Differential-Phase-Shift Quantum Key Distribution Using Single-Photon Detectors

Kyo Inoue

Osaka University
NTT Basic Research Laboratories
JST CREST

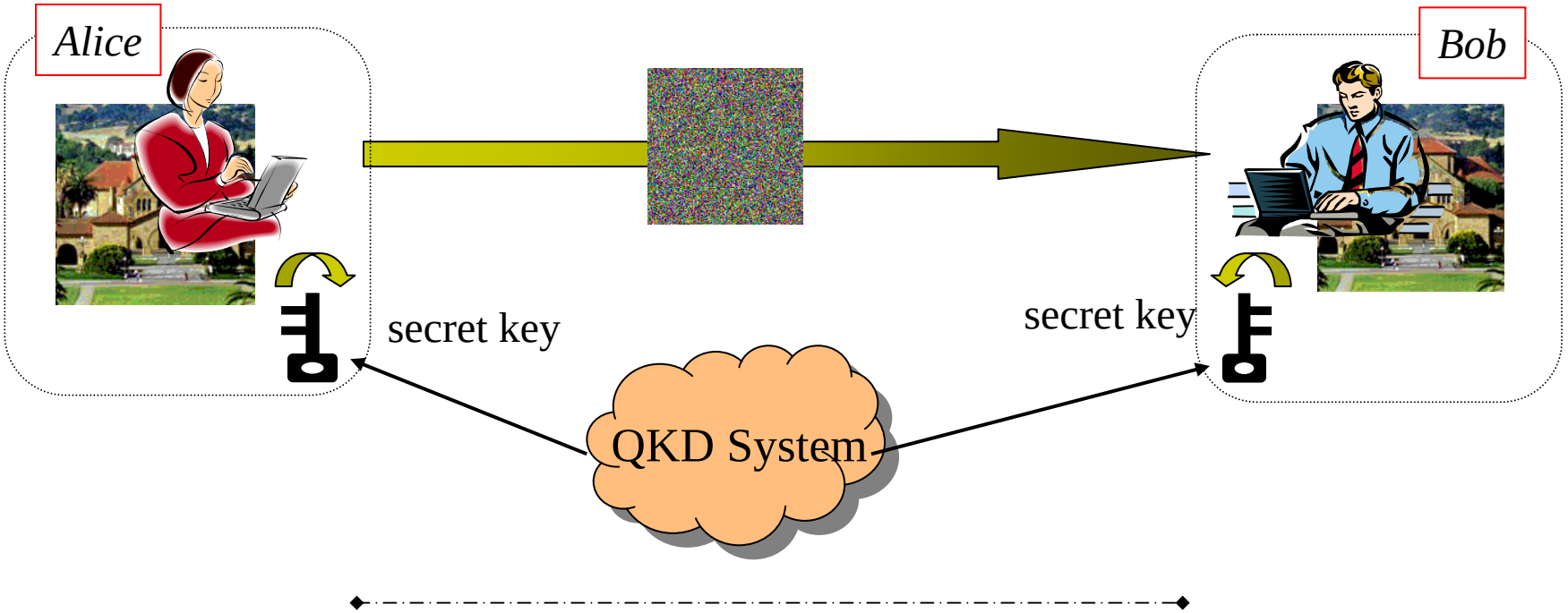
Collaboration with

H. Takesue, T. Honjo (*NTT Basic Res. Labs*.)

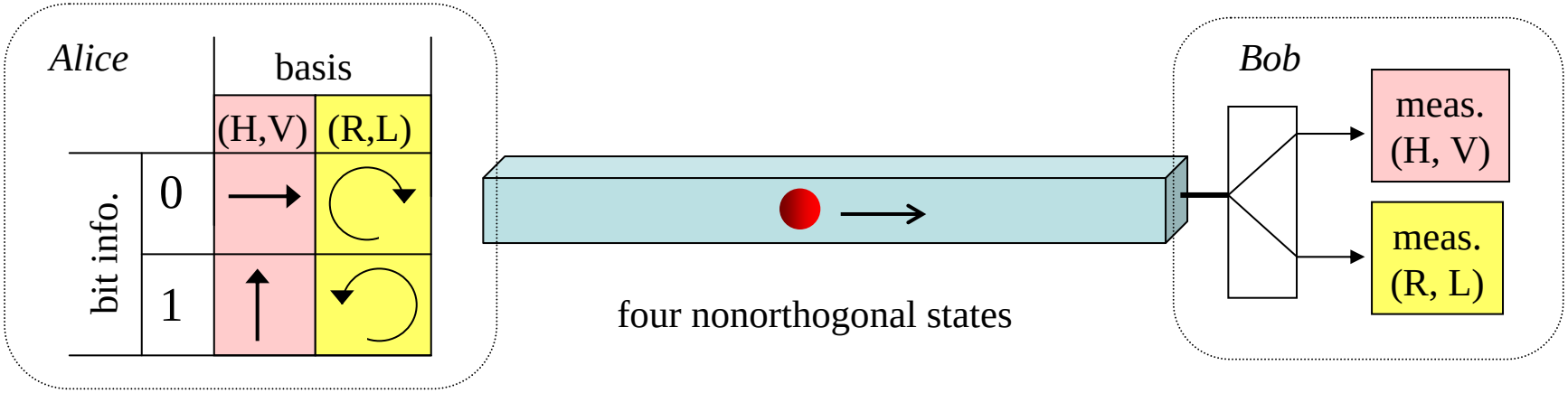
Yamamoto group (*Stanford Univ*.)

Contents

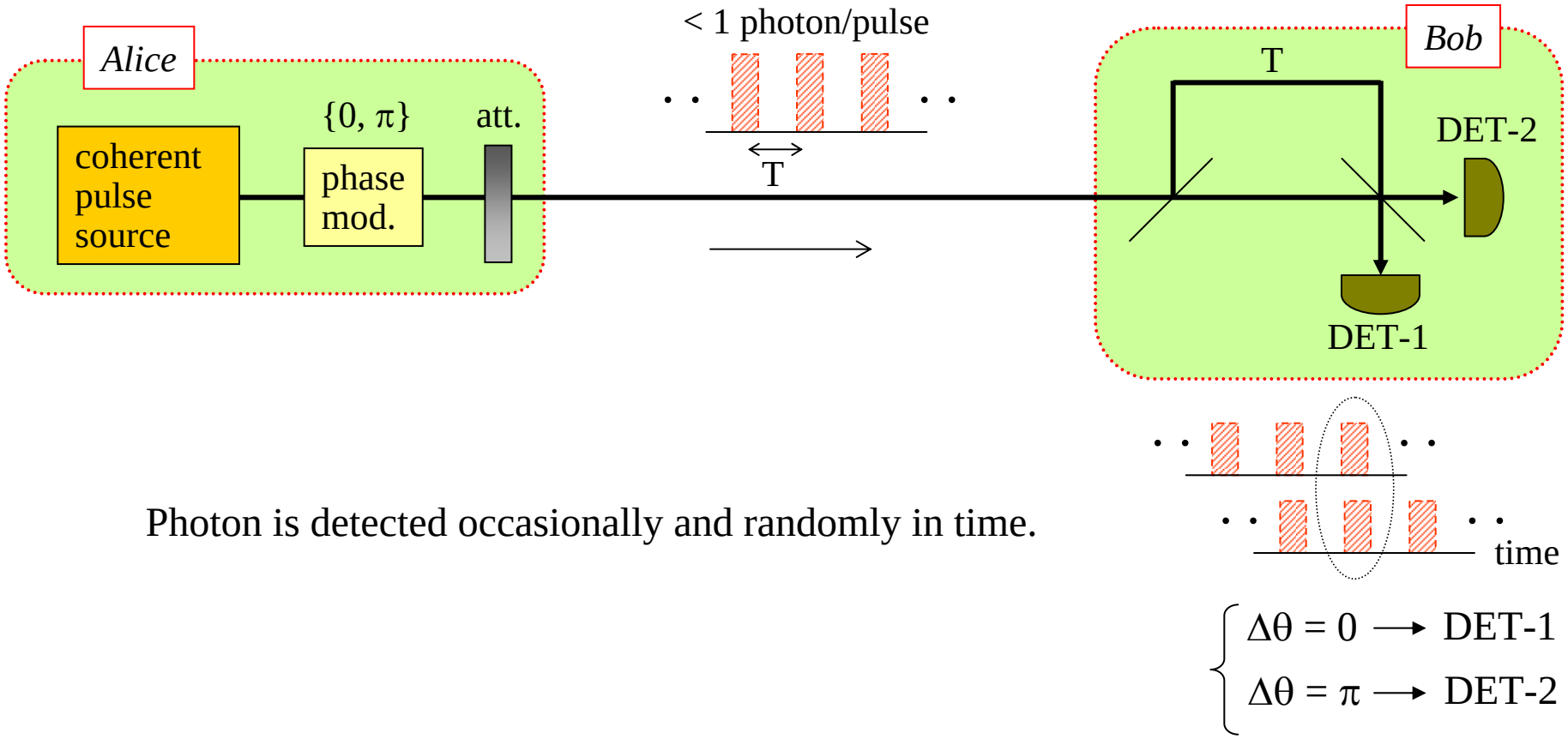
Quantum Key Distribution (QKD)



BB84 protocol



DPS (Differential-Phase-Shift) QKD



Photon is detected occasionally and randomly in time.

Protocol

(1) Signal transmission

(2) Bob → Alice: photon detection time

(3) Alice knows which detector clicked at Bob.

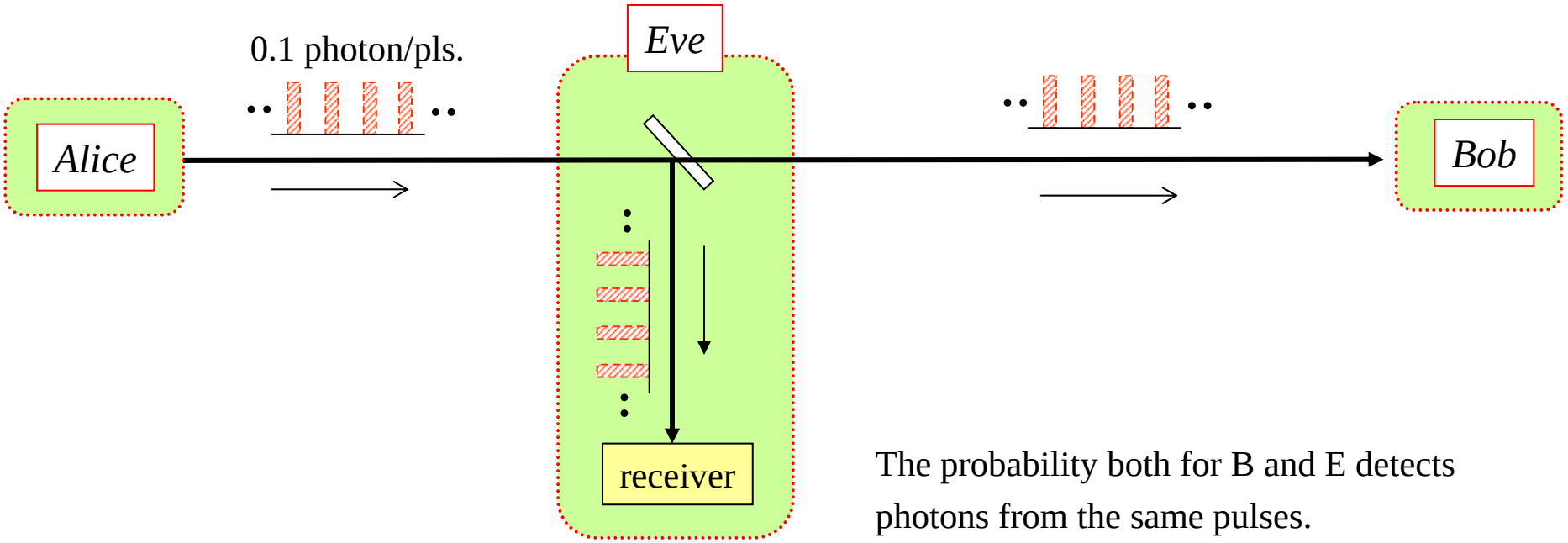
(4) Key bits are created as

DET-1 = “0” DET-2 = “1”

Features

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

Eavesdropping - beam splitting -



The probability both for B and E detects photons from the same pulses.

