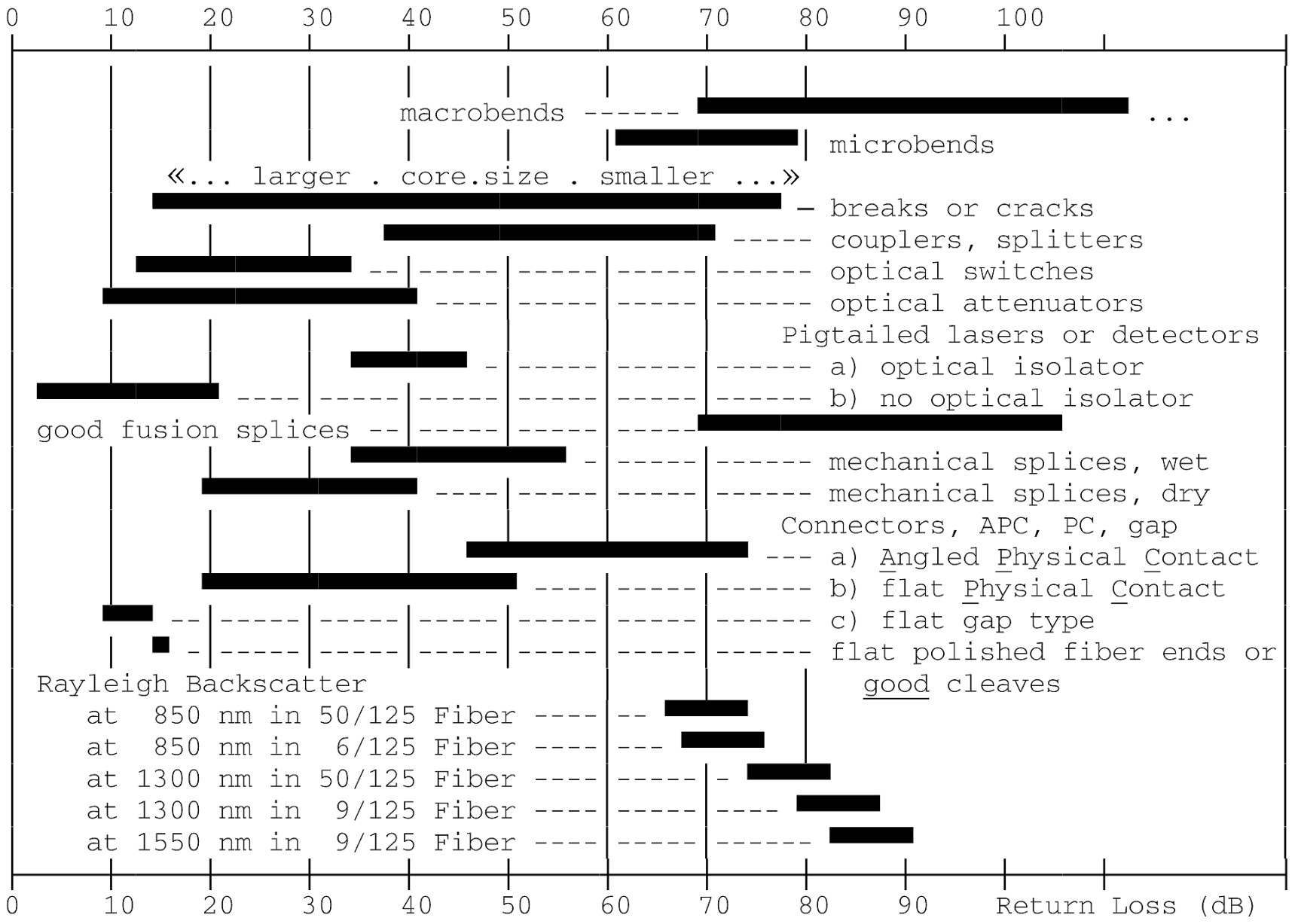
Practical security: large pulse attack

NTNU



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

