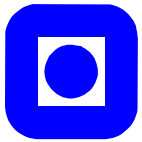
NTNU



Quantum Cryptography

Vadim Makarov and Dag R. Hjelme

Institutt for fysikalsk elektronikk NTNU

www.vad1.com/qcr/

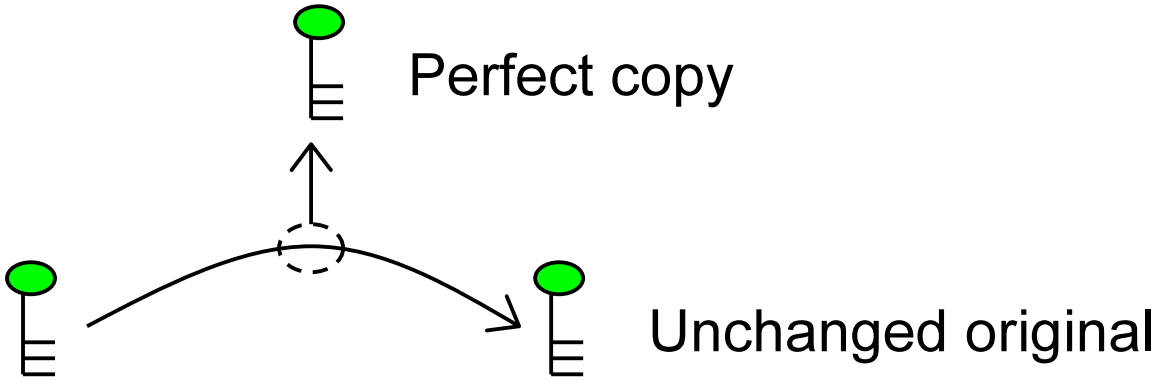
NTNU

Telenor
FoU

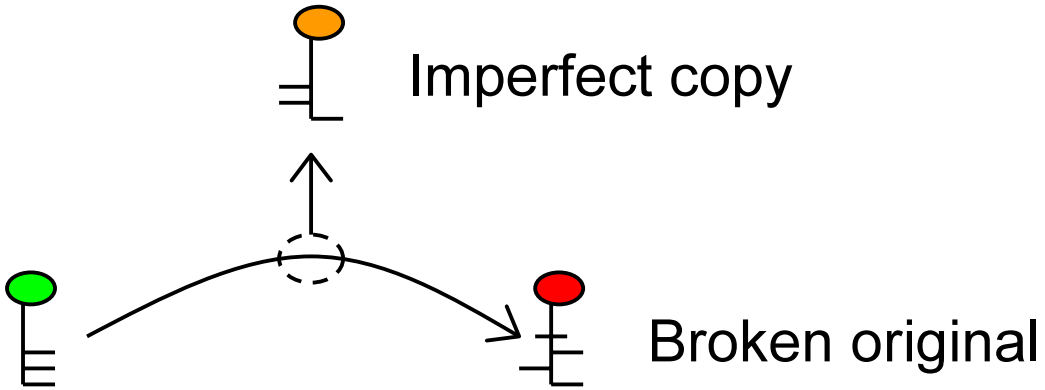
Classical vs. quantum information

NTNU

- **Classical information**

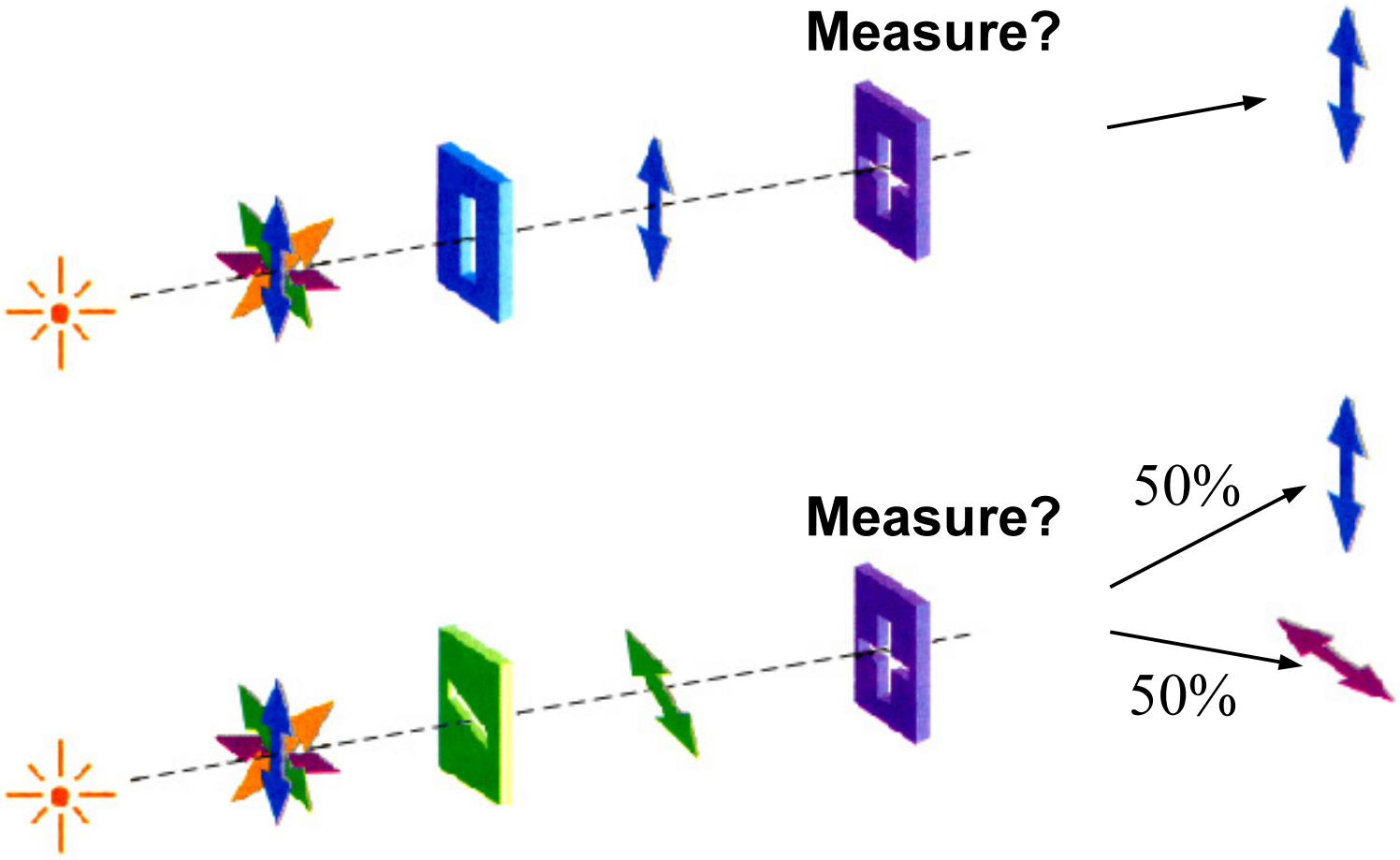


- **Quantum information**



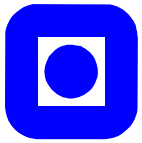
Qubit: polarization state of a single photon

NTNU



What is the problem with classical cryptography?

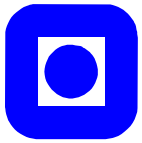
NTNU



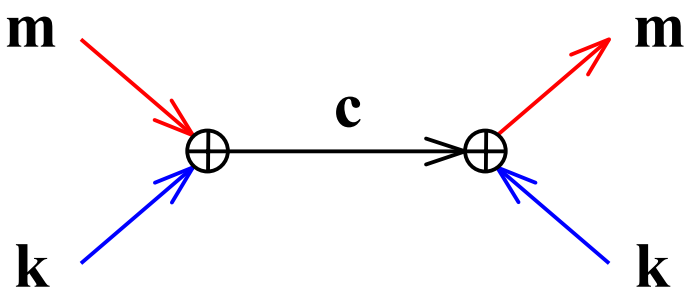
- **Secret key cryptography**
  - **Requires secure channel for key distribution**
  - ***In principle* every classical channel can be monitored passively**
  - **Security is mostly based on complicated non-proven algorithms**
- **Public key cryptography**
  - **Security is based on non-proven mathematical assumptions (e.g. 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***

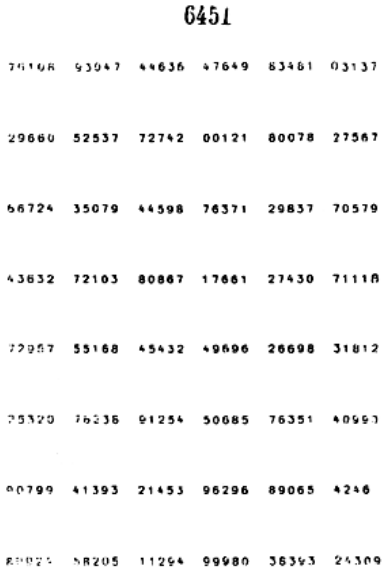
The holy grail: One-time pad

NTNU

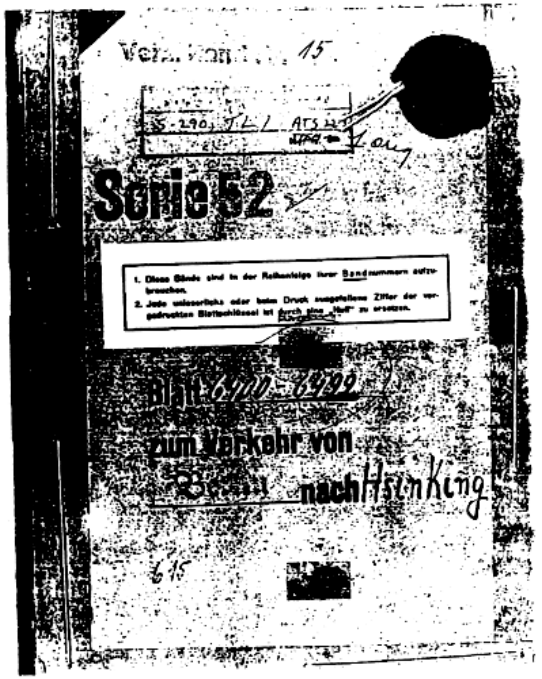


- **The only cipher mathematically proven**
- **Requires massive amounts of key material**