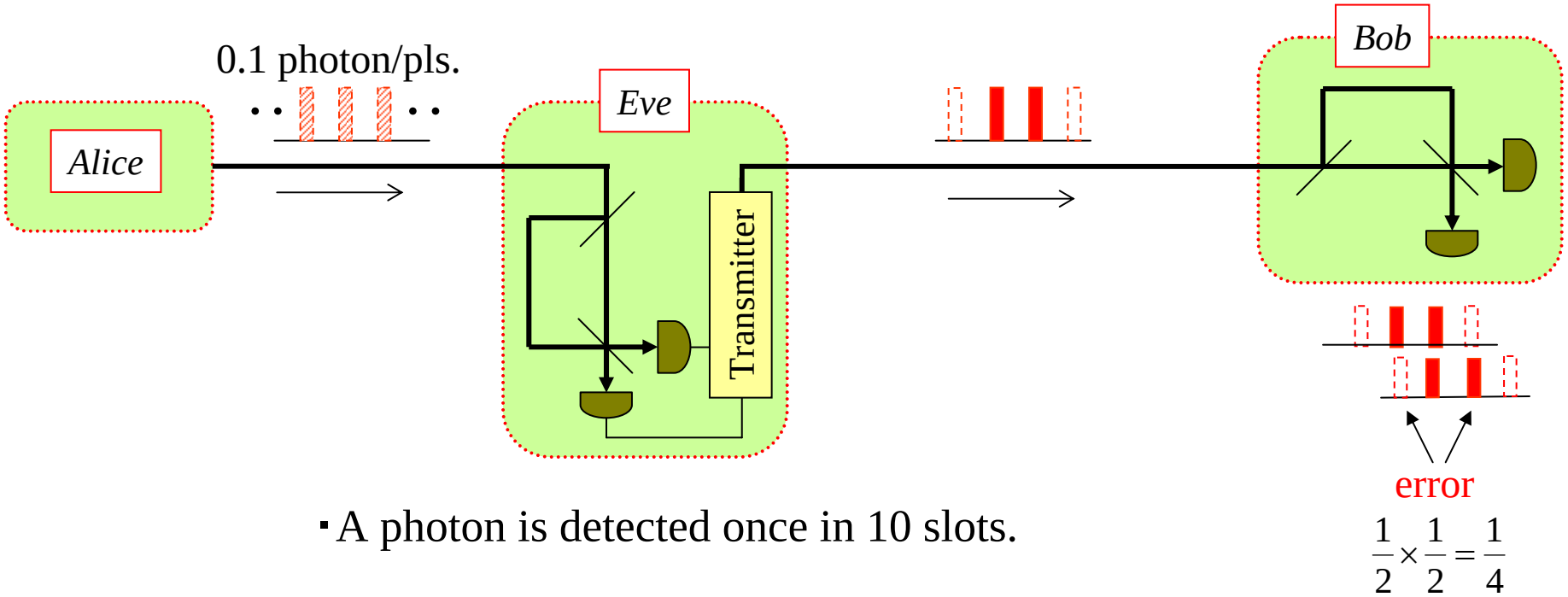
||

Stolen key bits are small.

↑

can be extinguished by privacy amplification

Eavesdropping - intercept & resend -

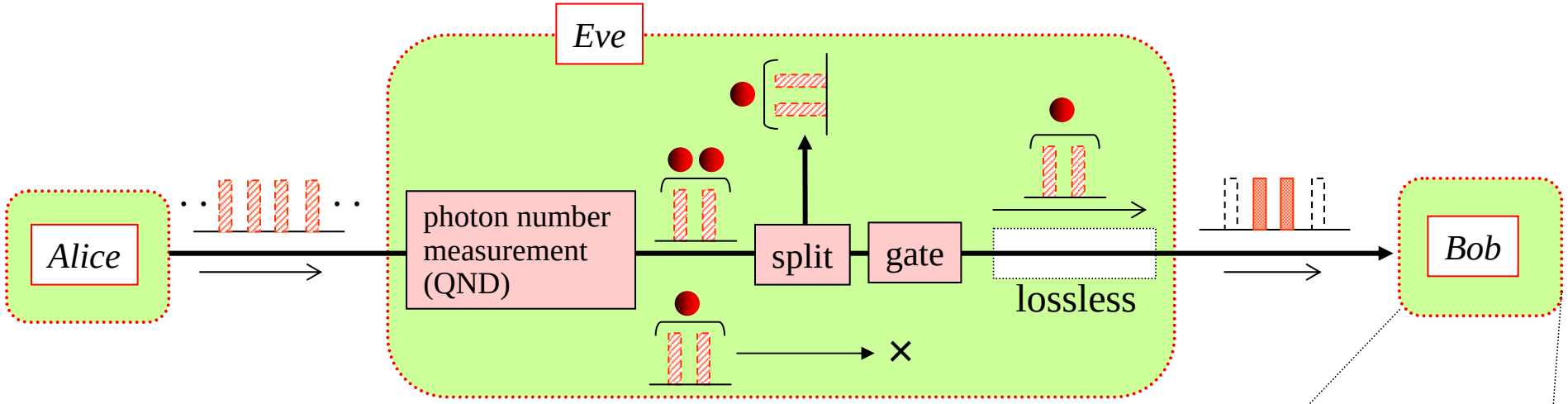


$$\frac{1}{2}\times\frac{1}{2}=\frac{1}{4}$$

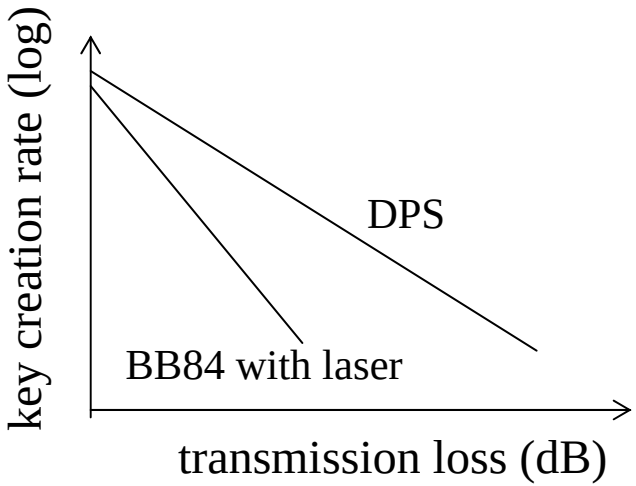
Eavesdropping !

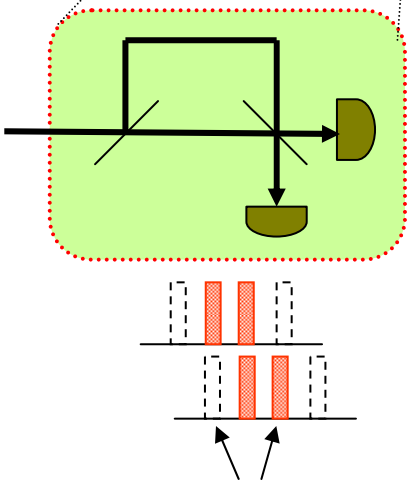
- A photon is detected once in 10 slots.
- She sends a photon over two pulses with measured phase difference.
- She sends nothing for unmeasured slots.

Eavesdropping - photon number splitting -



Induced error is independent of transmission loss.

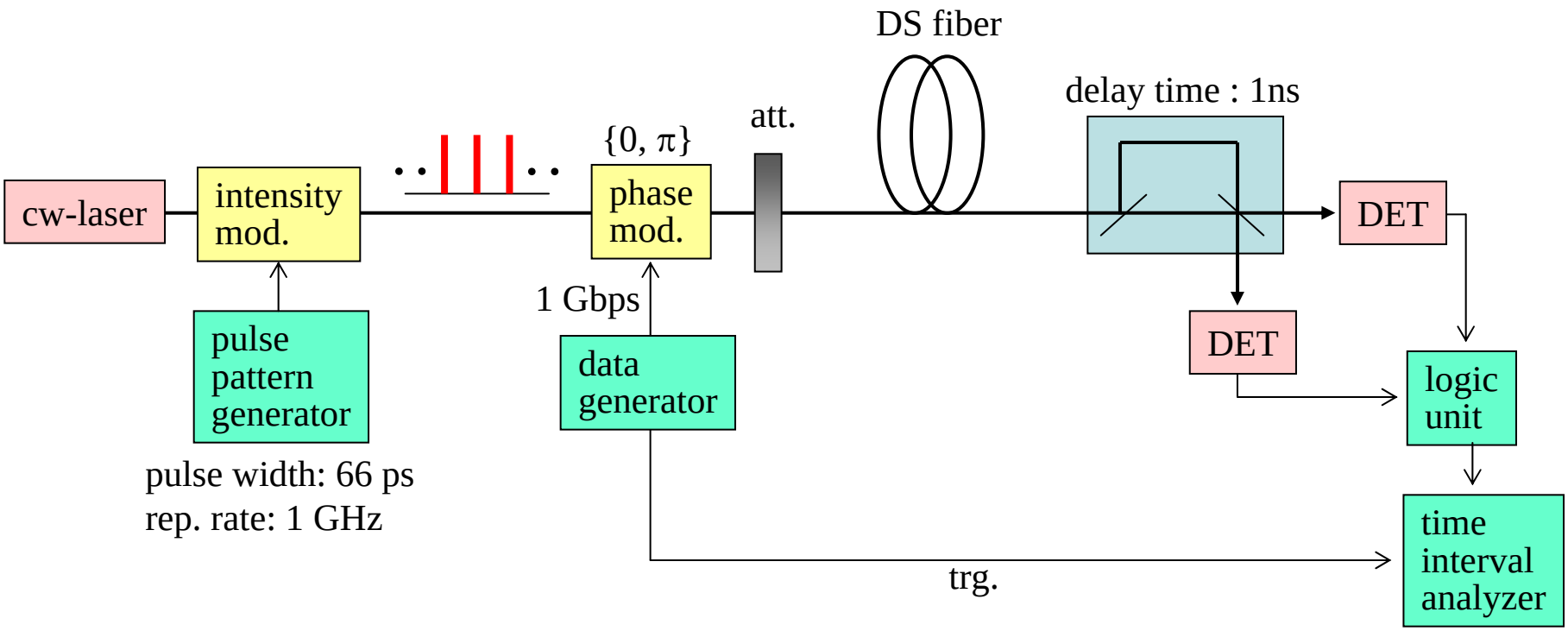




error

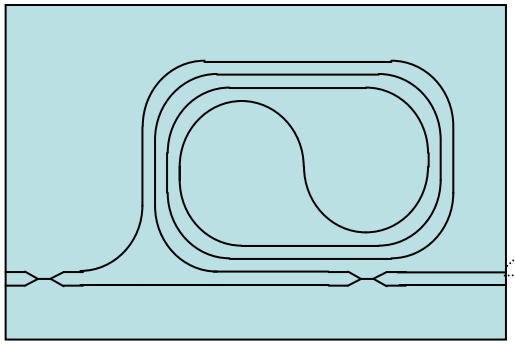
Eavesdropping !

