Differential Phase Shift Quantum Key Distribution

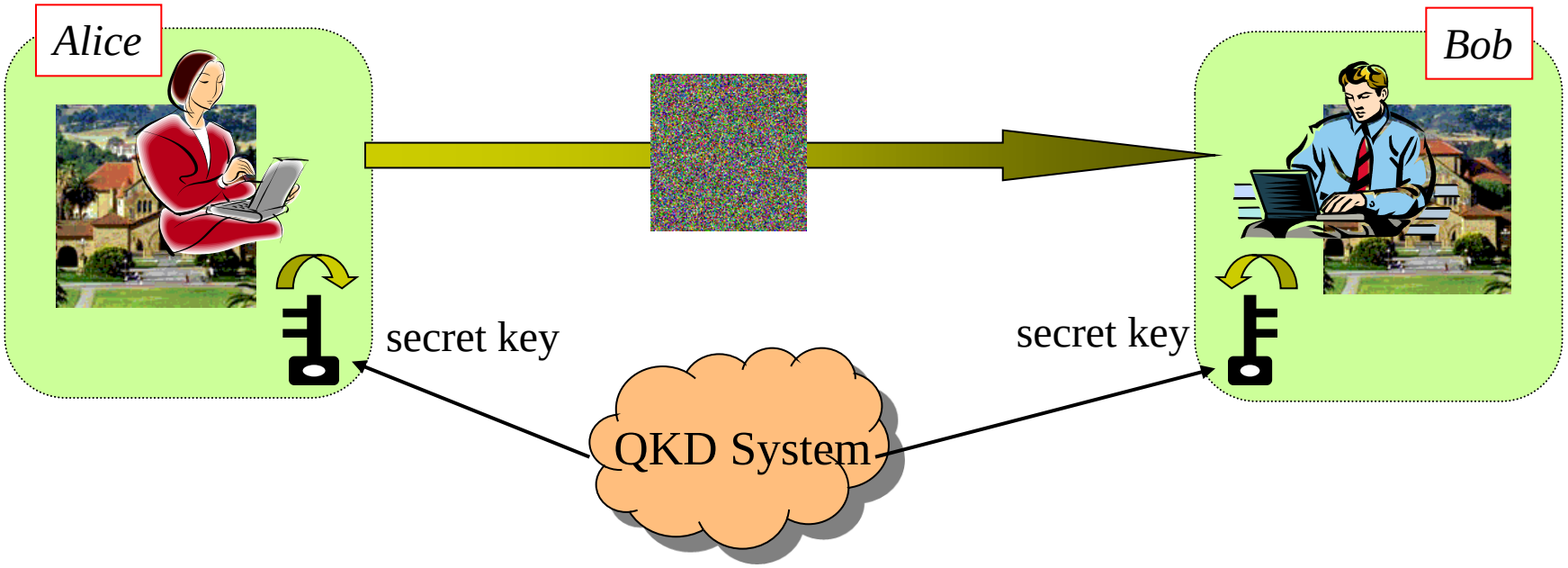
Kyo Inoue

Osaka University

Quantum Key Distribution (QKD)

- QKD provides a secret key for cryptography to legitimate parties.

- The security of the key is guaranteed by quantum mechanics.

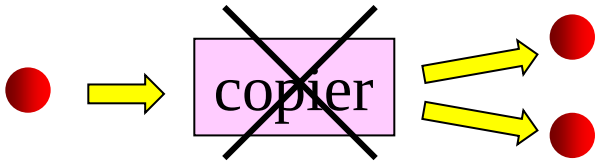


traditional

Quantum mechanics utilized in QKD

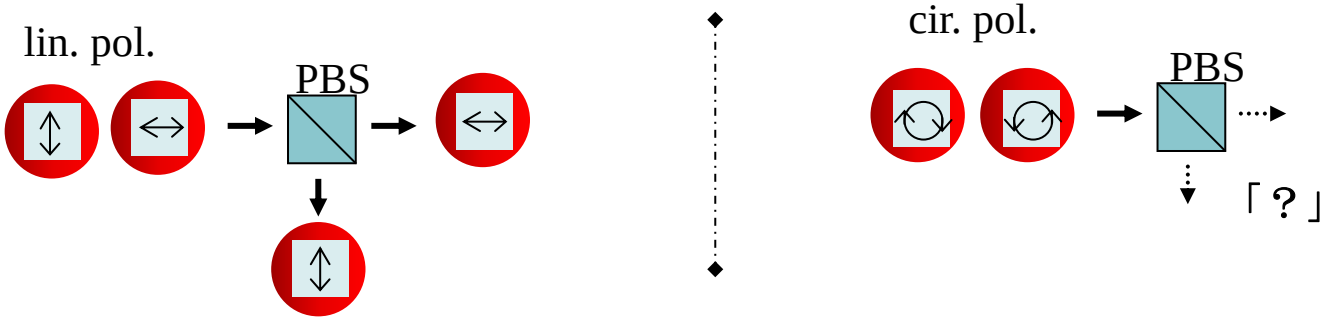
Non-cloning theory:

A quantum state cannot be perfectly copied without changed.



Uncertainty principle:

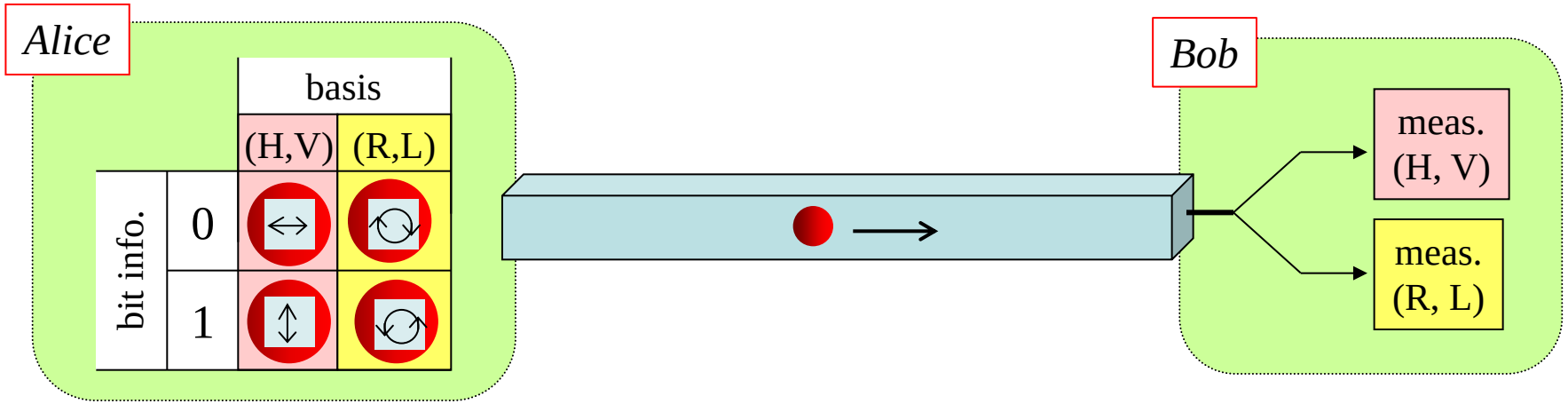
Two nonorthogonal physical quantity cannot be precisely measured at the same time.