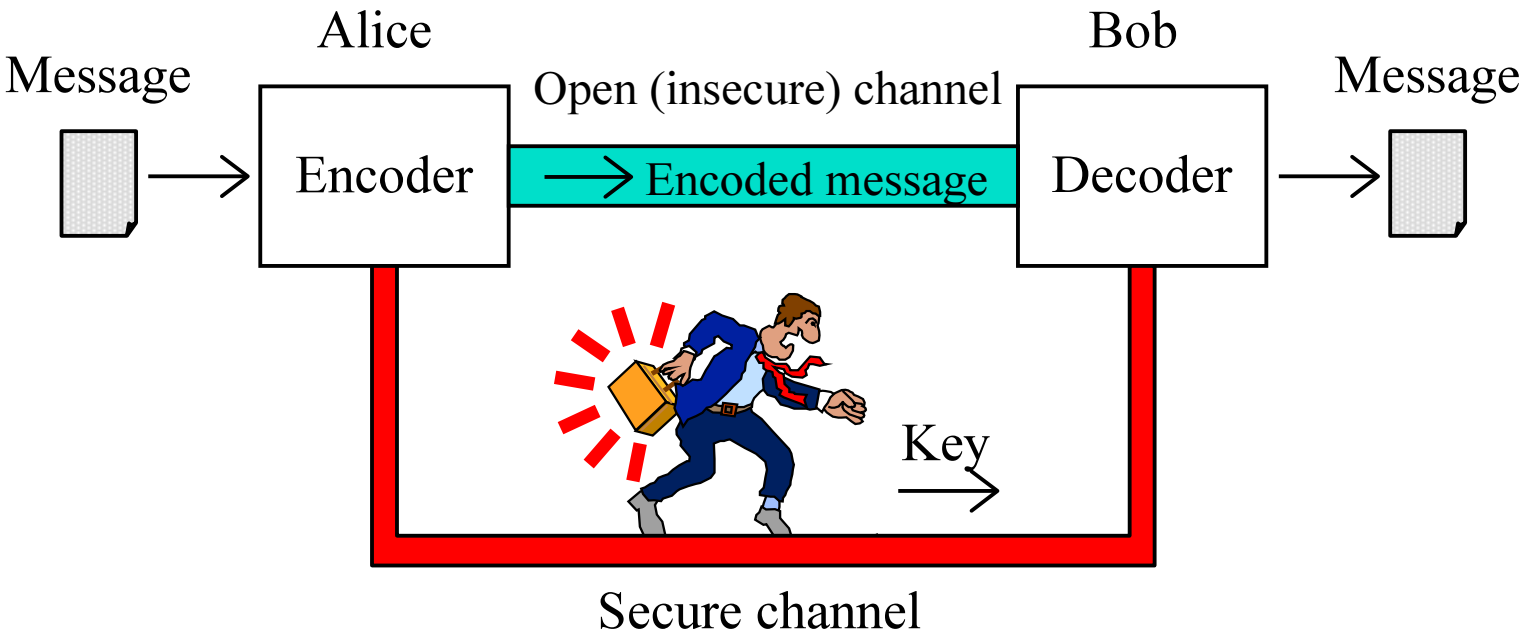

6451

76168	93947	44636	47649	83481	03137
29660	52537	72742	00121	80078	27567
56724	35079	44598	76371	29837	70579
43632	72103	80867	17661	27430	71118
72957	55168	45432	49696	26698	31812
75320	76236	91254	50685	76351	40993
90799	41393	21453	96296	89065	4246
[illegible]	58205	11294	99980	36343	24309



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

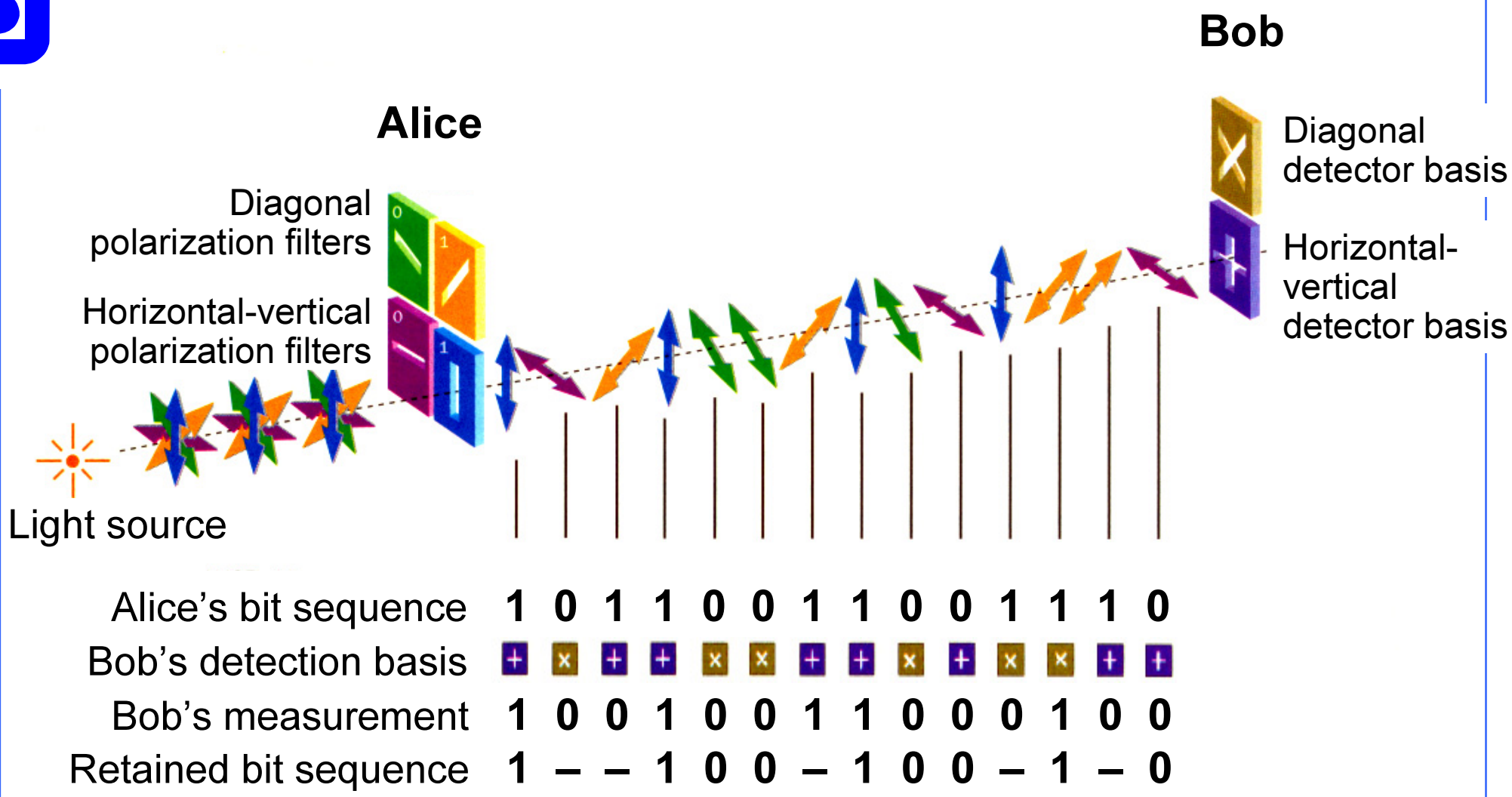
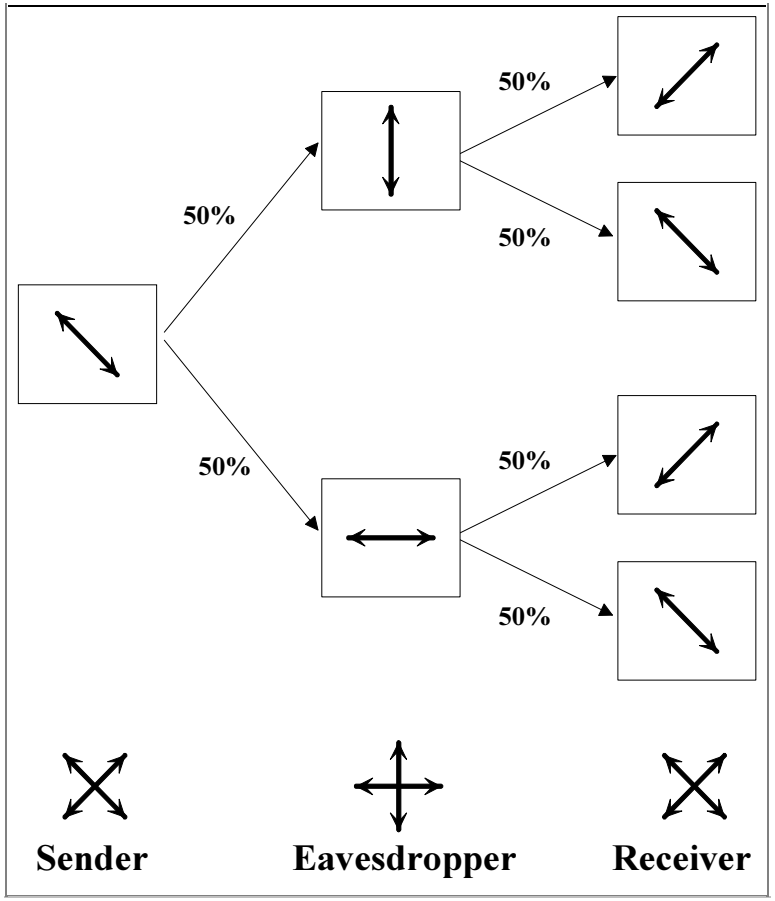