DPS-QKD Experiment

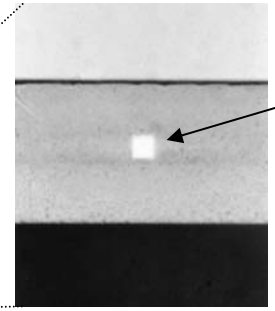


Waveguide Mach-Zehnder Interferometer

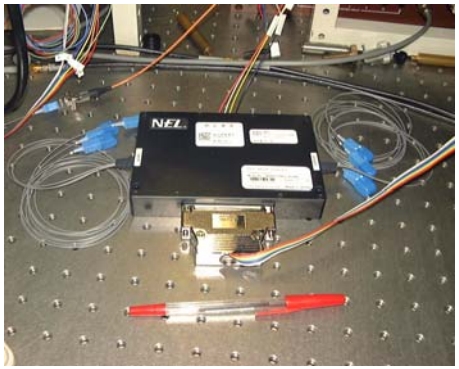
path difference: 20 cm
(delay time: 1 ns)

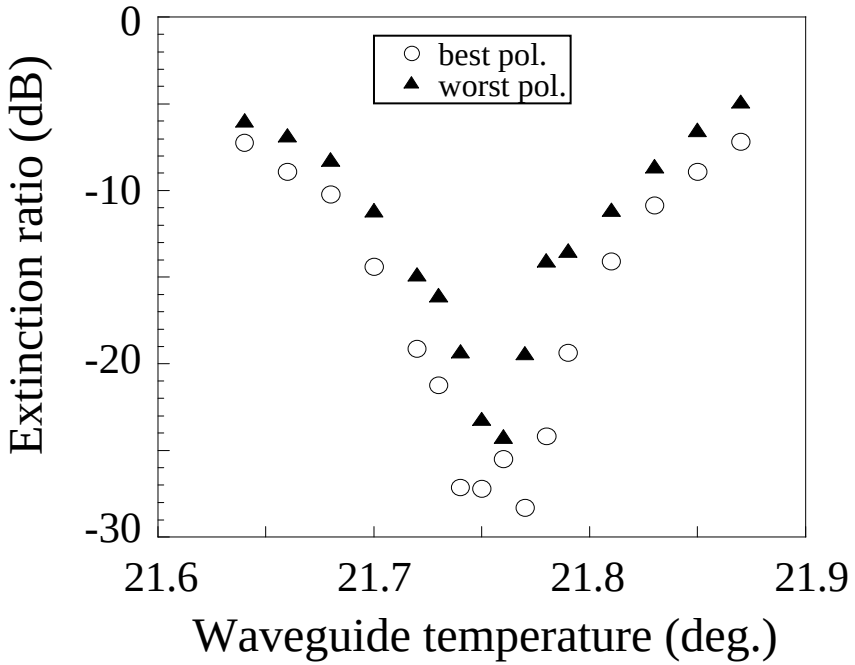


PLC (Planar Lightwave Circuit)



loss 2 dB（fiber-fiber）





Single Photon Detector

Conventionally, a high-biased APD is used.

Short wavelength : good Si-APD is commercially available.

Detection efficiency ~ 50%,

Dark count < 100cps

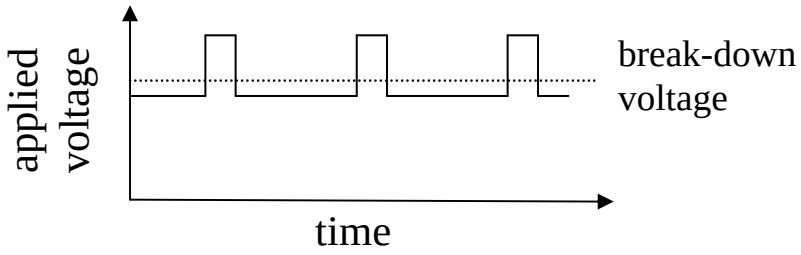
CW-operation

Long wavelength : InGaAs-APD is used in the gate mode.

Detection efficiency ~ 10%、

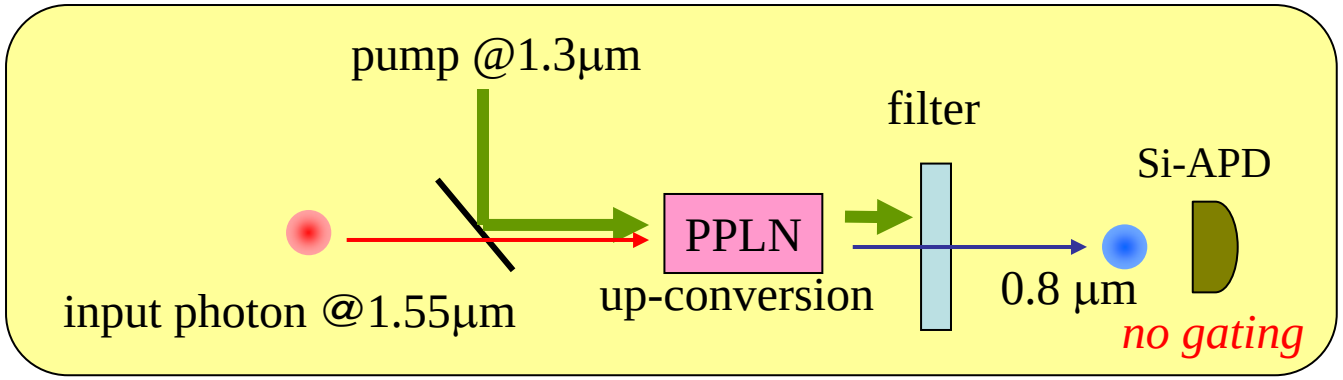
Dark count ~ 10^{-5}/gate、 → distance limitation

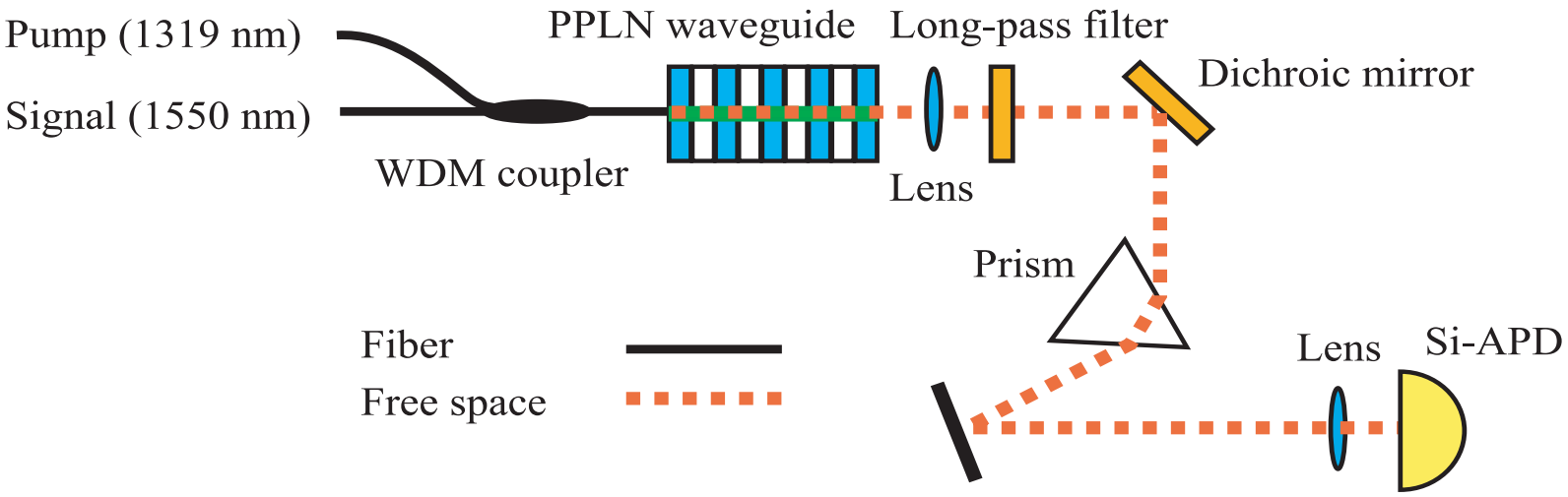
Gating rate ~ a few MHz → low key creation rate