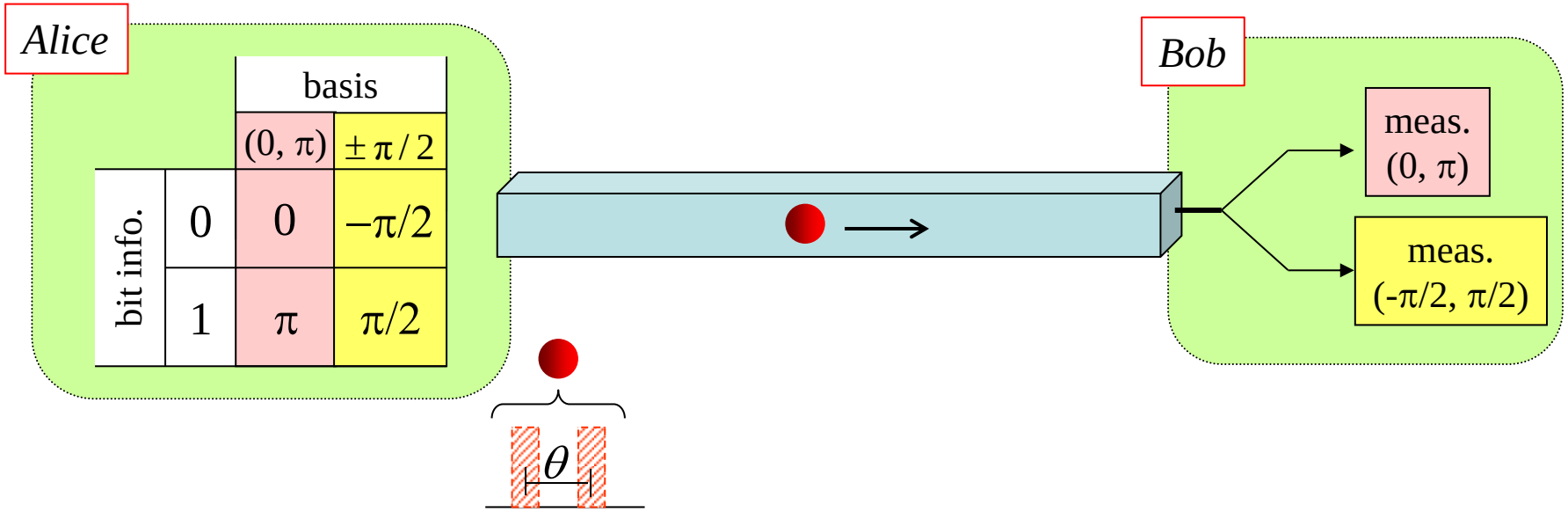
traditional

BB84 protocol

Polarization coding scheme



Phase coding scheme



this presentation

Differential phase shift (DPS) QKD

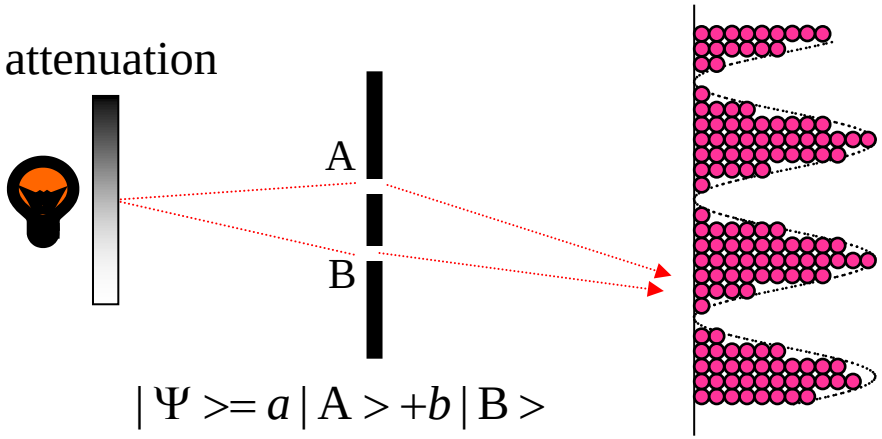
- A unique QKD protocol different from BB84 -

featuring simplicity, practicality, high efficiency, , , .

Contents

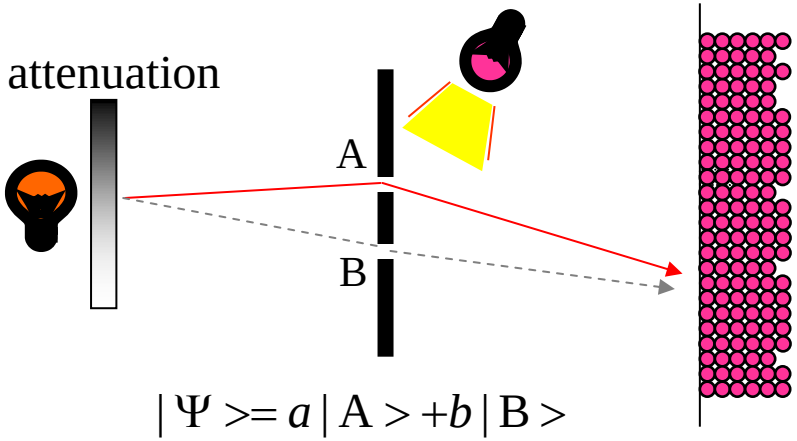
physics utilized in DPS-QKD

Wave & particle properties of light



$|\Psi\rangle = a|A\rangle + b|B\rangle$

(observing which slit)