Image reprinted from article: W. Tittel, G. Ribordy, and N. Gisin, "Quantum cryptography," Physics World, March 1998

Eavesdropping with wrong reference system

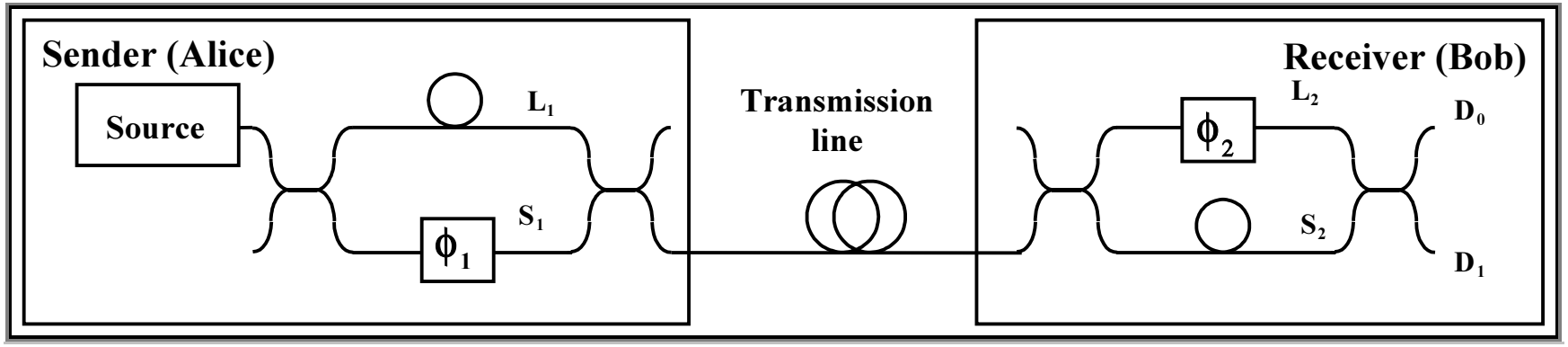
NTNU



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

Interferometric QKD channel

NTNU



$\phi_1 =$ 0° or 90° - "1"

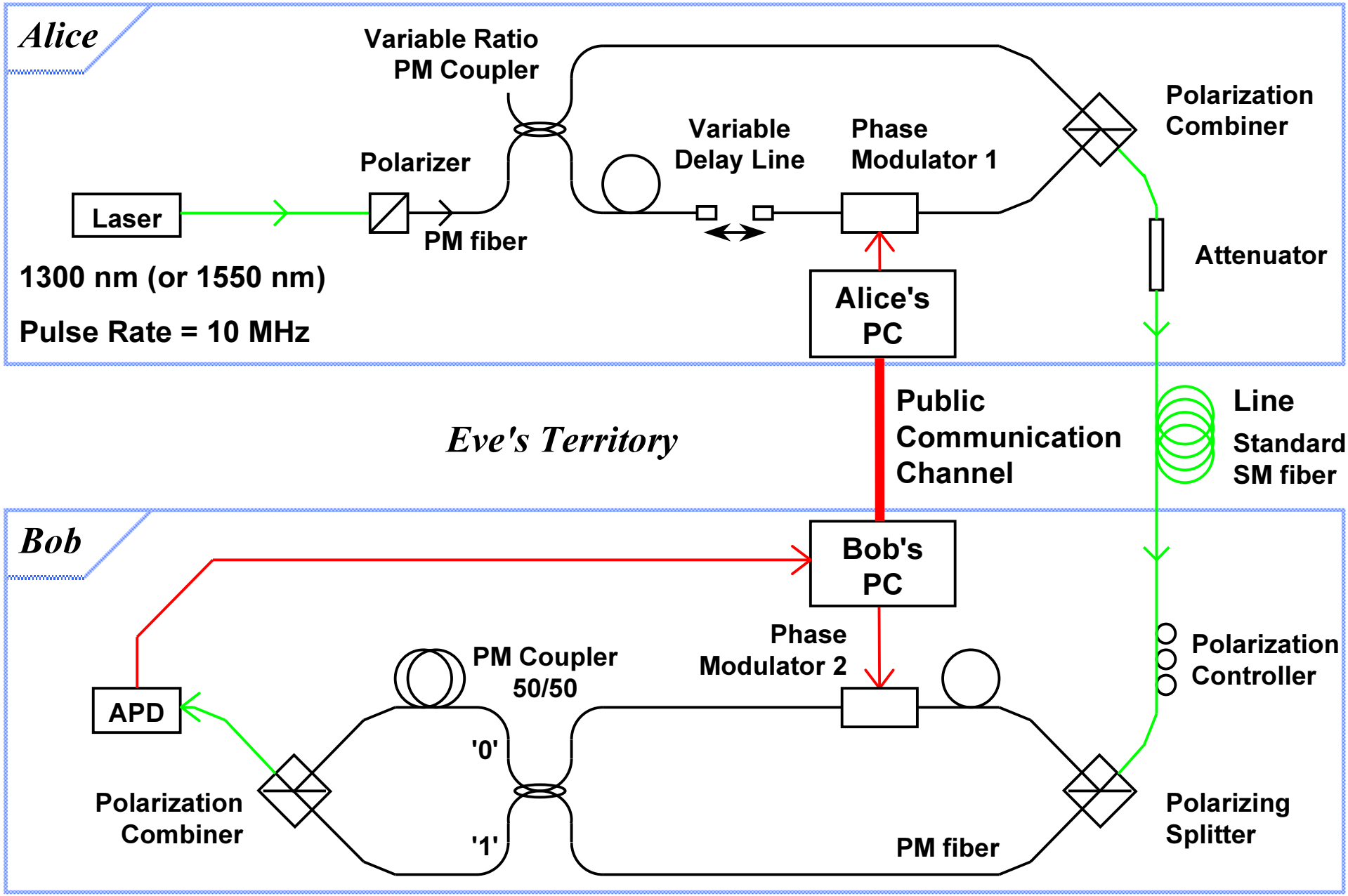
$\phi_1 =$ 180° or 270° - "0"

Reference systems:

$\phi_2 =$ 0°

$\phi_2 =$ 90°

Implementation: interferometer structure



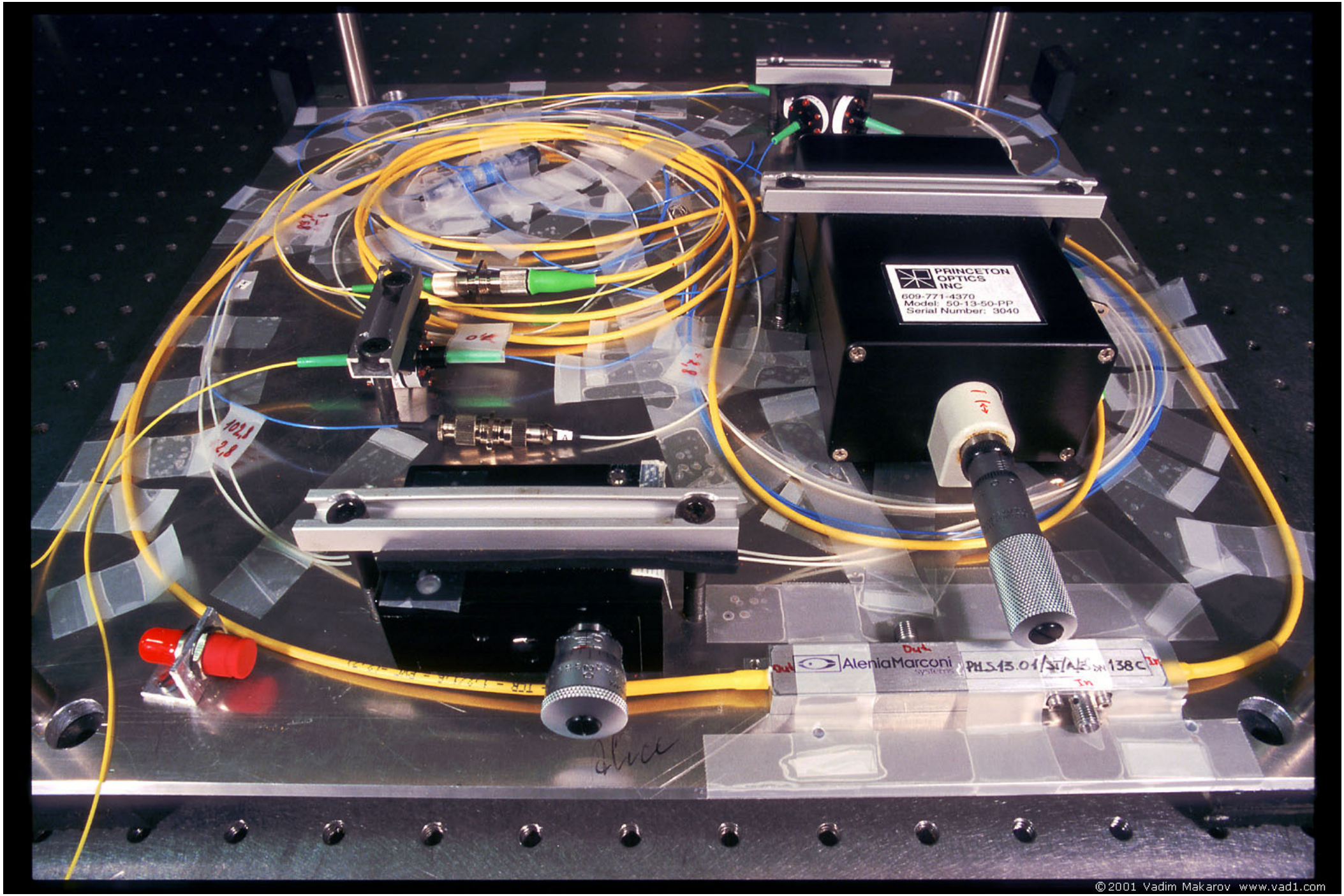


Photo 1. **Alice** (uncovered, no thermoisolation installed)