in our experiment

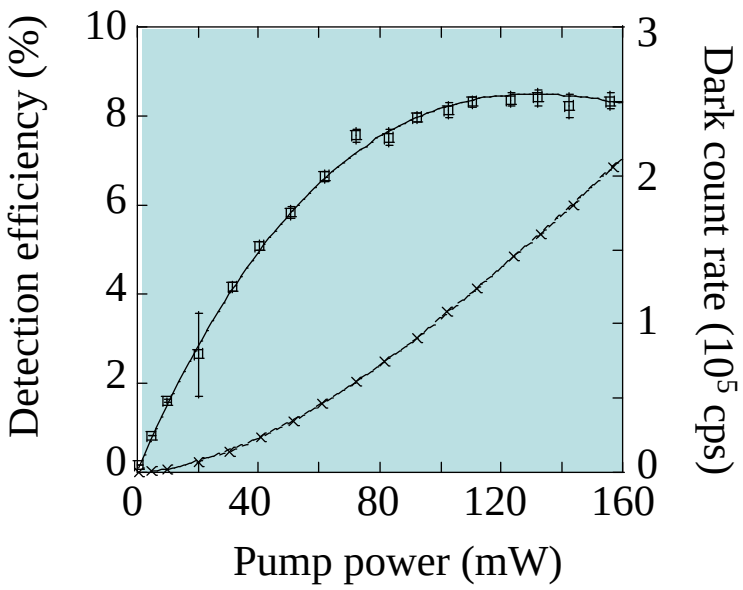
Up-conversion Photon Detector



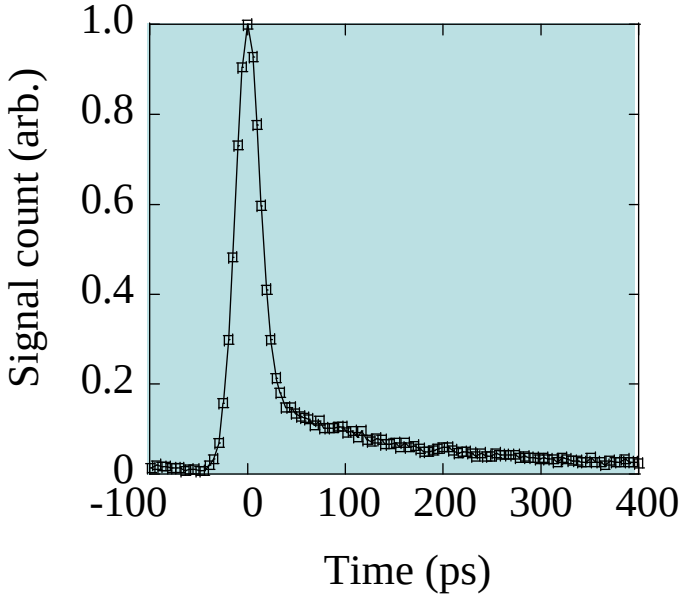


Performance

Efficiency & dark count



Temporal response

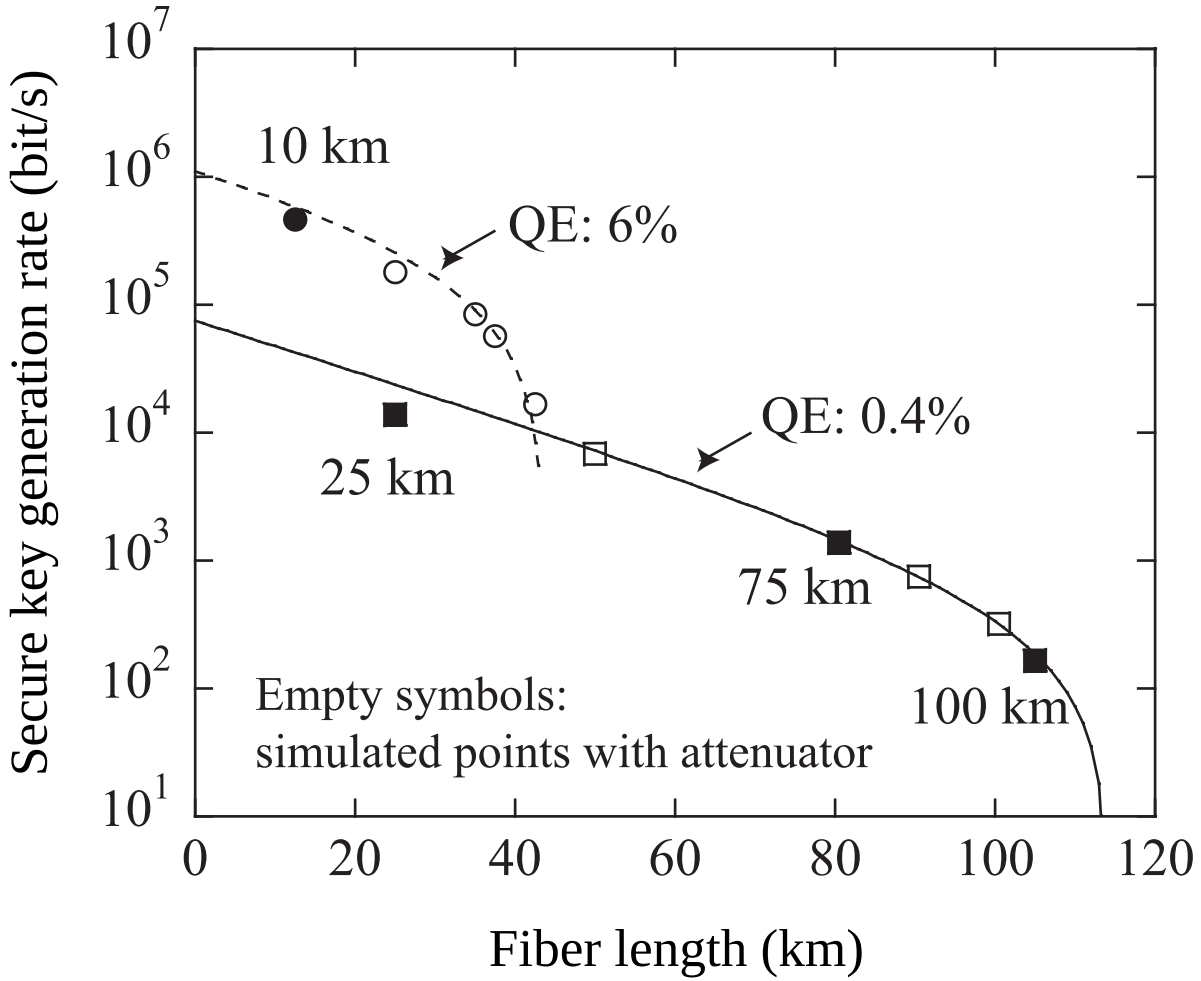


Dark count may be due to spontaneous Raman.

small jitter → low noise in effect

(Conventional jitter ~ several 100 ps)

Experimental Results



166 bit/s secure key at 100 km.
2 Mbit/s sifted key at 10 km.

Security is based on
Edo, Takesue, Yamamoto, PRA **73** (2006).

(1)DPS-QKD

- Setup & Protocol
- Eavesdropping
- Experiments

(2) Modified protocol with decoy slots

(3) System application

(4) Entanglement-based schemes

- Entanglement generation
- QKD experiment

Conventionally

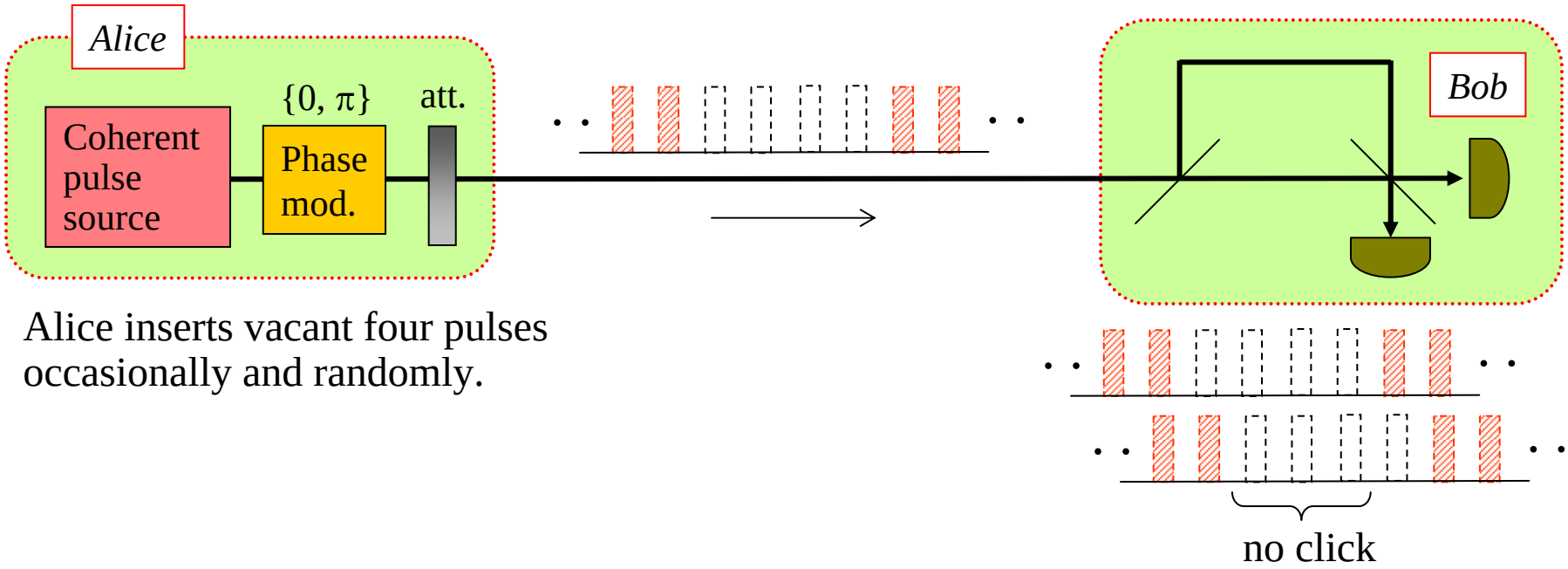
Eavesdropping is found by bit error rate

bit error (25 %)
eavesdropping !

Is there any other way of finding eavesdropping,
which may information leakage via bit error rate smaller ?