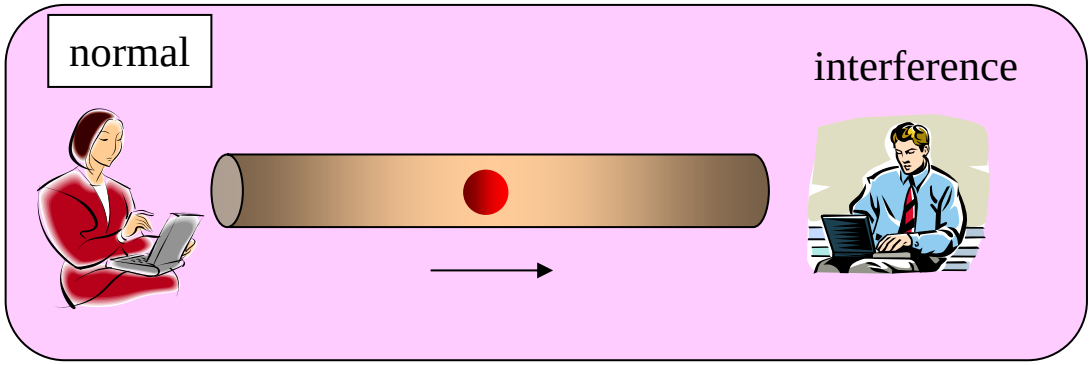


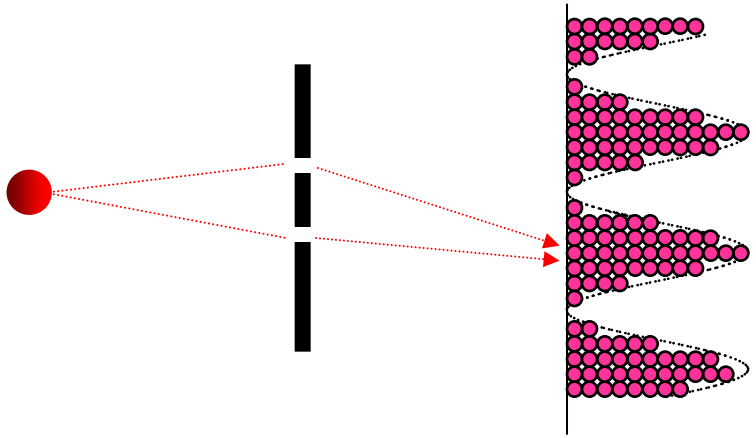
$|\Psi\rangle = a|A\rangle + b|B\rangle$

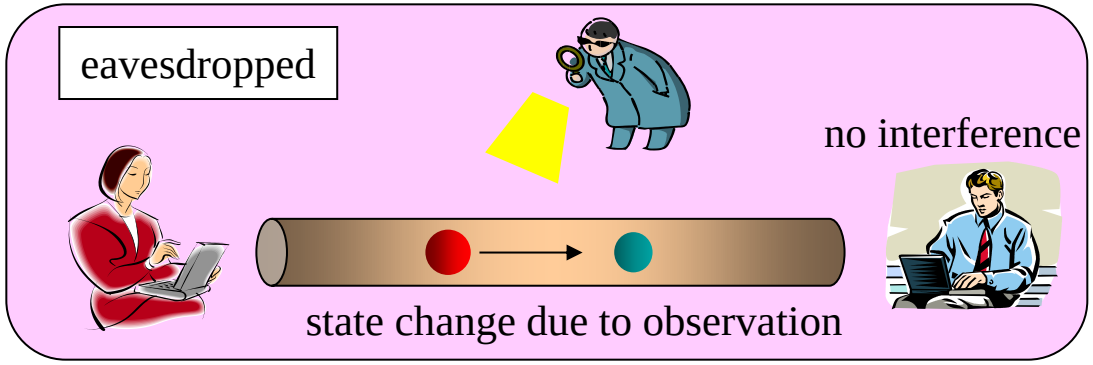
observation

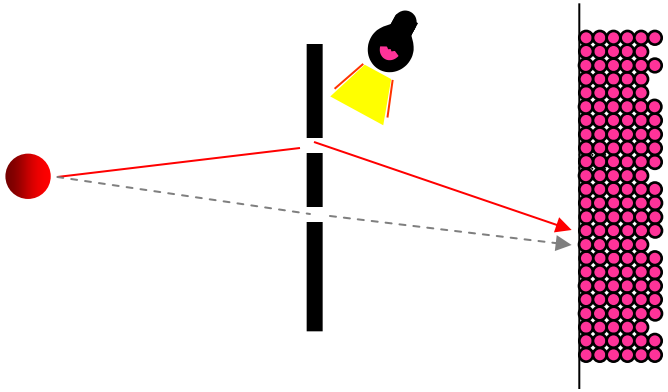
$|\Psi\rangle = |A\rangle$ or $|\Psi\rangle = |B\rangle$

QKD based on particle & wave properties



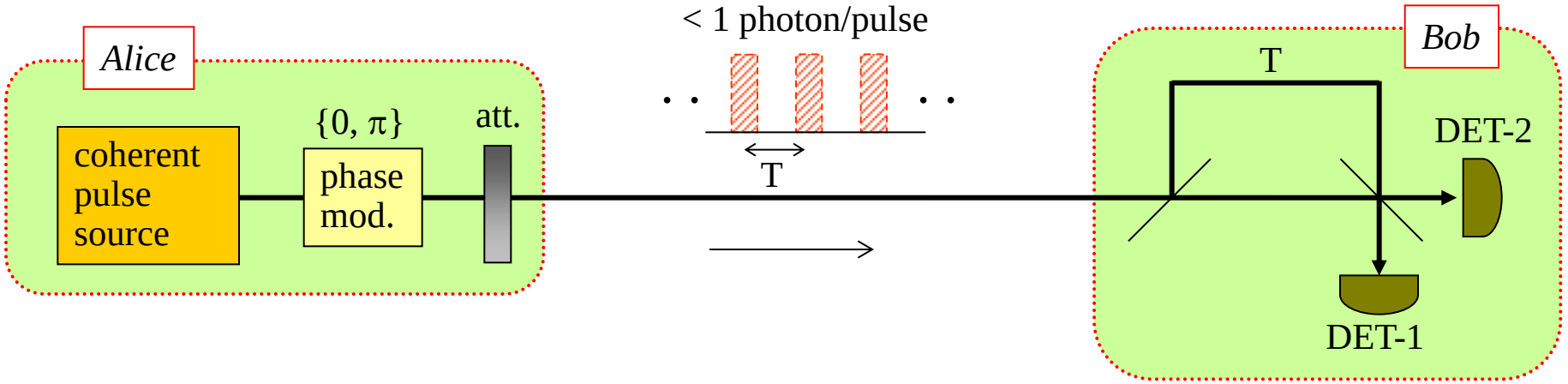




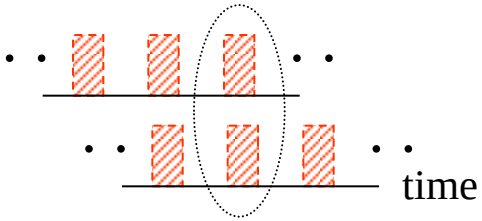


Eavesdropping is revealed from no or incorrect interference.