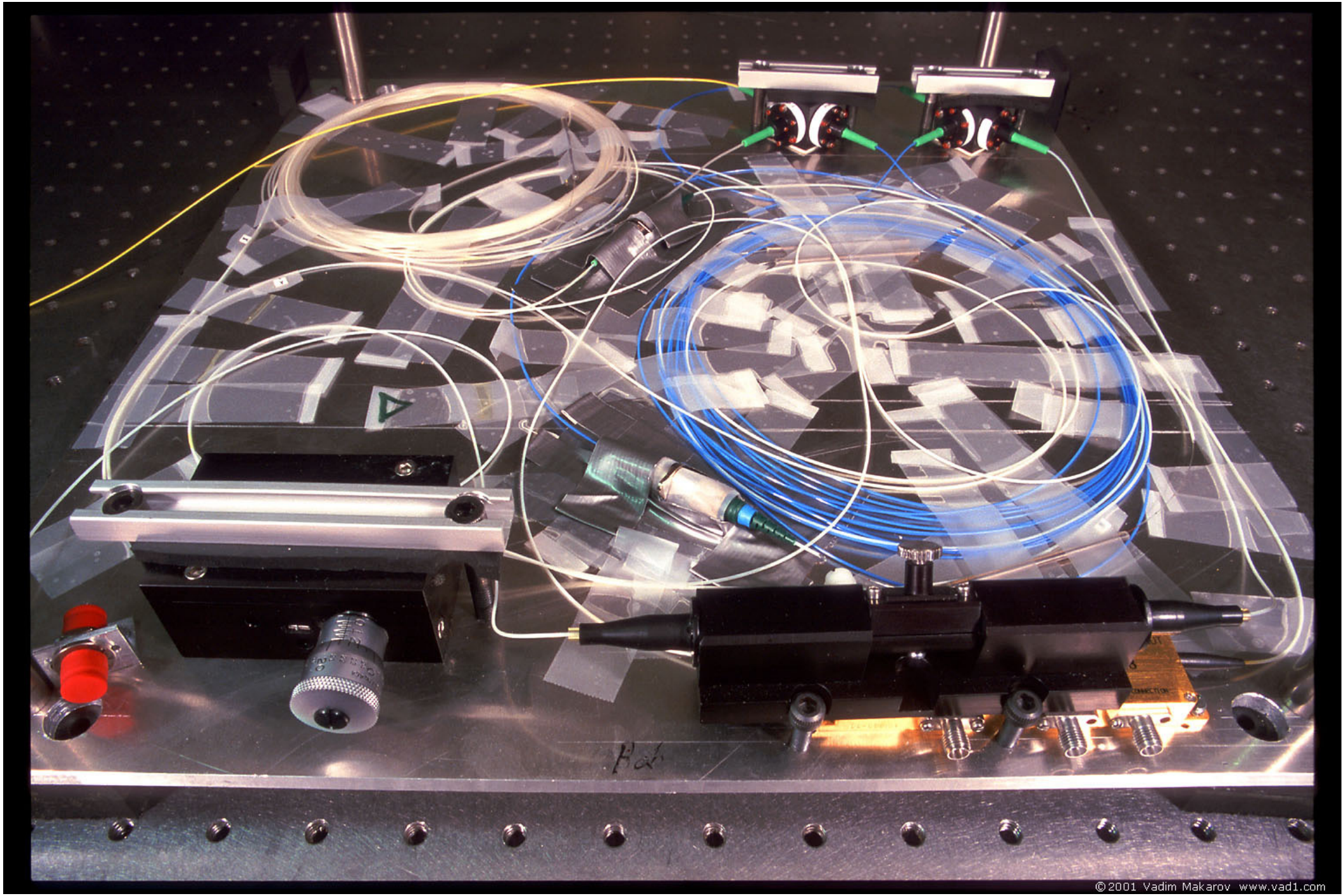
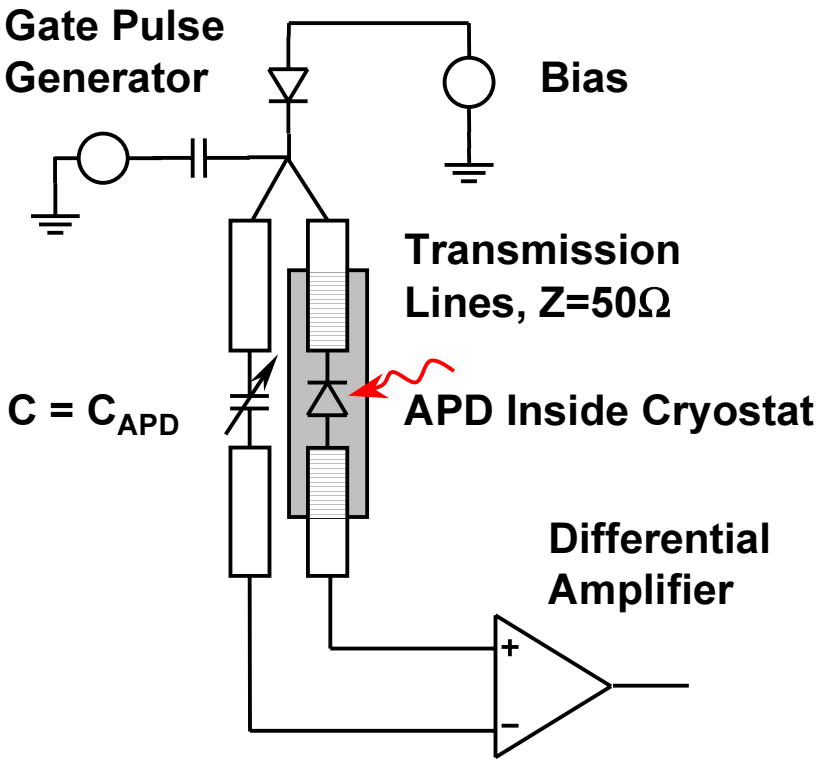
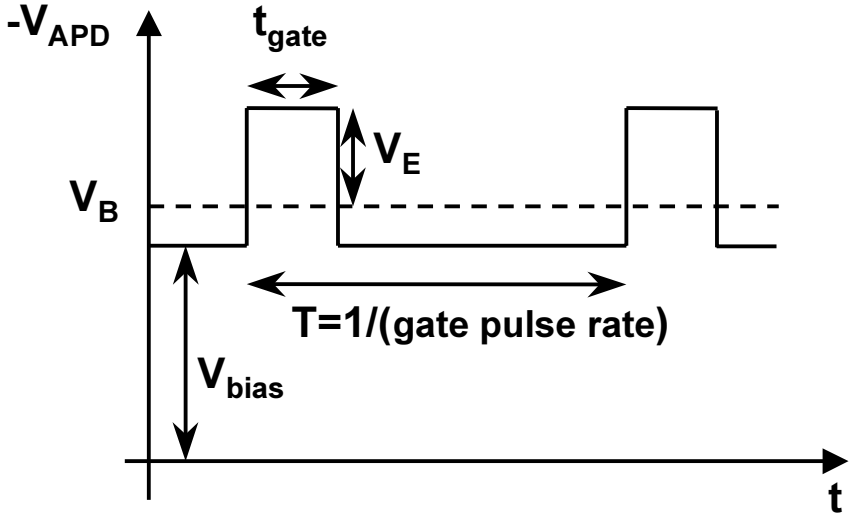


Photo 2. **Bob** (uncovered, no thermoisolation installed)