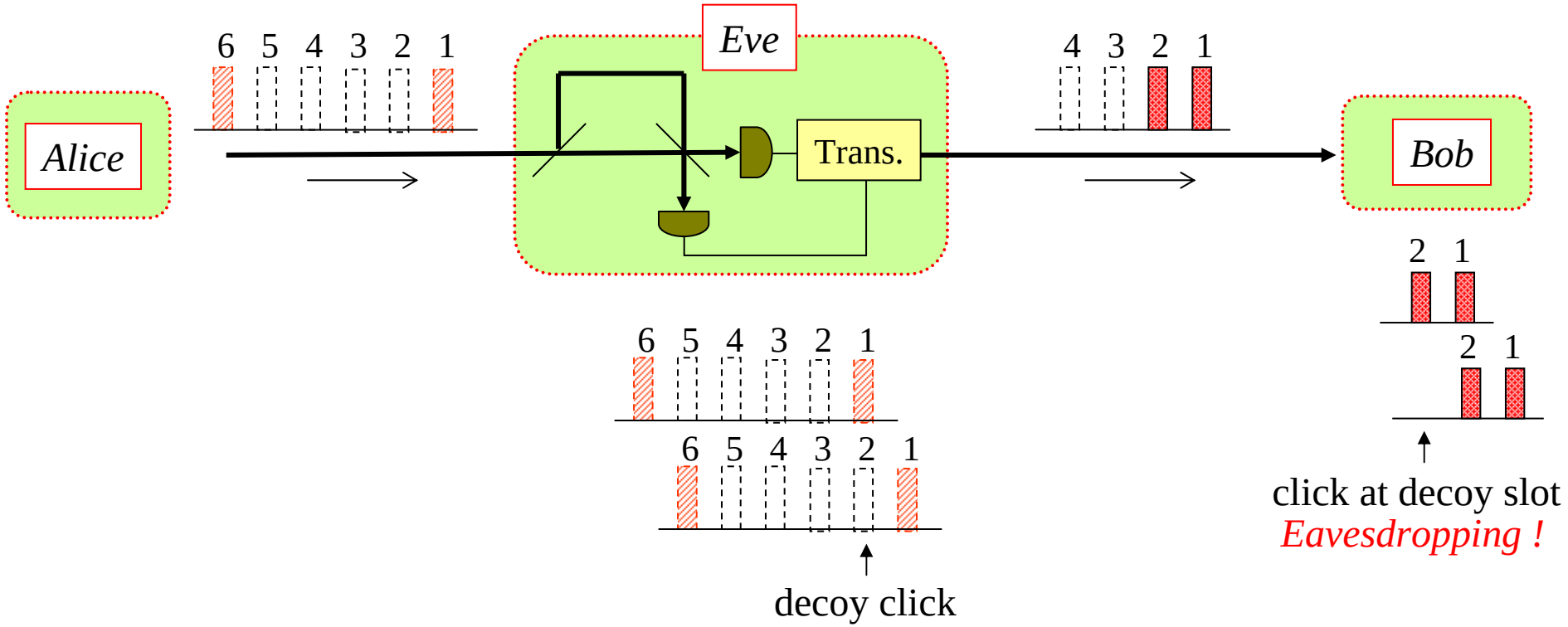
modified version

DPS-QKD with Decoy Slots



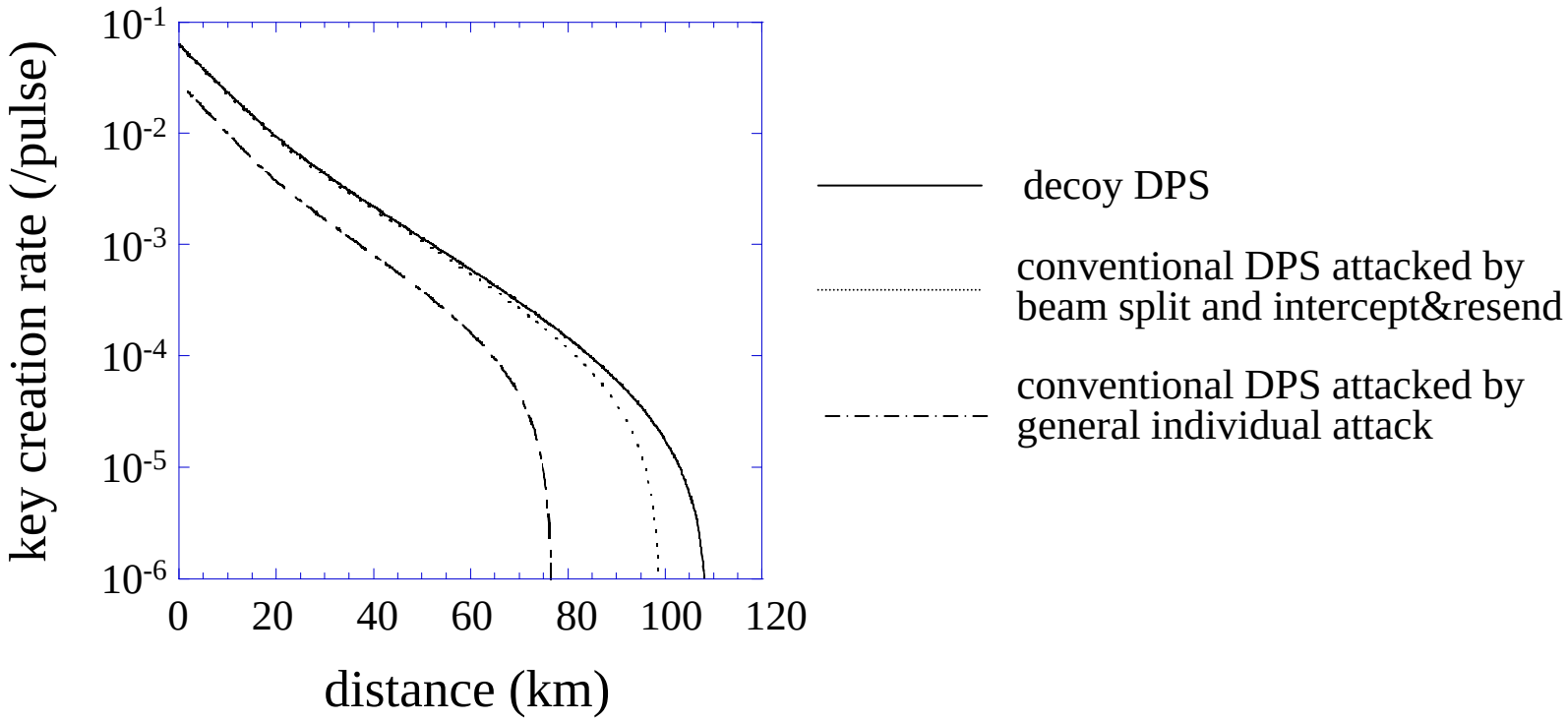
Alice inserts vacant four pulses occasionally and randomly.

Intercept & Resend against DPS-QKD with Decoy Slots



Intercept & Resend attack is prohibited.

Simulation


key creation rate (/pulse)
10-1
10-2
10-3
10-4
10-5
10-6
0
20
40
60
80
100
120
distance (km)
decoy DPS
conventional DPS attacked by beam split and intercept&resend
conventional DPS attacked by general individual attack

(1)DPS-QKD

- Setup & Protocol
- Eavesdropping
- Experiments

(2) Modified protocol with decoy slots

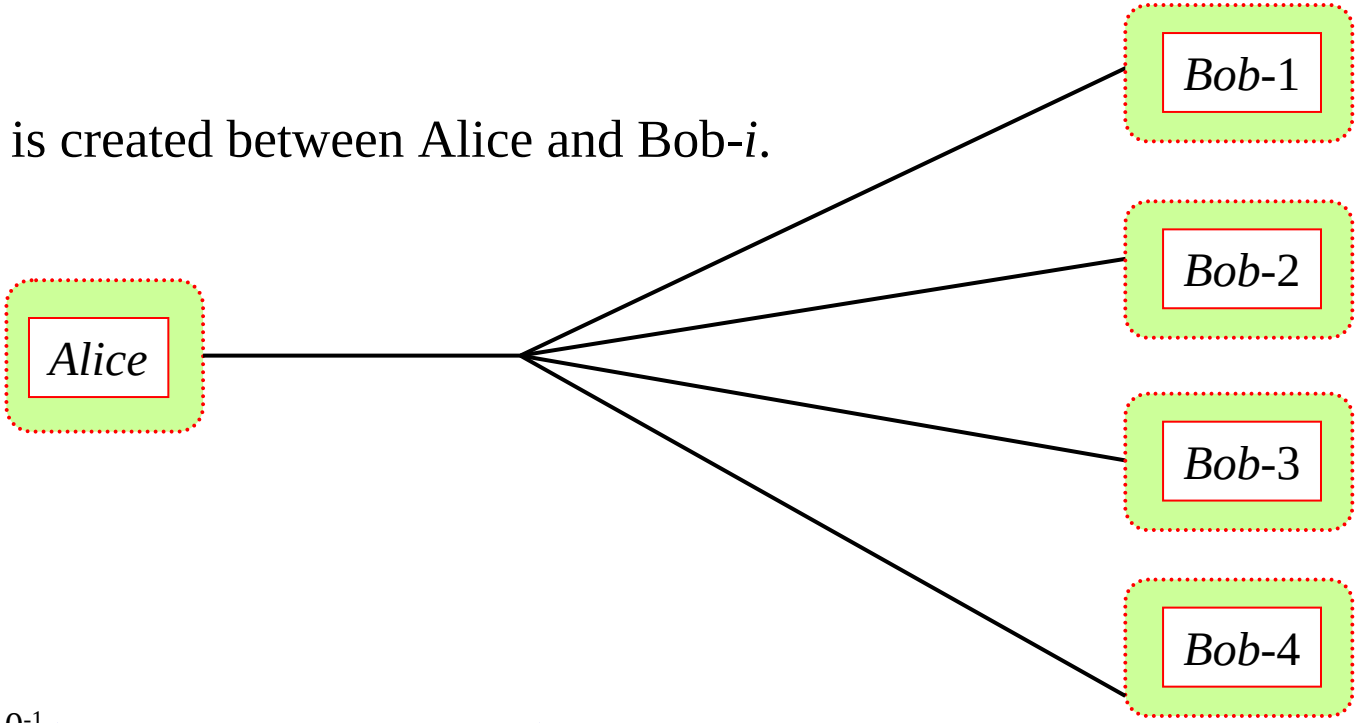
(3) System application

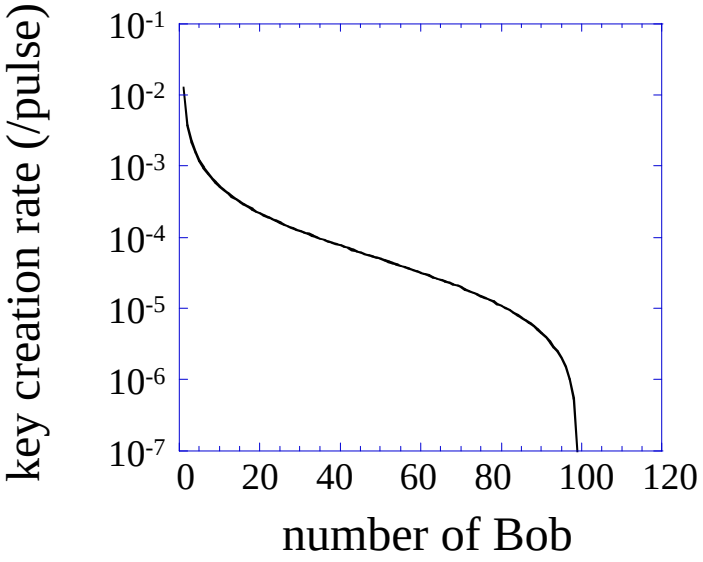
(4) Entanglement-based schemes

- Entanglement generation
- QKD experiment

Multiple Bobs : passive star

A secret key is created between Alice and Bob-*i*.