Setup



A photon is detected occasionally and randomly in time.



$\Delta\theta = 0 \longrightarrow$ DET-1

$\Delta\theta = \pi \longrightarrow$ DET-2

Protocol

(1) Signal transmission

(2) Bob → Alice: photon detection time

(3) Alice knows which detector clicked at Bob.

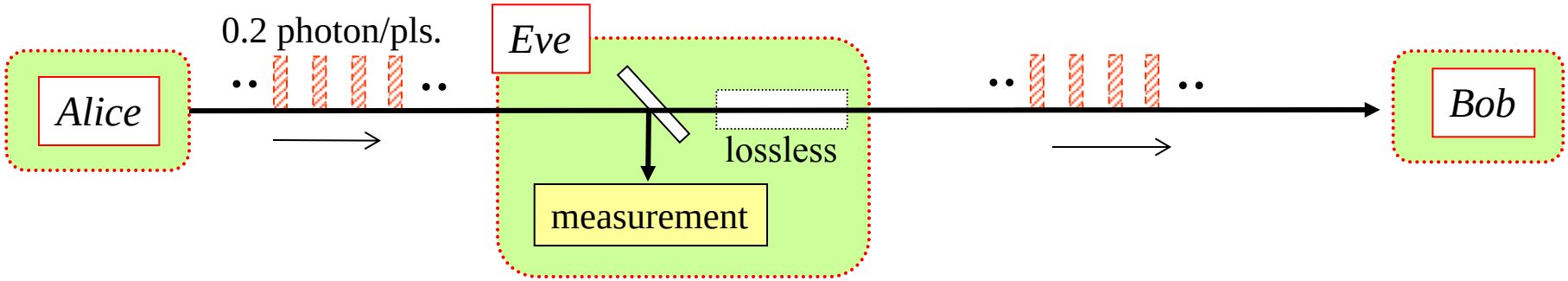
(4) Key bits are created according to

DET-1 = "0" DET-2 = "1"

security

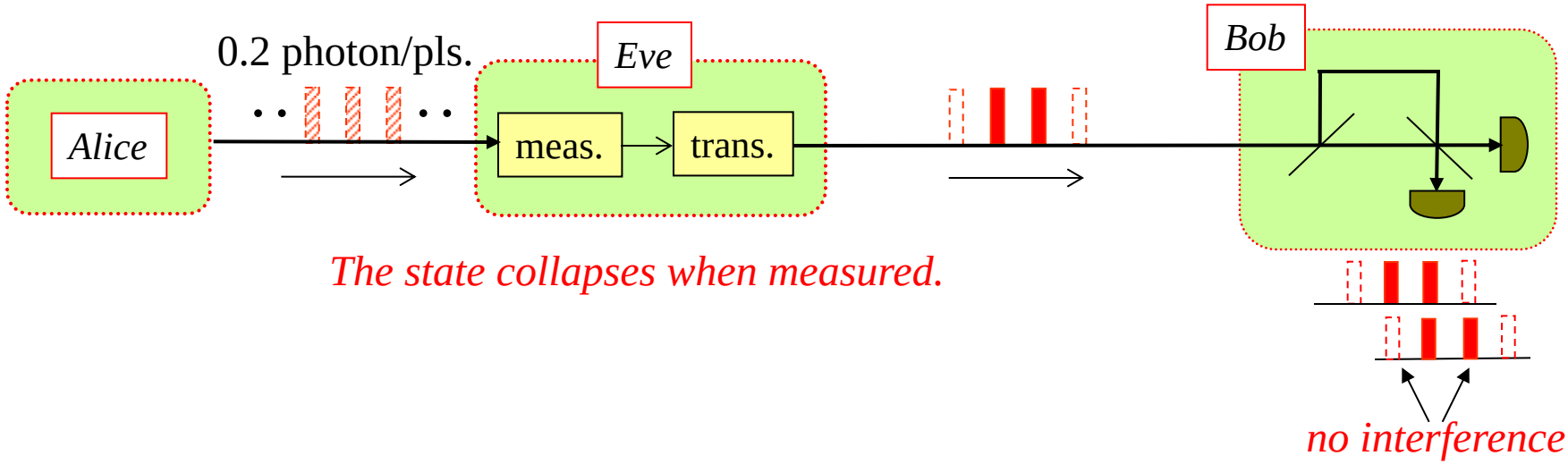
Eavesdropping

Beam splitting attack



Eve cannot fully measure the phase differences.

Intercept-resend attack

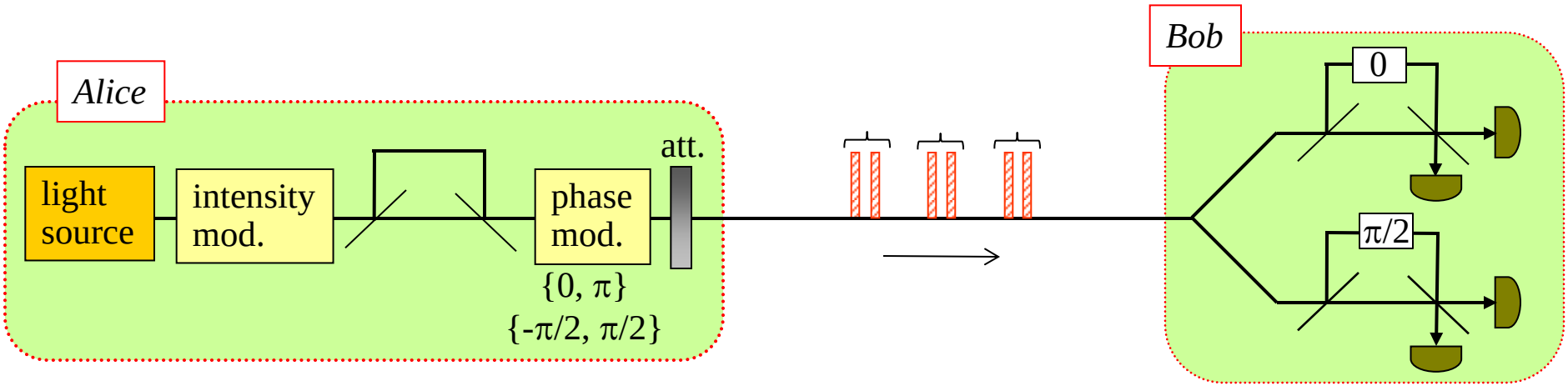


The state collapses when measured.

