Differential Phase Shift Protocol

Differential Phase Shift Protocol

Why this one?

VOLUME 89, NUMBER 3 PHYSICAL REVIEW LETTERS 15 JULY 2002

Differential Phase Shift Quantum Key Distribution

Kyo Inoue*
NTT Basic Research Laboratories, NTT Corporation, Atsugi-shi, 243-0198 Japan
and E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085

Edo Waks and Yoshihisa Yamamoto†
E. L. Ginzton Laboratory, Stanford University, Stanford, California 94305-4085
(Received 30 October 2001; revised manuscript received 25 March 2002; published 27 June 2002)

Some numbers from experimental papers

A mode-locked Ti:sapphire laser (Coherent Mira 900) produces pulses at $\lambda_p = 710$ nm with $150 - fs$ pulse width and $76MHz$ repetition rate.

$2.3\ fs$

$1.3 \times 10^{-8}\ s$

Some numbers from experimental papers

A mode-locked Ti:sapphire laser (Coherent Mira 900) produces pulses at $\lambda_p = 710$ nm with $150 - fs$ pulse width and $76MHz$ repetition rate.

$2.3\ fs$

$1.3 \times 10^{-8}\ s$

To remove all unwanted infrared light, the light passes through a series of dichroic mirrors, reflecting only wavelengths centered around 710 nm.

Some numbers from experimental papers

A mode-locked Ti:sapphire laser (Coherent Mira 900) produces pulses at $\lambda_p = 710$ nm with $150 - fs$ pulse width and $76MHz$ repetition rate.

$2.3\ fs$

$1.3 \times 10^{-8}\ s$

To remove all unwanted infrared light, the light passes through a series of dichroic mirrors, reflecting only wavelengths centered around 710 nm.

The superposition of discrete times is made by a bulk Michelson interferometer with a path-length difference of 1.2 ns.

The phase is tuned by varying the temperature of the interferometer.

PHYSICAL REVIEW A **66**, 062308 (2002)

Time-bin entangled qubits for quantum communication created by femtosecond pulses

I. Marcikic,[1] H. de Riedmatten,[1] W. Tittel,[1,2] V. Scarani,[1] H. Zbinden,[1] and N. Gisin[1]
[1]*Group of Applied Physics-Optique, University of Geneva, CH-1211, Geneva 4, Switzerland*
[2]*Danish Quantum Optics Center, Institute for Physics and Astronomy, University of Aarhus, Aarhus, Denmark*
(Received 10 June 2002; published 10 December 2002)

We create pairs of nondegenerate time-bin entangled photons at telecom wavelengths with ultrashort pump pulses. Entanglement is shown by performing Bell kind tests of the Franson type with visibilities of up to 91%. As time-bin entanglement can easily be protected from decoherence as encountered in optical fibers, this experiment opens the road for complex quantum communication protocols over long distances. We also investigate the creation of more than one photon pair in a laser pulse and present a simple tool to quantify the probability of such events to happen.

Some numbers from experimental papers

A mode-locked Ti:sapphire laser (Coherent Mira 900) produces pulses at $\lambda_p = 710$ nm with $150 - fs$ pulse width and $76MHz$ repetition rate.

$2.3\ fs$

$1.3 \times 10^{-8}\ s$

To remove all unwanted infrared light, the light passes through a series of dichroic mirrors, reflecting only wavelengths centered around 710 nm.

The superposition of discrete times is made by a bulk Michelson interferometer with a path-length difference of 1.2 ns.

The phase is tuned by varying the temperature of the interferometer.

PHYSICAL REVIEW A **66**, 062308 (2002)

Time-bin entangled qubits for quantum communication created by femtosecond pulses

I. Marcikic,[1] H. de Riedmatten,[1] W. Tittel,[1,2] V. Scarani,[1] H. Zbinden,[1] and N. Gisin[1]
[1]*Group of Applied Physics-Optique, University of Geneva, CH-1211, Geneva 4, Switzerland*
[2]*Danish Quantum Optics Center, Institute for Physics and Astronomy, University of Aarhus, Aarhus, Denmark*
(Received 10 June 2002; published 10 December 2002)

We create pairs of nondegenerate time-bin entangled photons at telecom wavelengths with ultrashort pump pulses. Entanglement is shown by performing Bell kind tests of the Franson type with visibilities of up to 91%. As time-bin entanglement can easily be protected from decoherence as encountered in optical fibers, this experiment opens the road for complex quantum communication protocols over long distances. We also investigate the creation of more than one photon pair in a laser pulse and present a simple tool to quantify the probability of such events to happen.

Some numbers from experimental papers

A mode-locked Ti:sapphire laser (Coherent Mira 900) produces pulses at $\lambda_p = 710$ nm with $150 - fs$ pulse width and $76MHz$ repetition rate.

$2.3\ fs$

$1.3 \times 10^{-8}\ s$

To remove all unwanted infr ries of dichroic mirrors, reflecting only wavelengths

ADVANTAGES W.R.T. Polarisation: Polarisation changes in fiber. Phase does not change.

The superposition of discre terferometer with a path-length difference of 1.2 ns.

The phase is tuned by varying the temperature of the interferometer.

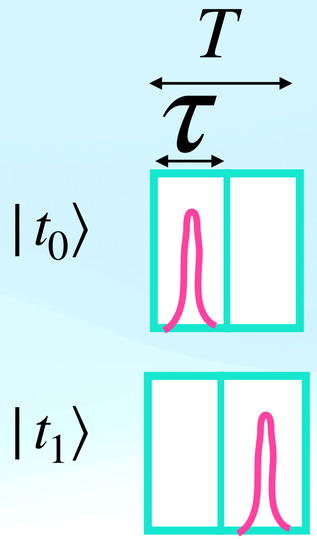
PHYSICAL REVIEW A **66**, 062308 (2002)

Time-bin entangled qubits for quantum communication created by femtosecond pulses

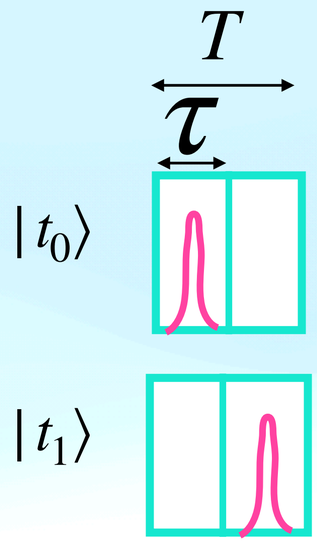
I. Marcikic,[1] H. de Riedmatten,[1] W. Tittel,[1,2] V. Scarani,[1] H. Zbinden,[1] and N. Gisin[1]
[1]*Group of Applied Physics-Optique, University of Geneva, CH-1211, Geneva 4, Switzerland*
[2]*Danish Quantum Optics Center, Institute for Physics and Astronomy, University of Aarhus, Aarhus, Denmark*
(Received 10 June 2002; published 10 December 2002)

We create pairs of nondegenerate time-bin entangled photons at telecom wavelengths with ultrashort pump pulses. Entanglement is shown by performing Bell kind tests of the Franson type with visibilities of up to 91%. As time-bin entanglement can easily be protected from decoherence as encountered in optical fibers, this experiment opens the road for complex quantum communication protocols over long distances. We also investigate the creation of more than one photon pair in a laser pulse and present a simple tool to quantify the probability of such events to happen.

Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol

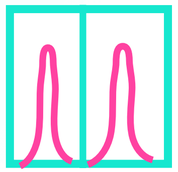


Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



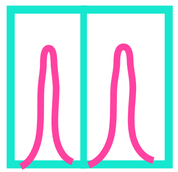
$$|f_0\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle + |t_1\rangle\right)$$

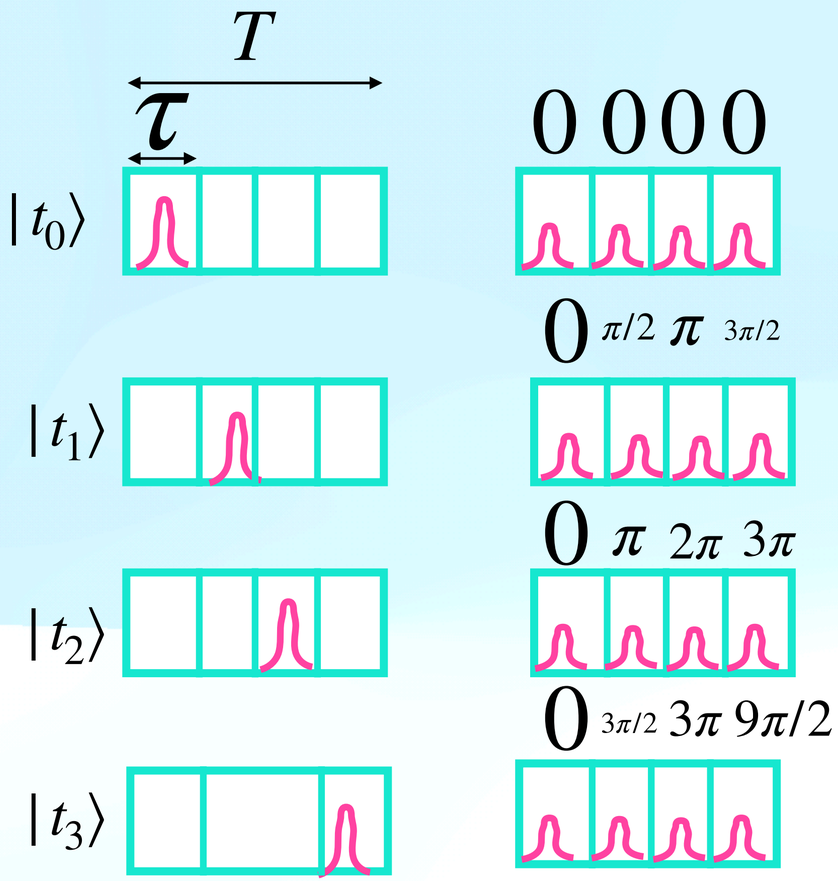
0 0



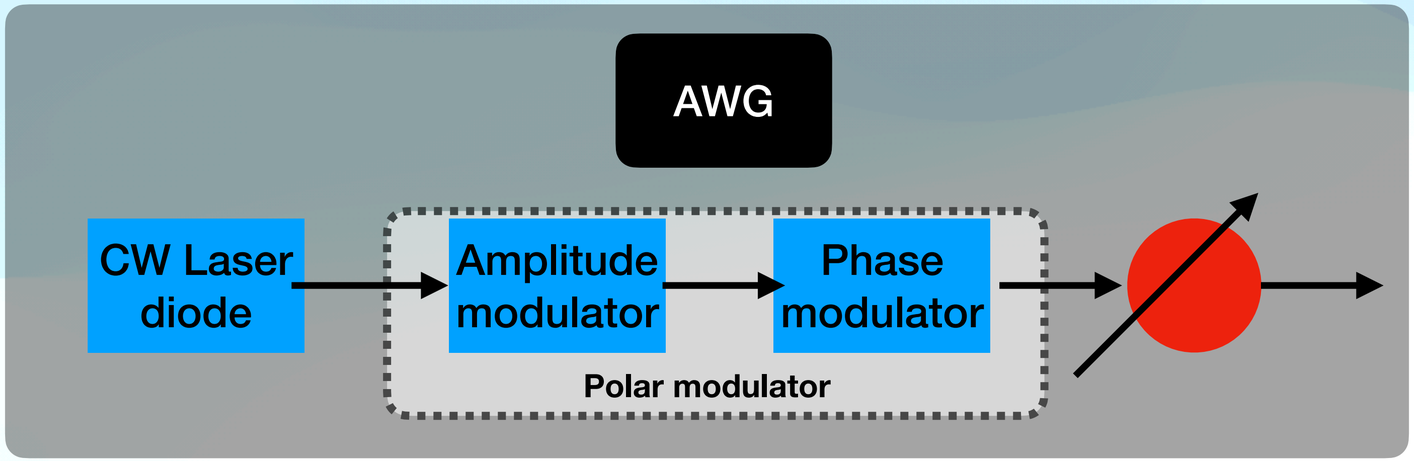
$$|f_1\rangle = \frac{1}{\sqrt{2}}\left(|t_0\rangle - |t_1\rangle\right)$$