Single-photon detector: APD in Geiger mode

NTNU



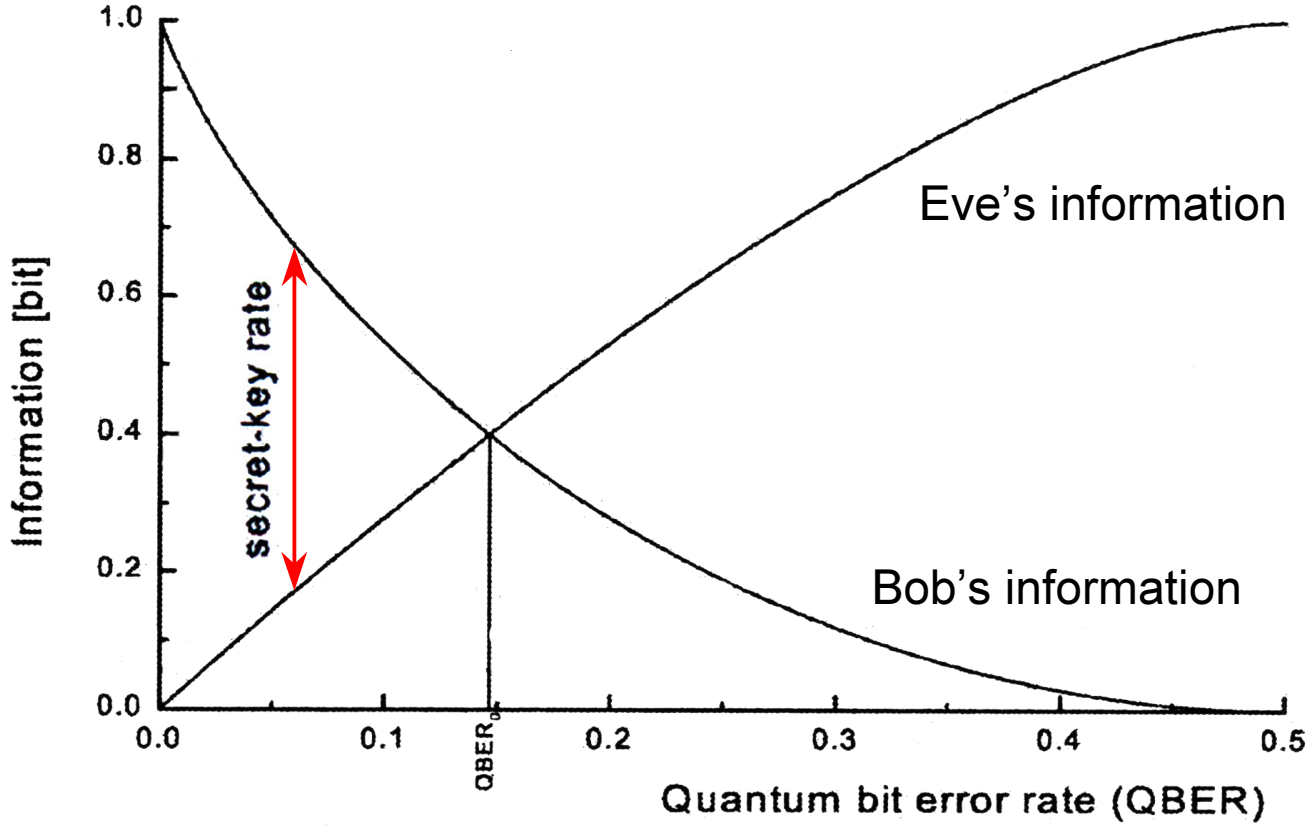


t_{gate} down to 1ns

gate pulse rate = 20 MHz

Recovery from errors

NTNU

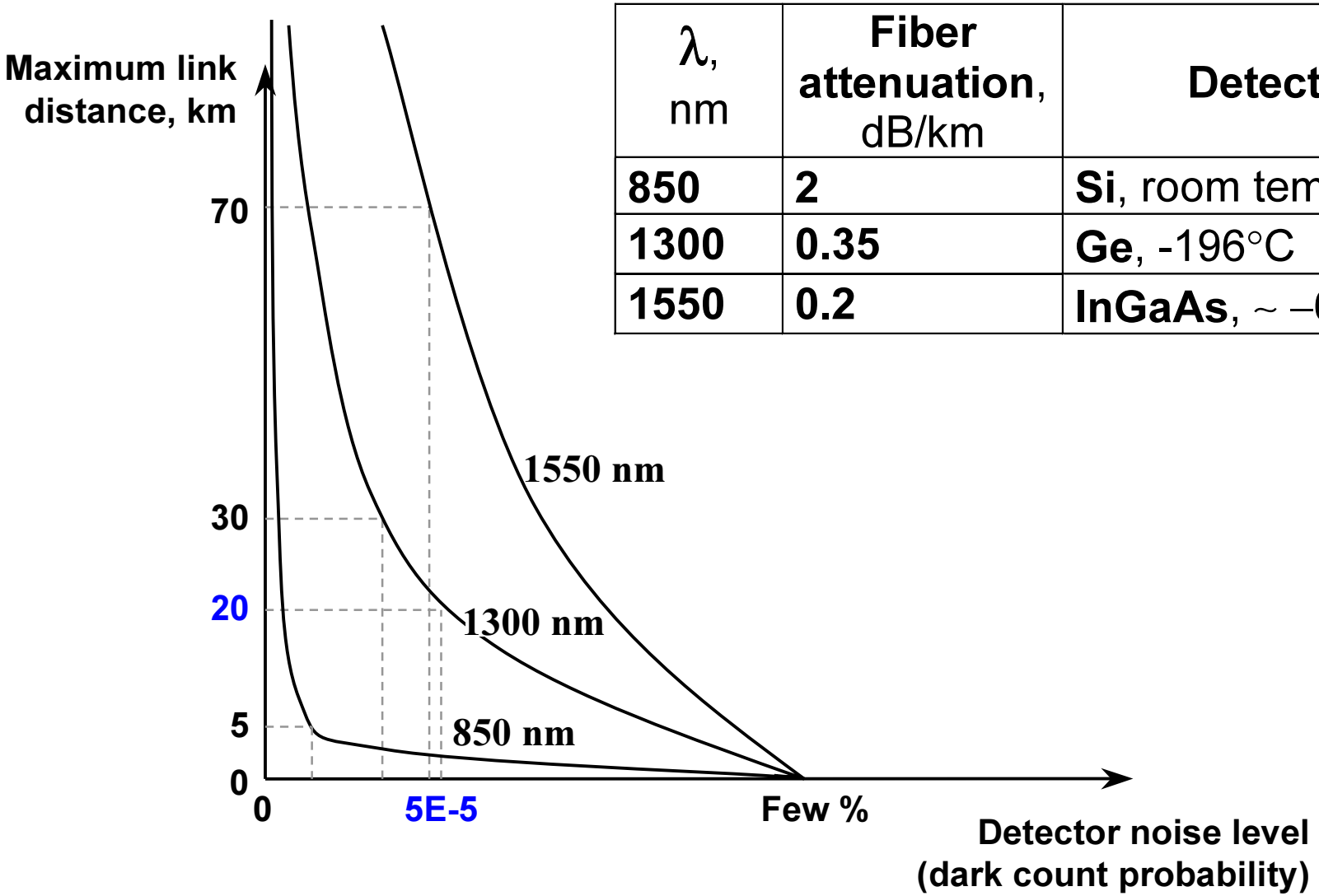


QBER limit:

