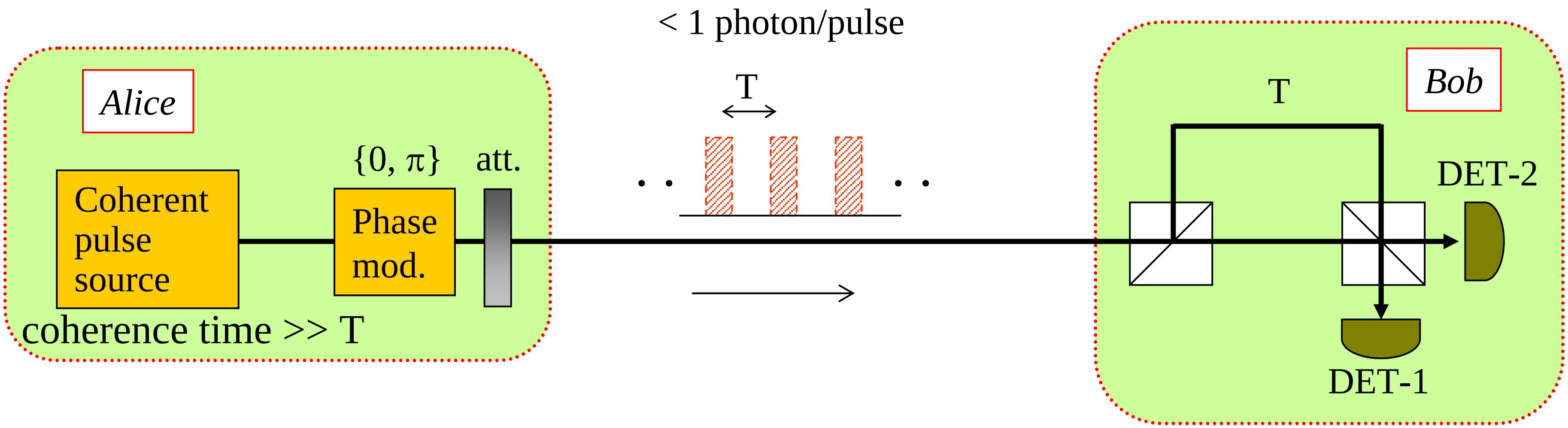
Differential-Phase-Shift Quantum Key Distribution

K. Inoue, H. Takesue, T. Honjo

Osaka University
NTT Basic Research Laboratories
JST CREST

Contents

Setup



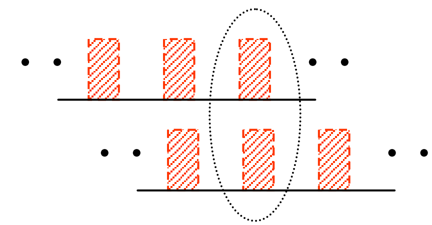
Protocol

(1) Alice → Bob: pulse trains

(2) Bob →Alice: photon detection time

(3) Alice knows which detector clicked.

(4) Key bits are created as
DET-1 = "0"   DET-2 = "1"



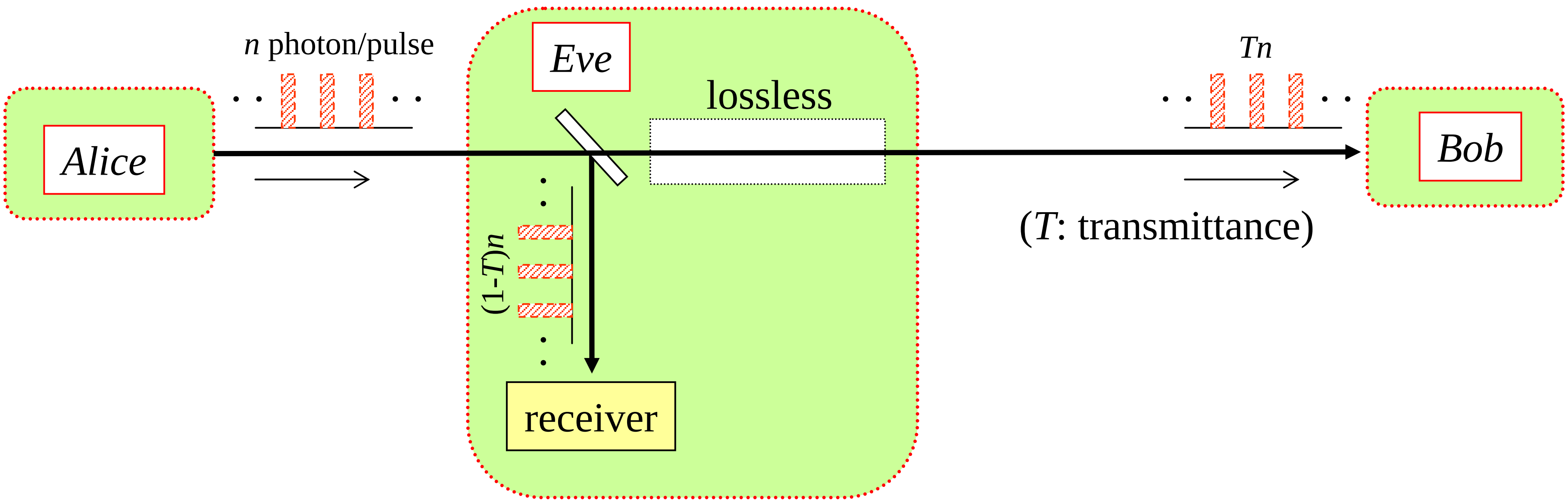
$\Delta\theta = 0 \longrightarrow$ DET-1

