Differential-Phase-Shift Quantum Key Distribution

Kyo Inoue

Osaka University
NTT Basic Research Laboratories
JST CREST

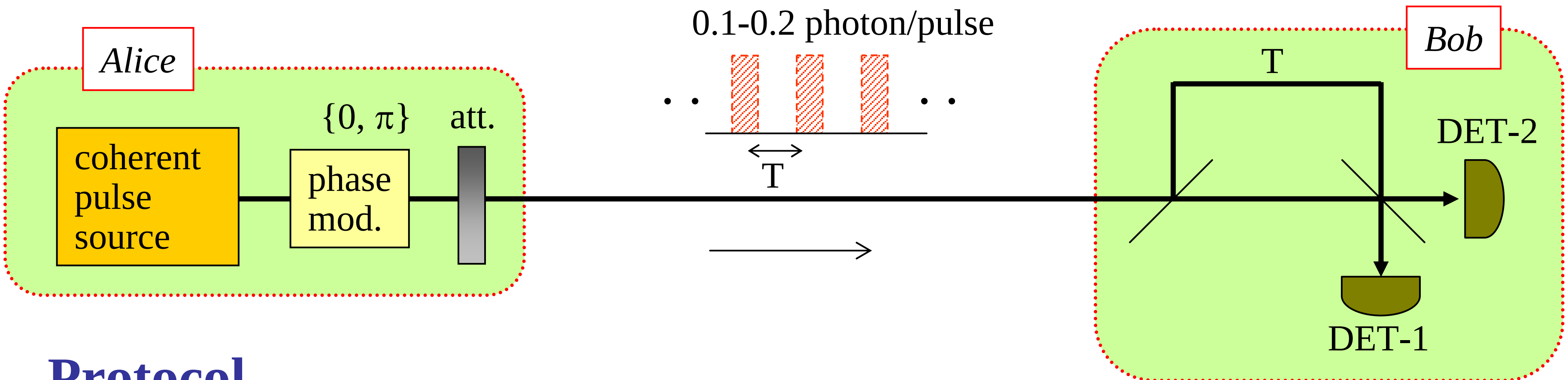
Collaboration with

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

Yamamoto group (*Stanford Univ*.)

Contents

DPS (Differential-Phase-Shift) QKD



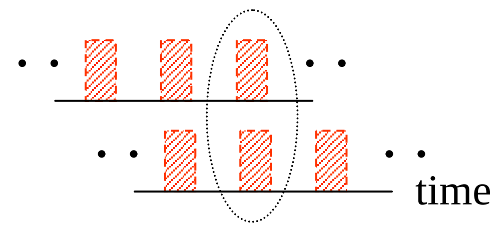
Protocol

(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”

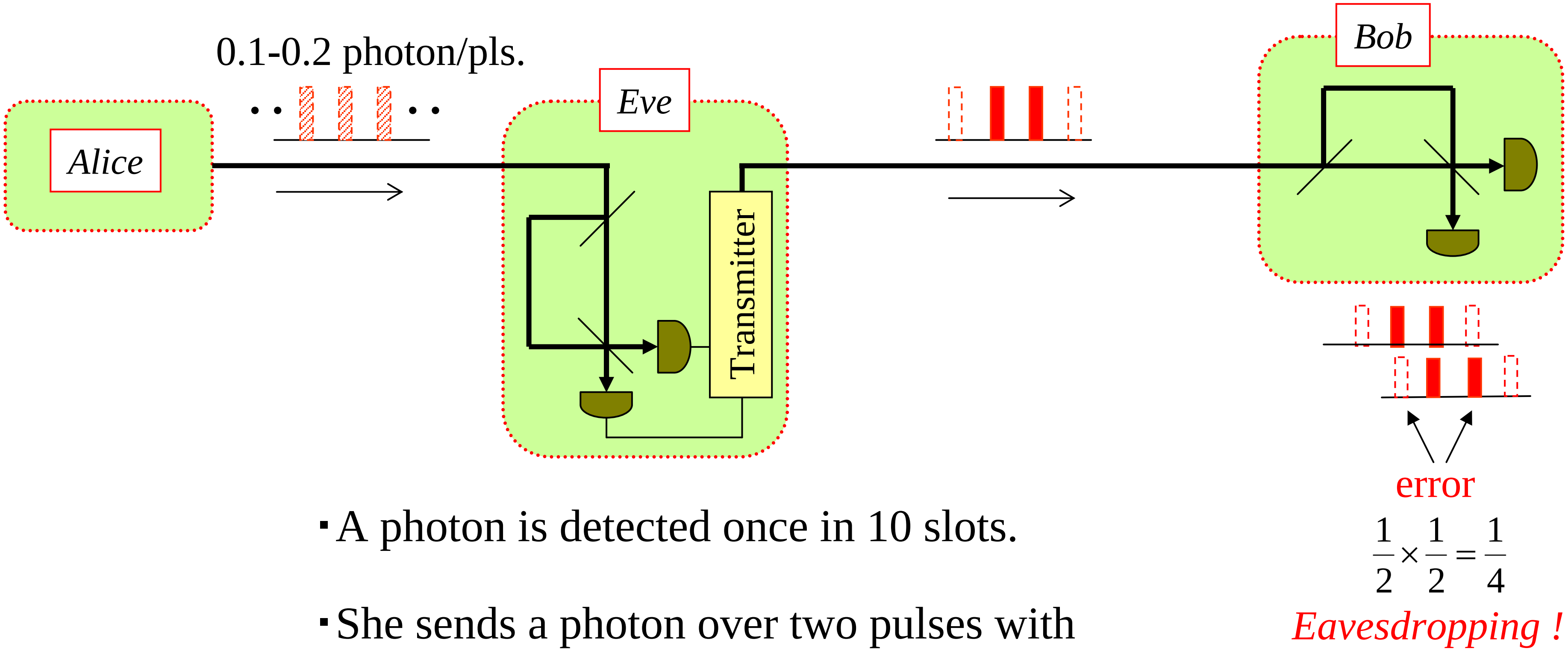


$$\begin{cases} \Delta\theta = 0 \longrightarrow \text{DET-1} \\ \Delta\theta = \pi \longrightarrow \text{DET-2} \end{cases}$$

Features

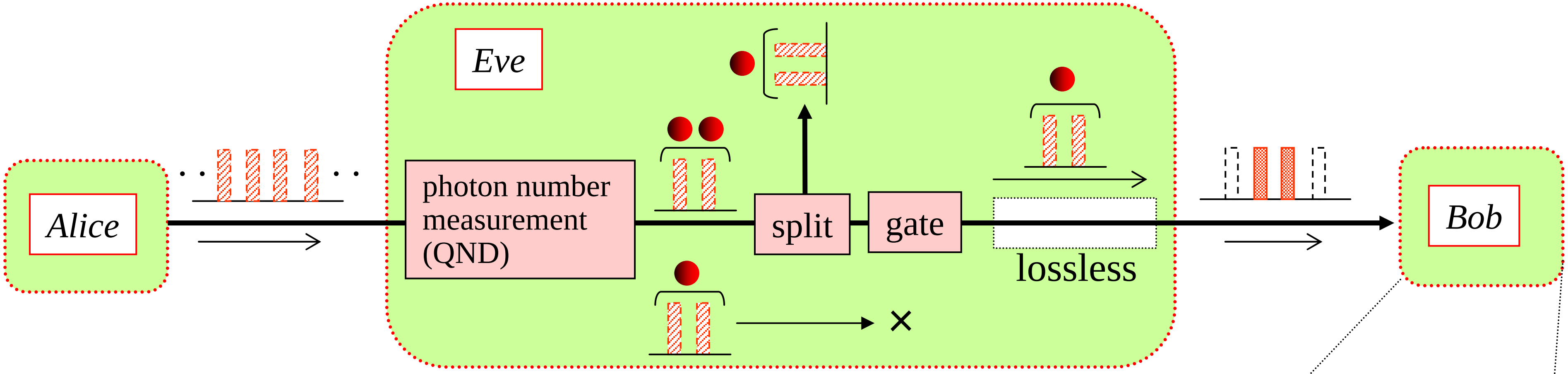
- Simple configuration
- Efficient usage of the time domain
- No photon discarded
- Robustness against photon number splitting attack

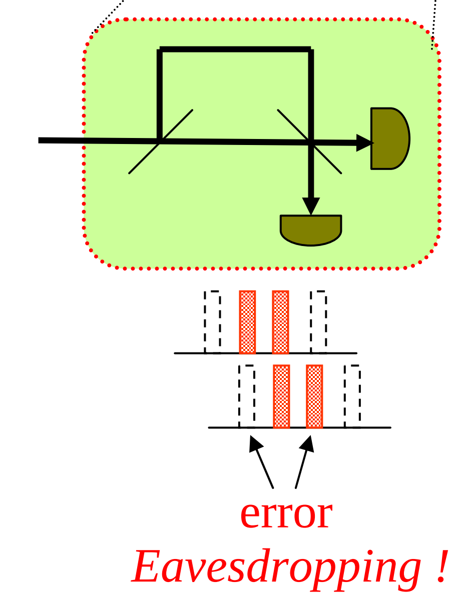
Eavesdropping - intercept & resend -

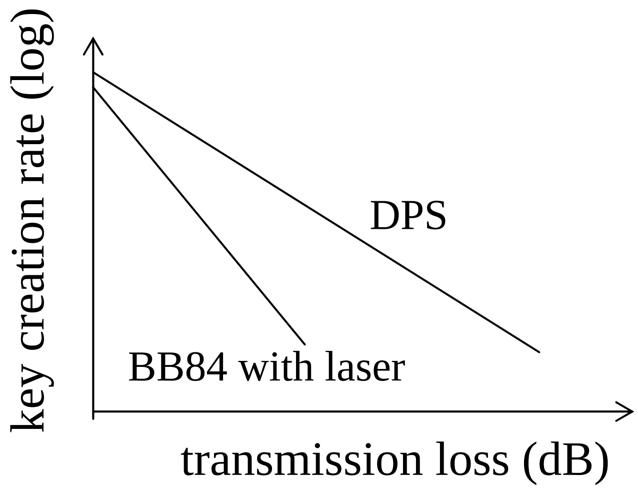


- A photon is detected once in 10 slots.
- She sends a photon over two pulses with measured phase difference.
- She sends nothing for unmeasured slots.