0 π



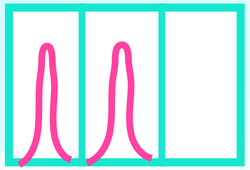


$$|f_d\rangle = \sum_{d=0}^{D-1} \omega^{dn} |t_n\rangle$$

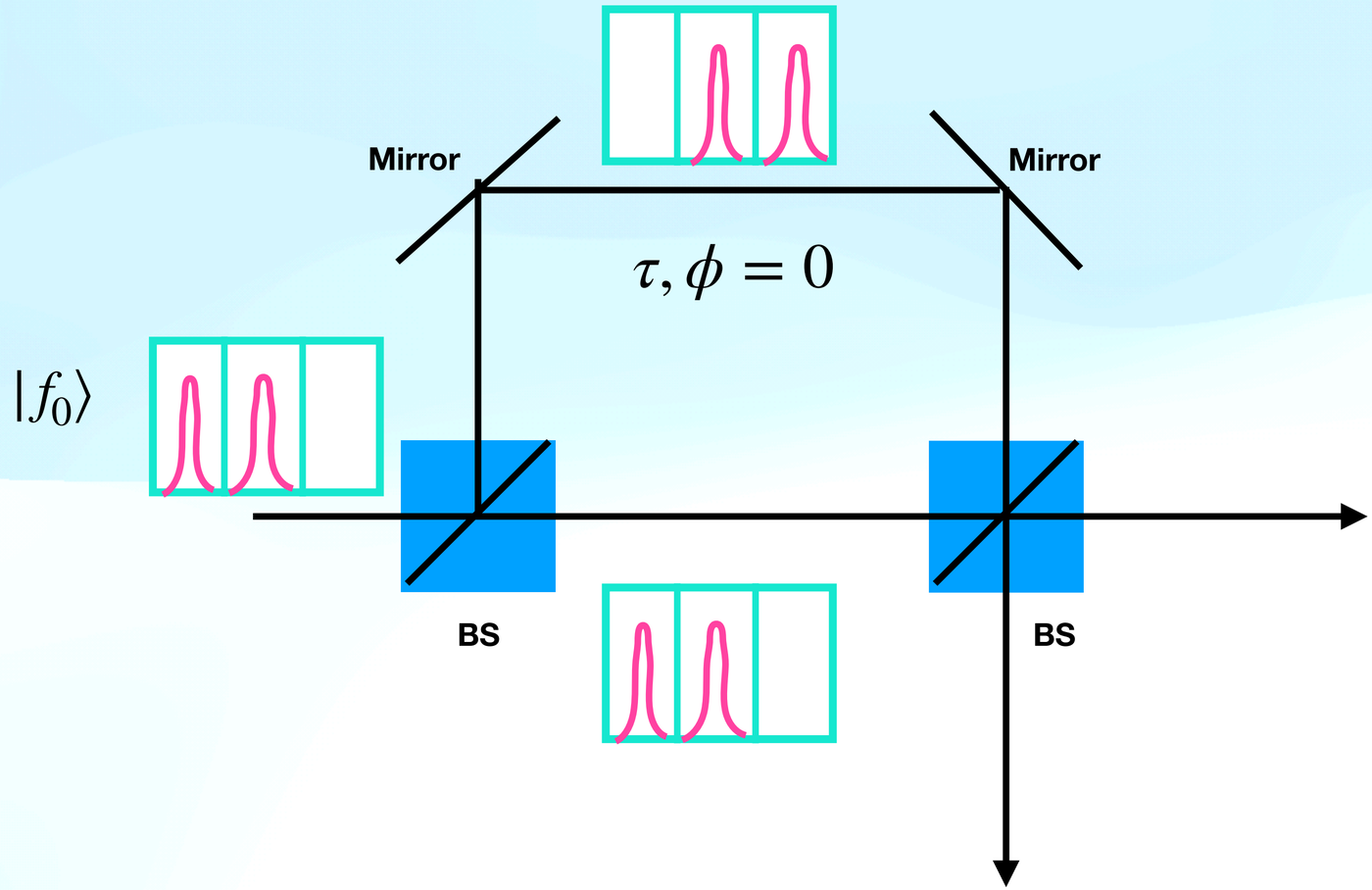

AWG
CW Laser diode
Amplitude modulator
Phase modulator
Polar modulator

Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol

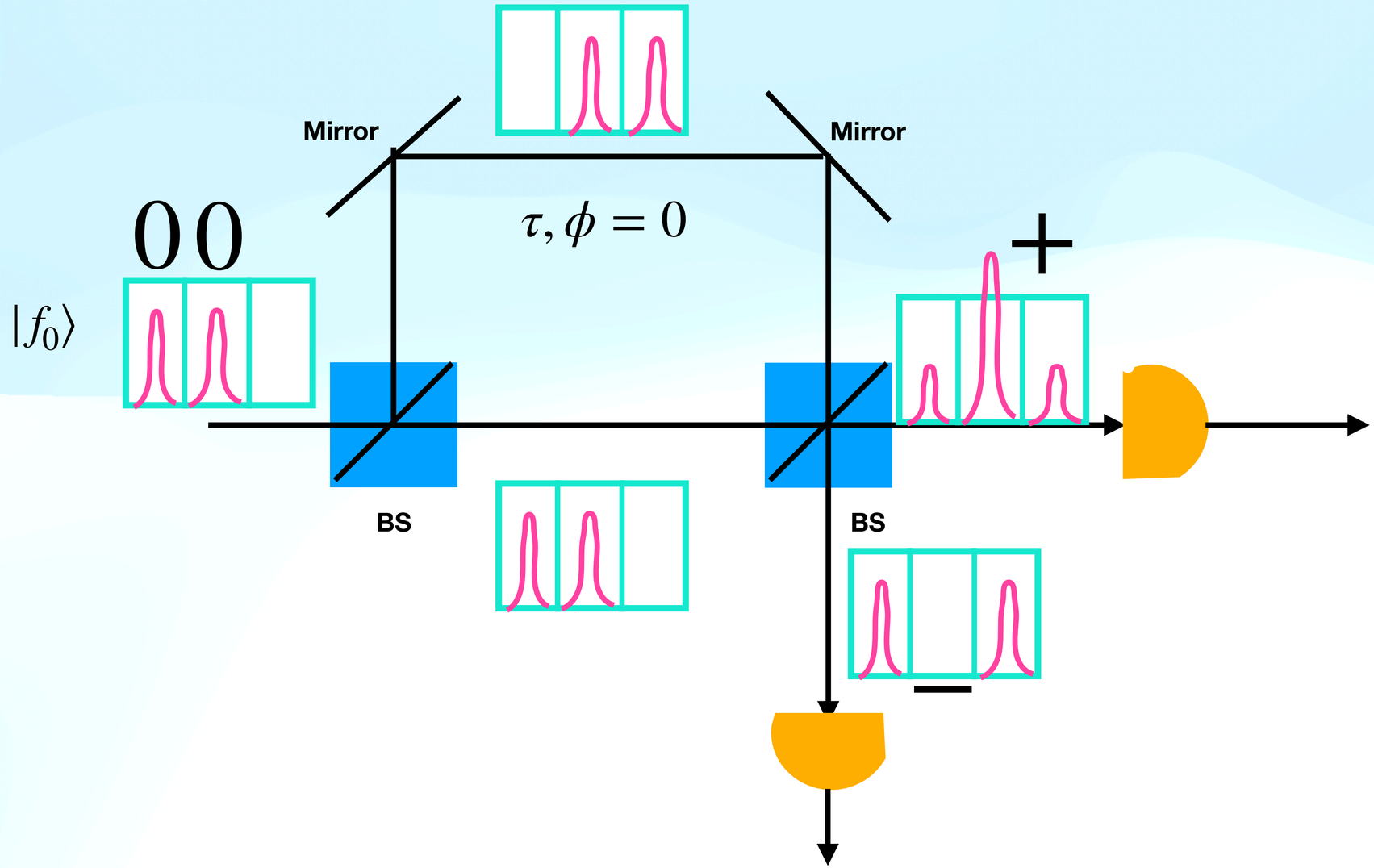
$|f_0\rangle$



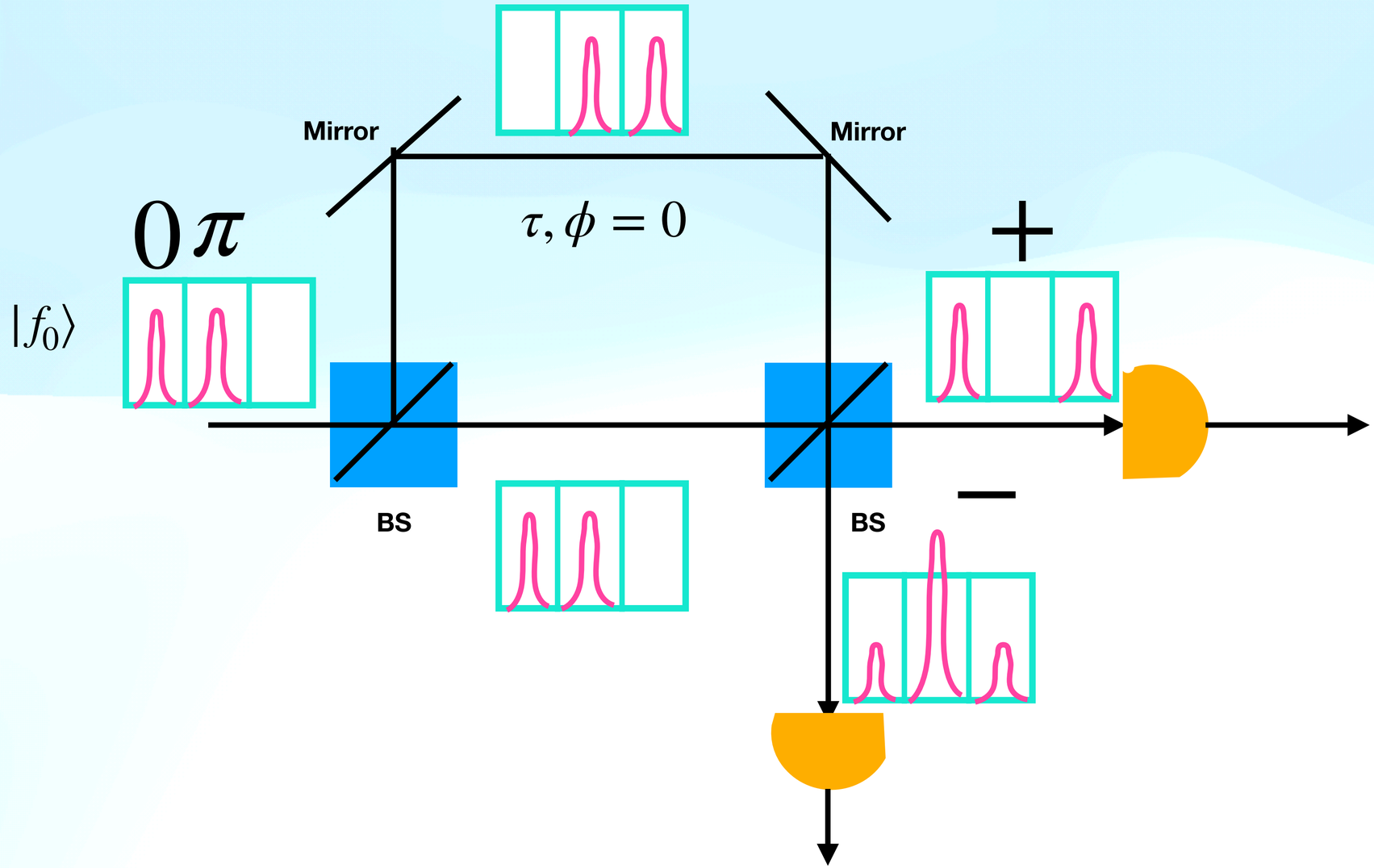
Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



Precursor: Schematic for experimental implementation
Time encoding based BB 84 protocol



DPS

Introduction

- QKD: Allows two parties to share an unconditionally secure secret key.
- Security is guaranteed by the laws of quantum mechanics.
- Typical schemes: BB84, B92, and E91, BBM92.

Introduction

- **QKD: Allows two parties to share an unconditionally secure secret key.**
- **Security is guaranteed by the laws of quantum mechanics.**
- **Typical schemes: BB84, B92, and E91, BBM92.**

Why another protocol?

Introduction

- **QKD: Allows two parties to share an unconditionally secure secret key.**
- **Security is guaranteed by the laws of quantum mechanics.**
- **Typical schemes: BB84, B92, and E91, BBM92.**

Why another protocol?