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

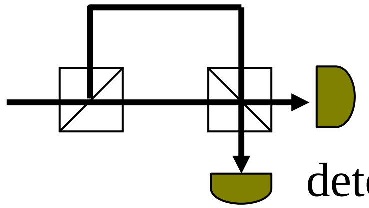
Features

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

Eavesdropping against DPS-QKD (1)
- beam splitting -



Passive receiver @ Eve



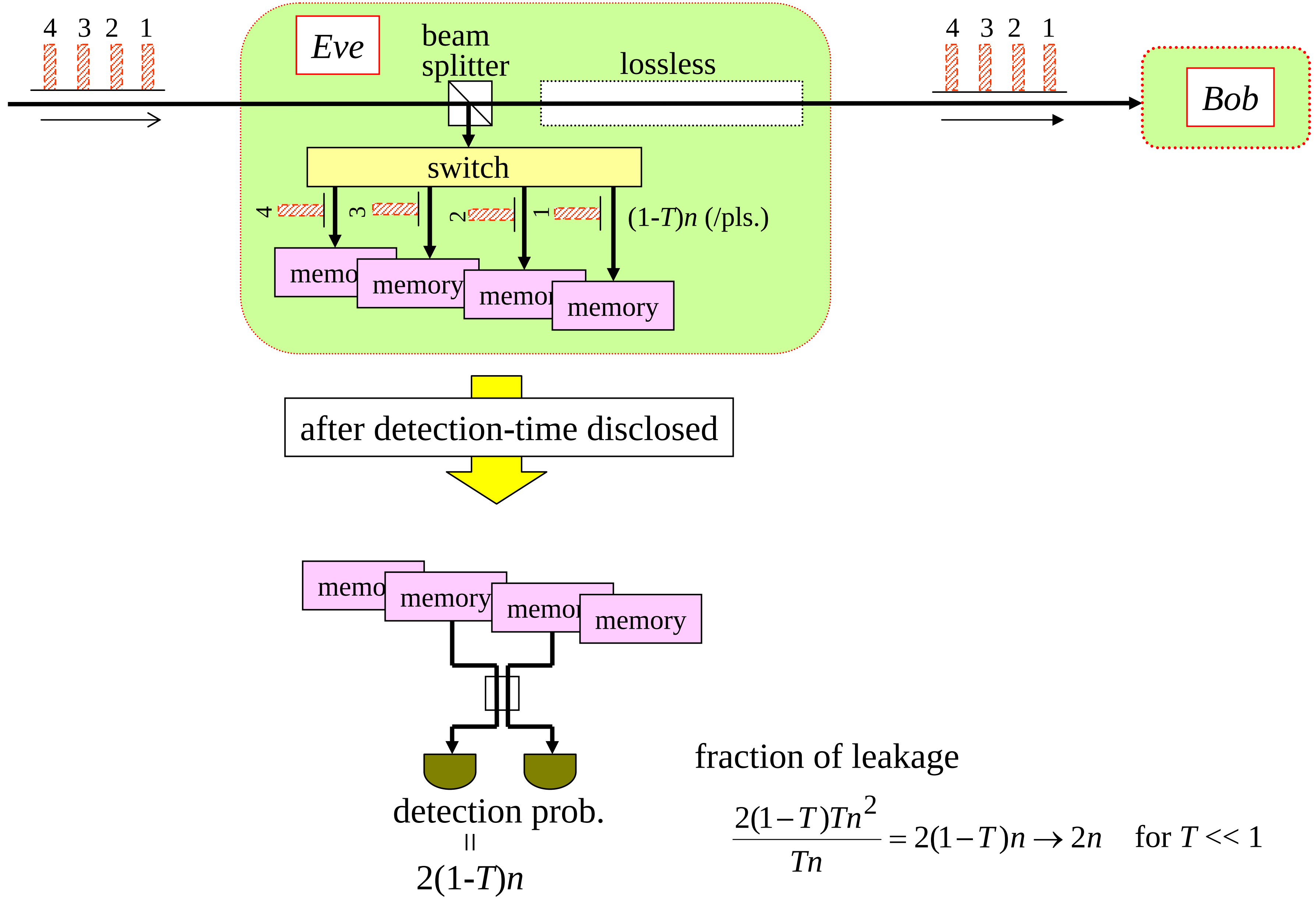
Coincident rate between Bob and Eve

$$Tn \times (1-T)n = (1-T)Tn^2$$

fraction of leakage

$$\frac{(1-T)Tn^2}{Tn} = (1-T)n \rightarrow n \quad \text{for } T << 1$$

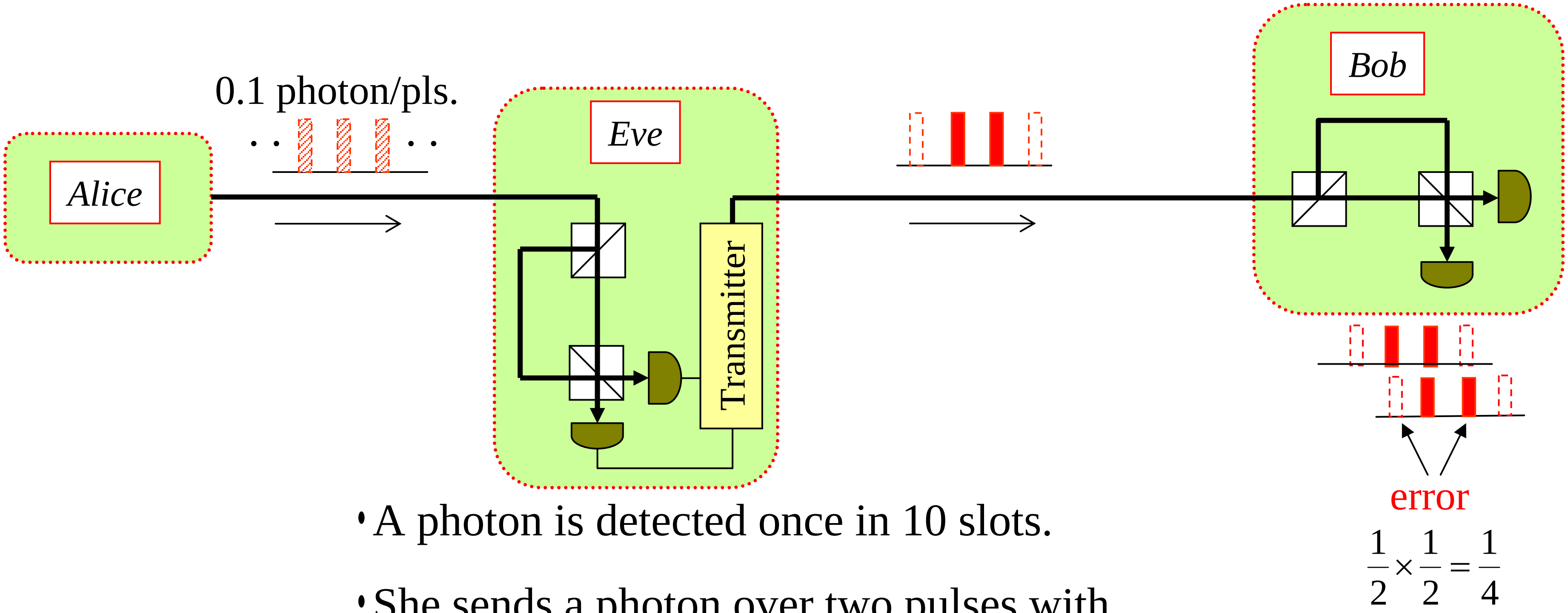
Receiver with quantum memory



fraction of leakage

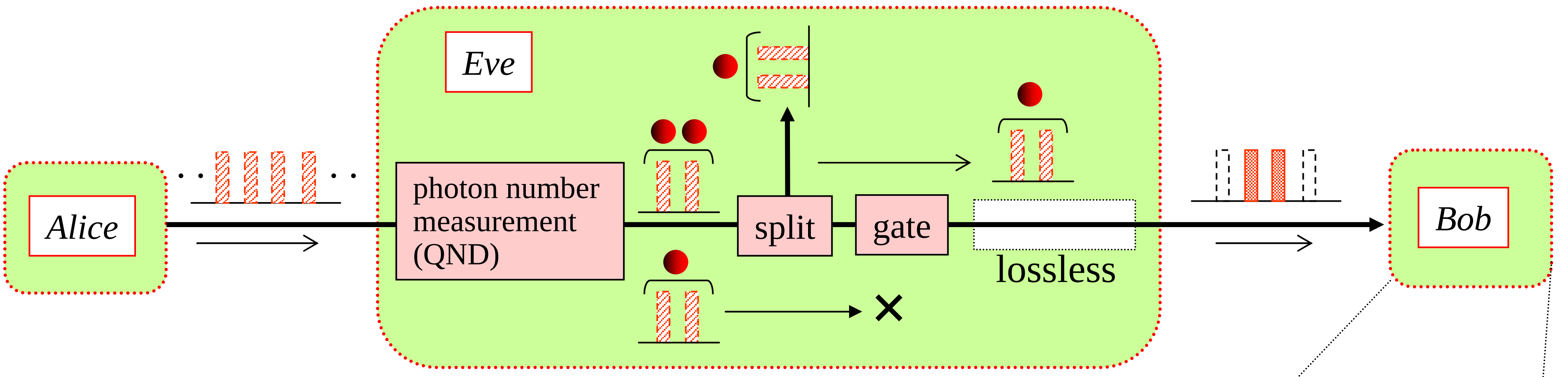
$$\frac{2(1-T)Tn^2}{Tn} = 2(1-T)n \to 2n \quad \text{for } T << 1$$

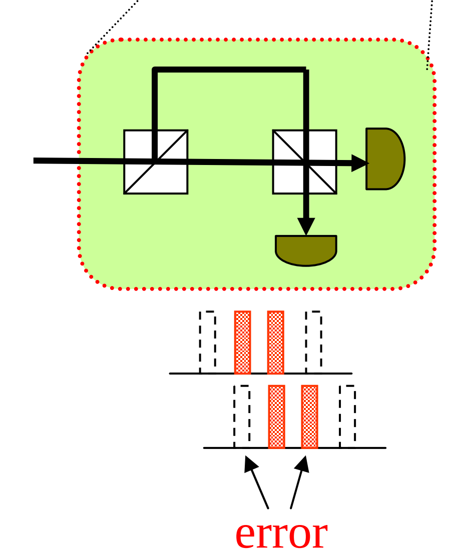
Eavesdropping against DPS-QKD (2)
- intercept & resend -



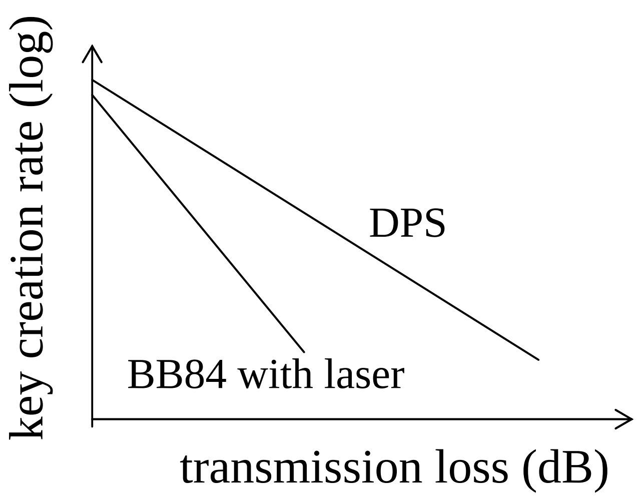
- A photon is detected once in 10 slots.
- She sends a photon over two pulses with measured phase difference.
- She sends nothing for unmeasured slots.