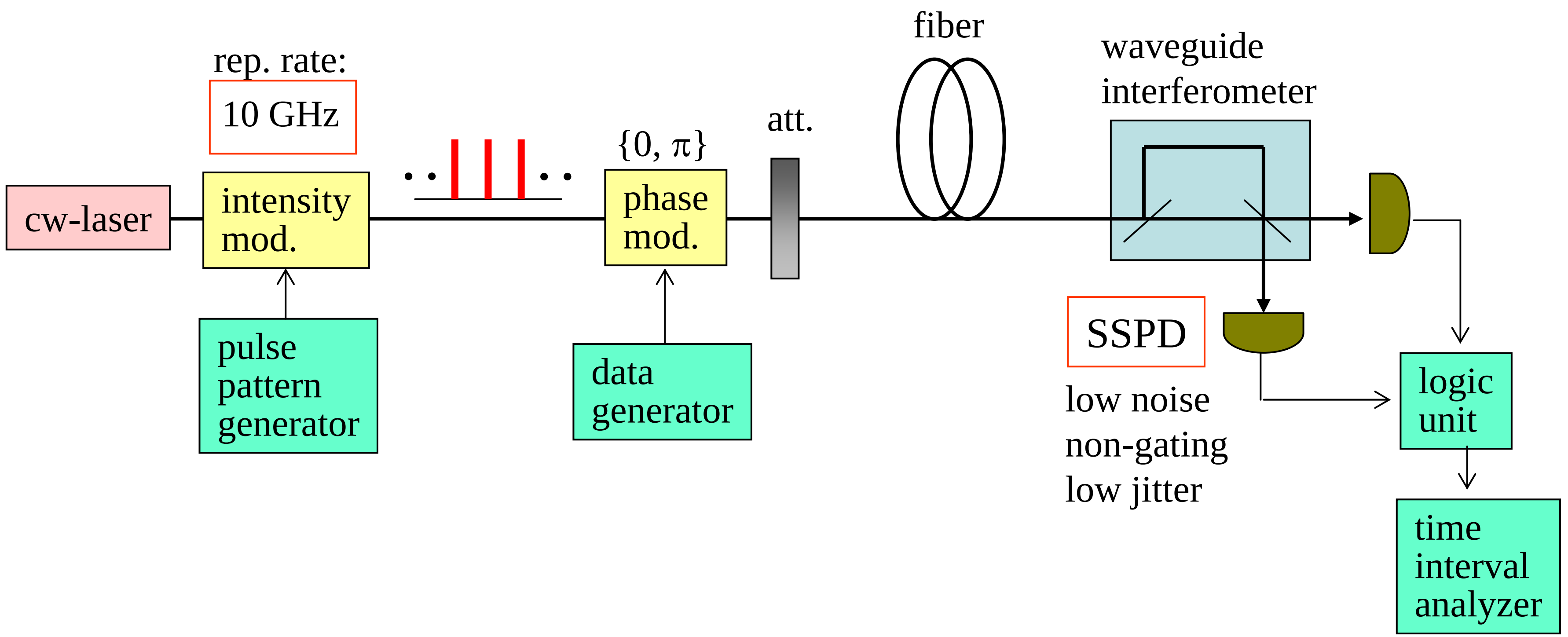
Eavesdropping - photon number splitting -





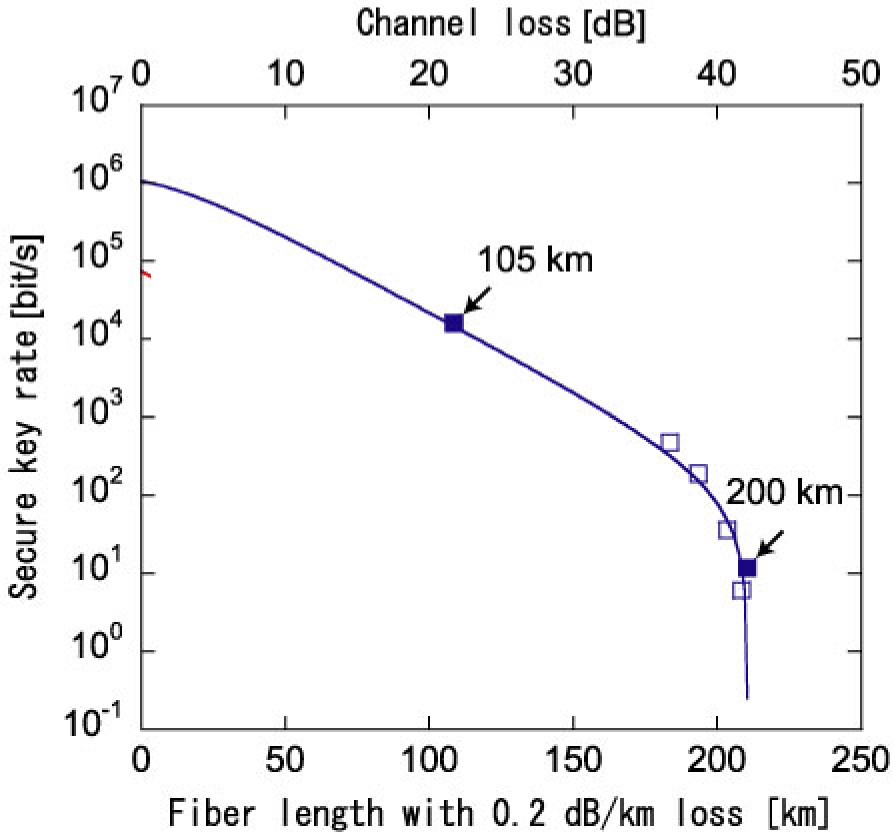


DPS-QKD Experiment



Takesue et al., *Nature Photon*., **1**, 343 (2007)
collaborating with NIST

Result



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

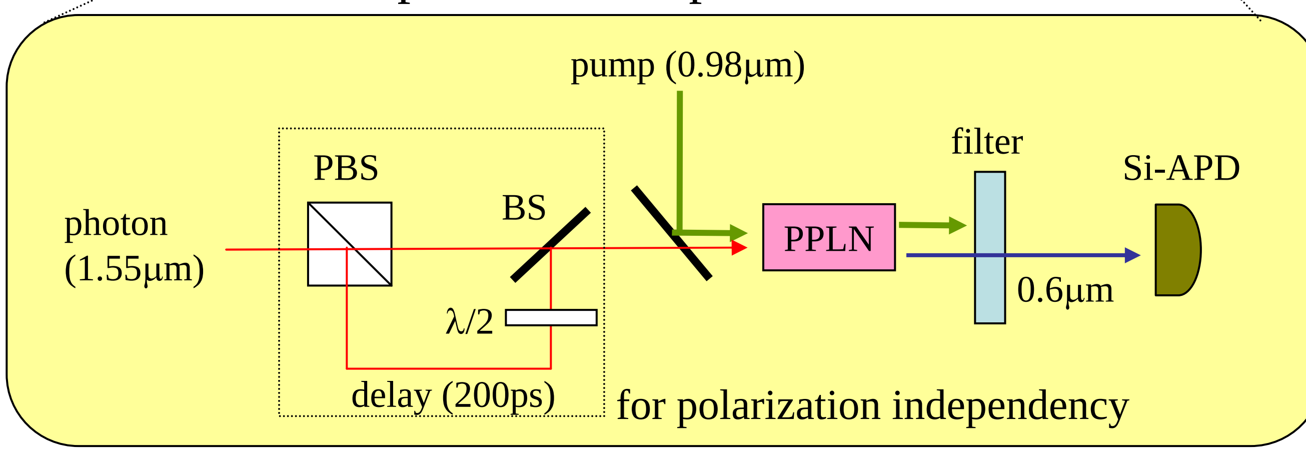
SSPD QE=1.4 %
d.c.=50 cps

Secure key against general individual attack
based on Edo, Takesue, Yamamoto, PRA **73**, 012344 (2006).