Features

- Simple configuration
- Efficient usage of the time domain
- No photon discarded
- Robustness against photon number splitting attack

(ref.) Phase encoding BB84 using a laser

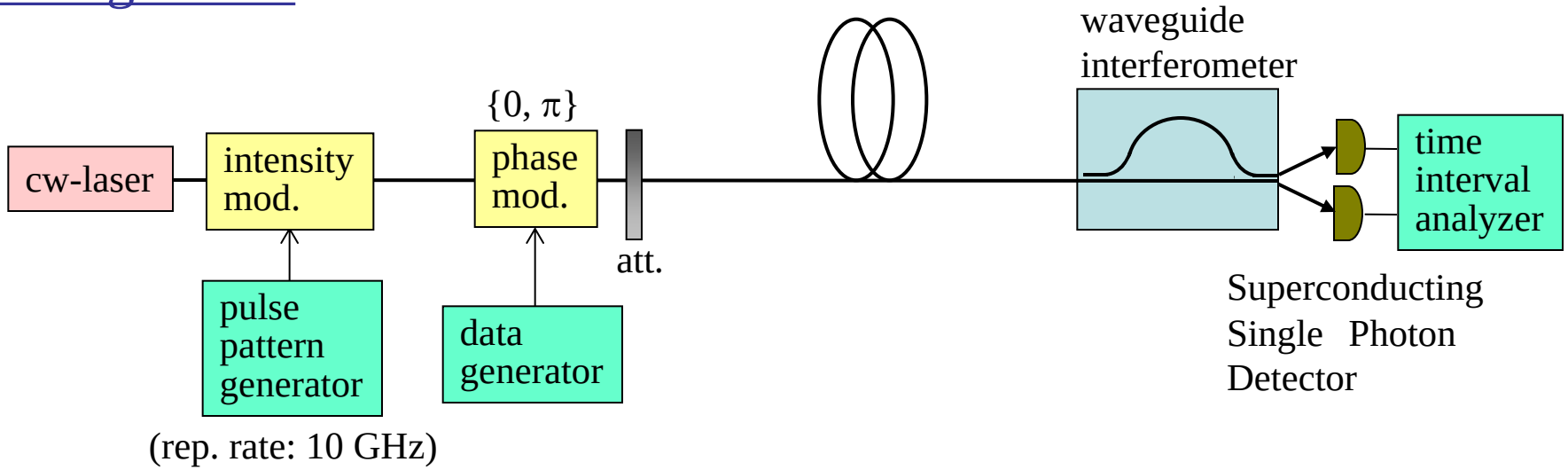


Experimental effort

Long distance experiment

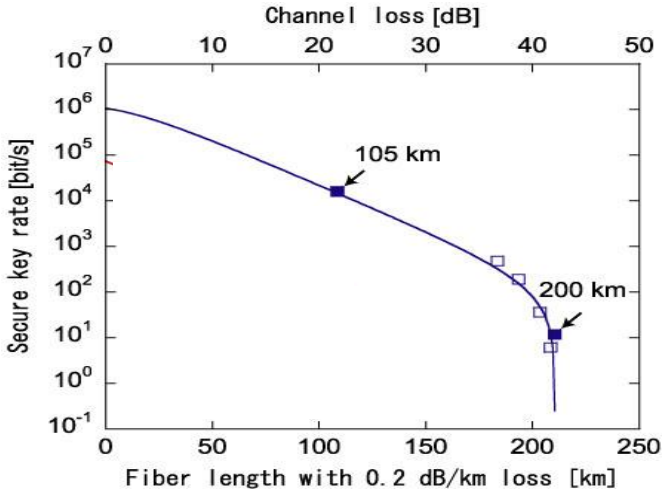
[Takesue et al., *Nat. Photon.*, **1**, 343 (2007)]

Configuration



(rep. rate: 10 GHz)

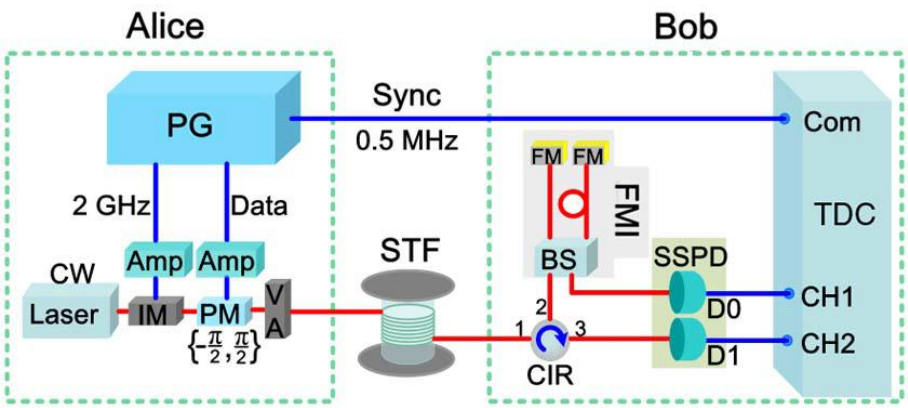
Result

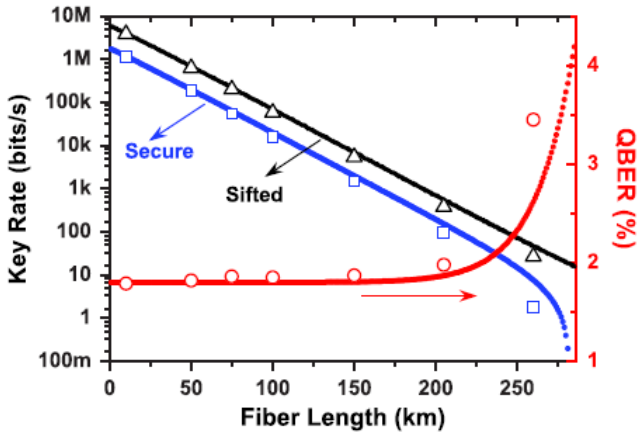


17 kbit/s over 100 km.
12 bit/s over 200 km.

Other experiments

performance	detector	year	organization	note
0.33Mbps@15km	APD	2007	NTT/Nihon U.	
1.3Mbps@10km	up-conv.	2009	NTT/Stanford U.	
24kbps@100km	APD	2011	NTT/Nihon U.	
2.1kbps@90km	SSPD	2011	NTT/NICT	field experiment (Tokyo QKD-NW)
1.85bps@260km	SSPD	2012	U. Sic. Tech. China	

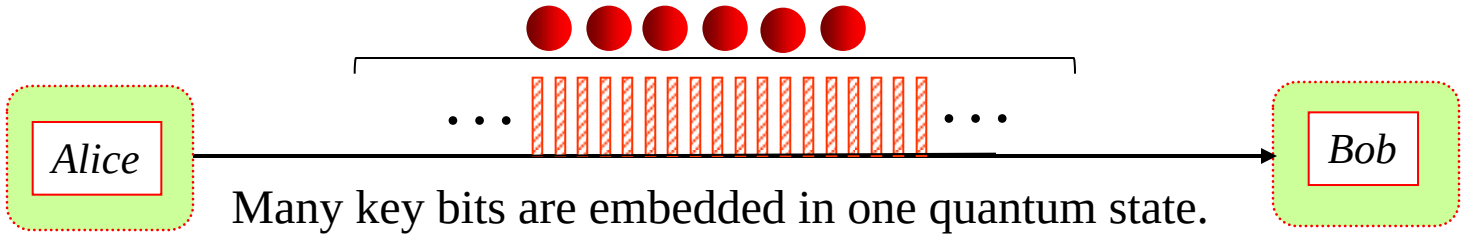




Security issue

Security analysis is challenging for DPS-QKD.