Eavesdropping against DPS-QKD (3)
- photon number splitting -



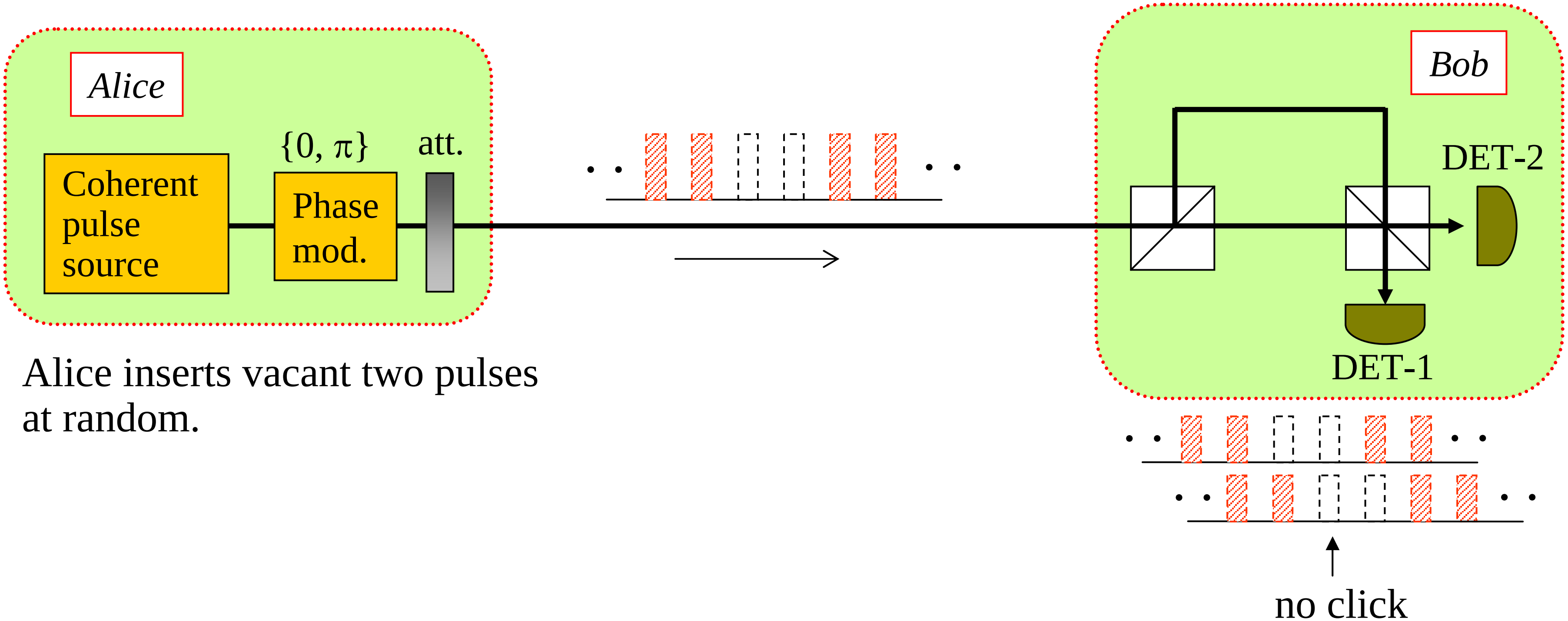


Induced error is independent of transmission loss.



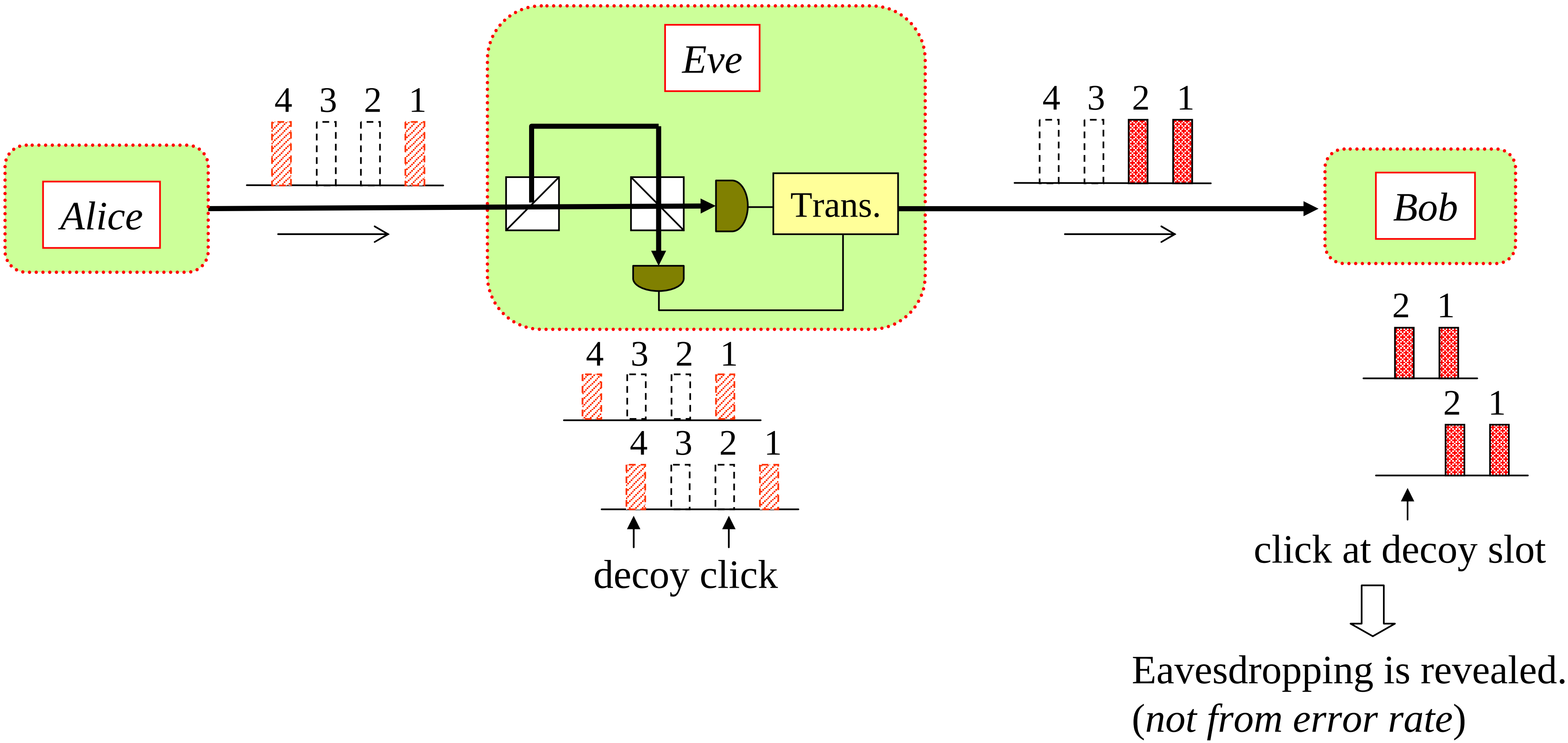
modified version

Differential-Phase-Shift QKD with Decoy Slots



Alice inserts vacant two pulses at random.