Field Transmission

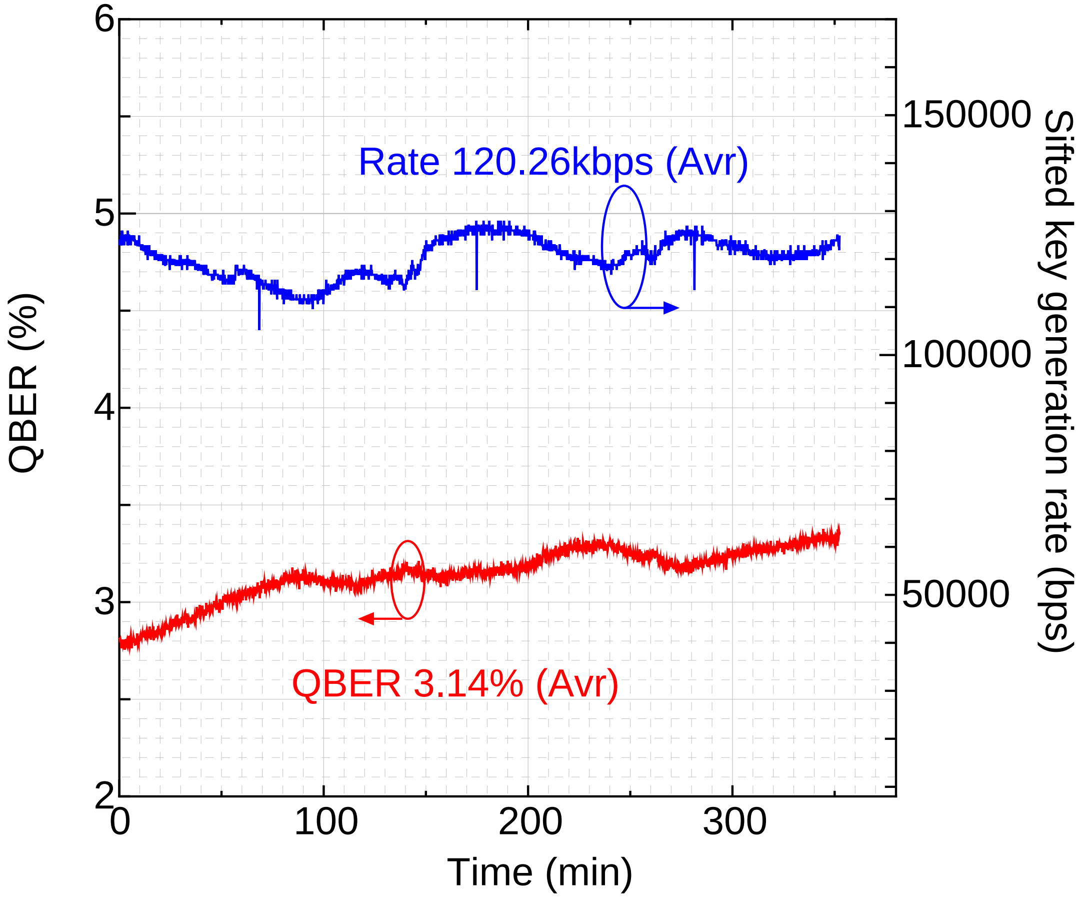
pulse rate: 1 GHz

Up-conversion photon detector



QE: 2 %, d.c.: 2.8 kcps

Result



Sifted key:120 kbit/s with a QBER of 3.14 %.

(1)DPS-QKD

Setup & Protocol

Eavesdropping

Experiments

(2) Modified protocol with decoy pulses

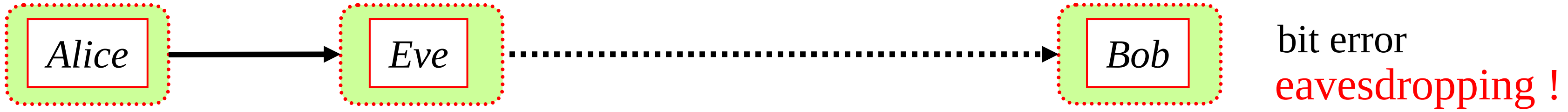
(3) Entanglement-based schemes

(4) DPS-QKD using macroscopic coherent light

(5) DPS quantum secret sharing

Conventionally

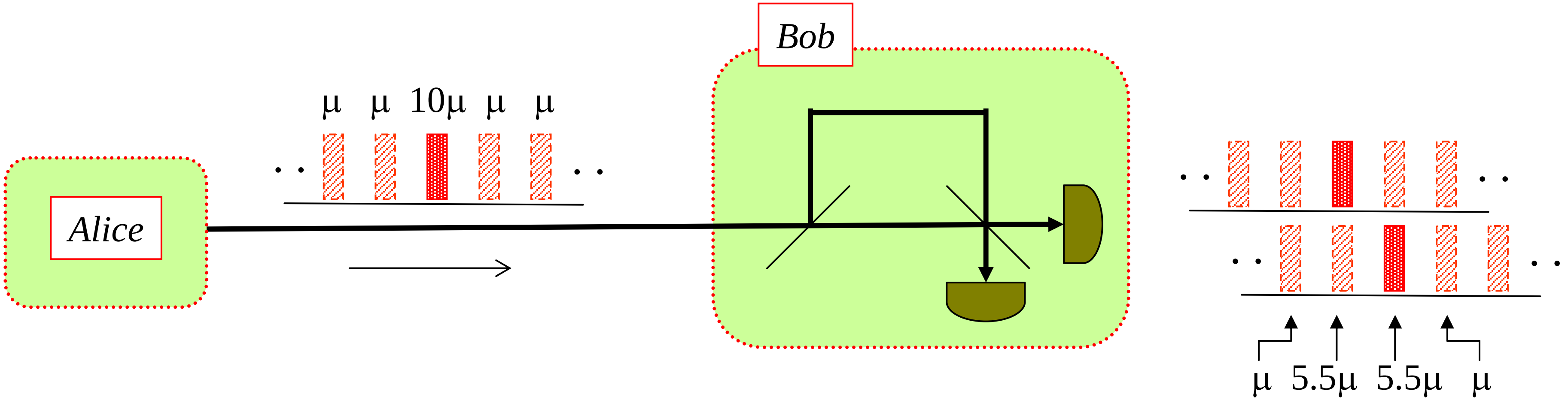
Eavesdropping is found by bit error rate



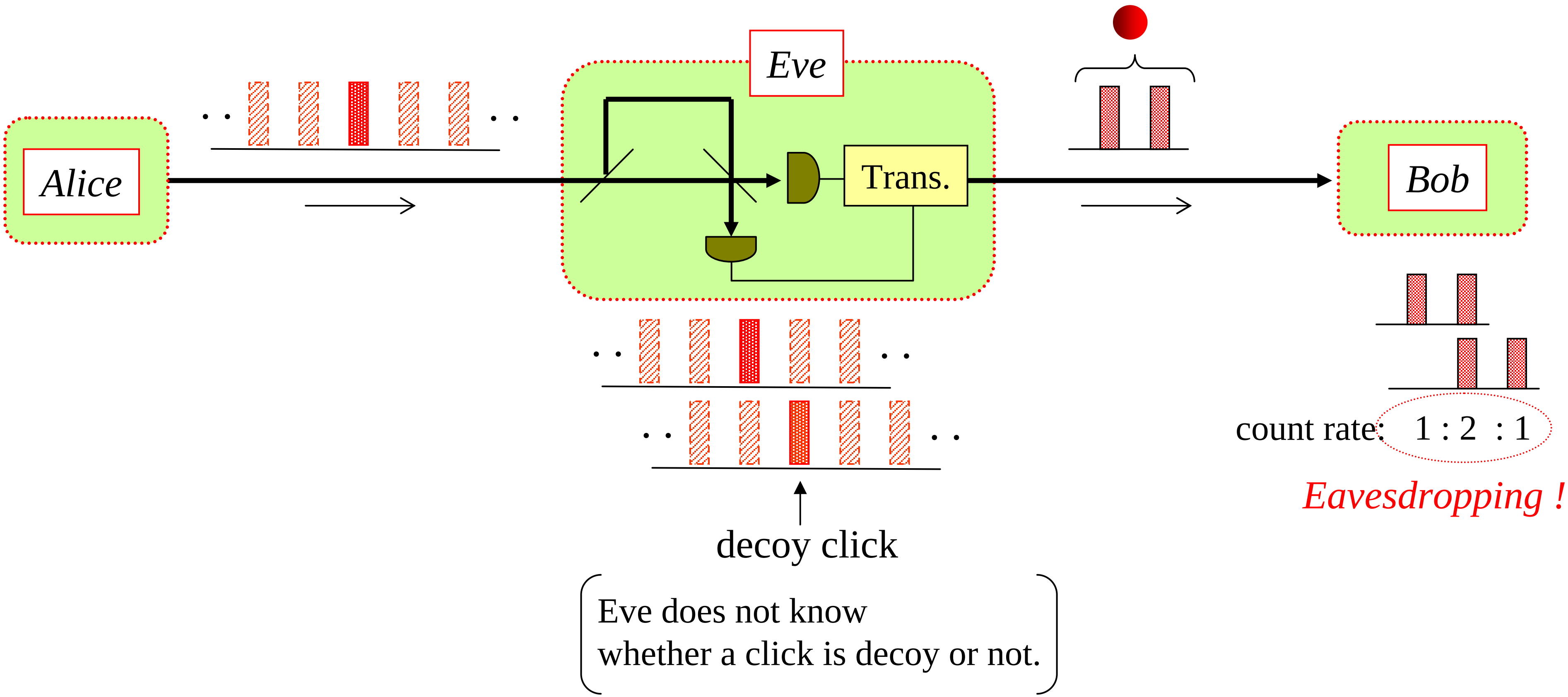
Eve gets some key bits, utilizing system errors.