DPS

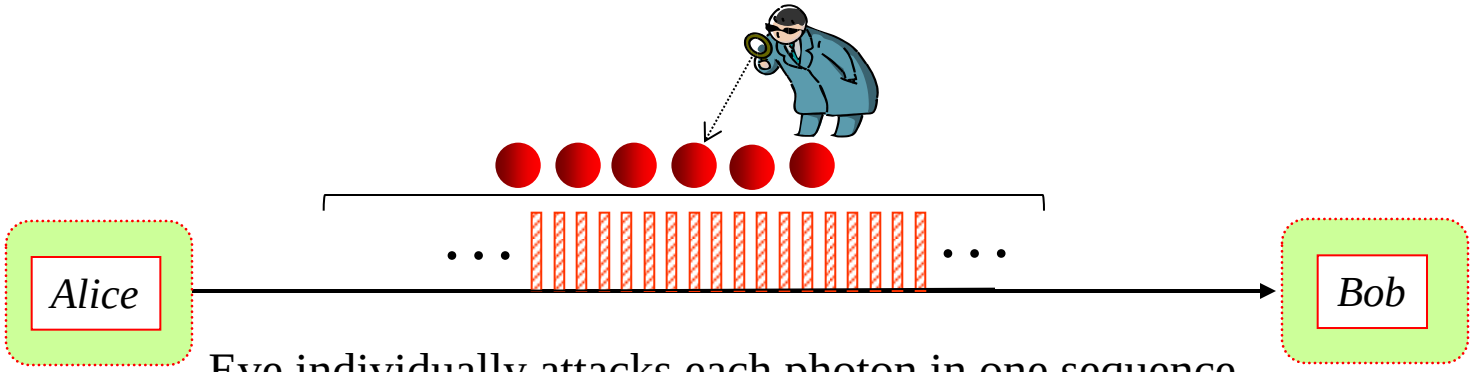


Many key bits are embedded in one quantum state.
(one coherent sequence)

BB84

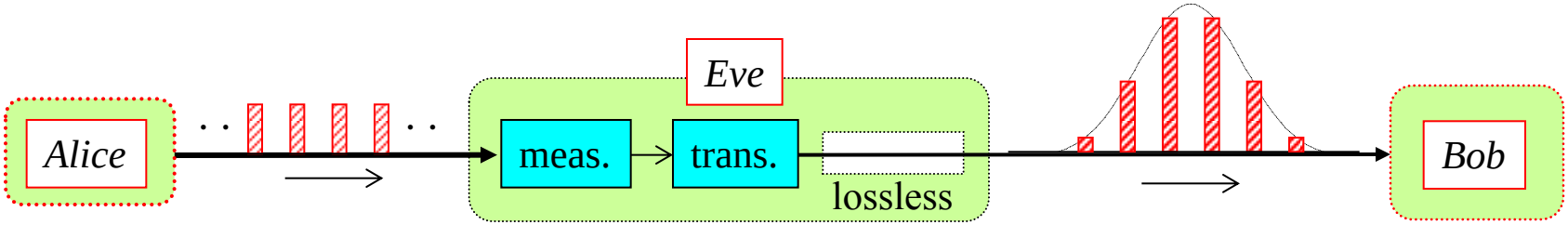
One key bit is carried by one quantum state.

- General individual attack was analyzed (2006).



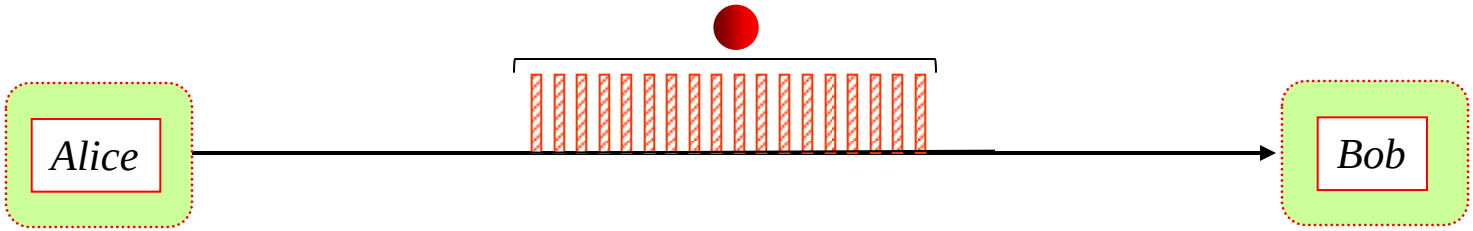
Eve individually attacks each photon in one sequence.

- Sequential attack was proposed (2007).



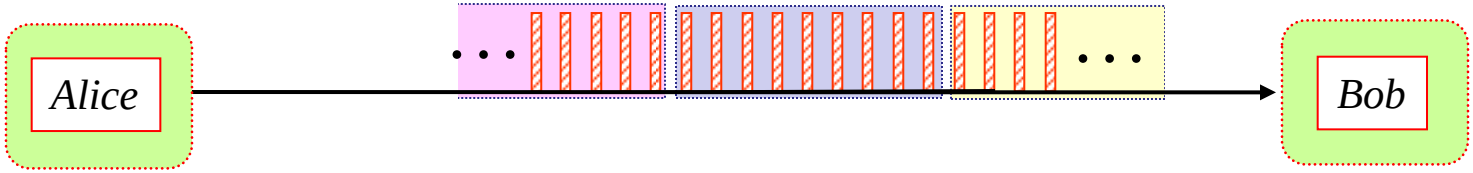
Eve resends a signal when conclusive results are sequentially obtained.

- Unconditional security was proved for single-photon DPS (2009).



One photon is super-positioned over a number of pulses.