- **A photon split into three pulses is sent from Alice to Bob, in which the phases of two sequential probability amplitudes are randomly modulated.**
- **Bob extracts the bit information by measuring the differential phase.**
- **Suitable for fiber transmission systems, while offering a key creation efficiency higher than conventional fiber-based BB84.**

Introduction

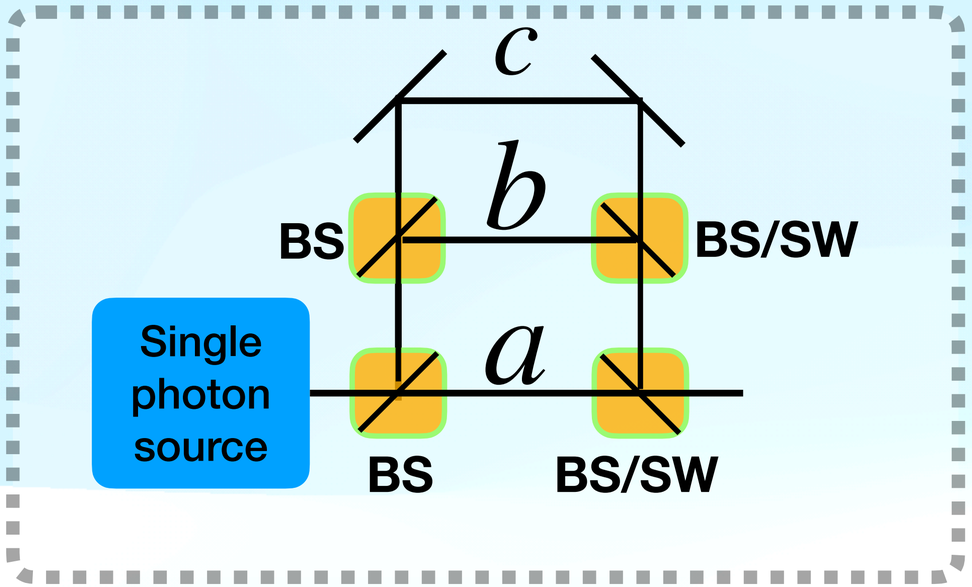
- **QKD: Allows two parties to share an unconditionally secure secret key.**
- **Security is guaranteed by the laws of quantum mechanics.**
- **Typical schemes: BB84, B92, and E91, BBM92.**

Why another protocol?

- **A photon split into three pulses is sent from Alice to Bob, in which the phases of two sequential probability amplitudes are randomly modulated.**
- **Bob extracts the bit information by measuring the differential phase.**
- **Suitable for fiber transmission systems, while offering a key creation efficiency higher than conventional fiber-based BB84.**

Setup of the proposed QKD system

Setup of the proposed QKD system



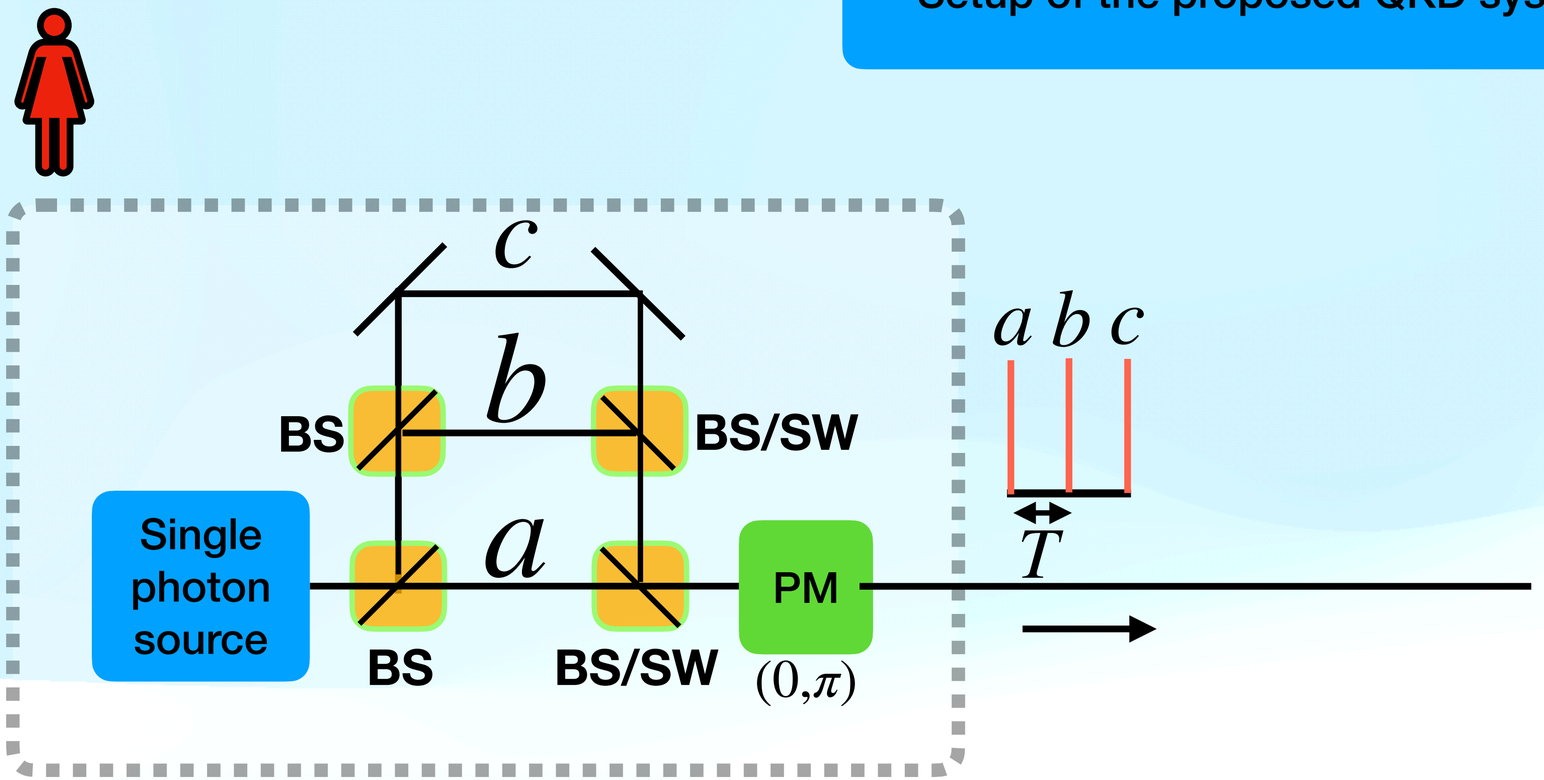
BS: beam splitter
SW: switch

The time delays between paths a and b and between paths b and c are equally T.

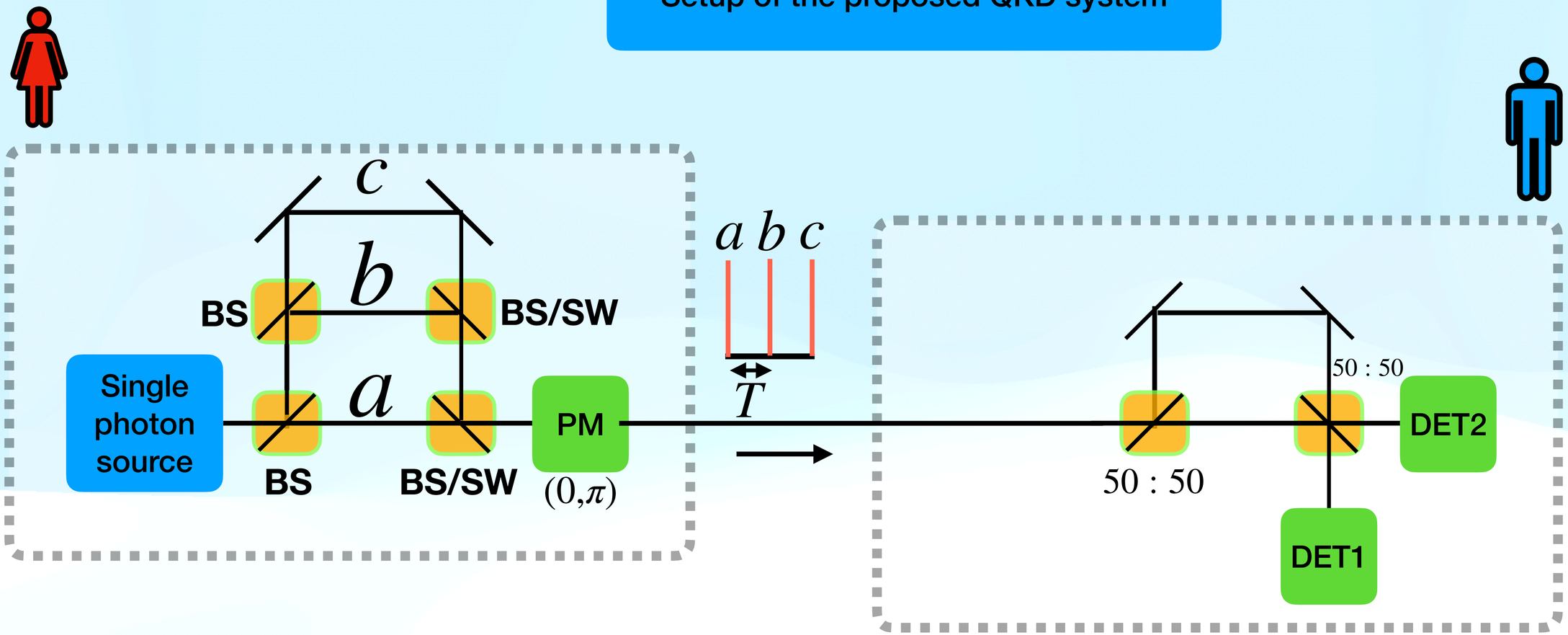
$$\frac{1}{\sqrt{3}}\left(|1\rangle_A|0\rangle_B|0\rangle_C \pm |0\rangle_A|1\rangle_B|0\rangle_C \pm |0\rangle_A|0\rangle_B|1\rangle_C\right)$$

The splitting ratios of the beam splitters are such that the probabilities for a photon to pass through each route are equal.