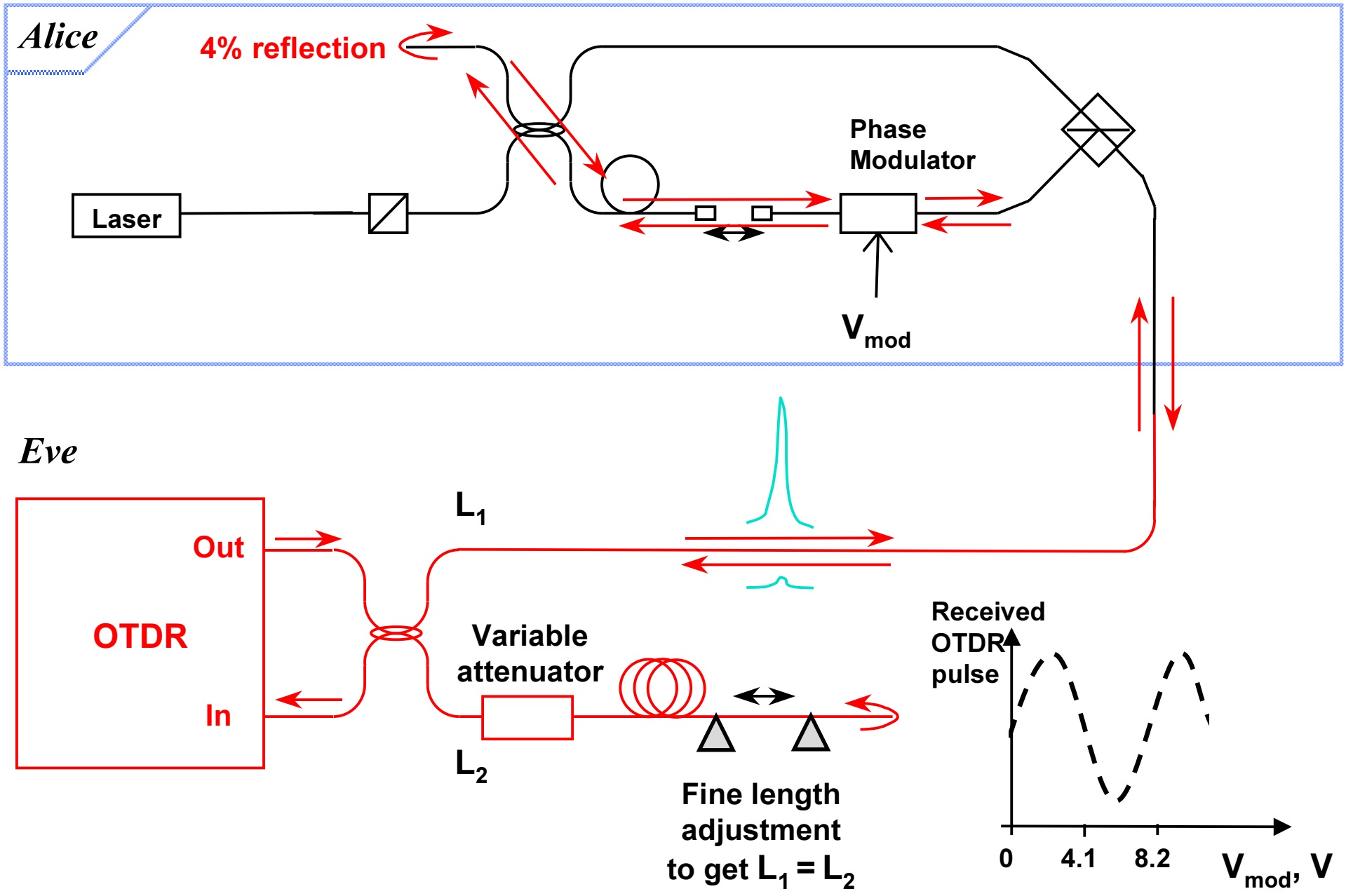
NTNU



Typical values of reflection coefficients for different fiber-optic components

(courtesy Opto-Electronics, Inc.)