modified version

DPS-QKD with Decoy Pulses

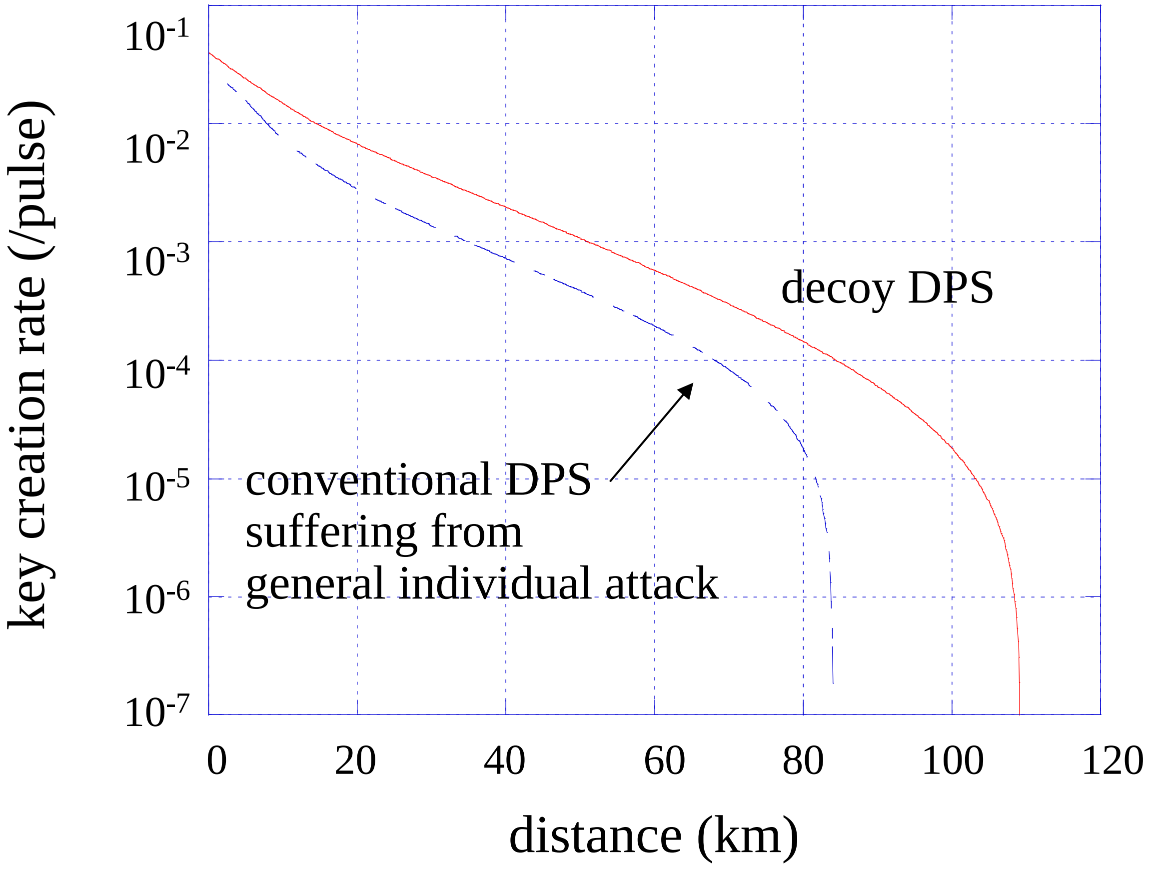


Intercept & Resend against DPS-QKD with Decoy



Intercept & Resend attack is prohibited.

Simulation



fiber loss: 0.25 dB/km
dark count: 10^{-5}/gate
detection efficiency: 0.1
20% fluctuates in detection rate.

Transmission length can be extended.