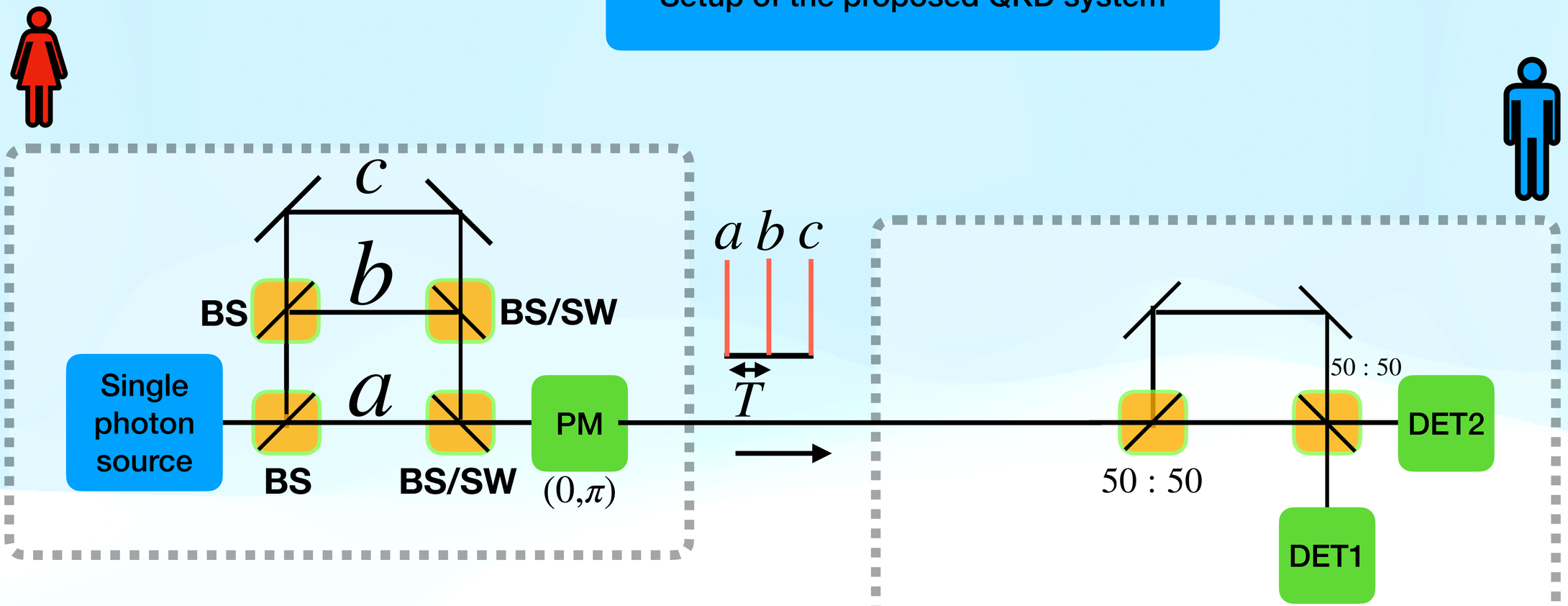
Setup of the proposed QKD system



Setup of the proposed QKD system



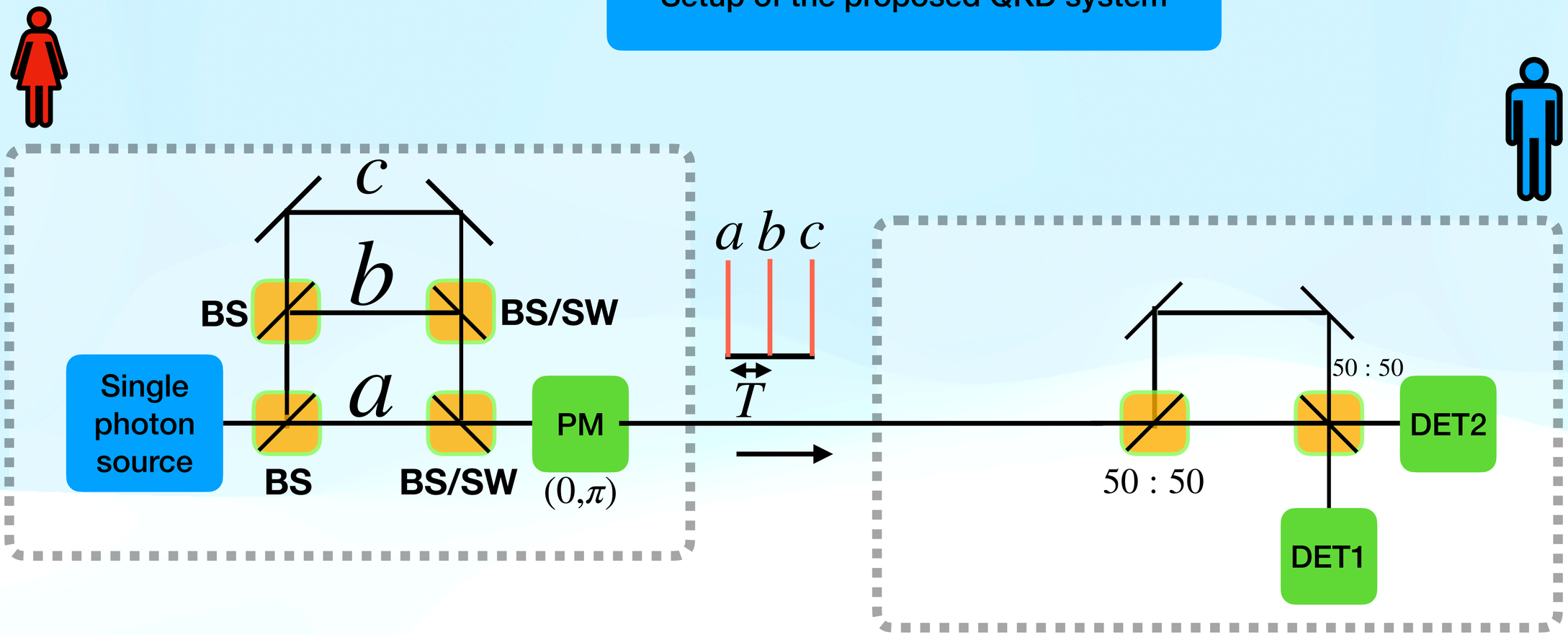
Setup of the proposed QKD system



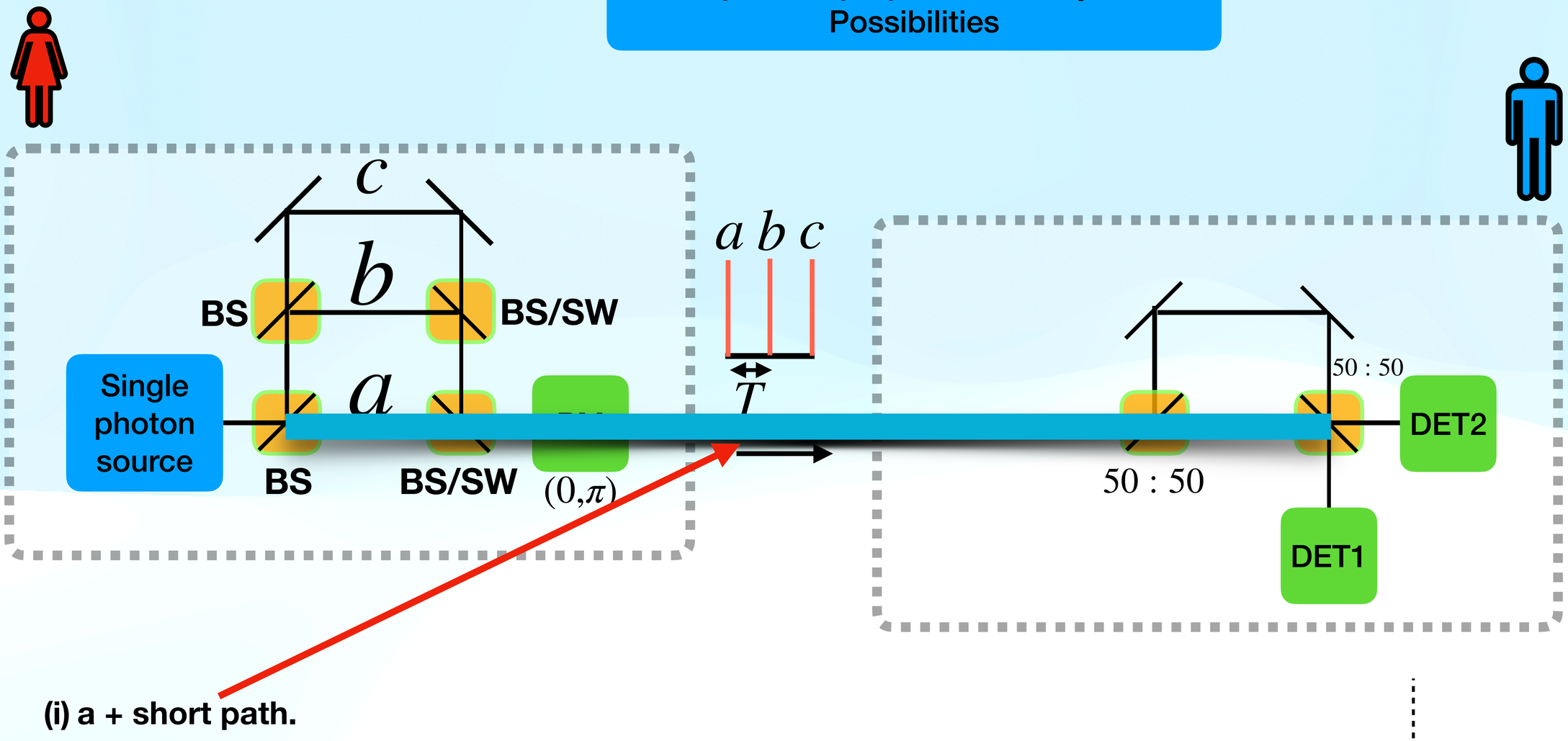
:Beam Splitter

PM :Phase modulator

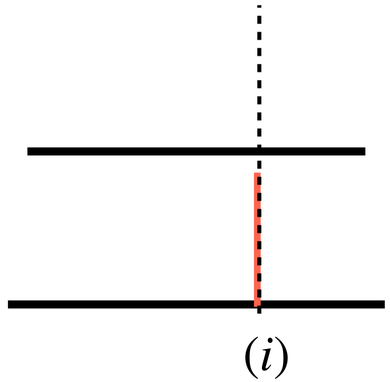