Eavesdropping experiment



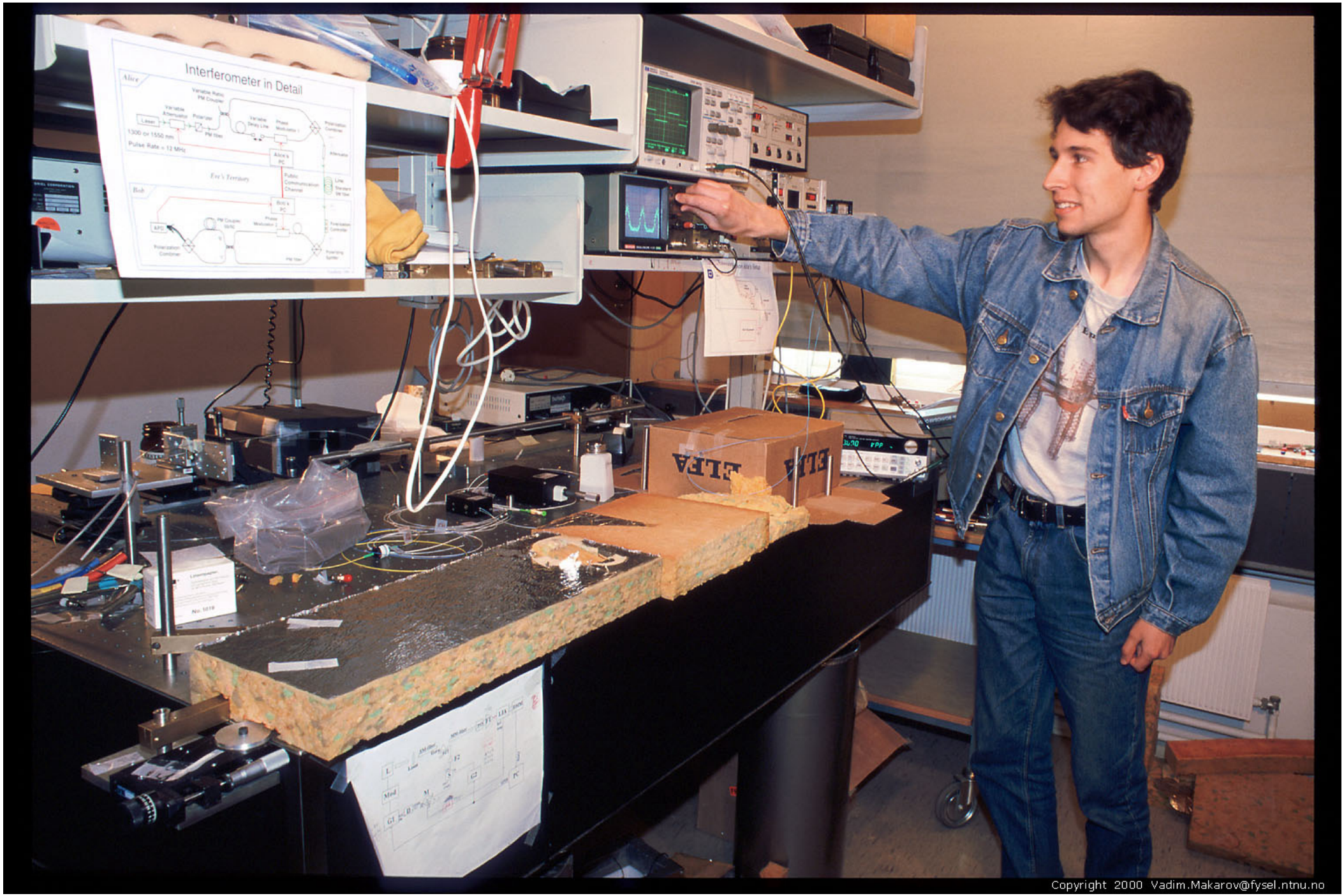