- **Individual attacks: 15%**
- **All theoretically possible attacks: 11%**

Distance limitation

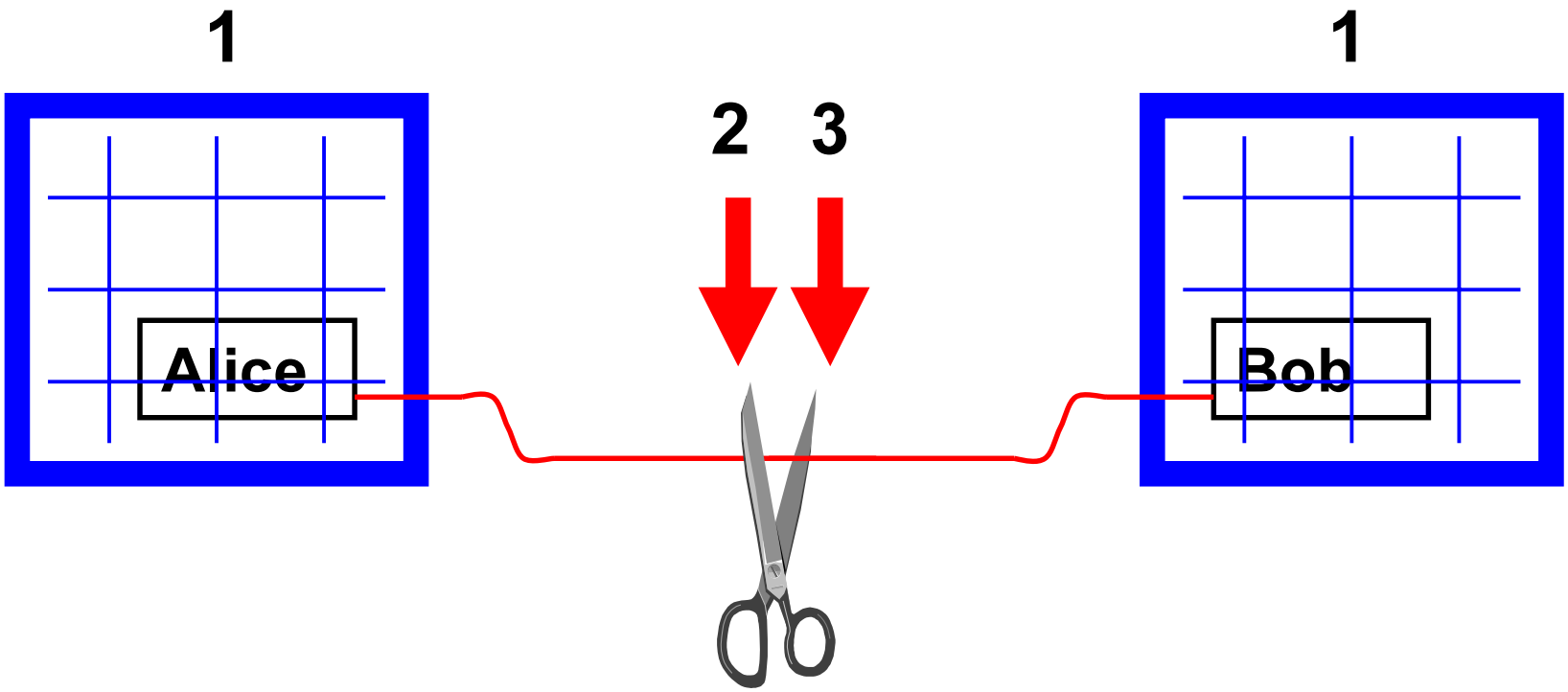
NTNU



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

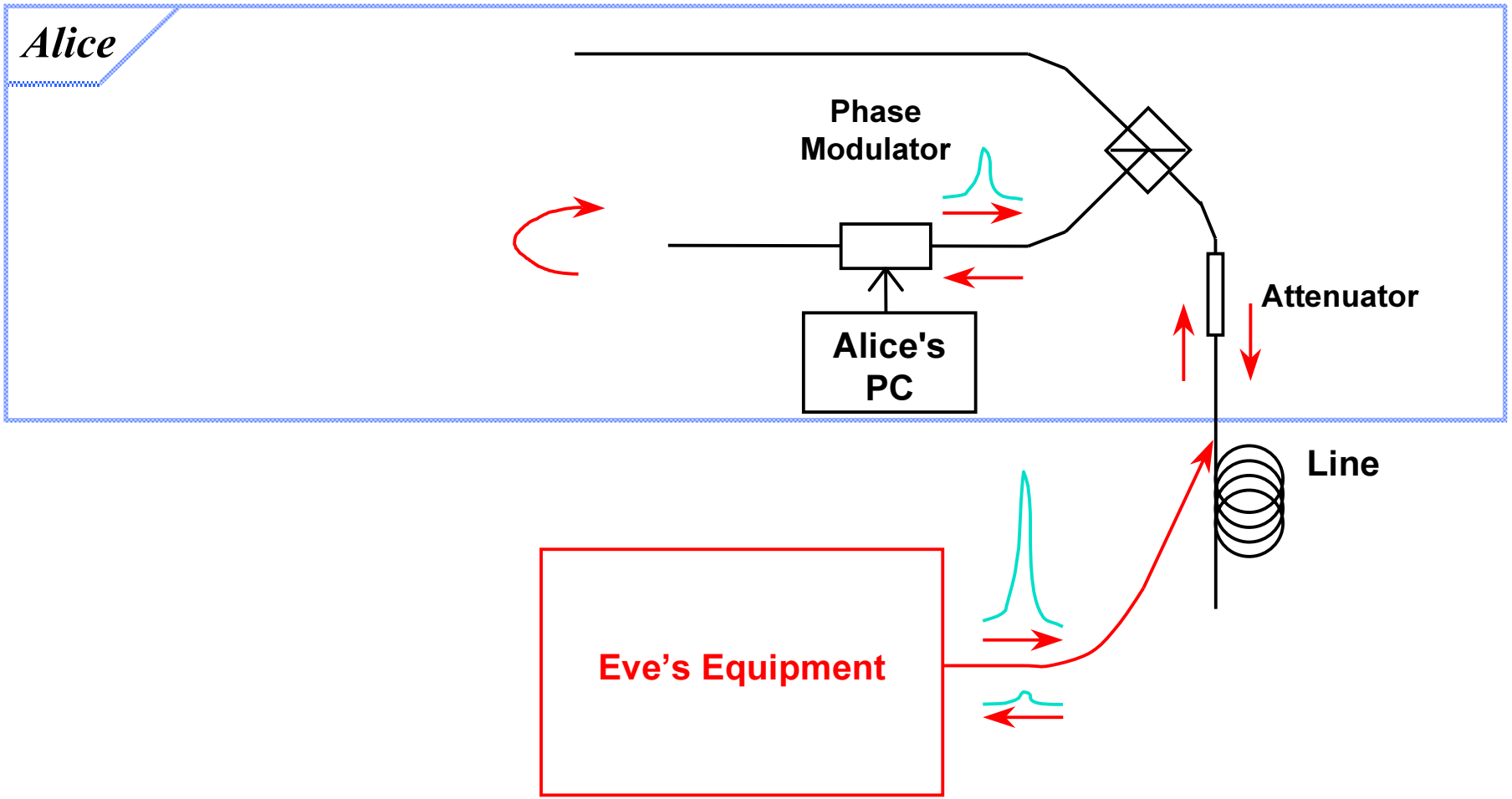


1. **Conventional security**
2. **Security against quantum attacks**
3. **Security against Trojan horse attacks**