(1)DPS-QKD

Setup & Protocol

Eavesdropping

Experiments

(2) Modified protocol with decoy pulses

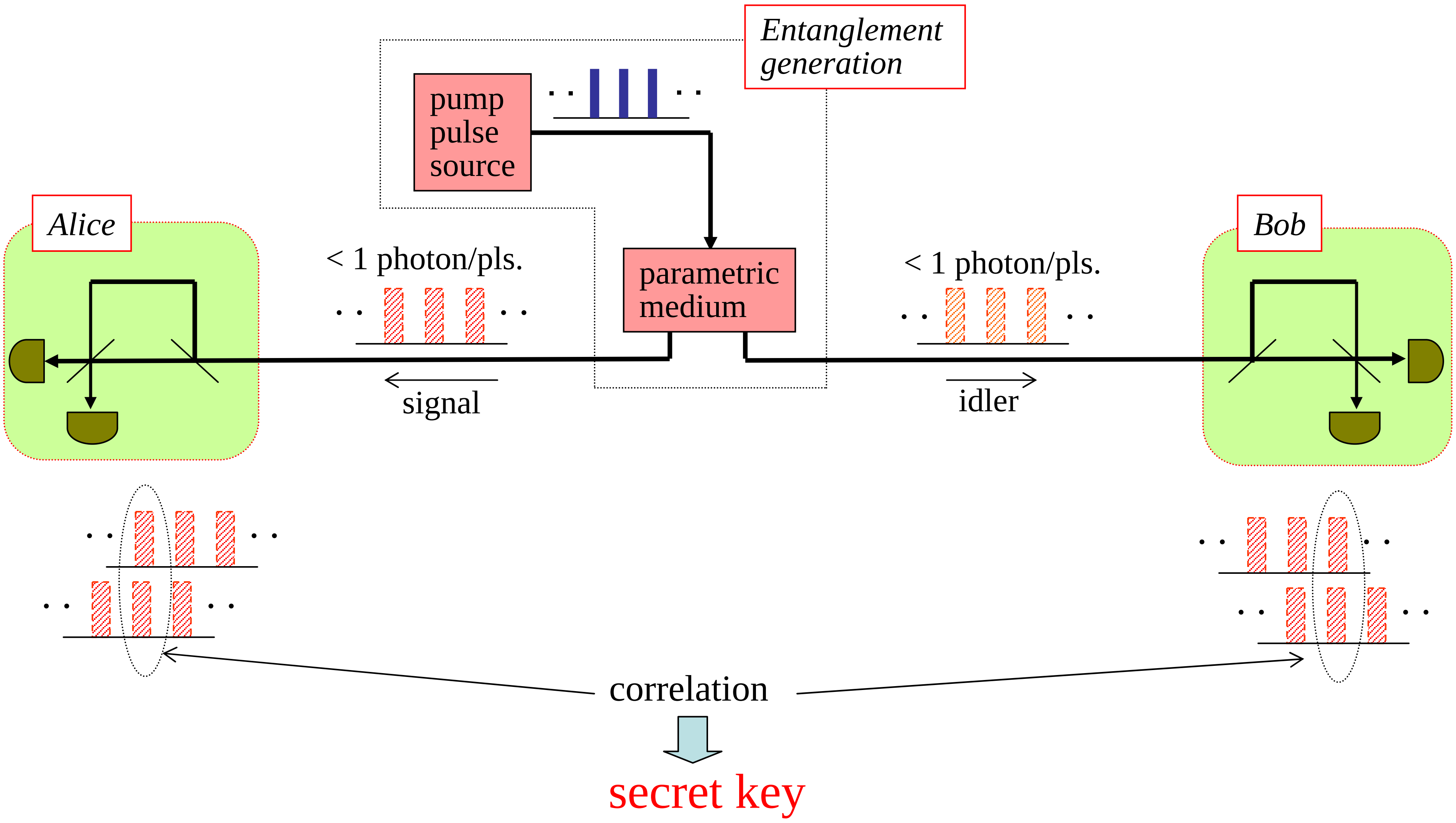
(3) Entanglement-based schemes

(4) DPS-QKD using macroscopic coherent light

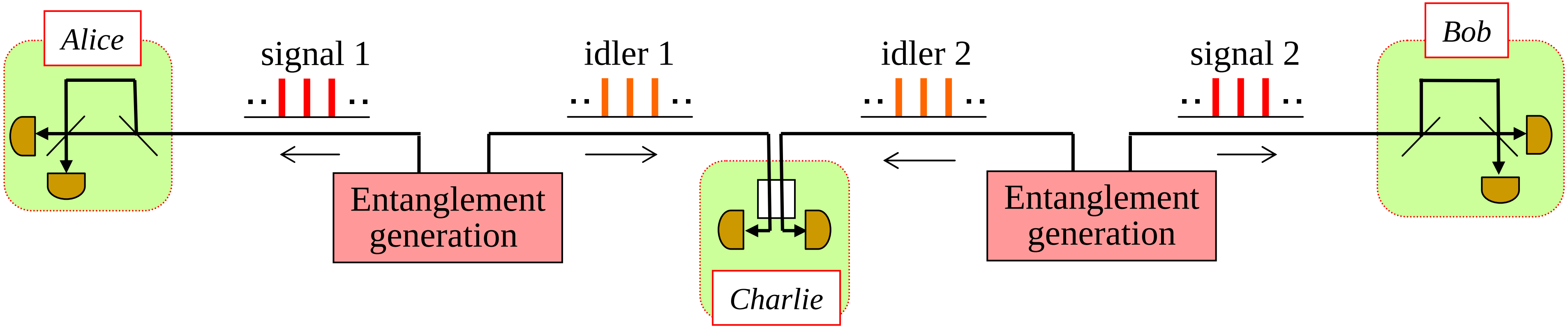
(5) DPS quantum secret sharing

future scheme for long distance

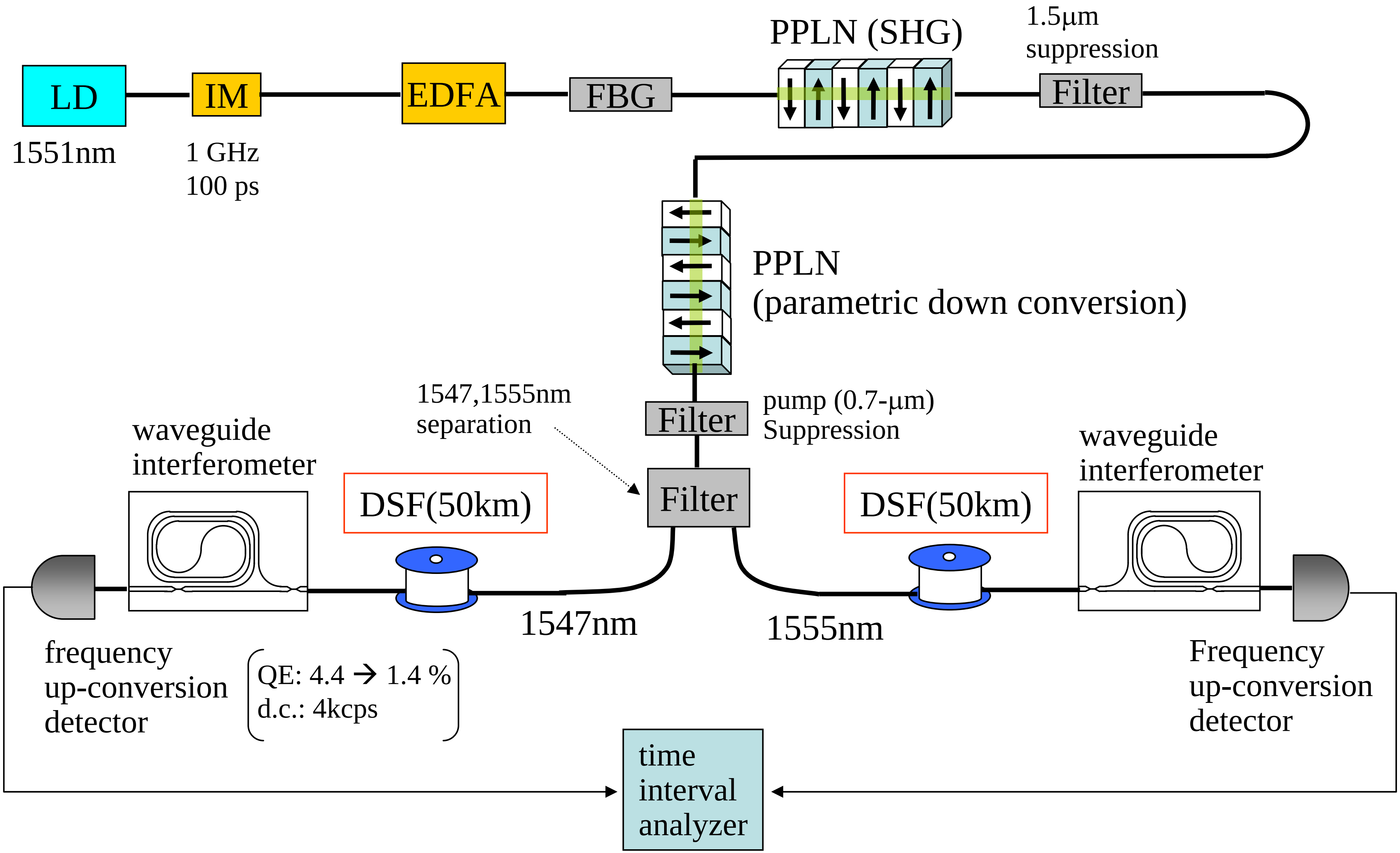
DPS-QKD utilizing Entanglement



Quantum Relaying DPS-QKD

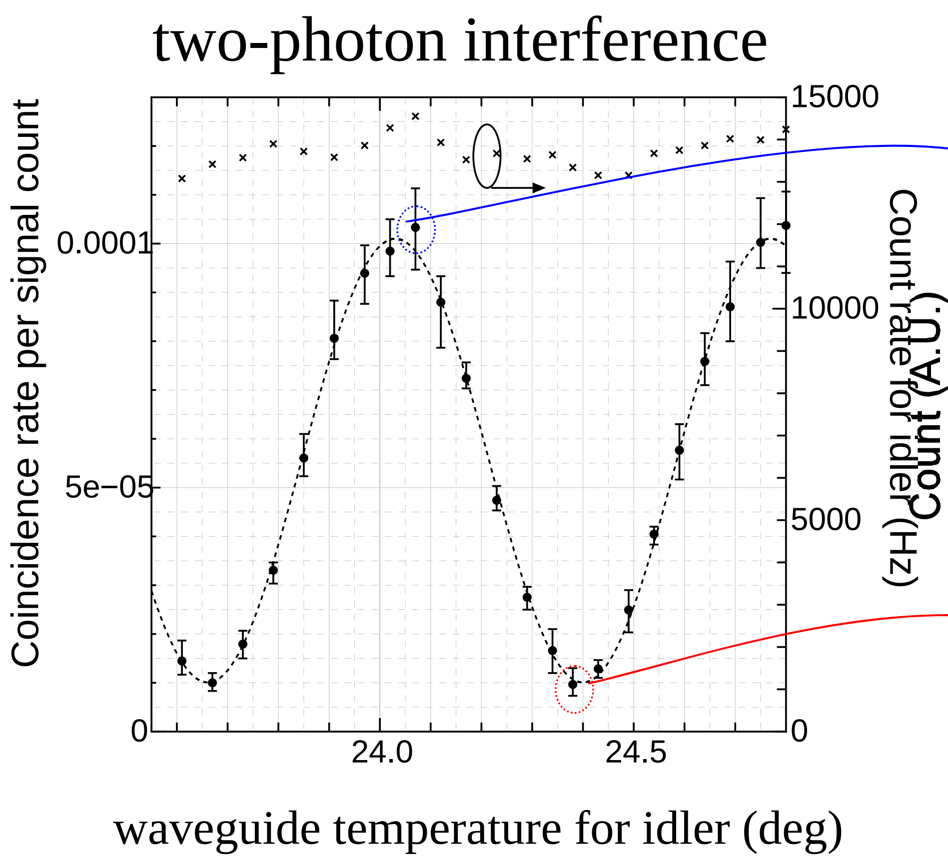


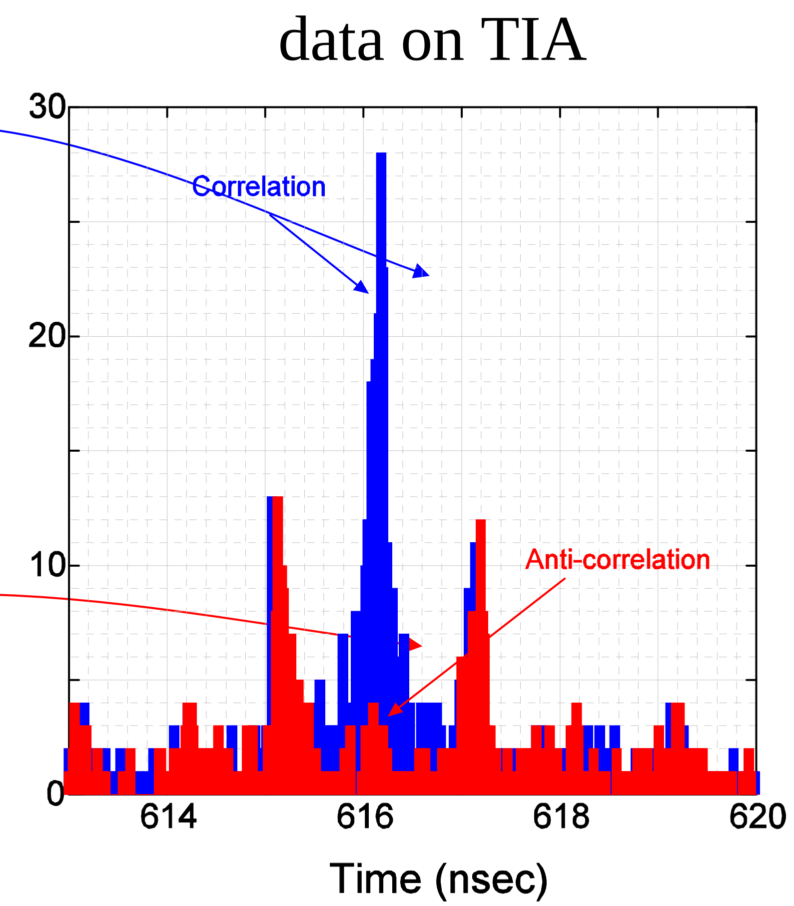
Experiment: Entanglement Transmission



Result

Average number of photon pair: 0.07/pilse.