(1)DPS-QKD

- Setup & Protocol
- Eavesdropping
- Experiments

(2) Modified protocol with decoy slots

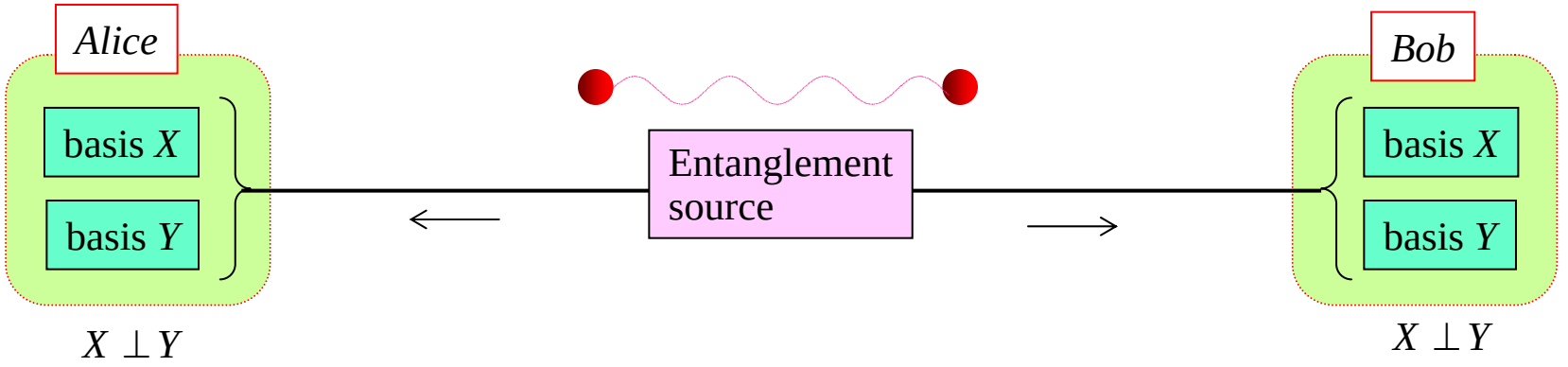
(3) System application

(4) Entanglement-based schemes

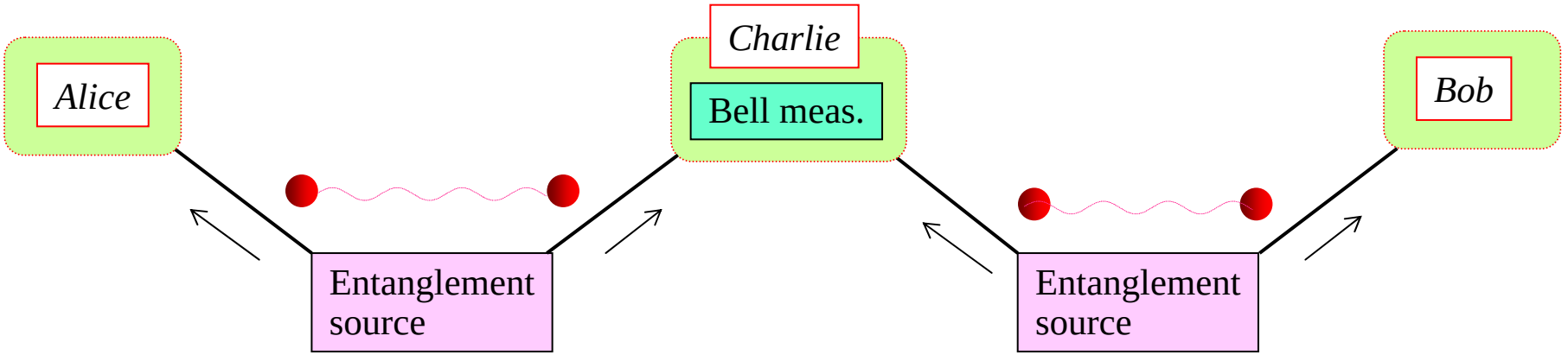
future scheme for long distance

QKD utilizing Entanglement

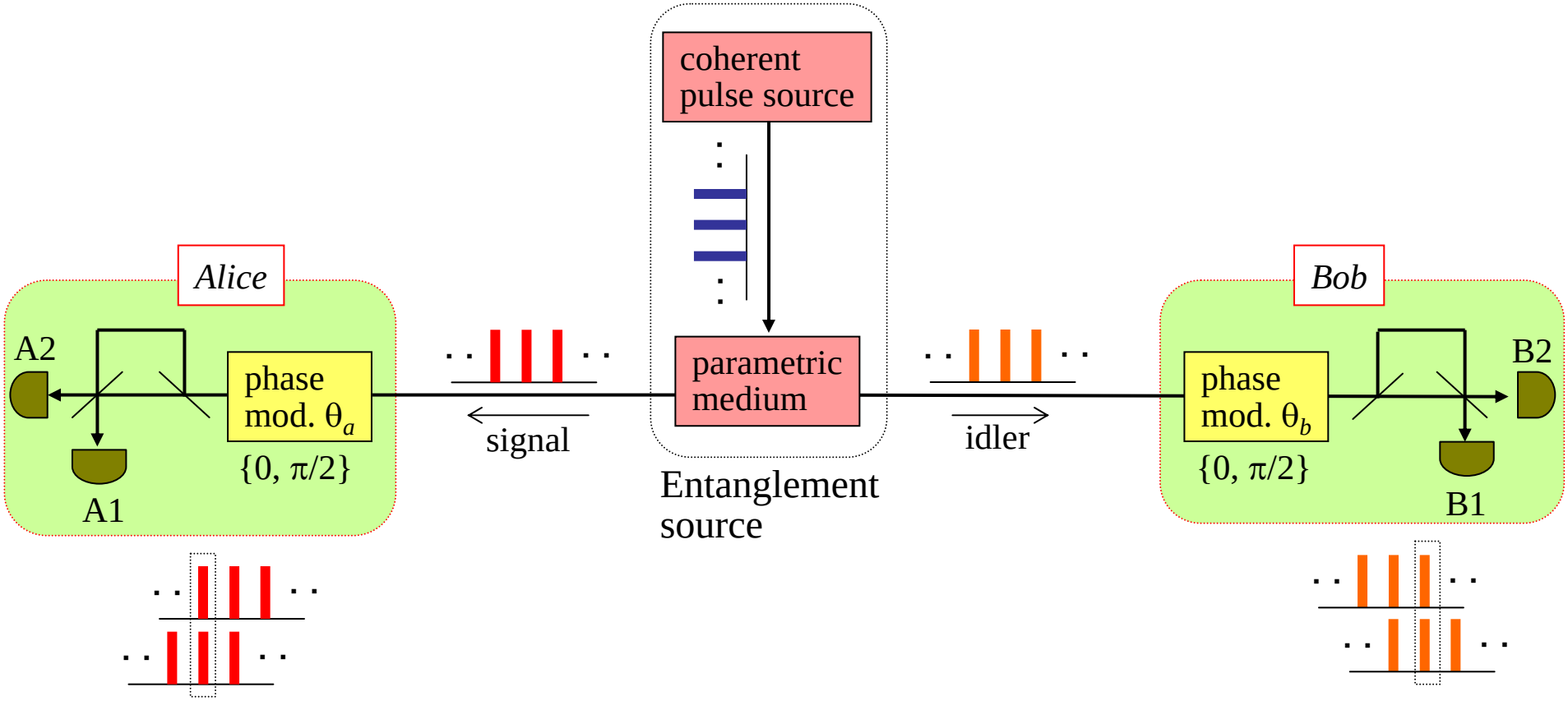
BBM92



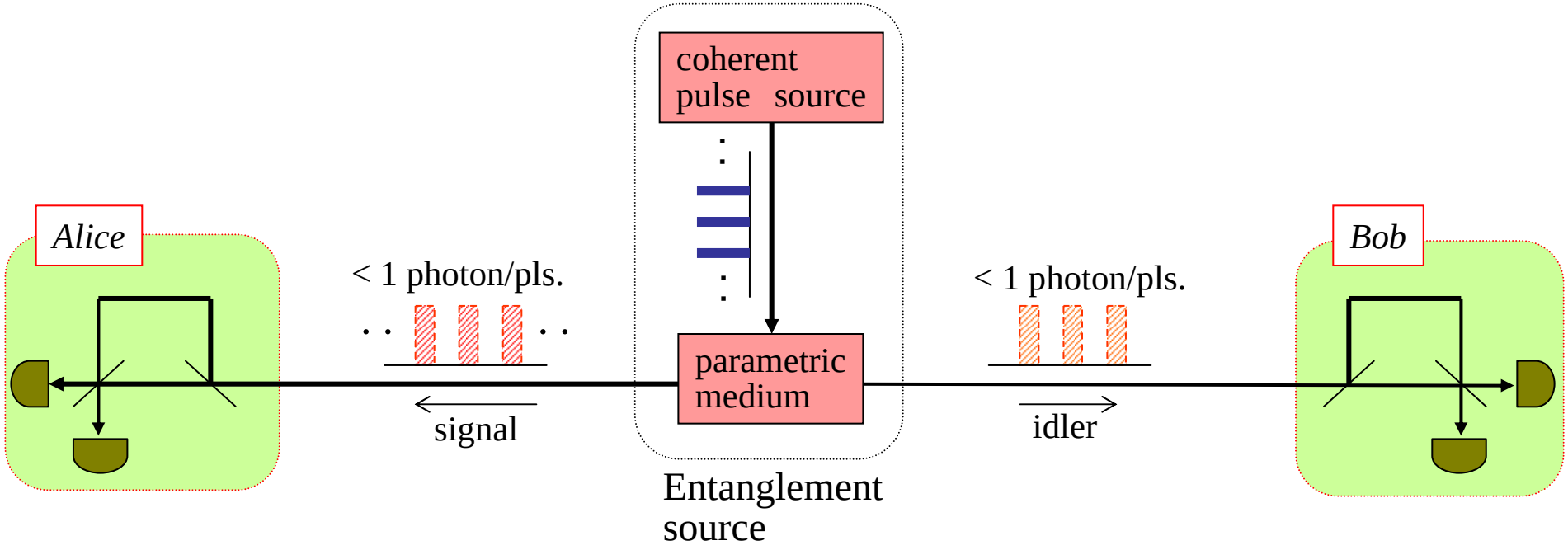
Quantum relay (entanglement swapping)



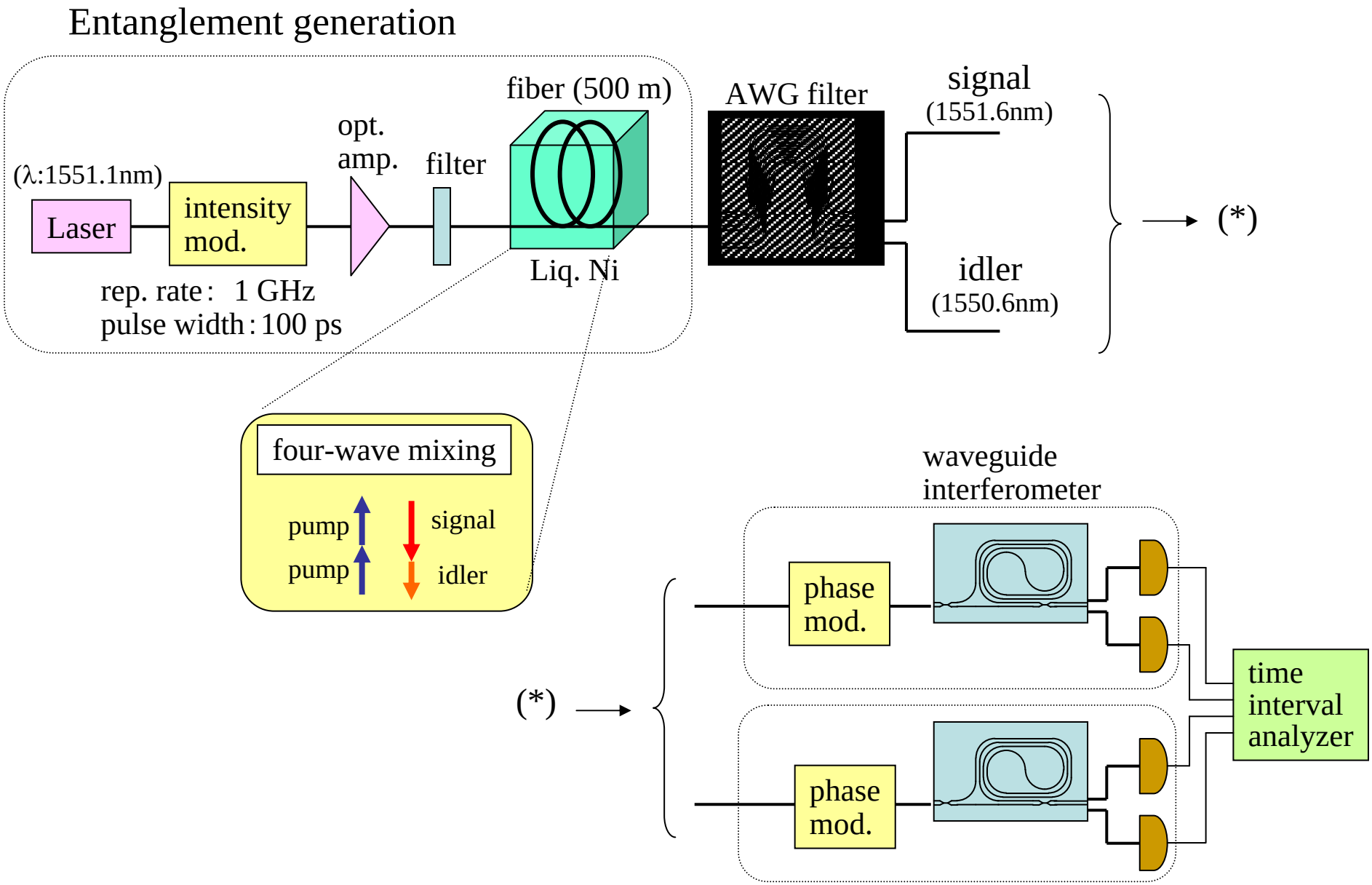
Entanglement-based QKD scheme
- BBM92+DPS -