Intercept & Resend against DPS-QKD with Decoy Slots

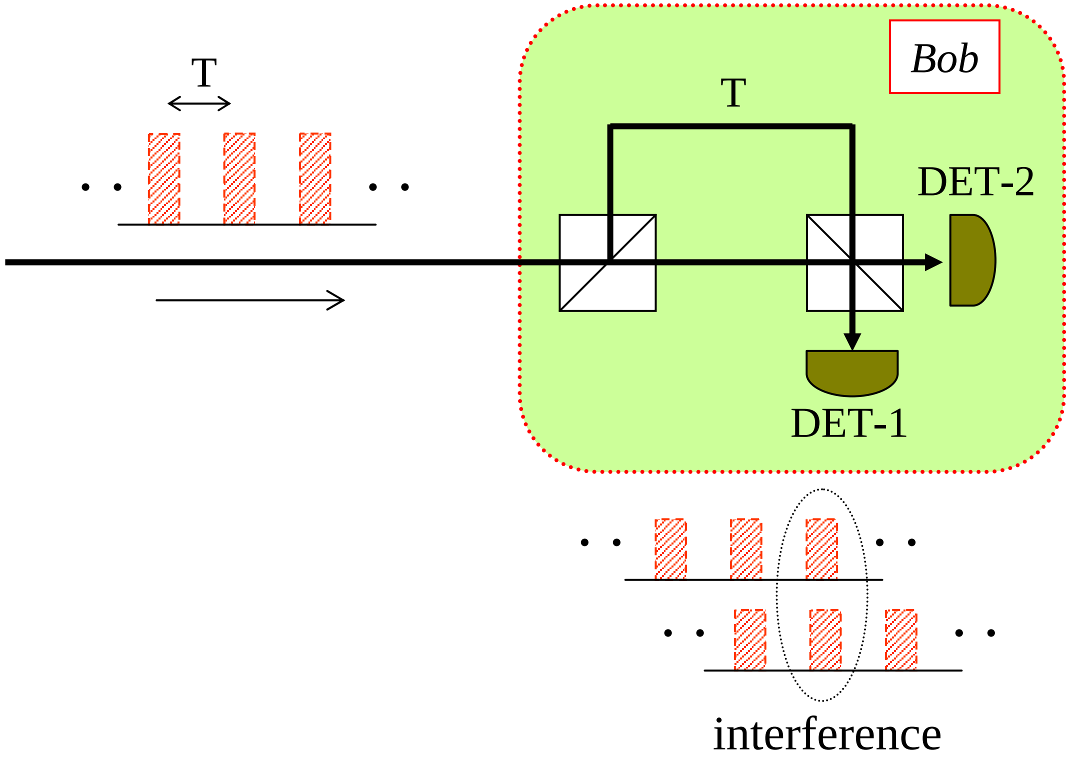


Intercept & Resend attack is prohibited,
provided that dark count rate is constant.

supplement

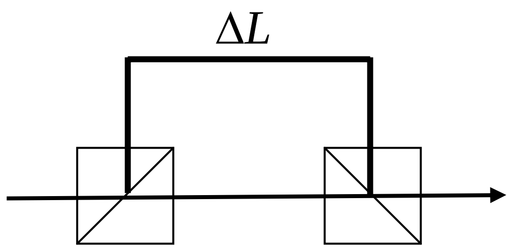
Requirement for light source in DPS-QKD

In DPS-QKD, it is assumed that
(the coherence time of light source) >> (pulse interval).



Question: How long the coherence time should be ?

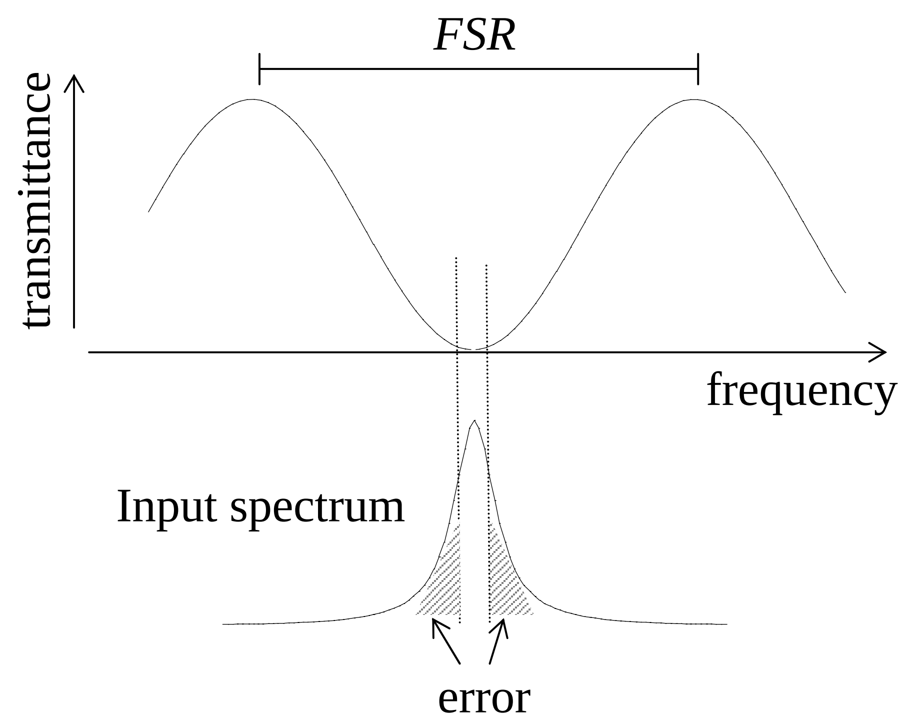
Coherence time is evaluated by spectral linewidth.



$$T = \sin^2\left[\frac{k\Delta L}{2}\right] = \sin^2\left[\frac{\pi f}{FSR}\right]$$

$$\left(FSR = \frac{v}{\Delta L} \text{: free spectrum range} \right)$$

Transmittance of Mach-Zehnder interferometer



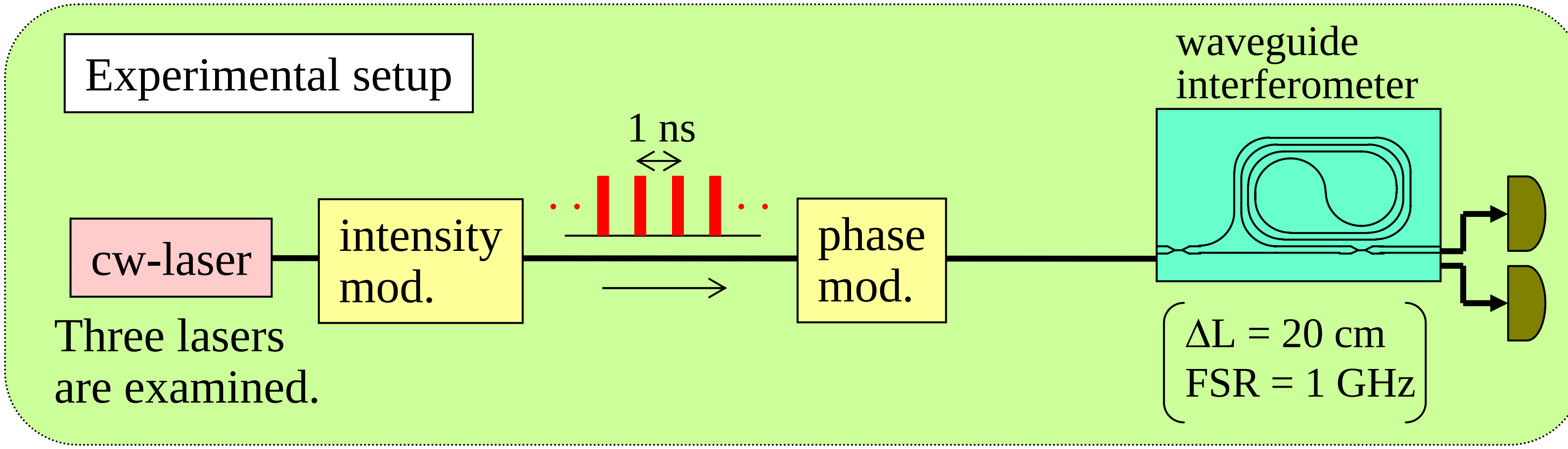
$$\text{Error rate} = \int_{-\infty}^{\infty} T(f)F(f)\,df$$