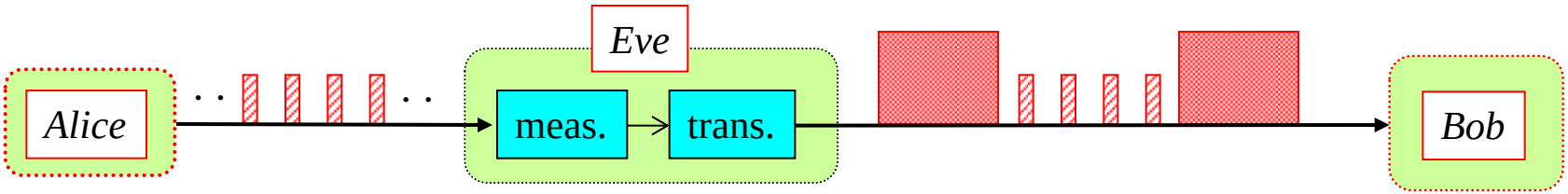
- Unconditional security is discussed for block-wise DPS (2012-).



A pulse sequence is assumed to be composed of individual uncorrelated blocks.

Security issue in practical system

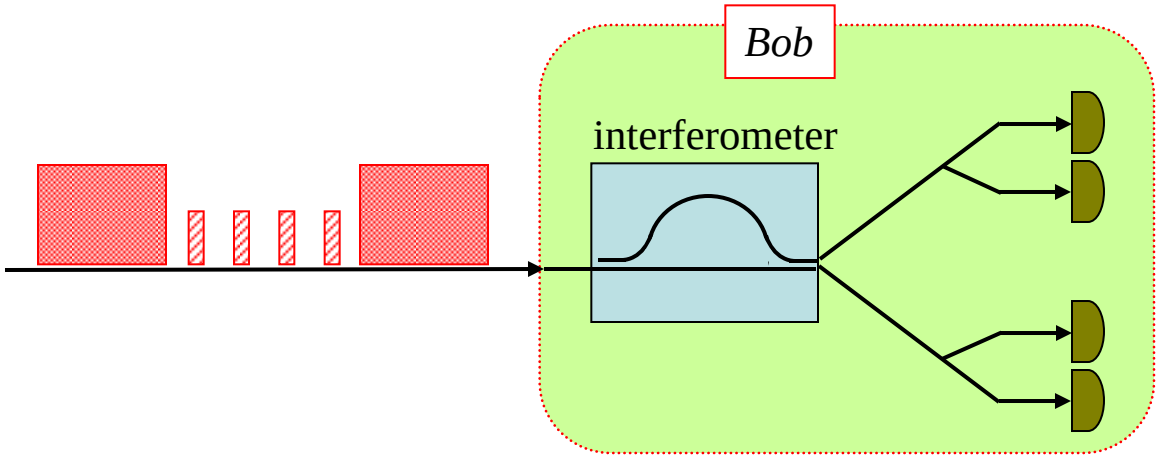
- Bright illumination attack was proposed (2011).



Eve manipulates Bob's detectors by sending bright light.

threshold detection

A counter measure was proposed (2013).



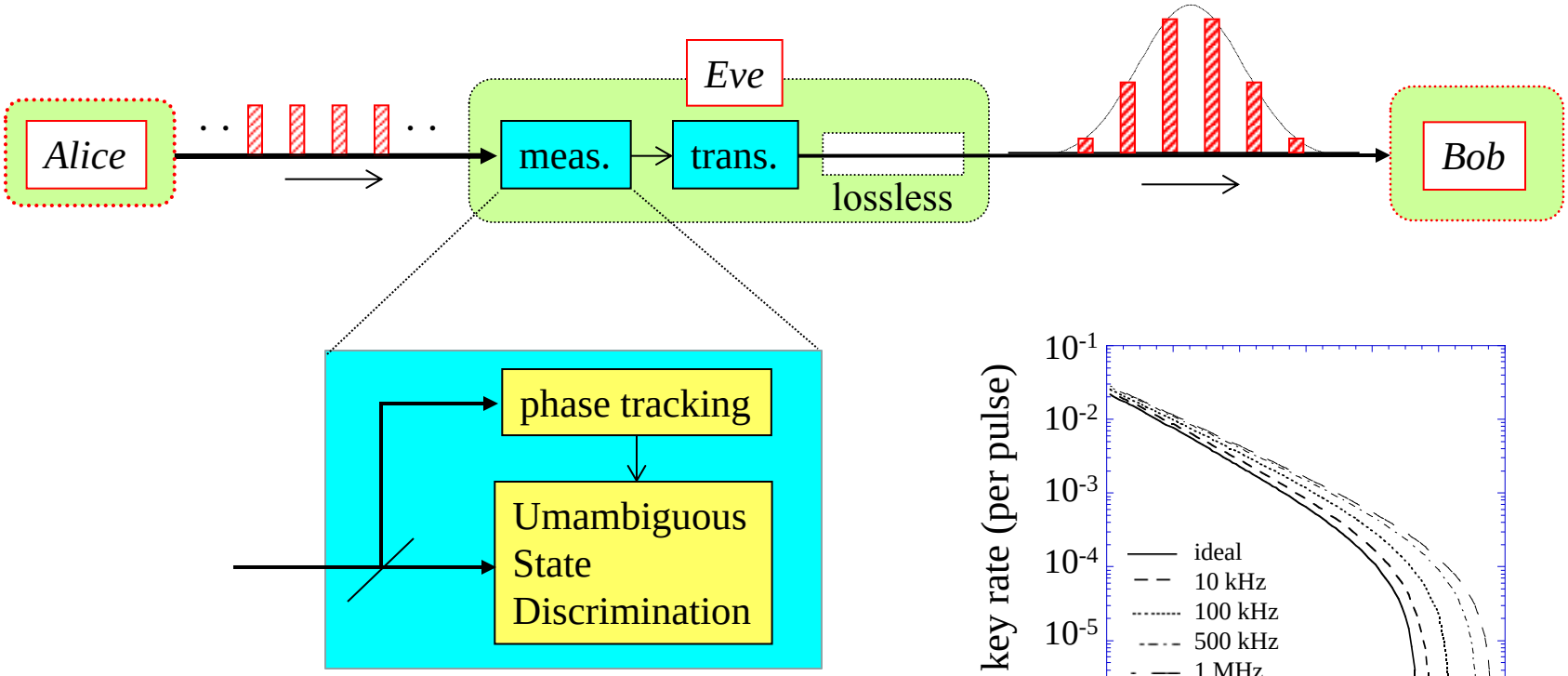
Bright light is detected by using 4 detectors.

Laser light is not a pure coherent state (2013-).

Theoretical analyses assumes ideal coherent states.

However, laser light has the finite spectral linewidth, which is not pure coherent state.