Visibility of 81.6% without removing background noise.

Time-bin entangled photons are successfully transmitted over 50 x 2 km.

(1)DPS-QKD

- Setup & Protocol
- Eavesdropping
- Experiments

(2) Modified protocol with decoy pulses

(3) Entanglement-based schemes

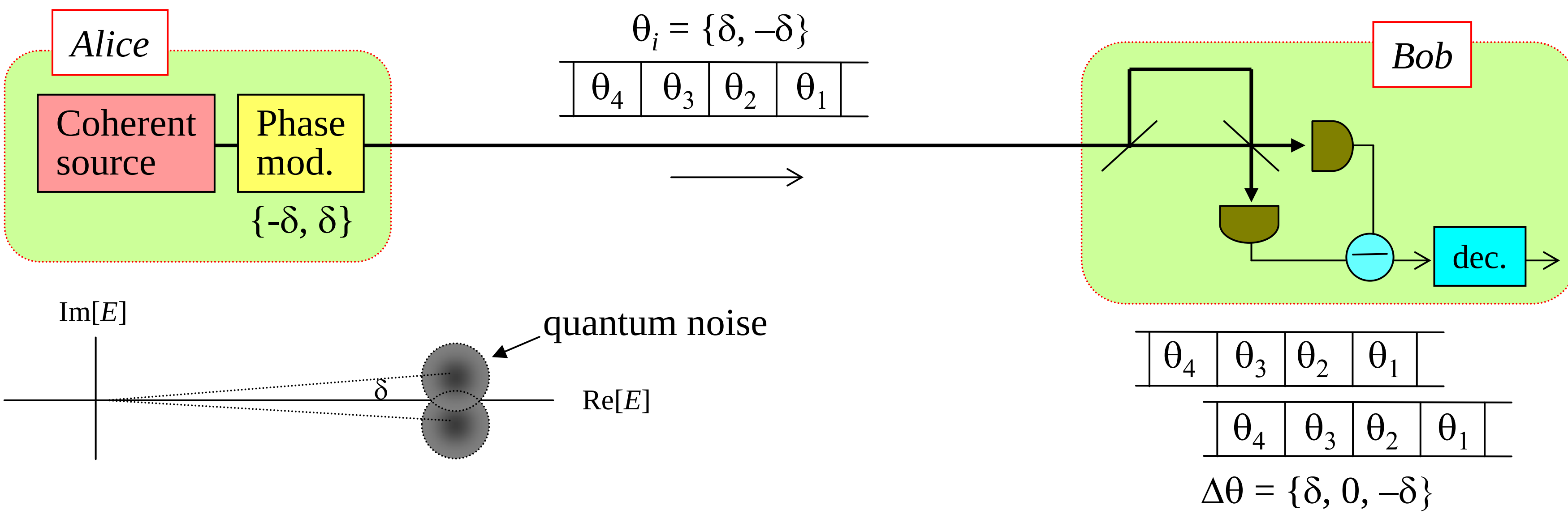
(4) DPS-QKD using macroscopic coherent light

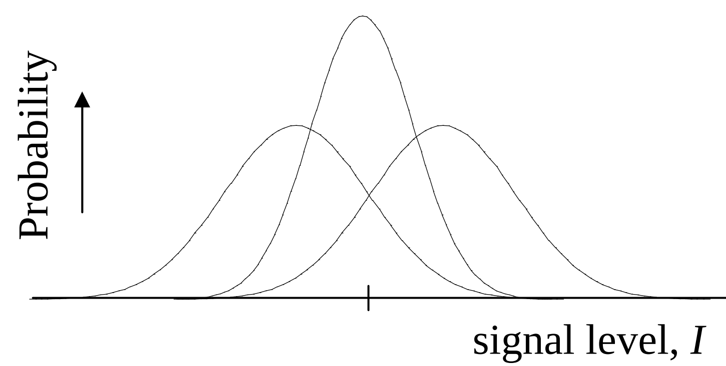
(5) DPS quantum secret sharing

Conventionally, photon counting is needed.

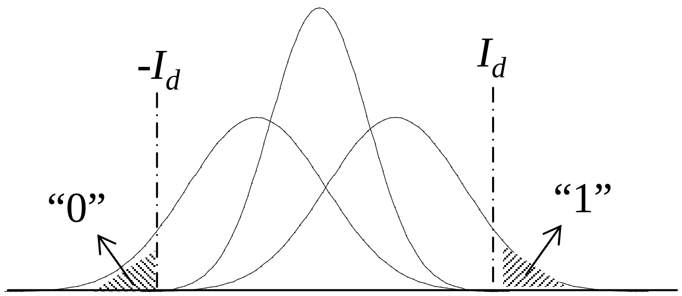
⇩

DPS-QKD using Macroscopic Coherent Light





Protocol



(1) Alice → Bob : Signal transmission

(2) Bob creates bit "1" when $I > I_d$

bit "0" when $I < -I_d$

(3) Bob → Alice : Time slot at which bit was created

(4) Alice creates bit "1" in case $\theta_i - \theta_{i+1} = 2\delta$

bit "0" in case $\theta_i - \theta_{i+1} = -2\delta$

for the time slot at which Bob created bit.

(5) Alice → Bob : Time slots for which $\theta_i - \theta_{i+1} = 0$

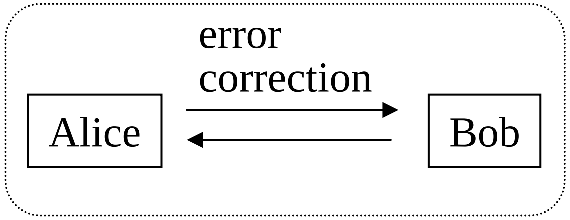
(6) Bob discards the bits for $\theta_i - \theta_{i+1} = 0$

⇩

Secret key

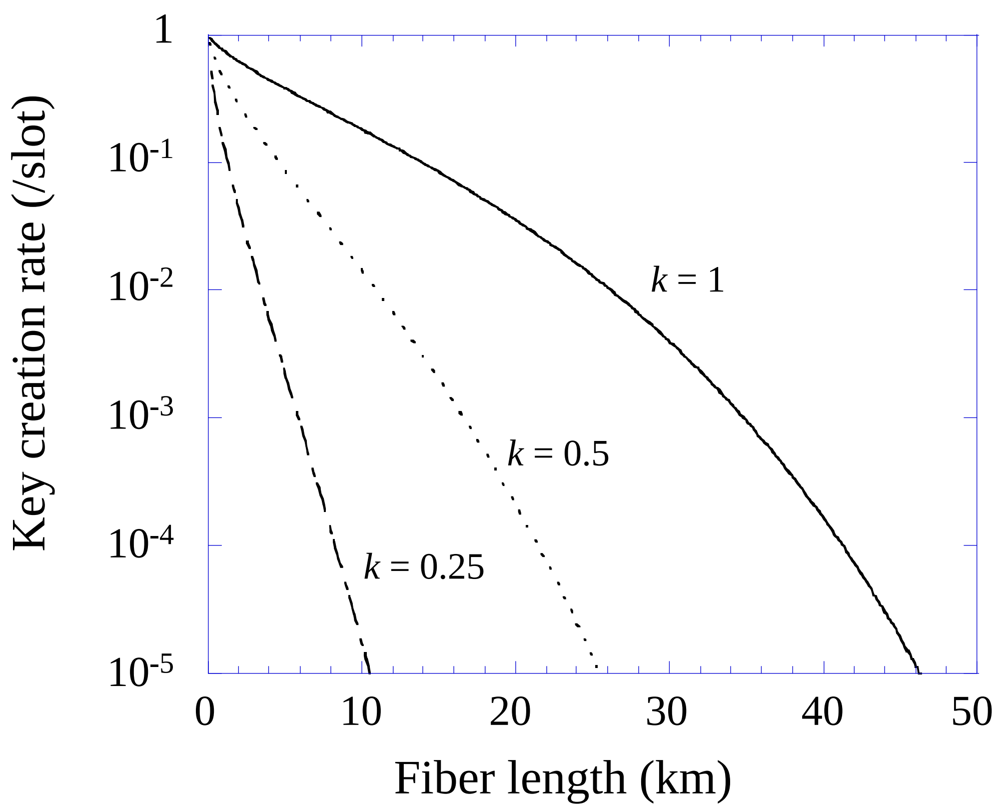
Conventional photodetectors are available.