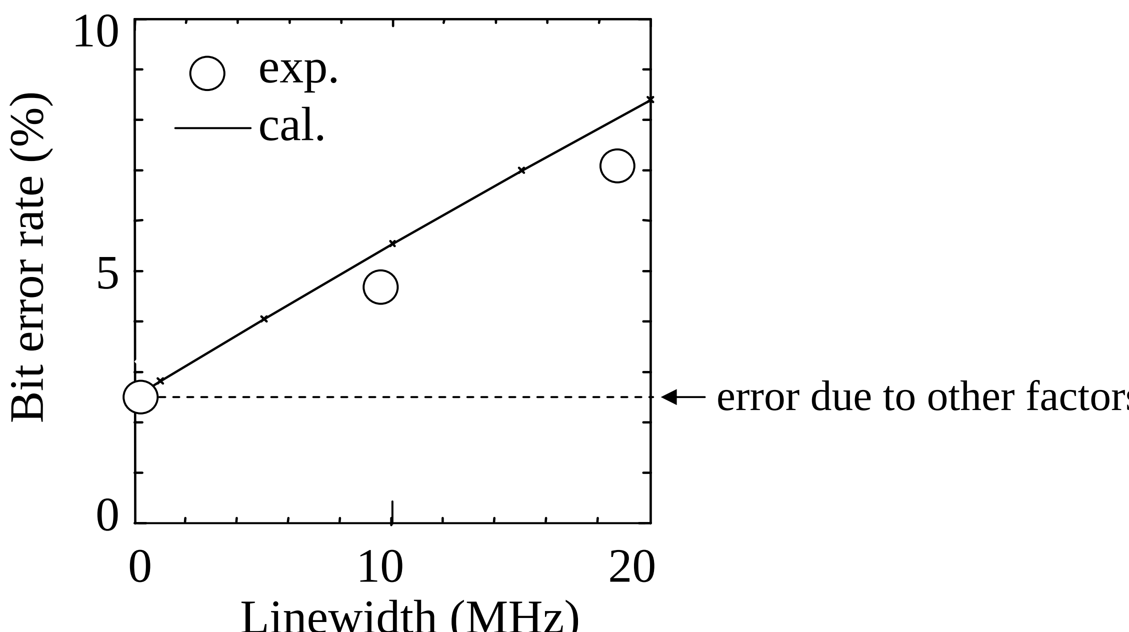
$$T(f) = \sin^2\left[\pi \frac{f}{FSR}\right] \quad \text{: transmittance of MZI}$$

$$F(f) = \frac{\delta f}{2\pi} \cdot \frac{1}{f^2 + (\delta f/2)^2} \quad \text{: spectrum shape}$$

(δf: linewidth)

Experiment & Calculation

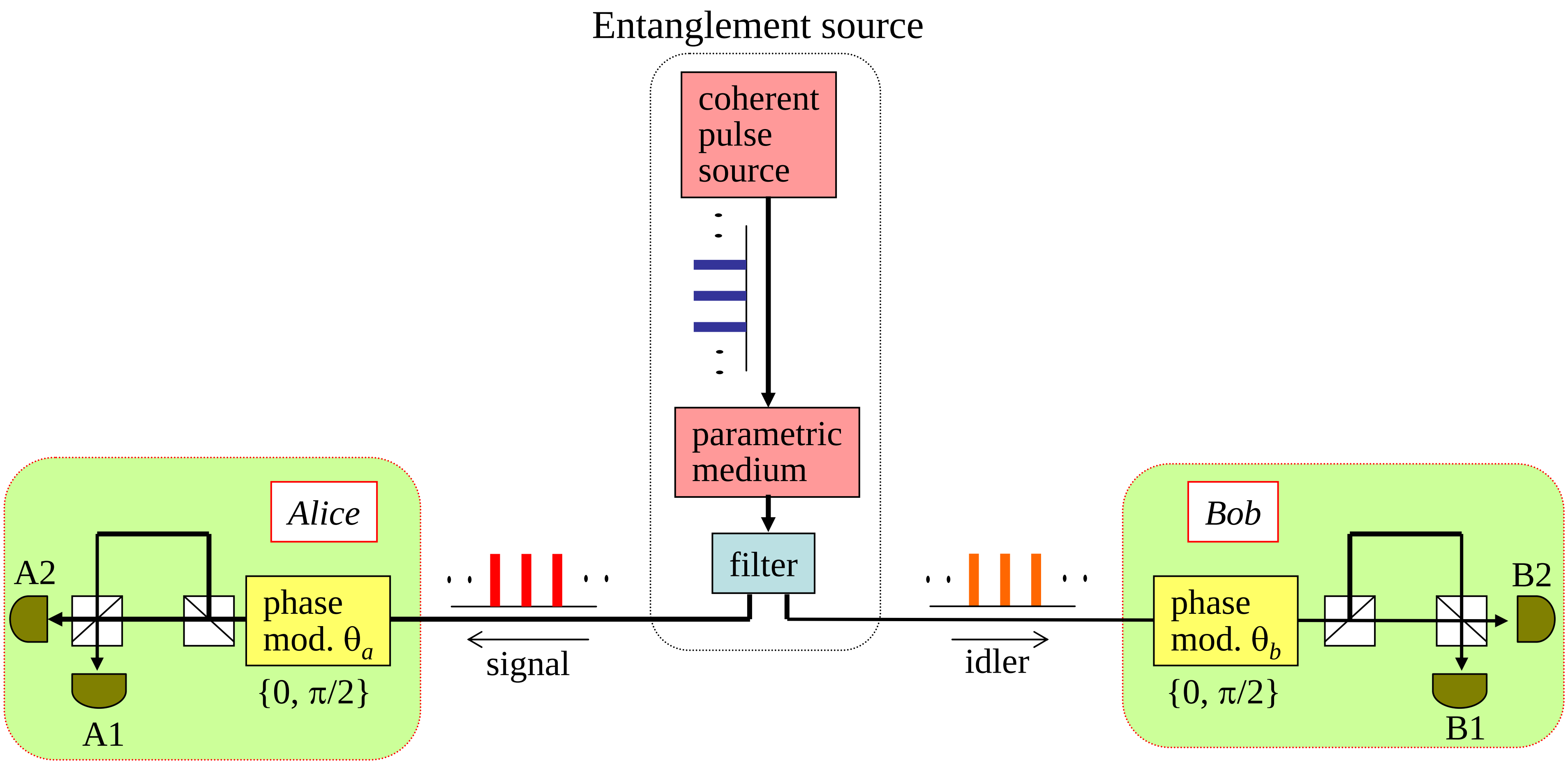




Linewidth should be < 0.06 % of FSR.

future scheme for long distance

Entanglement-based Scheme (A)
- BBM92+DPS -



System length is double of photon transmission distance.