Entanglement-based QKD
- DPS -

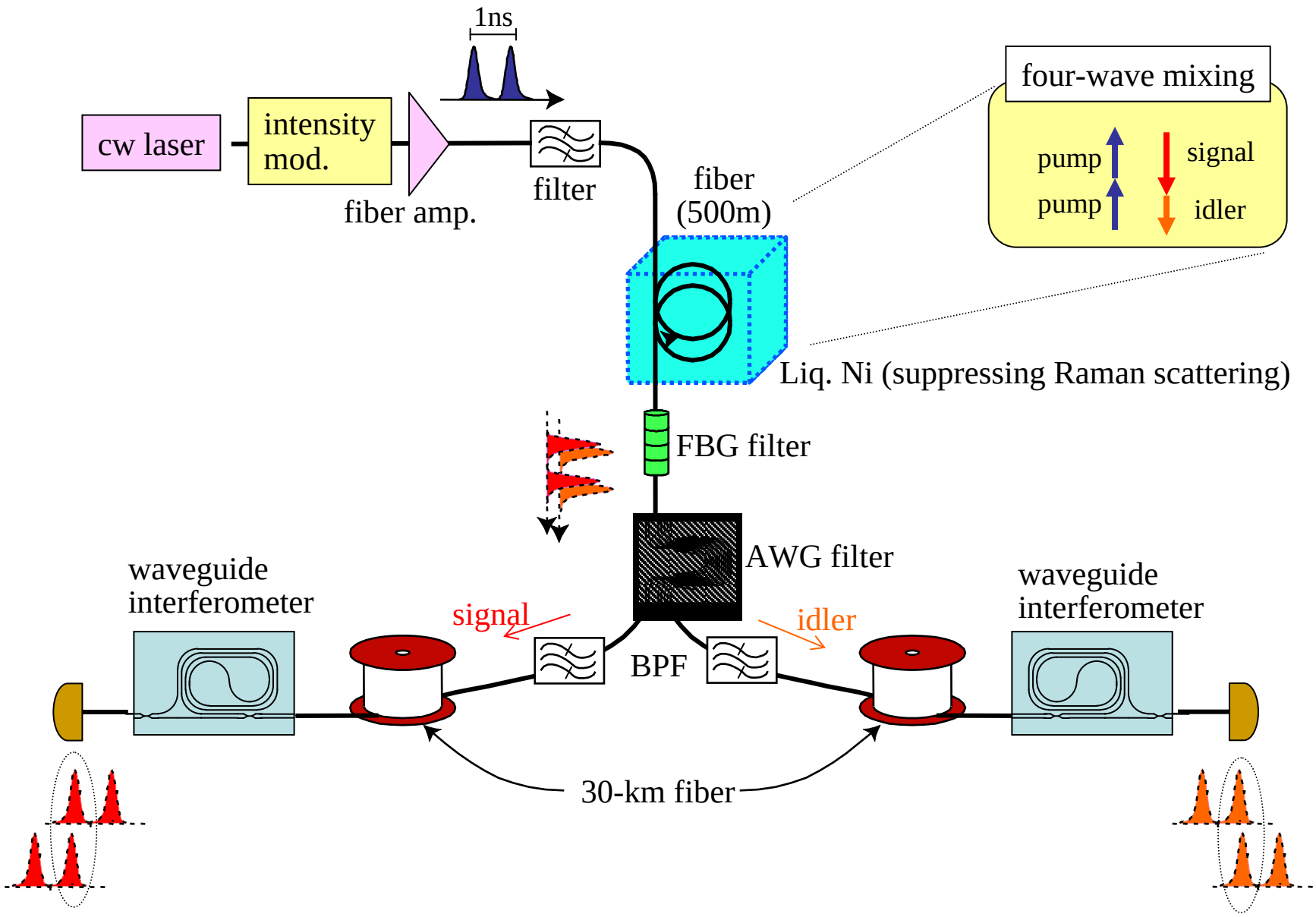


Experiment of Entanglement-based QKD
- BBM92 + DPS -



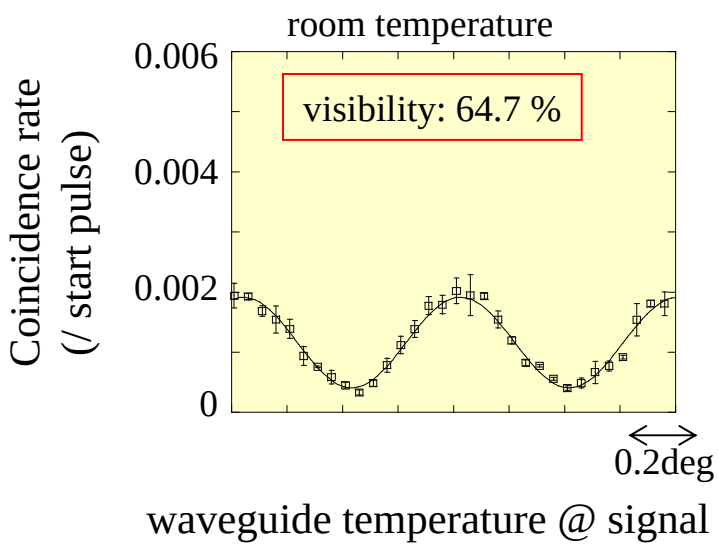
experiment

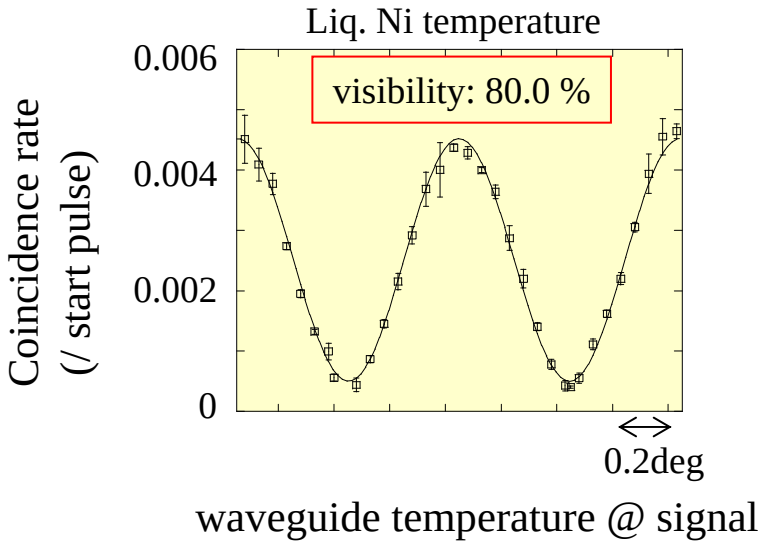
Entangled-Photon Generation



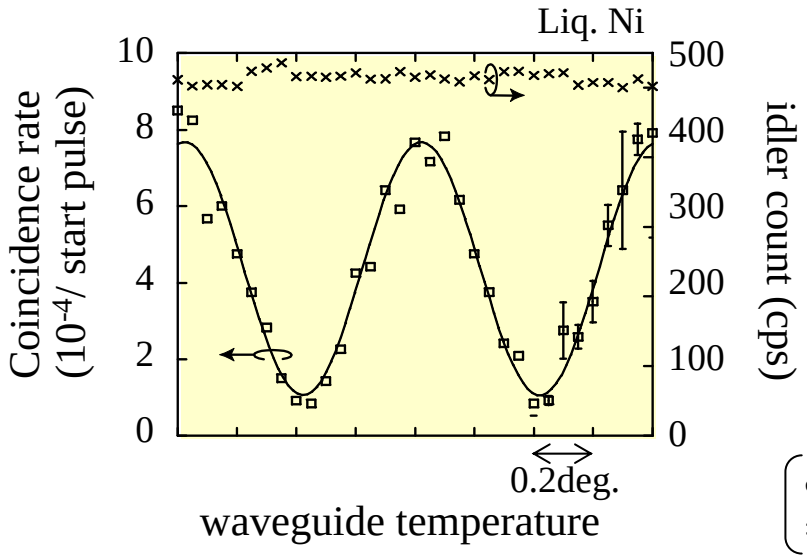
Two-Photon Interference

without transmission fiber



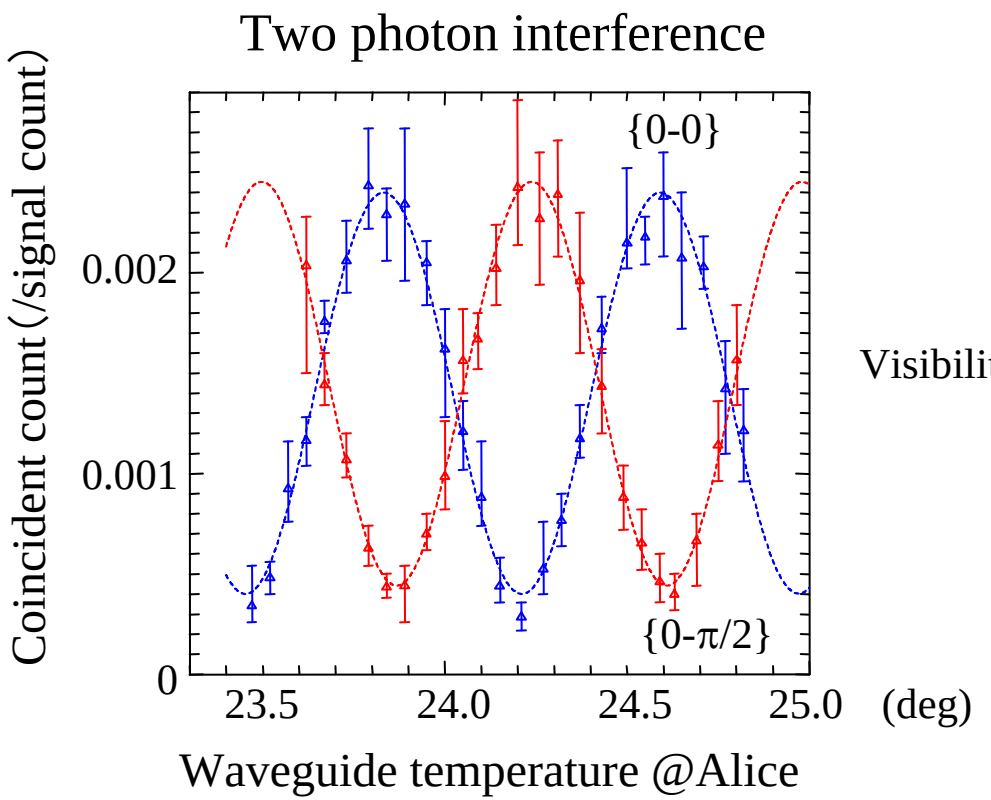


(30-km x 2) fiber transmission



average number of photon pairs
=0.06 (/pulse)

Experimental Results



Visibility = 70 %

⇩

Key creation

data rate:0.34 bps, error rate: 8.6 %

Summary

Differential-phase-shift QKD is presented.

(1) Setup & protocol, eavesdropping

Simple configuration, no photon discarded.

Robust against photon-number-splitting attack

(2) DPS-QKD experiment

featuring PLC interferometer and up-conversion photon detectors

166 bit/s at 100 km, 2 Mbit/s at 10 km for secure key

(3) Modified protocol with decoy slots

Eavesdropping is revealed from click at decoy slots.

(4) Entanglement-based schemes

Experiment utilizing fiber four-wave mixing for entanglement generation.

Source output:

$$|\Psi_{in}\rangle = \sum_j \sqrt{\mu} e^{2i\phi_p} |t_j\rangle_s |t_j\rangle_i$$

$|t_j\rangle_s$: signal photon at time t_j
$|t_j\rangle_i$: idler photon at time t_j
μ: probability of one-pair generation
ϕ_p: pump phase

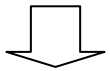
Interferometer output for coincident detection

$$|\Psi_{out}\rangle \propto \{1+\exp[i(\Delta\theta_a+\Delta\theta_b)]\}(|A1\rangle|B1\rangle+|A2\rangle|B2\rangle) + \{1-\exp[i(\Delta\theta_a+\Delta\theta_b)]\}(|A1\rangle|B2\rangle+|A2\rangle|B1\rangle)$$

|A1> : one photon @ DET-A1
|A2> : one photon @ DET-A2
|B1> : one photon @ DET-B1
|B2> : one photon @ DET-B2

$$= \begin{cases} |A1\rangle|B1\rangle+|A2\rangle|B2\rangle & \text{for } \Delta\theta_a+\Delta\theta_b = 0 \\ |A1\rangle|B2\rangle+|A2\rangle|B1\rangle & \text{for } \Delta\theta_a+\Delta\theta_b = \pi \\ (1\pm i)(|A1\rangle|B1\rangle+|A2\rangle|B2\rangle) + (1\mp i)(|A1\rangle|B2\rangle+|A2\rangle|B1\rangle) & \text{for } \Delta\theta_a+\Delta\theta_b = \pm\pi/2 \end{cases}$$