Setup of the proposed QKD system



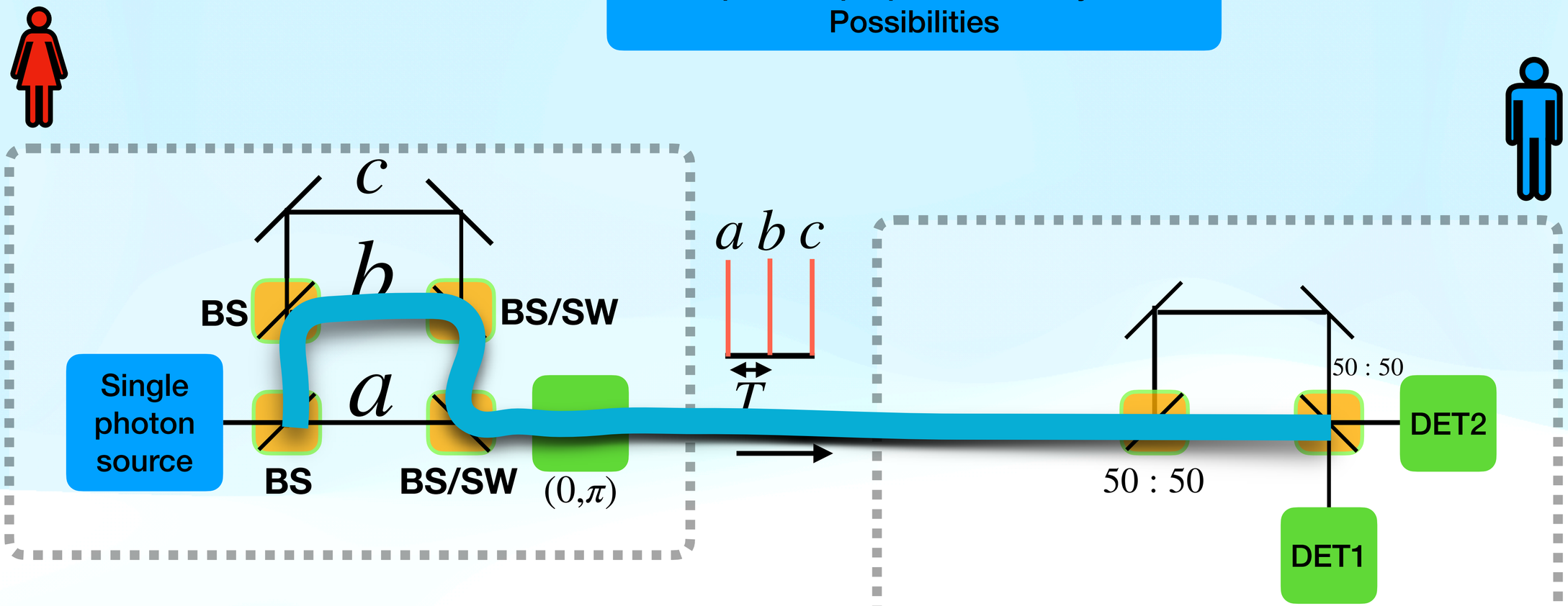
Setup of the proposed QKD system: Possibilities



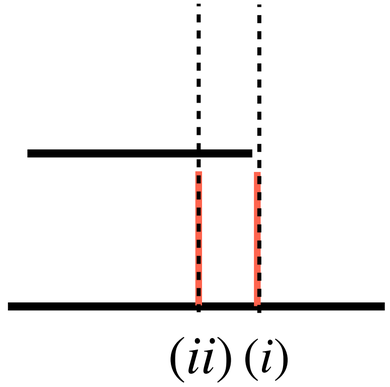
(i) a + short path.



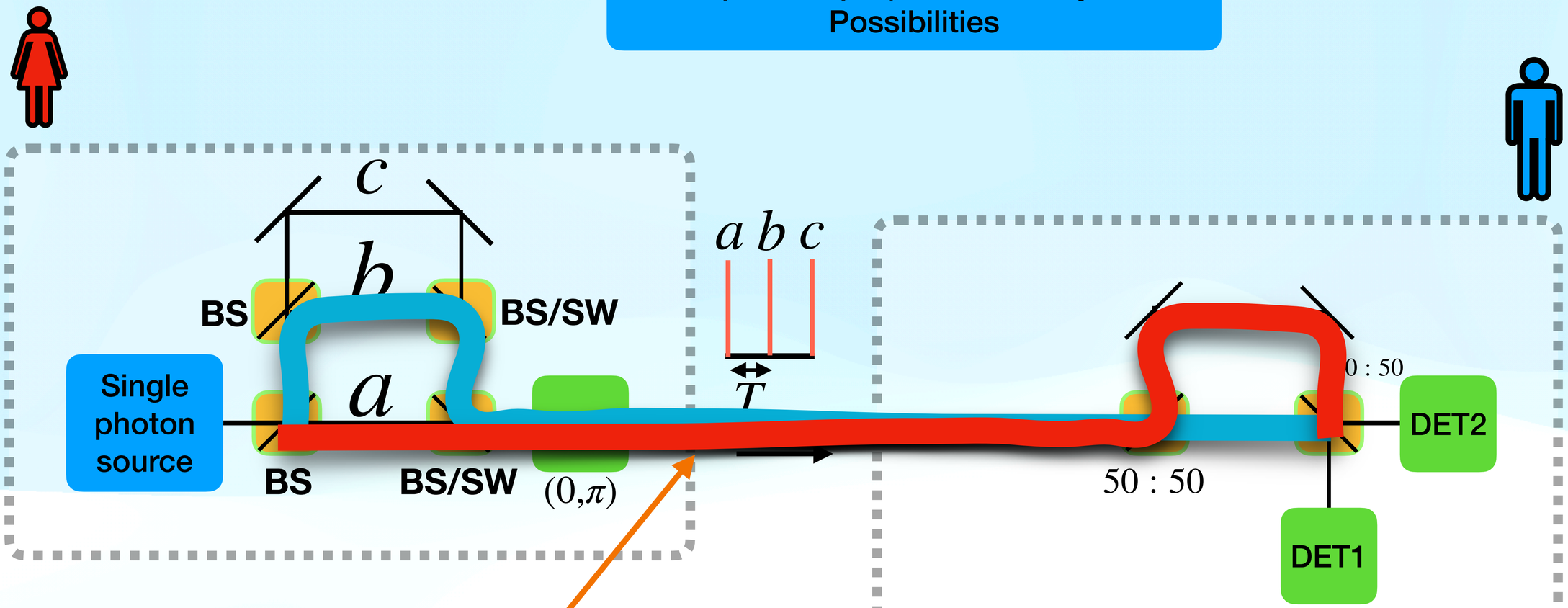
Setup of the proposed QKD system: Possibilities