Source output:

$$|\Psi_{in}>=\sum_j \sqrt{\mu} e^{2i\phi_p} |t_j>_s |t_j>_i$$

- $|t_j>_s$: signal photon at time t_j
- $|t_j>_i$: idler photon at time t_j
- μ: probability of one-pair generation
- ϕ_p: pump phase

Interferometer output for coincident detection

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

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

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

		$\Delta\theta_a$ = 0	$\Delta\theta_a$ = ±π/2
$\Delta\theta_b$	0	○	?
	±π/2	?	○

⇩

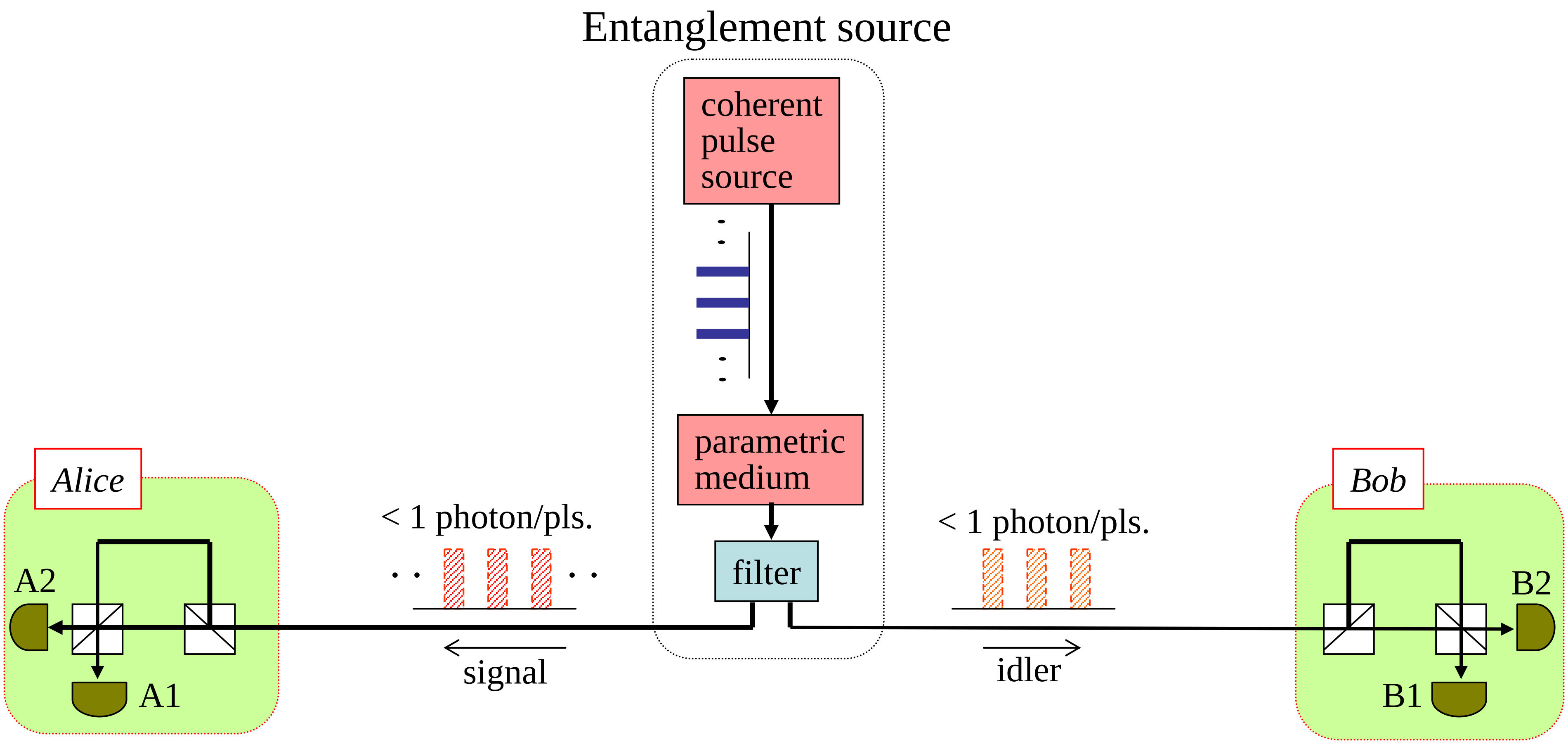
Key bits are created as

DET-A1, DET-B1 = "0"; DET-A2, DET-B2 = "1" for $\Delta\theta_a + \Delta\theta_b = 0$

DET-A1, DET-B2 = "0"; DET-A2, DET-B1 = "1" for $\Delta\theta_a + \Delta\theta_b = \pi$

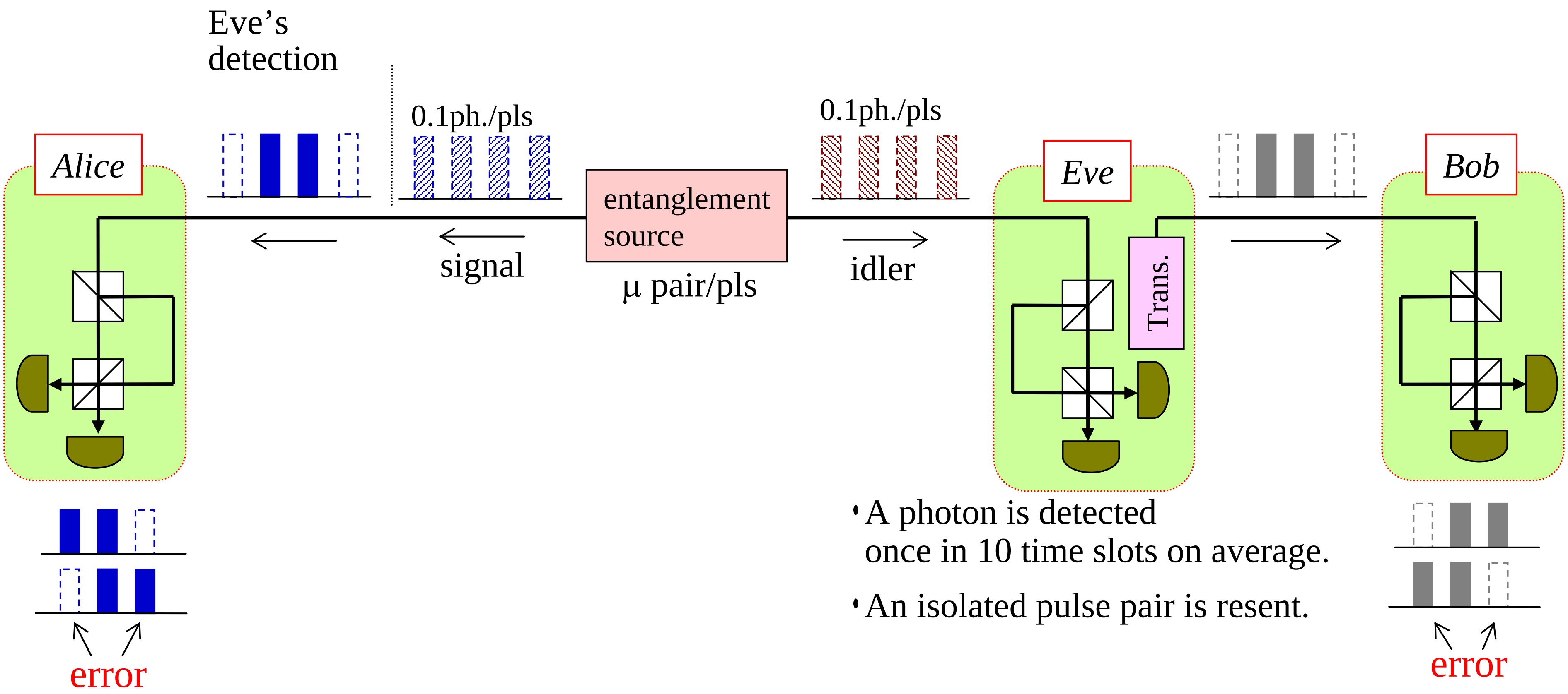
Data are discarded for $\Delta\theta_a + \Delta\theta_b = \pm\pi/2$

Entanglement-based QKD (B)
- DPS -



No basis selection at receivers.

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



• A photon is detected once in 10 time slots on average.