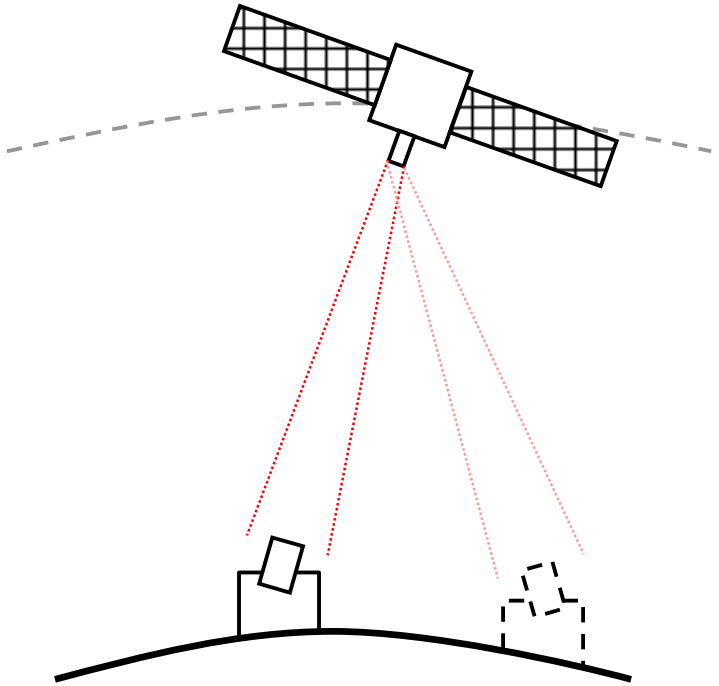
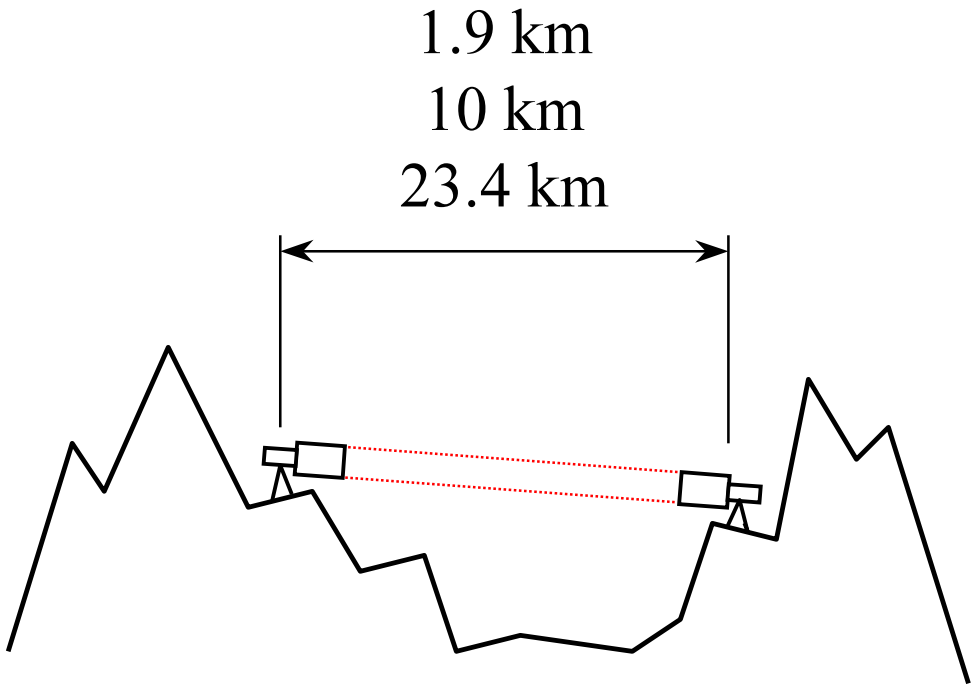