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

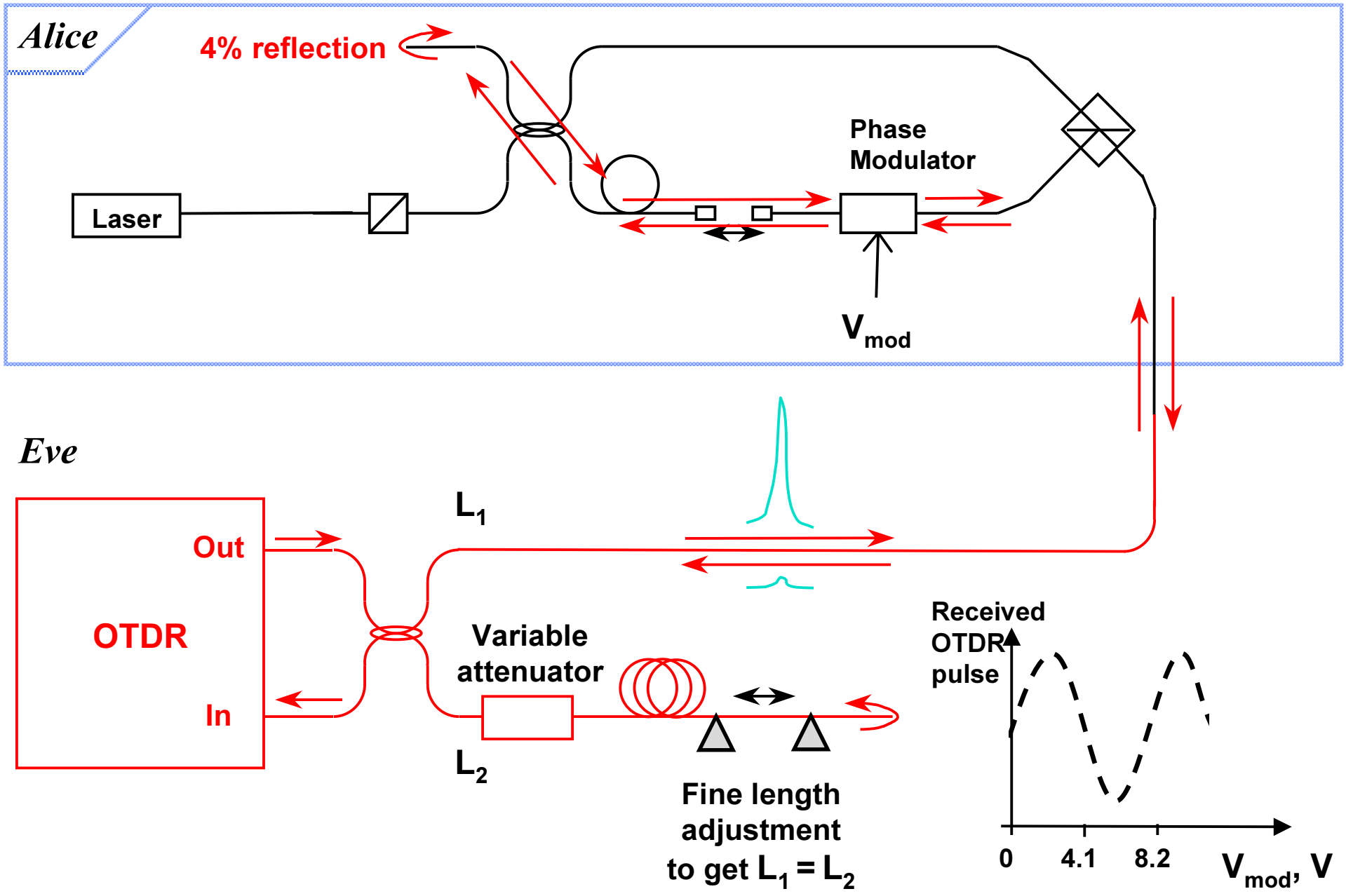
Practical security: large pulse attack

NTNU



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

Eavesdropping experiment



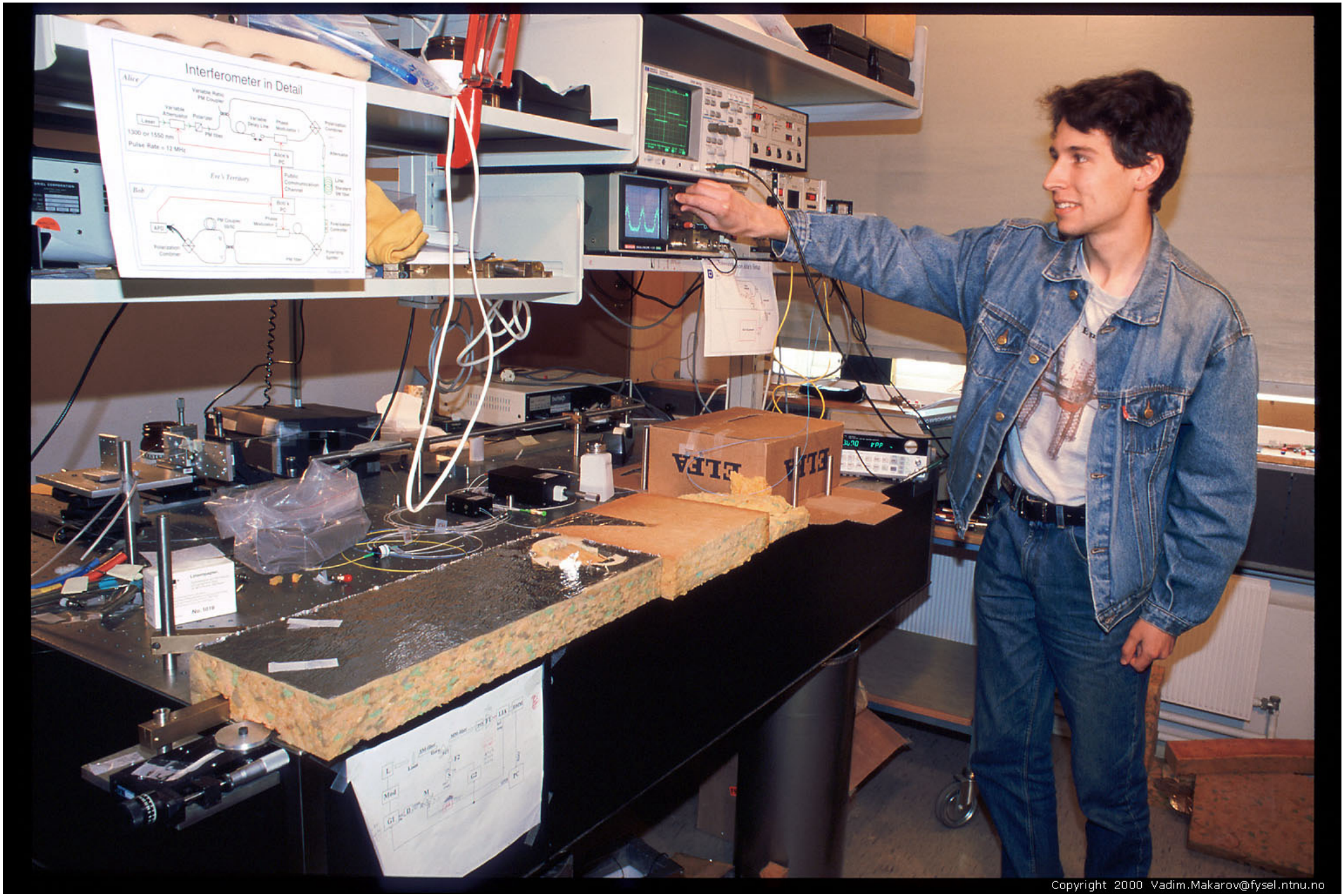
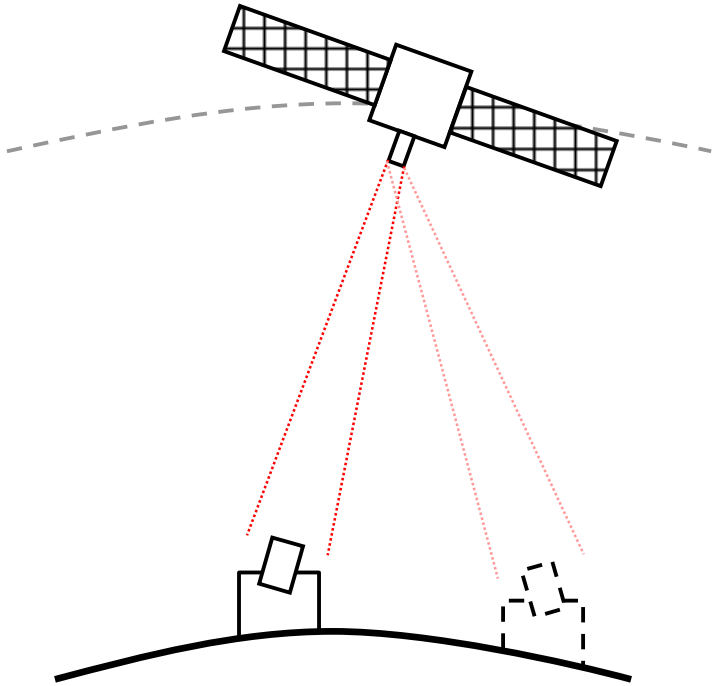
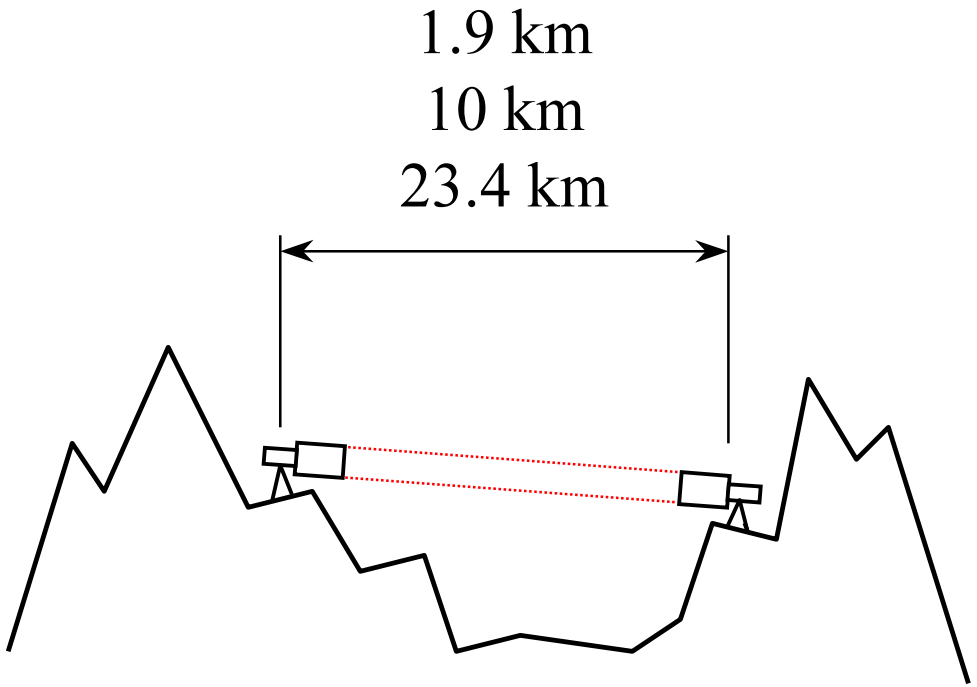