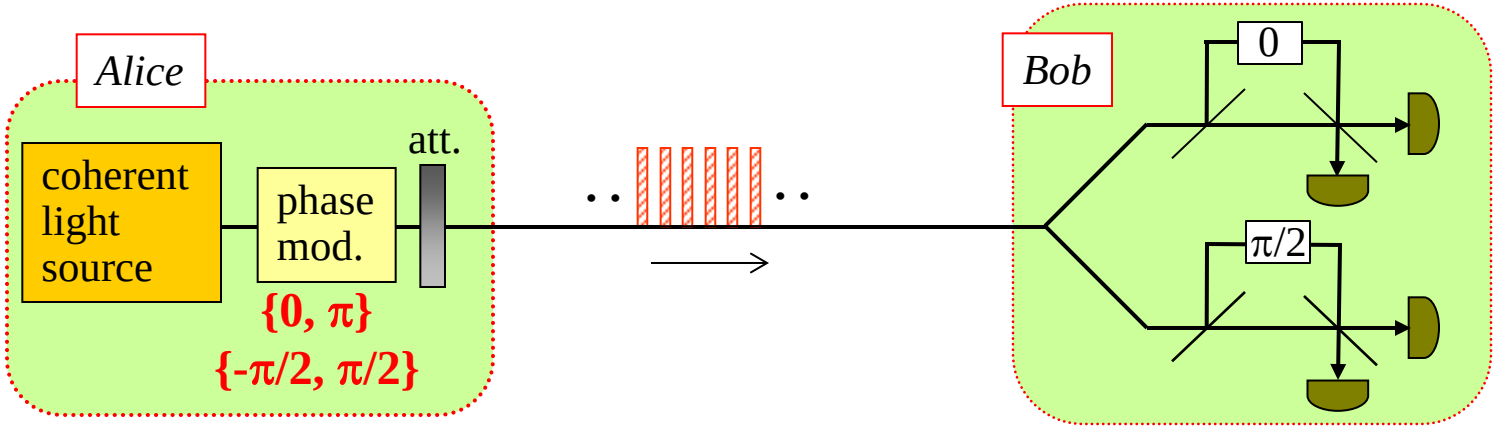
(Sequential attack)



Modified DPS protocol

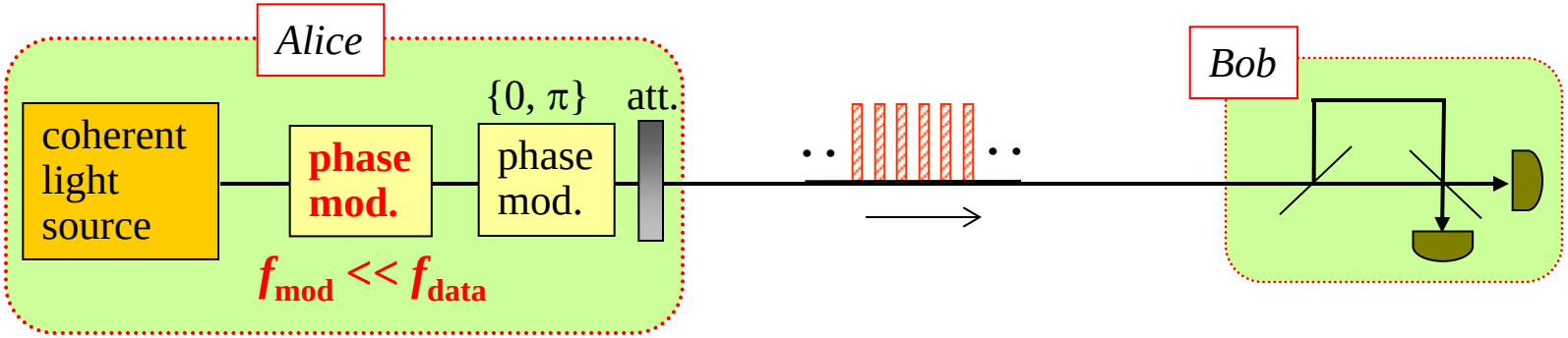
Differential quadrature phase shift scheme

A combination of DPS & BB84

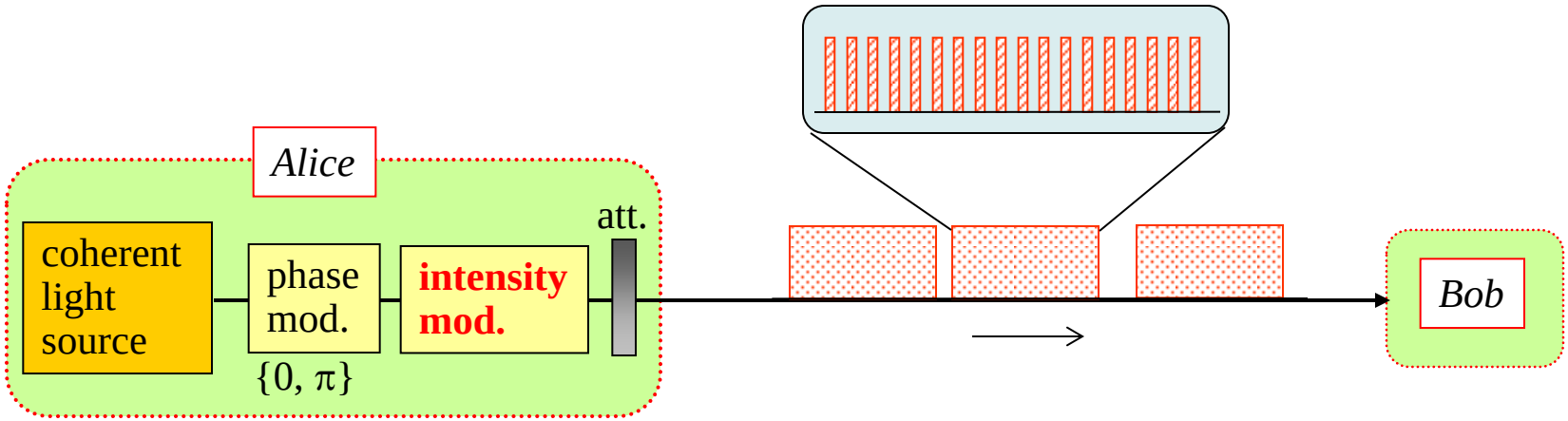


Slow phase modulation scheme

phase randomization



Segmented sequence scheme



Blanks are randomly inserted.

Eve cannot distinguish between signal and blank pulses.

↓

Temporal photon distribution is changed when eavesdropped.

Summary

Differential-phase-shift (DPS) QKD is presented.

(1) Setup & Protocol

featuring simplicity, practicality, high key efficiency

(2) Experiments

A long distance QKD has been achieved.

(3) Security issues

Security analysis is challenging because the system structure is much different .

(4) Modified protocol

Efforts to improve the system performance