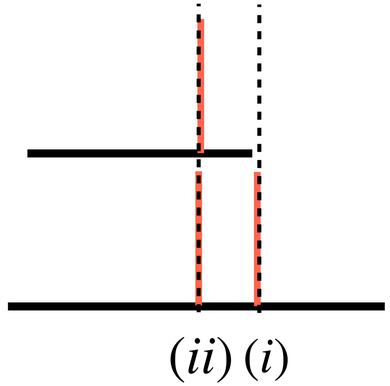
(i) a + short path.



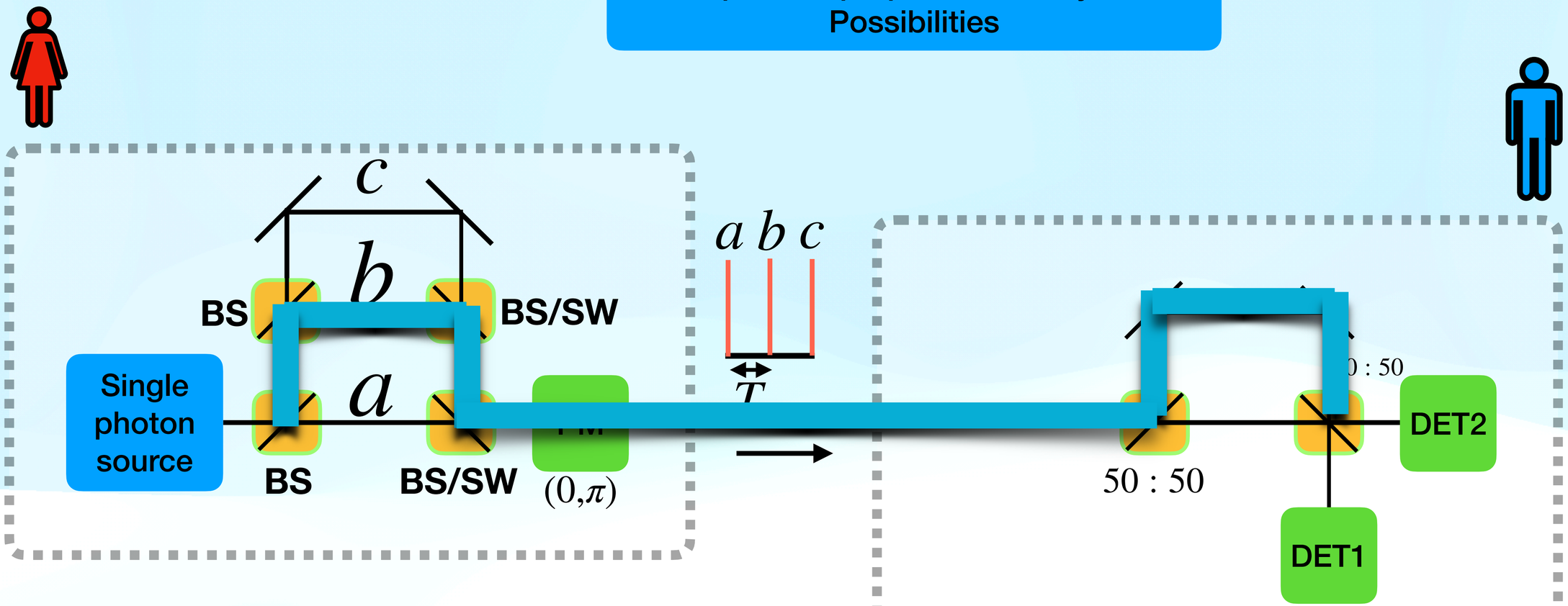
Setup of the proposed QKD system: Possibilities



(i) a + short path.
(ii) a + long path, b + short path.

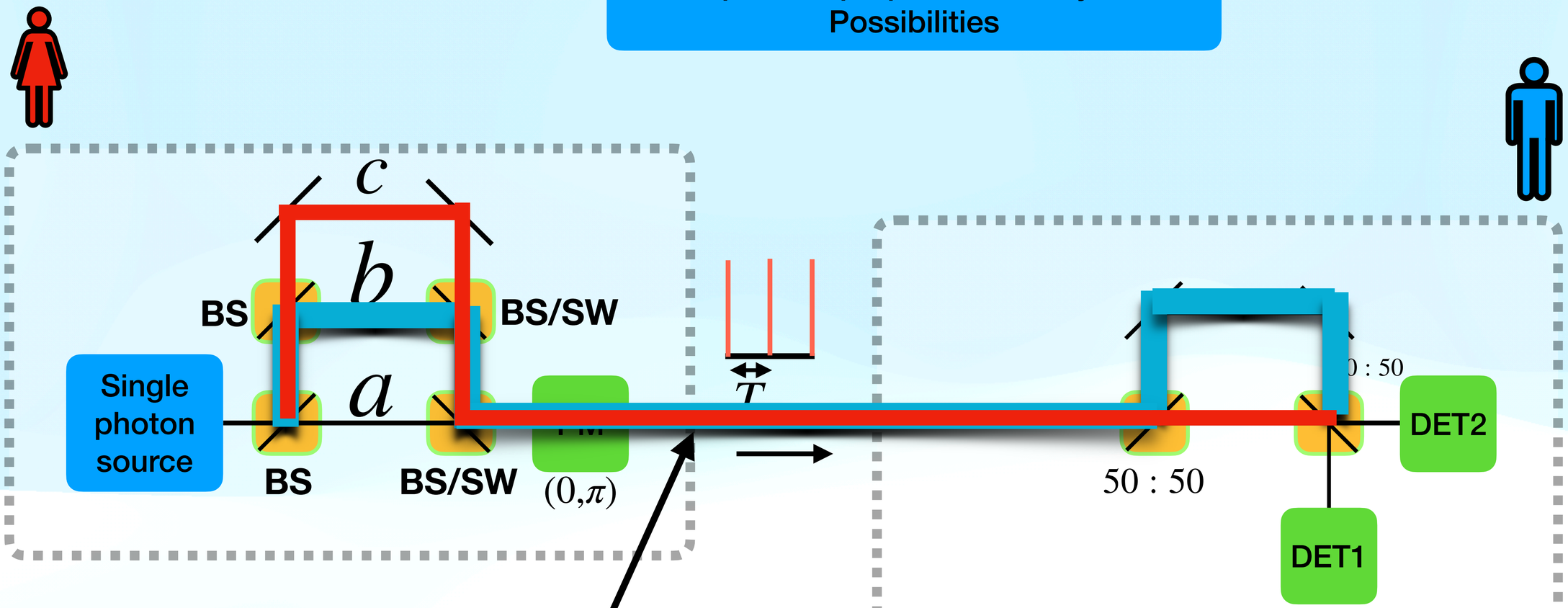


Setup of the proposed QKD system: Possibilities

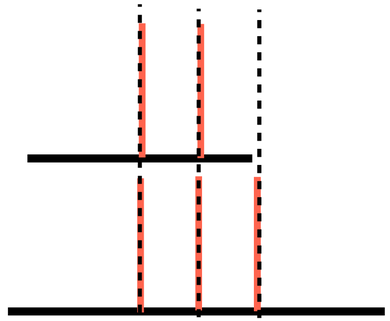


(i) a + short path.
(ii) a + long path, b + short path.
(iii) b + long path, c + short path.