Simulation (1)



Final key creation rate: $R_s(I_{AB} - \max\{I_{AE}, I_{BE}\})$

- R_s: sifted key rate
- I_{AB}: mutual information between Alice & Bob
- I_{AE}: mutual information between Alice & Eve
- I_{BE}: mutual information between Bob & Eve

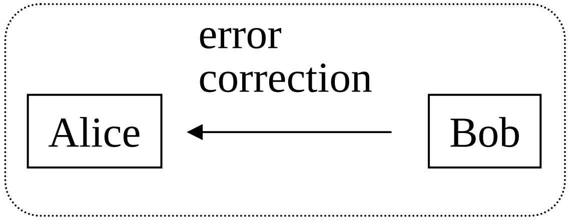


k is a parameter indicating performance of Bob's detector relative to Eve's.

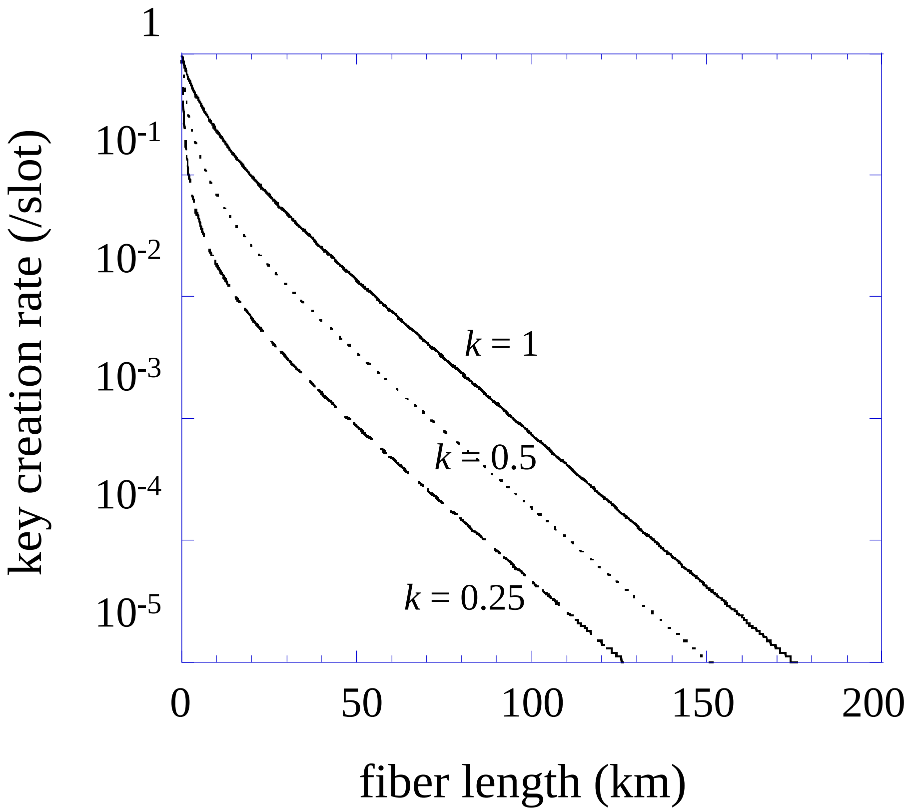
$$k \equiv \frac{\alpha_B}{\alpha_E}\sqrt{\frac{\beta_E}{\beta_B}}$$

- α : detection efficiency
- β : noise factor

Simulation (2)



Final key creation rate: $R_s(I_{AB} - I_{BE})$



(1)DPS-QKD

Setup & Protocol

Eavesdropping

Experiments

(2) Modified protocol with decoy pulses

(3) Entanglement-based schemes

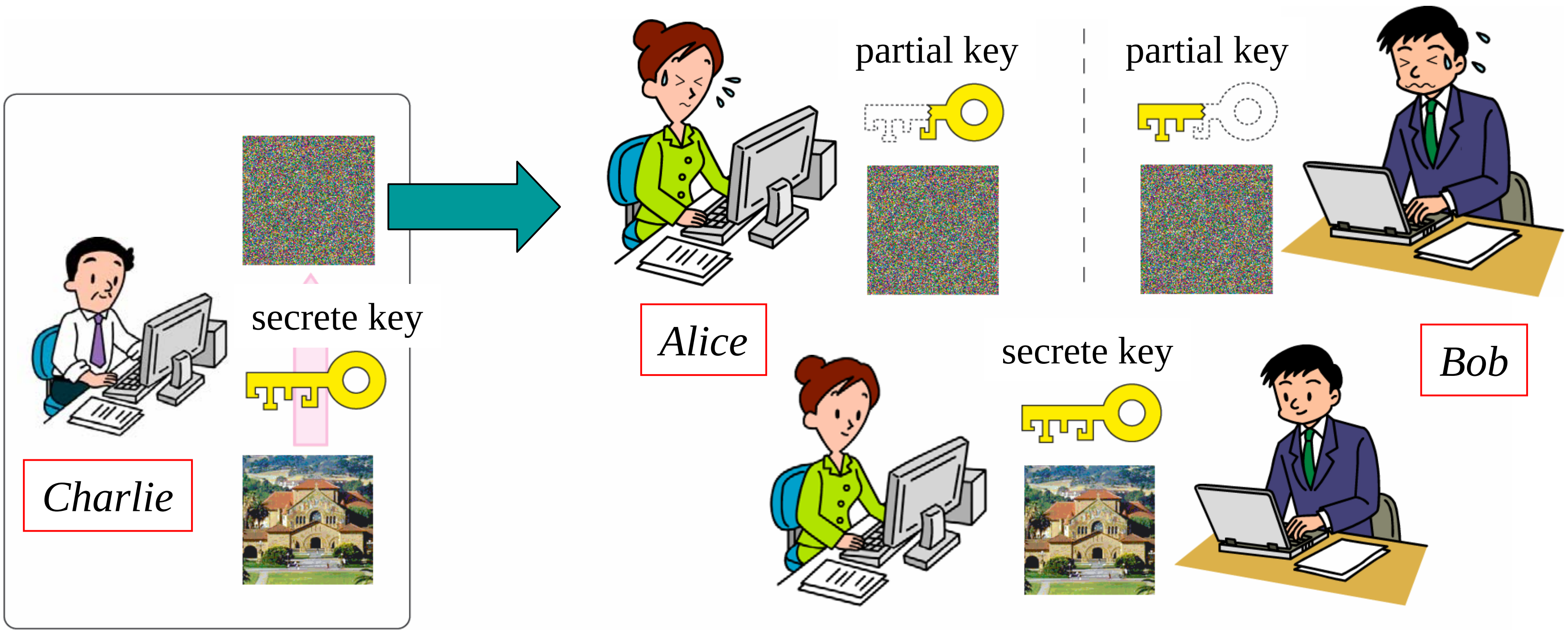
(4) DPS-QKD using macroscopic coherent light

(5) DPS quantum secret sharing

Quantum Secret Sharing (QSS)

Function

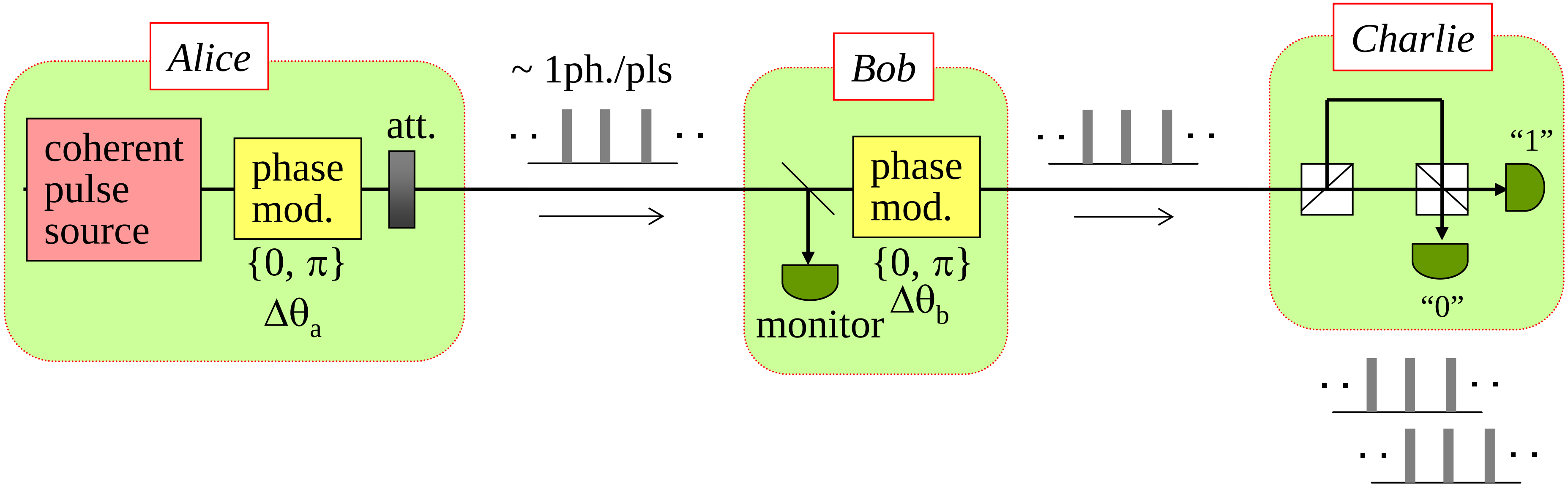
Alice and Bob have fractions of a secret key shared with Charlie.
Alice (or Bob) cannot decipher message from Charlie by her (or him) alone.