Photo 3. Artem Vakhitov tunes up Eve's setup

Re-keying satellites/ Global key distribution network

NTNU

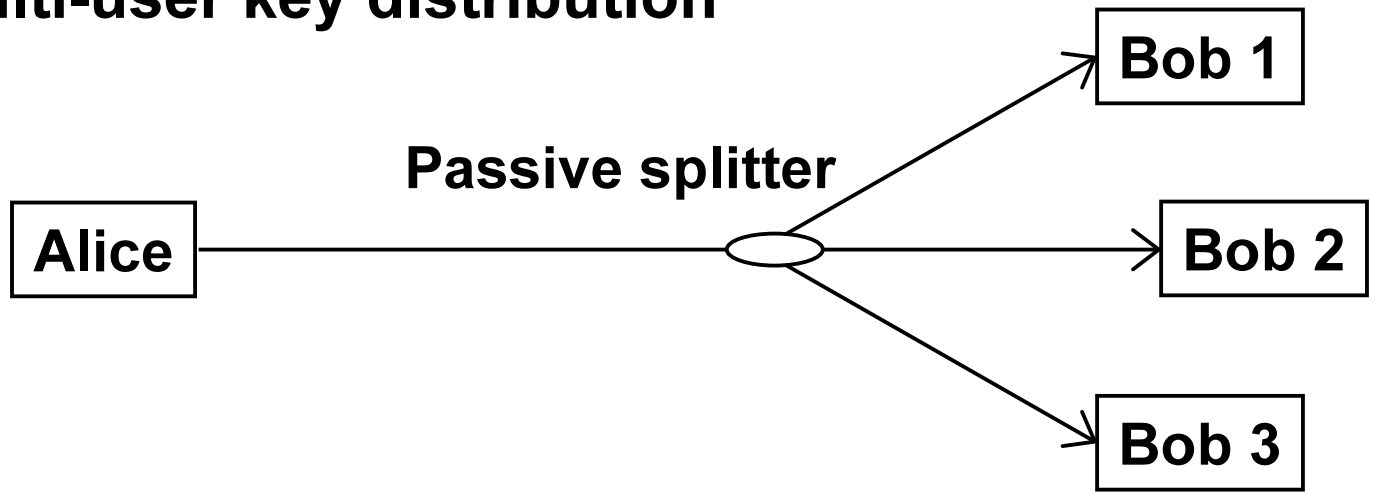




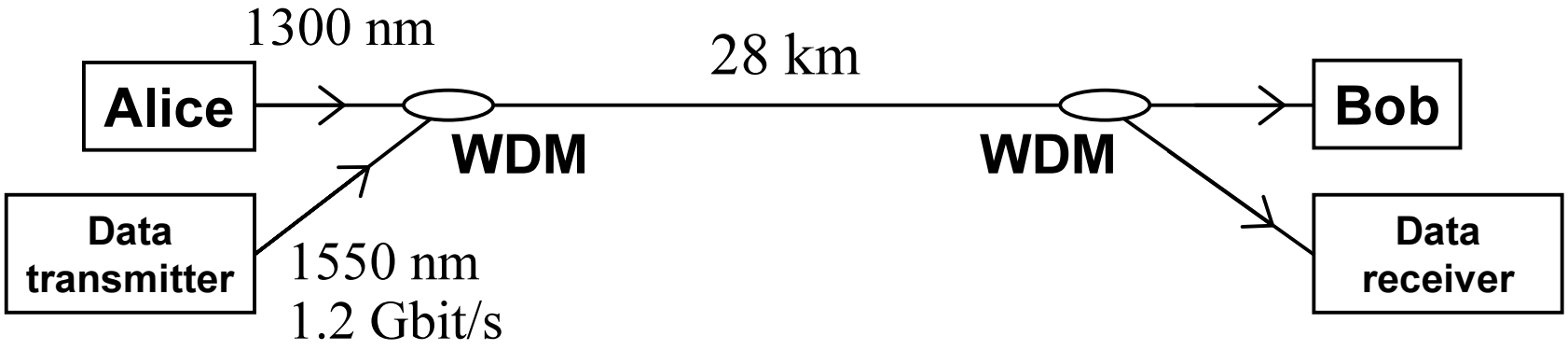
Quantum key distribution in network

NTNU

- **Multi-user key distribution**

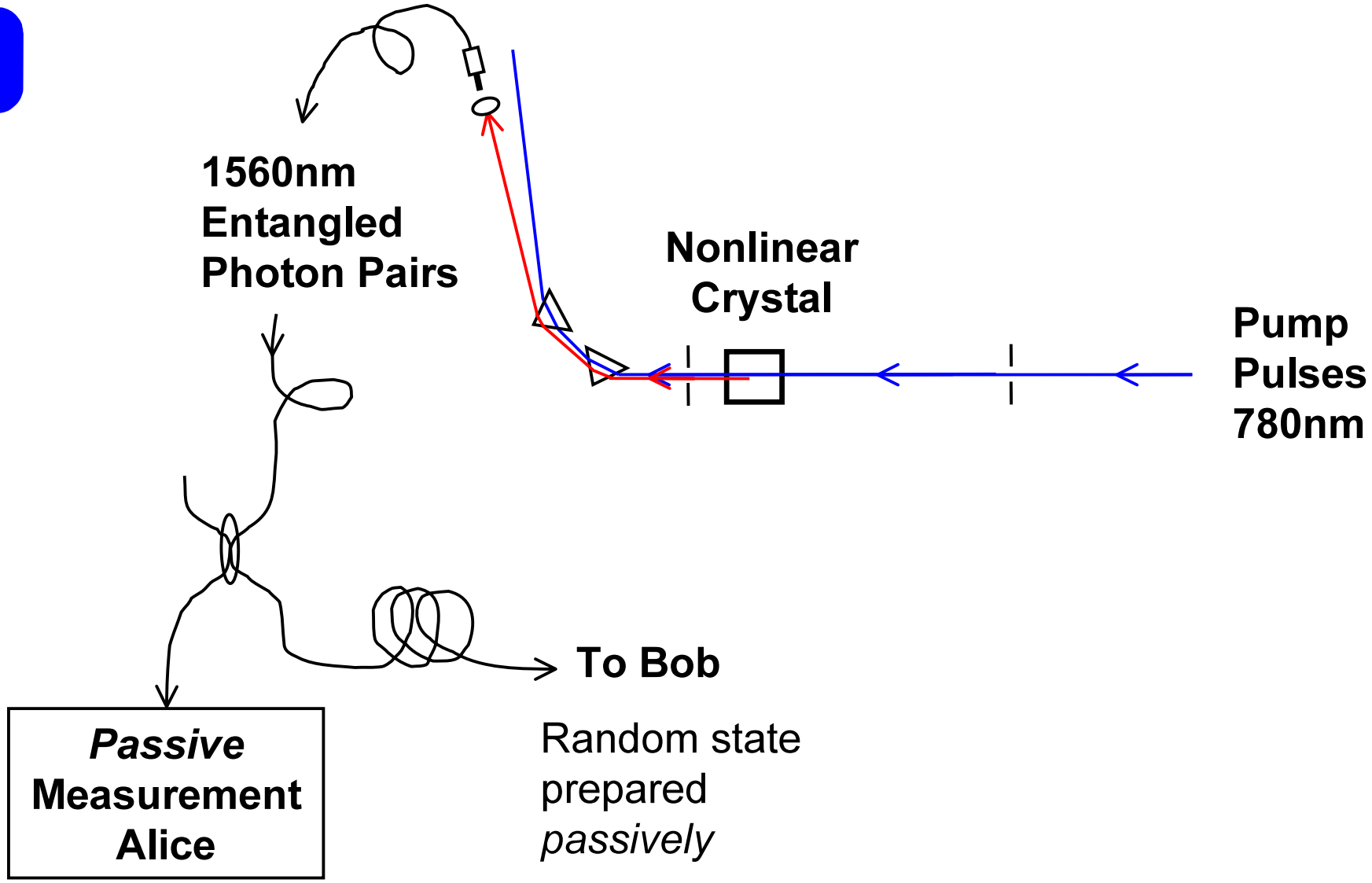


- **Multiplexing with telecom traffic**



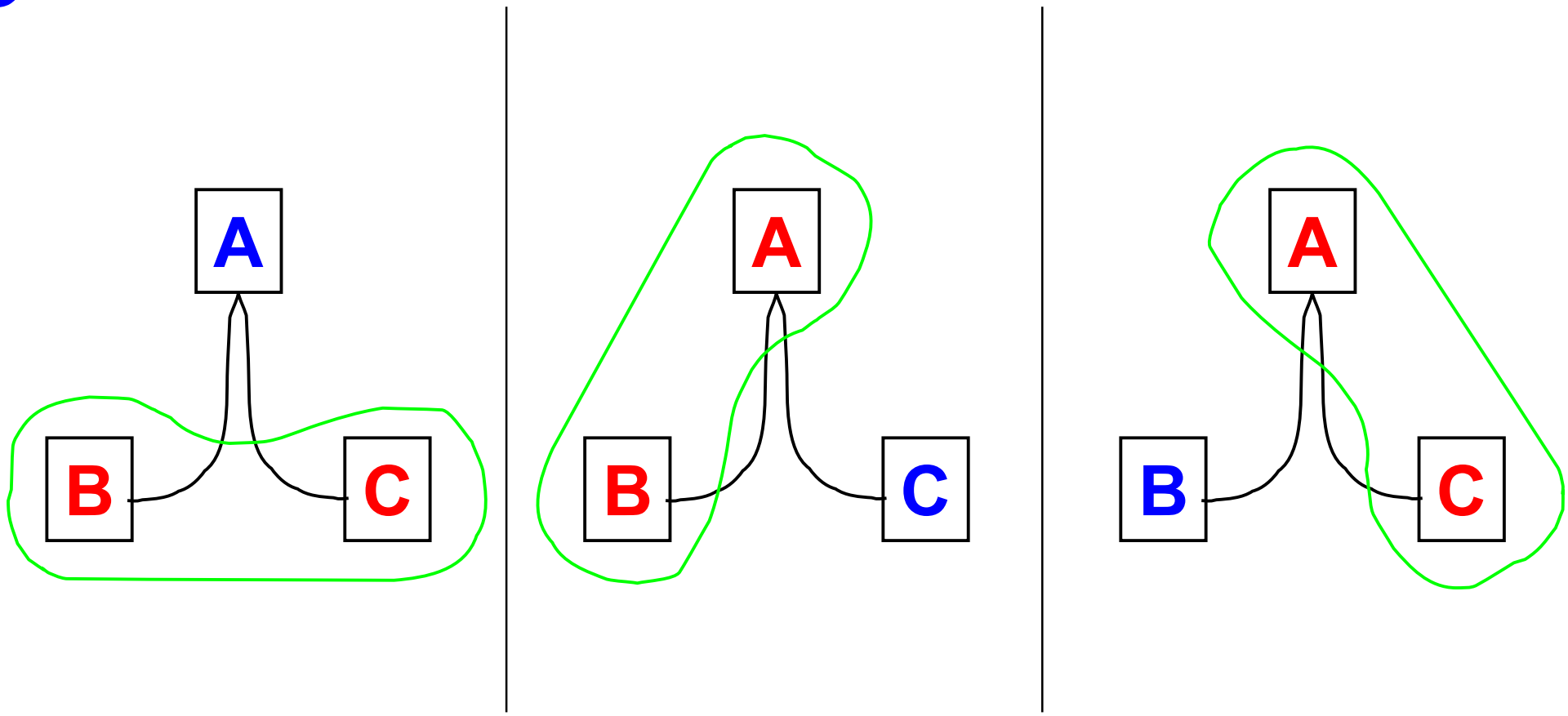
Entangled photon pairs

NTNU



Advanced multi-party protocols: Secret sharing and splitting

NTNU

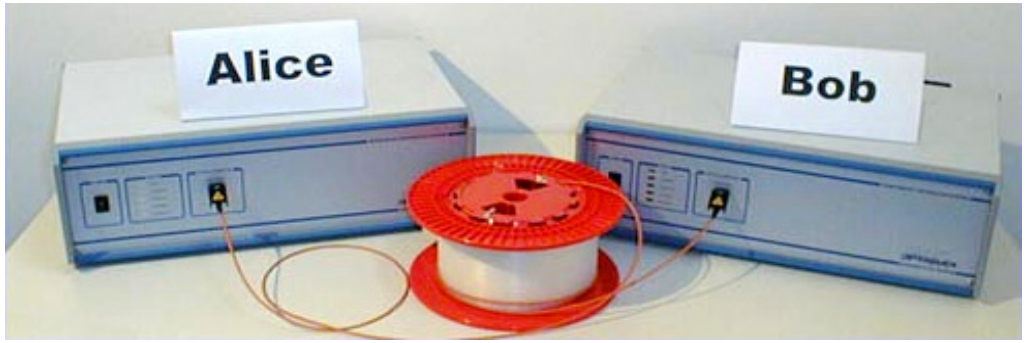


Commercial status

NTNU

- **id Quantique (Geneva)**

  first commercially available quantum key distribution system:



- **MagiQ Technologies (Boston)**
- **EQUIS project (Heriot-Watt University and Corning; UK)**

  compact integration into standard PCs
- **+ several research groups, telecom/ electronics companies**