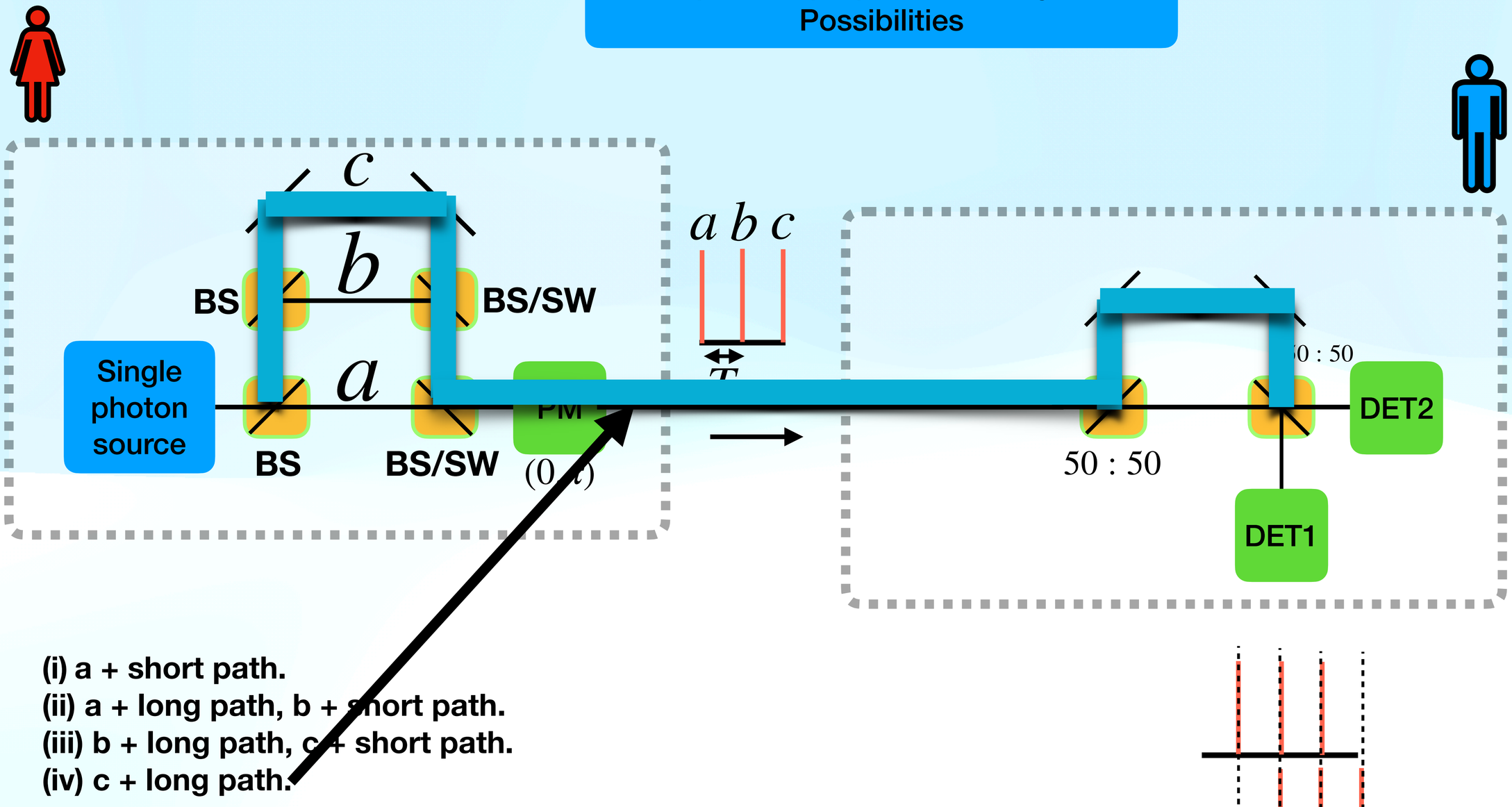
Setup of the proposed QKD system: Possibilities



(i) a + short path.
(ii) a + long path, b + short path.
(iii) b + long path, c + short path.



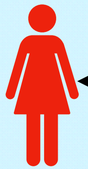
Setup of the proposed QKD system: Possibilities



(i) a + short path.
(ii) a + long path, b + short path.
(iii) b + long path, c + short path.
(iv) c + long path.

But, KGR?????

Claimed KGR

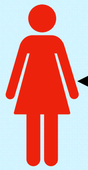


time instance of the photon detection/ **NOT WHICH DETECTOR!!!**

II/III

Time+which detector recorded.

KGR



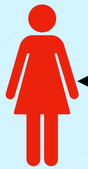
time instance of the photon detection/ **NOT WHICH DETECTOR!!!**

II/III

Time+which detector recorded.

From this information and her modulation data, Alice knows which detector clicked in Bob's site.

KGR



time instance of the photon detection/ NOT WHICH DETECTOR!!!

II/III
Time+which detector recorded.

(1) From this information and her modulation data, Alice knows which detector clicked in Bob's site.

(2) Alice and Bob have an identical bit string, provided that the DET1 click represents "0" and the DET2 click represents "1." In the above protocol, Bob only tells the time-instance to Alice, and the bit information is not leaked to the public.

Resilience to eavesdropping

Beam splitting attack

Eve taps one photon out of multiple photons in a coherent pulse, and then obtains bit information by measuring the photon after Alice and Bob exchange supplementary information through a public channel.

Resilience to eavesdropping

Beam splitting attack

Eve taps one photon out of multiple photons in a coherent pulse, and then obtains bit information by measuring the photon after Alice and Bob exchange supplementary information through a public channel.

In conventional BB84, Eve can measure bit information perfectly from a tapped photon. In the present scheme, on the other hand, Eve cannot do so because she cannot measure one of the two phase differences with 100% probability.

Thus, the present scheme may be more robust against the beam splitting attack for weak coherent light.

A smarter eve

an intercept/resend attack using the same receiver setup as Bob.

A smarter eve

an intercept/resend attack using the same receiver setup as Bob.

- **Eve detects a photon at four possible time instances as Bob does.**
- **obtains partial information when a photon is counted at (ii) or (iii), while she gets no information when it is counted at (i) or (iv).**

A smarter eve

an intercept/resend attack using the same receiver setup as Bob.

- **Eve detects a photon at four possible time instances as Bob does.**
- **obtains partial information when a photon is counted at (ii) or (iii), while she gets no information when it is counted at (i) or (iv).**

- **From the measurement at (ii) or (iii), Eve knows one of the two phase-differences.**

- **If Eve sends a photon split into two pulses having the measured phase difference, she changes the counting rate at each time instance in Bob.**

When Eve measures the phase difference between the first two pulses and resends a fake photon accordingly, Bob counts the photon at time-instances (i), (ii), or (iii). The probability ratio of the click at (i), (ii), and (iii) is 1:2:1. When Eve measures the phase difference between the sec- ond two pulses, Bob's detectors can click at time-instances (ii), (iii), and (iv) with a probability ratio of 1:2:1. Thus, the overall ratio of the clicks at (i), (ii), (iii), and (iv) be- comes 1:3:3:1. On the other hand, the counting ratio for a photon split into three pulses is 1:2:2:1. Therefore, this cheating is revealed by

A smarter eve

an intercept/resend attack using the same receiver setup as Bob.

- **Eve detects a photon at four possible time instances as Bob does.**
- **obtains partial information when a photon is counted at (ii) or (iii), while she gets no information when it is counted at (i) or (iv).**

- **From the measurement at (ii) or (iii), Eve knows one of the two phase-differences.**

- **If Eve sends a photon split into two pulses having the measured phase difference, she changes the counting rate at each time instance in Bob.**

A smarter eve

an intercept/resend attack using the same receiver setup as Bob.

- **Eve detects a photon at four possible time instances as Bob does.**
- **obtains partial information when a photon is counted at (ii) or (iii), while she gets no information when it is counted at (i) or (iv).**

- **From the measurement at (ii) or (iii), Eve knows one of the two phase-differences.**

- **If Eve sends a photon split into two pulses having the measured phase difference, she changes the counting rate at each time instance in Bob.**

Sources/ References

1. Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. *Physical review letters* 89.3 (2002): 037902.

2. Djordjevic, Ivan B. Physical-layer security and quantum key distribution. Berlin/Heidelberg, Germany: Springer, 2019.

We have to put the things a little loosely before you because we are still searching for the comparison data for different hardware implementation.