Photo 3. Artem Vakhitov tunes up Eve's setup

Re-keying satellites/ Global key distribution network

NTNU

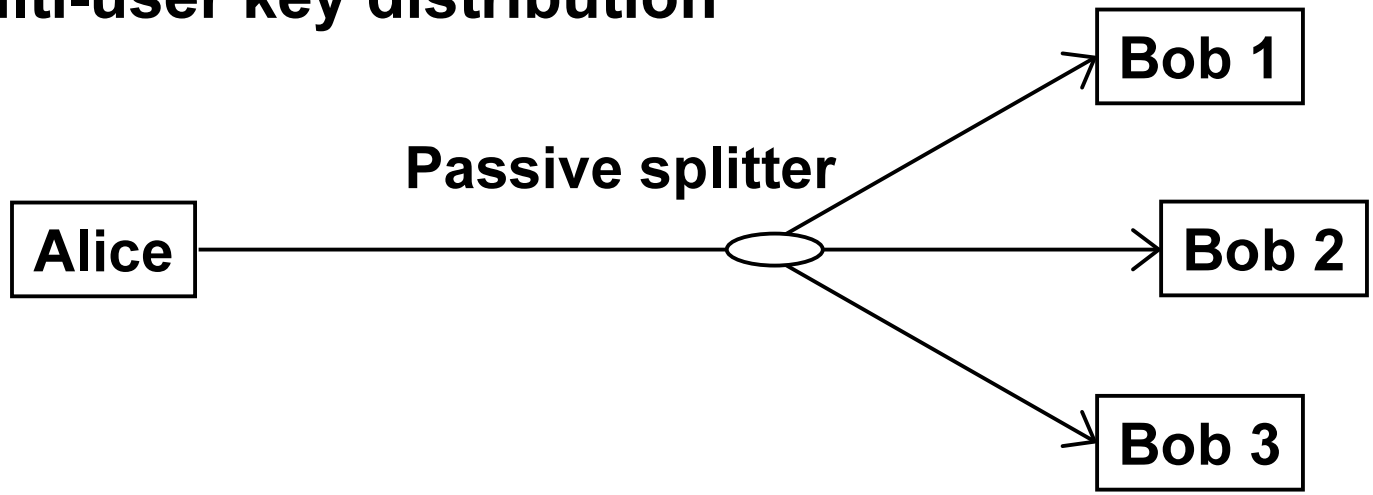




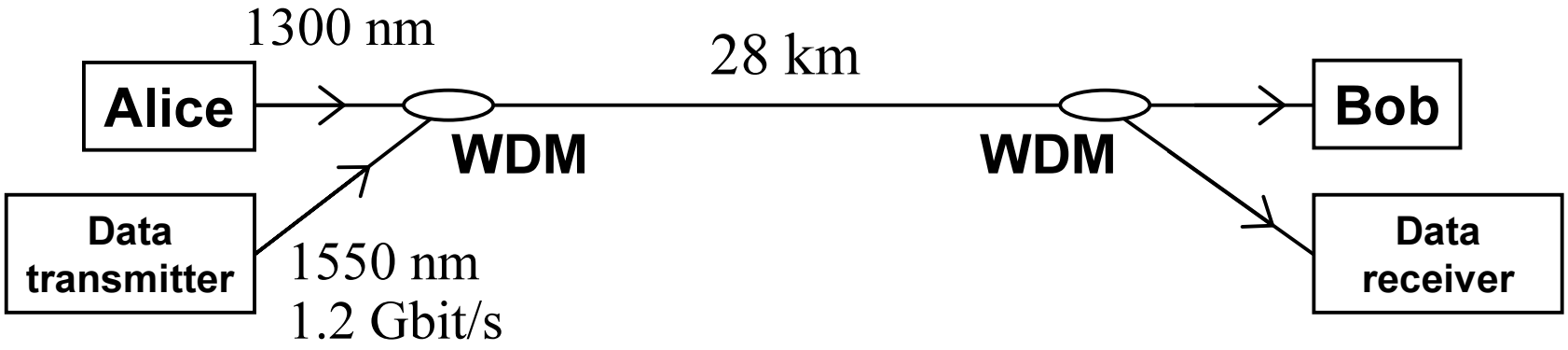
Quantum key distribution in fiber-optic network

NTNU

- **Multi-user key distribution**



- **Multiplexing with telecom traffic**

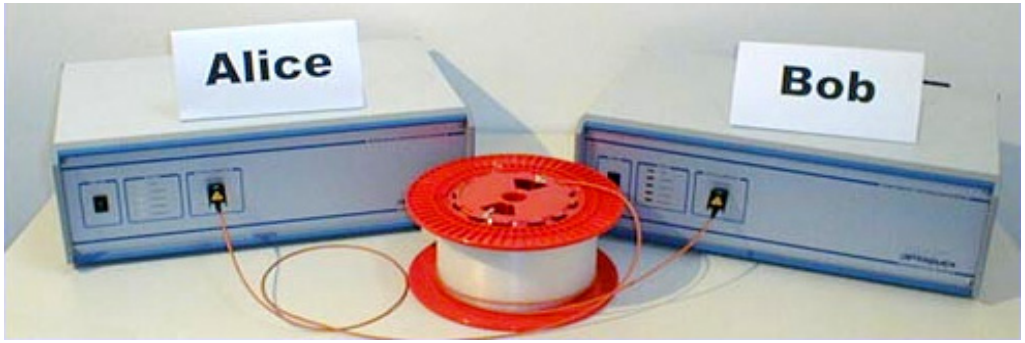


Commercial status

NTNU

Two small companies *trying* to sell QKD systems:

- **id Quantique (Geneva)**
  2002



- **MagiQ Technologies (Boston)**
  November 2003

- **+ several telecom/ electronics companies, research groups keep close eye on commercializing but don't develop a production version yet.**

Faglærere: Dag R. Hjelme,
Astrid Dyrseth

Diploma
Thesis
Available!