Previous scheme

- Entanglement based scheme
- BB84 based scheme

DPS Quantum Secret Sharing (QSS)



Charlie's data are XOR of Alice's and Bob's.

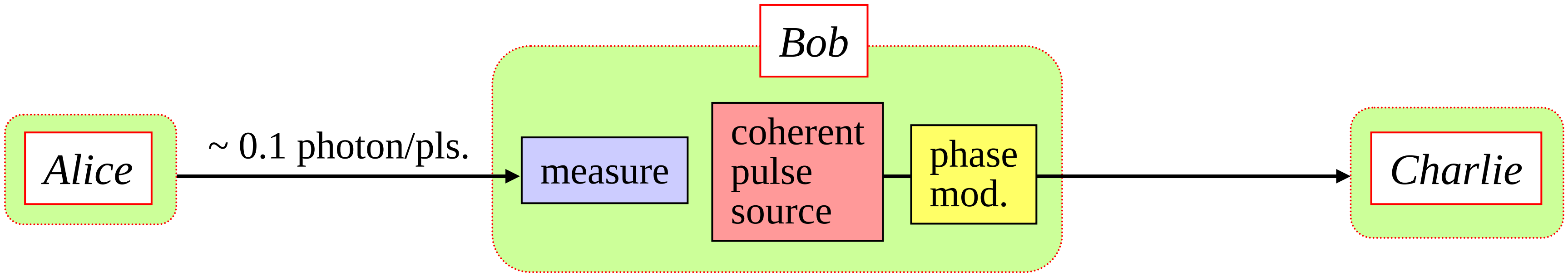
		$\Delta\theta_a$ 0	$\Delta\theta_a$ π
$\Delta\theta_b$	0	"0"	"1"
	π	"1"	"0"

Charlie's data are recovered in collaboration of Alice and Bob.

QSS

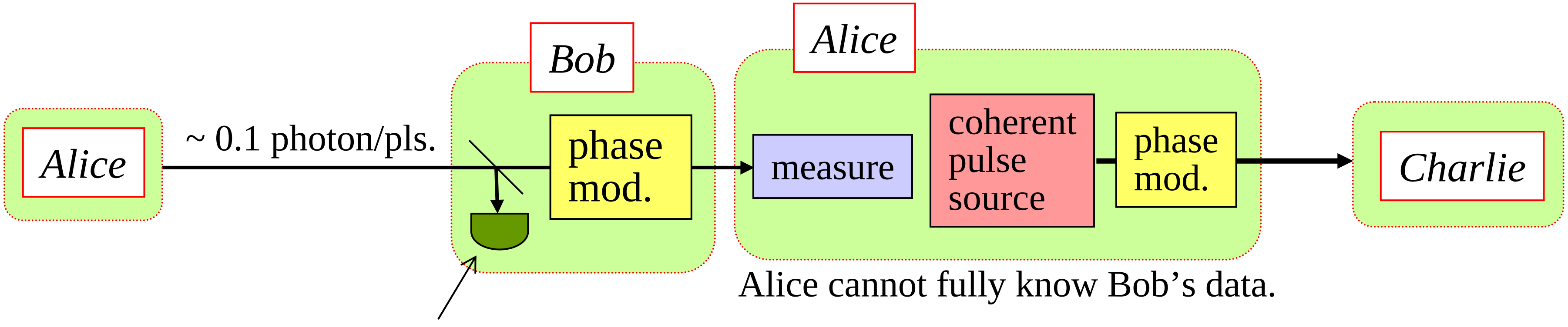
Eavesdropping against DPS-QSS

Eavesdropping by dishonest Bob



Bob cannot fully know Alice’s data.

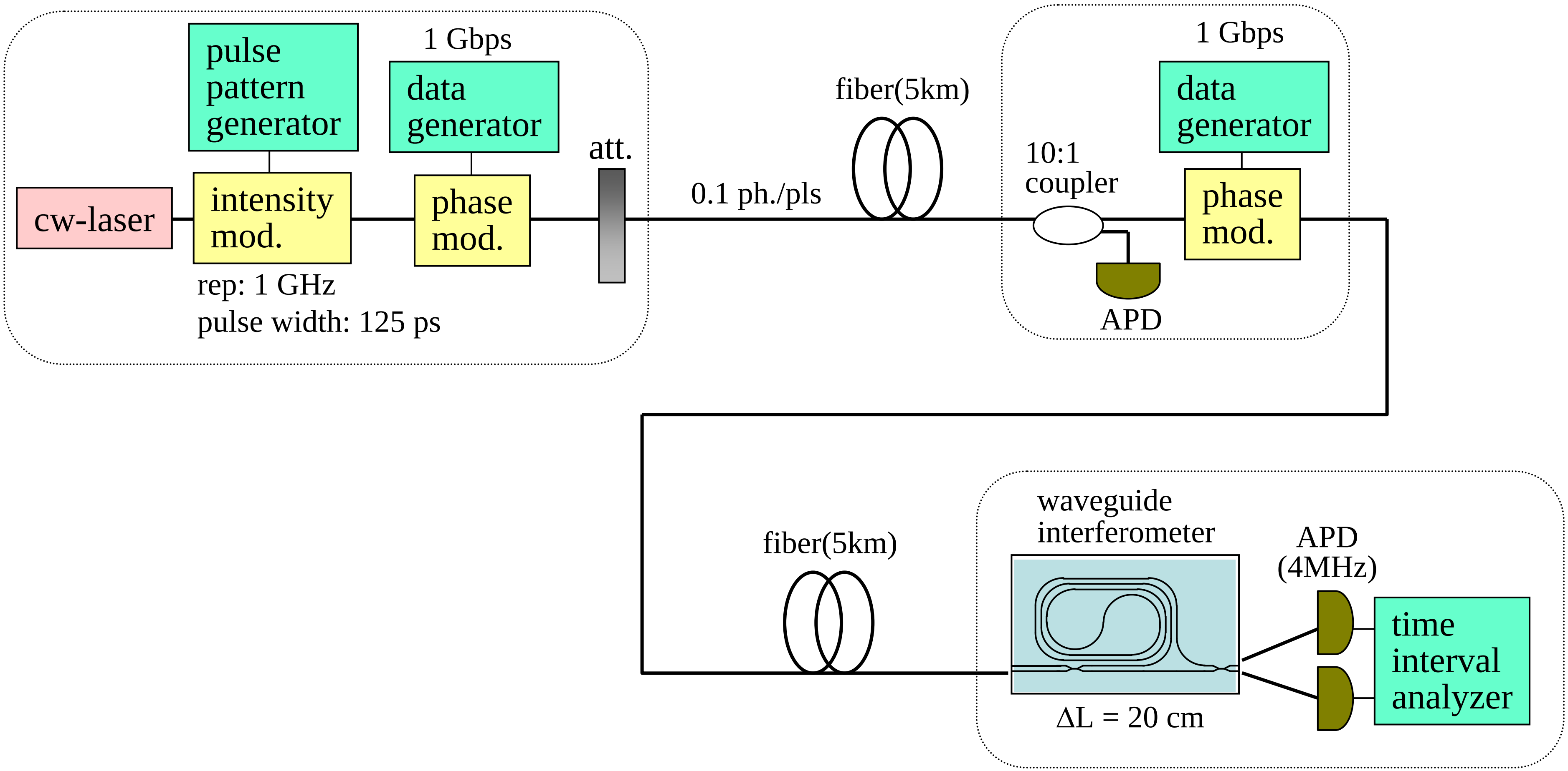
Eavesdropping by dishonest Alice



Alice cannot fully know Bob’s data.

Bob’s monitoring forces Alice to send 0.1 ph/pls.

Experiment



QBER: 6.4 %
sifted key rate: 3.9 kbps

error correction
privacy amplification

final key rate: 1.5 kbps

Summary

DPS-QKD is presented.

(1) Setup & protocol, eavesdropping, experiments

Simple configuration, no photon discarded.

Robust against photon-number-splitting attack

12 bit/s at 200 km, 17 kbit/s at 100 km for secure key (with SSPD)

(2) Modified protocol with decoy slots

Intercept-resend attack is prohibited.

(3) Entanglement-based schemes

Experiment utilizing fiber four-wave mixing for entanglement generation.

(4) DPS-QKD using macroscopic coherent light

Conventional photodetectors are available.

(5) DPS quantum secret sharing

Simple configuration