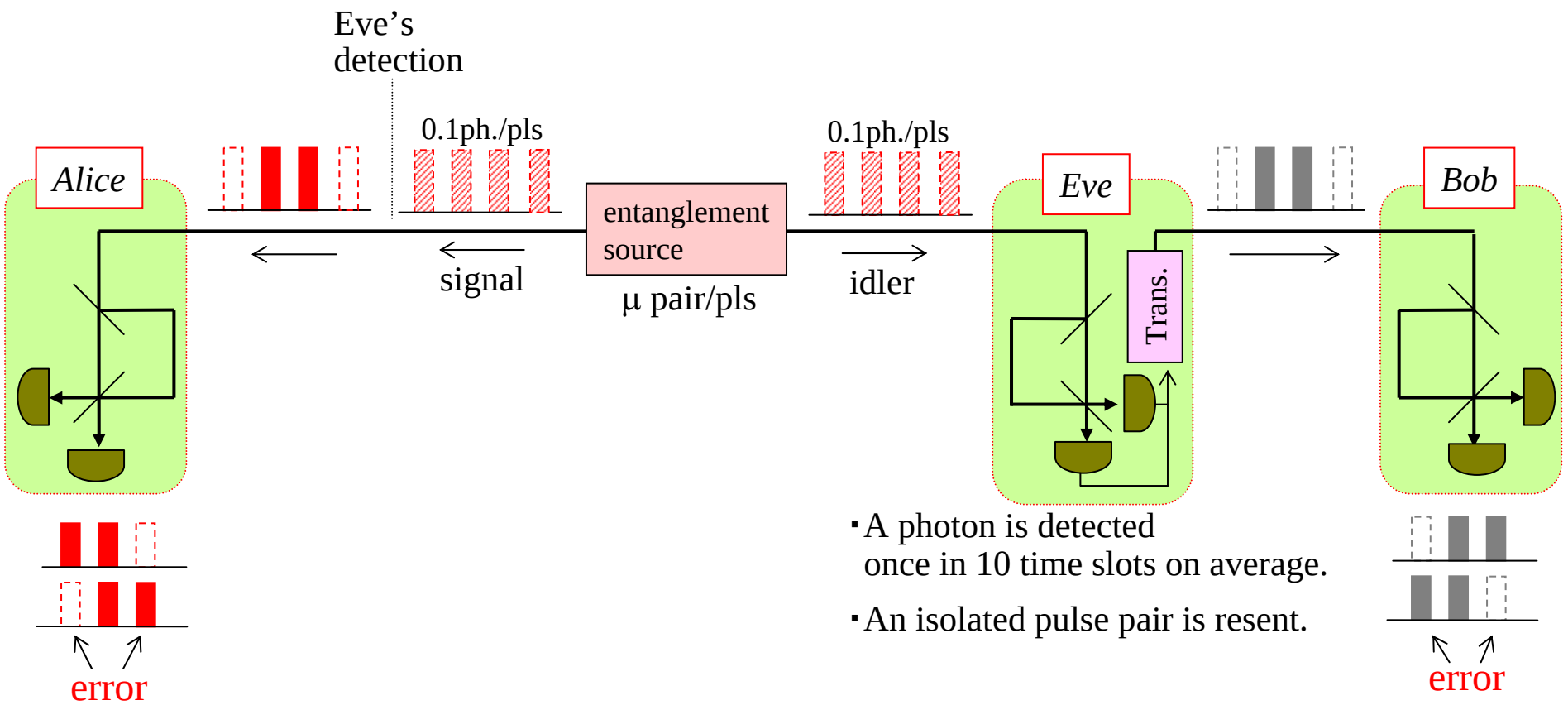
detection@*A*	$\Delta\theta_a + \Delta\theta_b$ 0	$\pi/2$	π
A1	B1	B1/B2	B2
A2	B2	B1/B2	B1



Key creation

$\Delta\theta_a + \Delta\theta_b = 0$: {A1, B1} = "0", {A2, B2} = "1"
$\Delta\theta_a + \Delta\theta_b = \pi$: {A1, B2} = "0", {A2, B1} = "0"
$\Delta\theta_a + \Delta\theta_b = \pi/2$: ignore

Eavesdropping against Entanglement-based DPS-QKD (1) - Intercept & Resend -



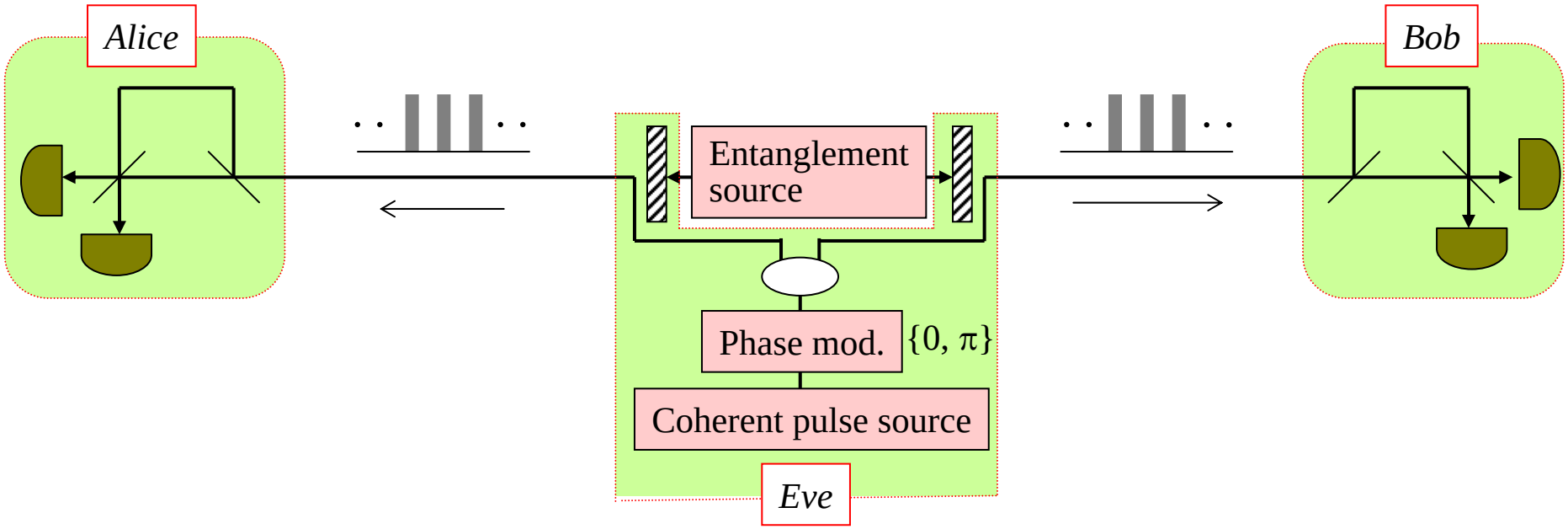
- A photon is detected once in 10 time slots on average.
- An isolated pulse pair is resent.

◆ Eavesdropping is revealed from bit error rate.

◆ Eavesdropping is also revealed from coincident count rate.

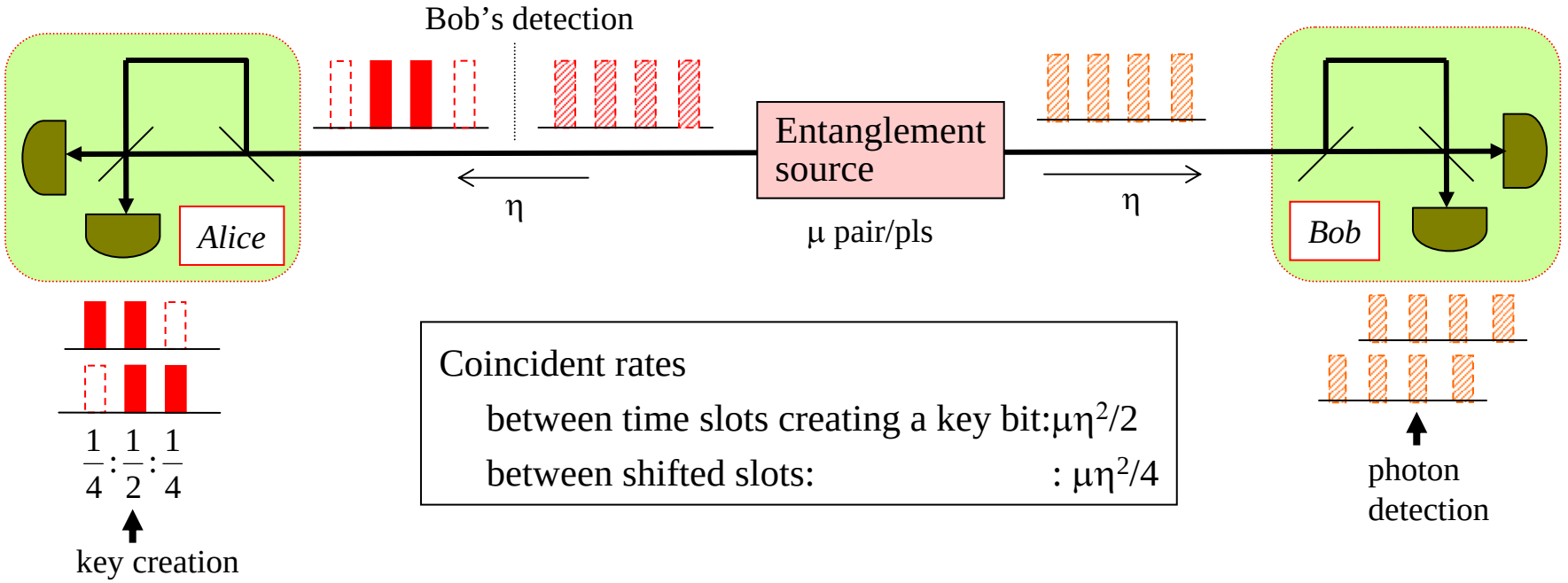
normal: $(1/2)\mu\eta^2$ eavesdropped: $(3/8)\mu\eta^2$ (η: line transmittance)

Eavesdropping against Entanglement-based DPS-QKD (2)
- Source Replacement -

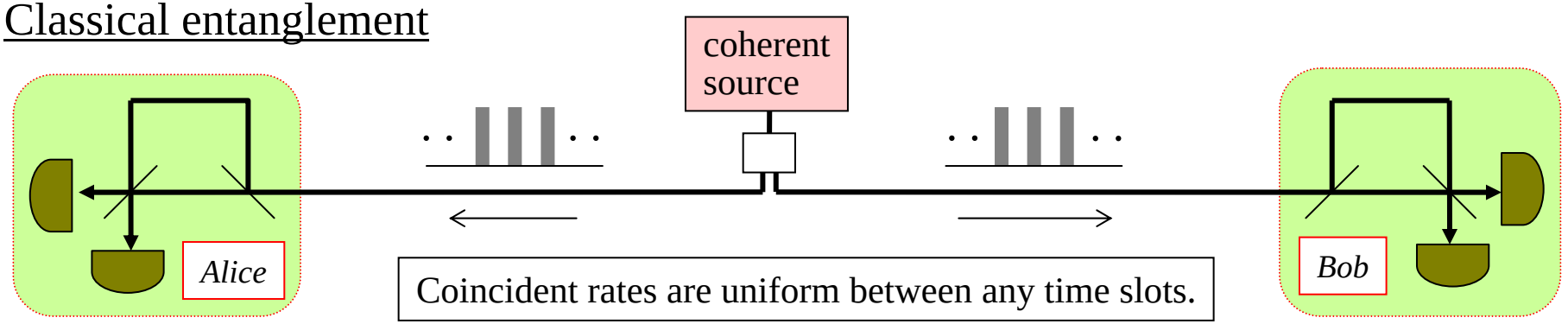


Eve gets key information without inducing bit errors.
However,,,,,

Quantum entanglement



Classical entanglement



The eavesdropping is revealed from the coincident rates.

Quantum Relaying DPS-QKD