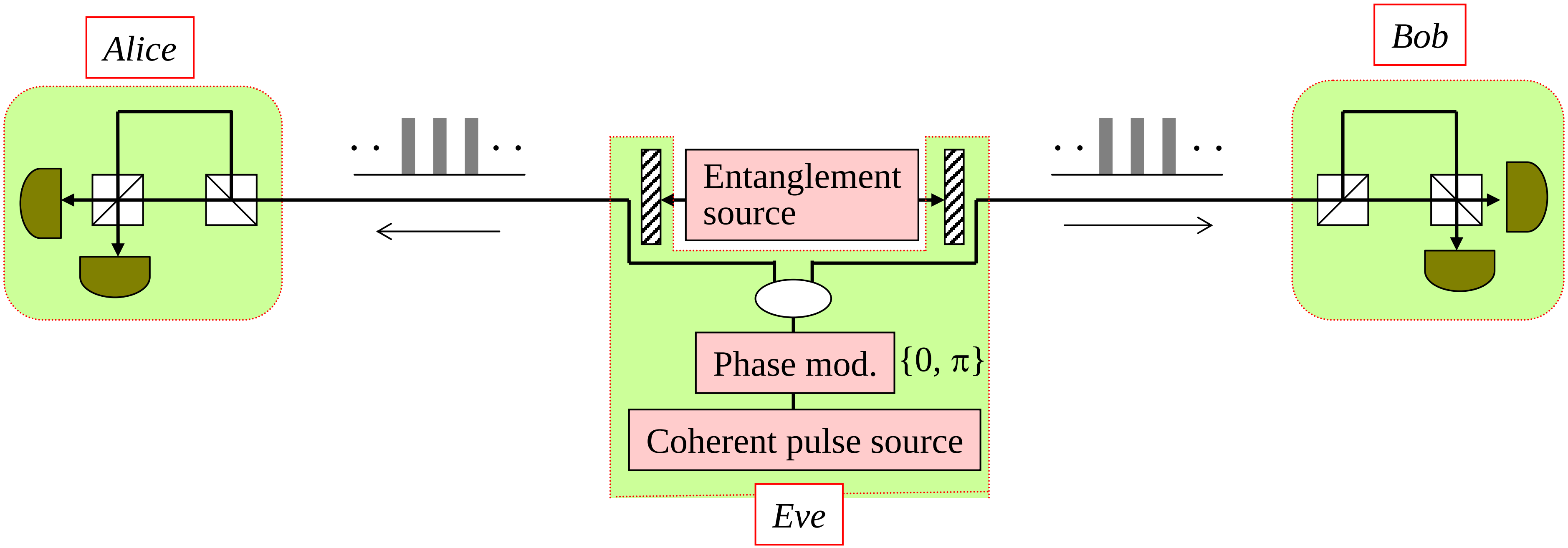
• An isolated pulse pair is resent.

◆ Eavesdropping is revealed from bit error rate.

◆ Eavesdropping is also revealed from coincident count rate.

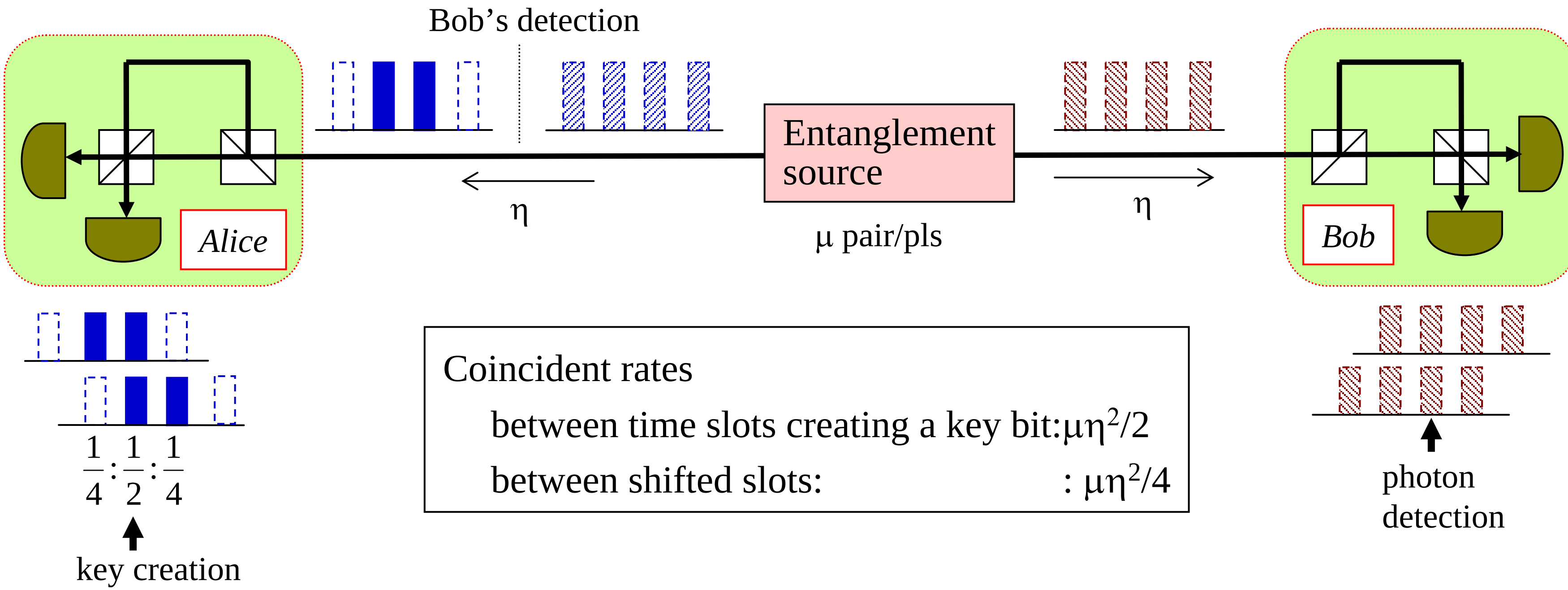
normal: $(1/2)\mu\eta^2$ eavesdropped: $(3/8)\mu\eta^2$ (η: line transmittance)

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

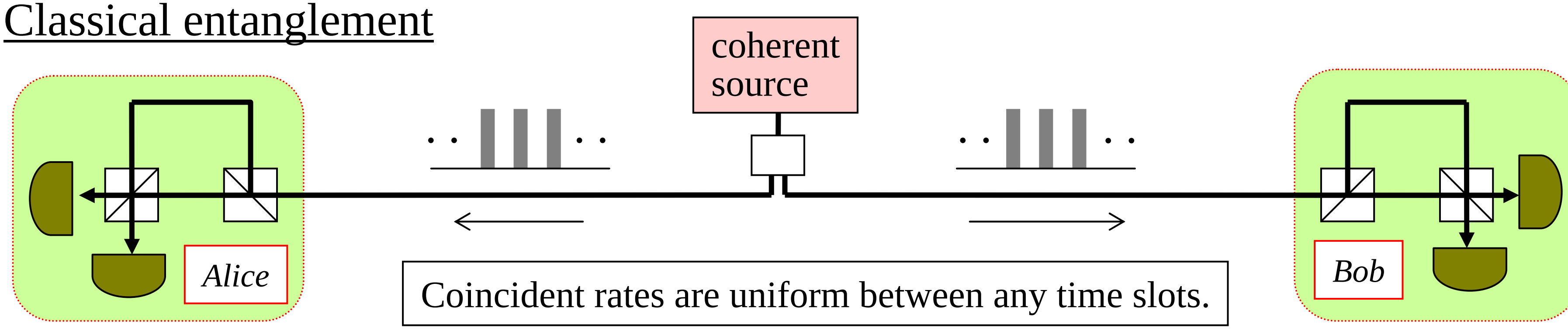


Eve gets key information without inducing bit errors.
However,,,,,

Quantum entanglement

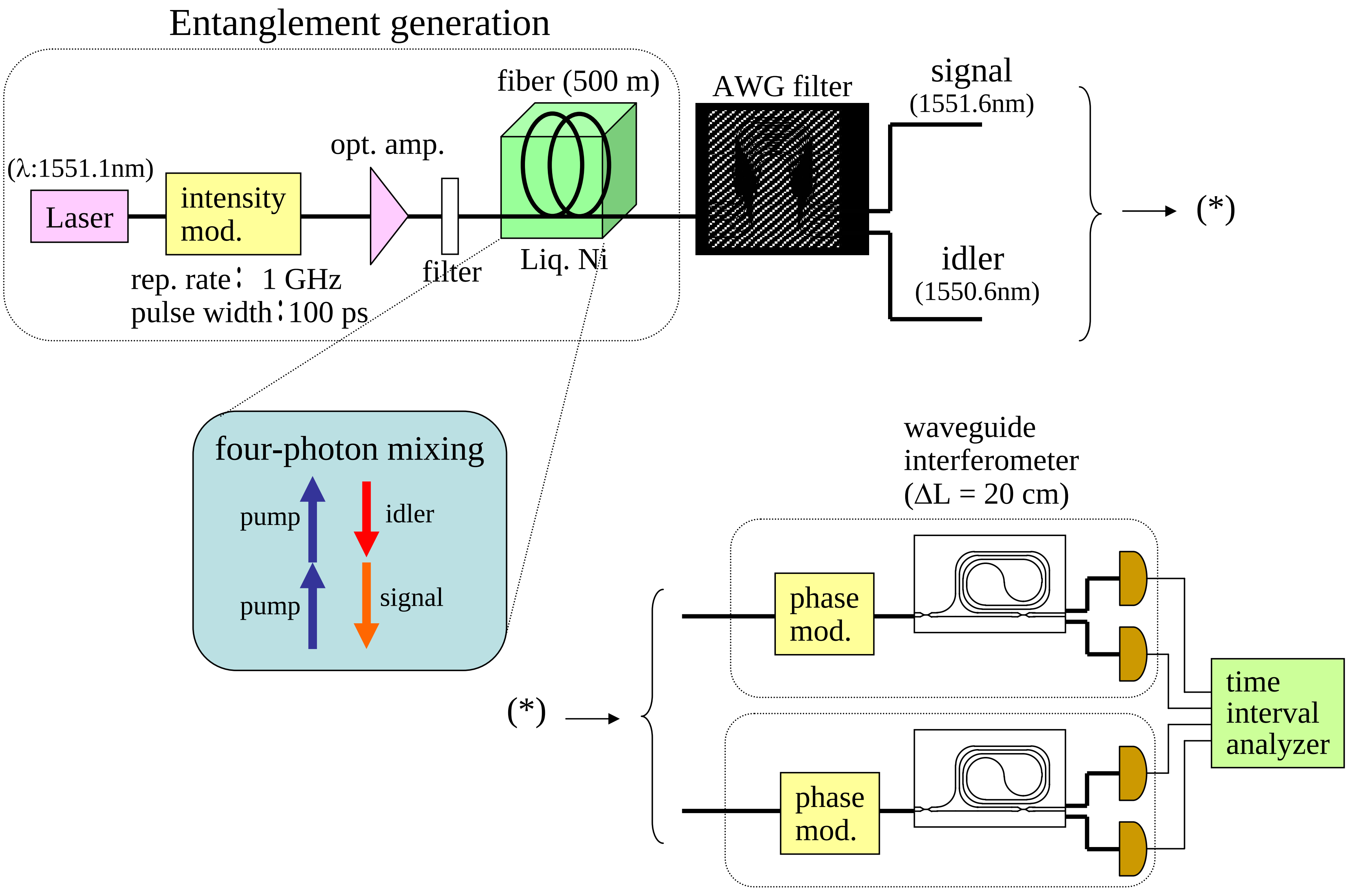


Classical entanglement



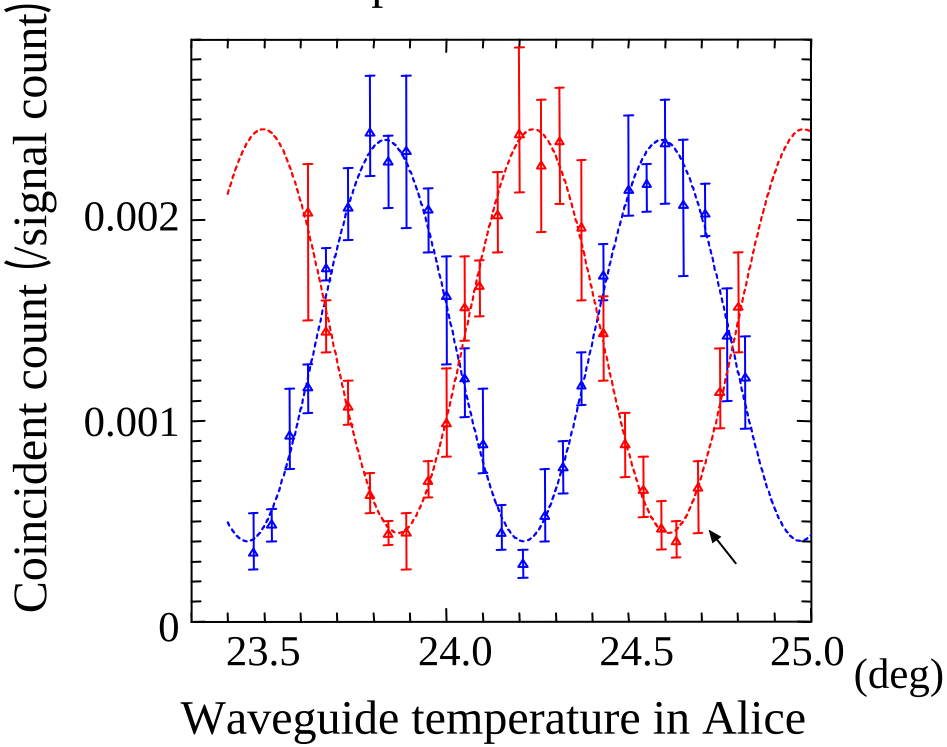
The eavesdropping is revealed from the coincident rates.

Experiment of entanglement-based QKD (A)



Experimental results

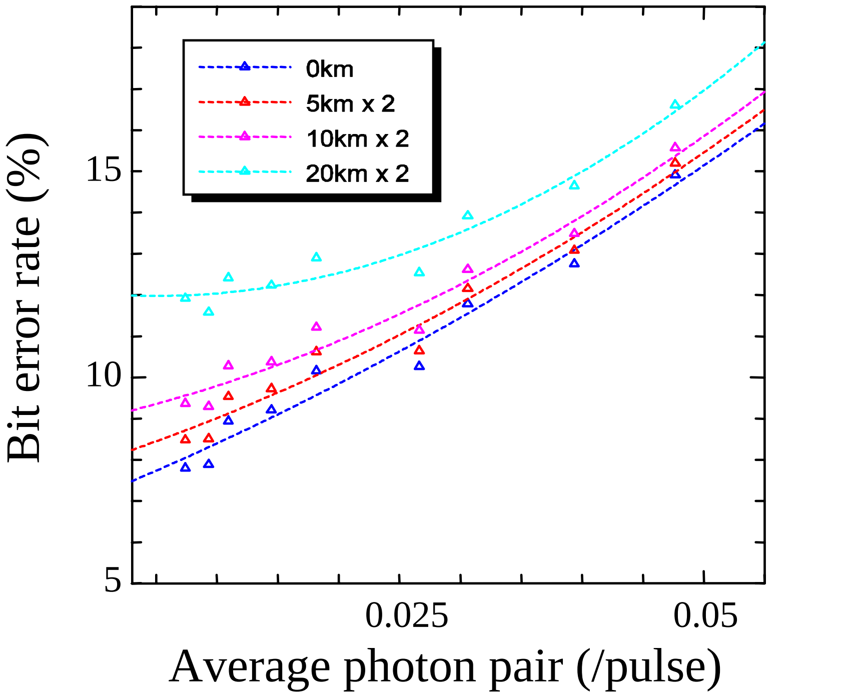
Two photon interference



Blue: $\Delta\theta_b = 0$, red: $\Delta\theta_b = \pi$.

Visibility = 70 %

Bit error rate vs. average photon number



Key creation rate = 0.34 bps with 8.6 % error

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

Summary

Differential-phase-shift QKD is presented.

(1) Setup & protocol

Simple configuration, no photon discarded.

(2) Eavesdropping

Robust against photon-number-splitting attack

(3) Modified protocol with decoy slots

Eavesdropping is revealed from click at decoy slots.

(4) Requirement for light source

Linewidth should be < 0.06 % of FSR of MZI.

(5) Entanglement-based schemes

No basis selection in receivers

First demonstration of creating a key using fiber four-wave mixing.