Security of Quantum Key Distribution from Cryptographic Perspectives

Hao Chung (鍾豪)
National Taiwan University
March 22, 2018

Outline

Assumptions of Different Protocols

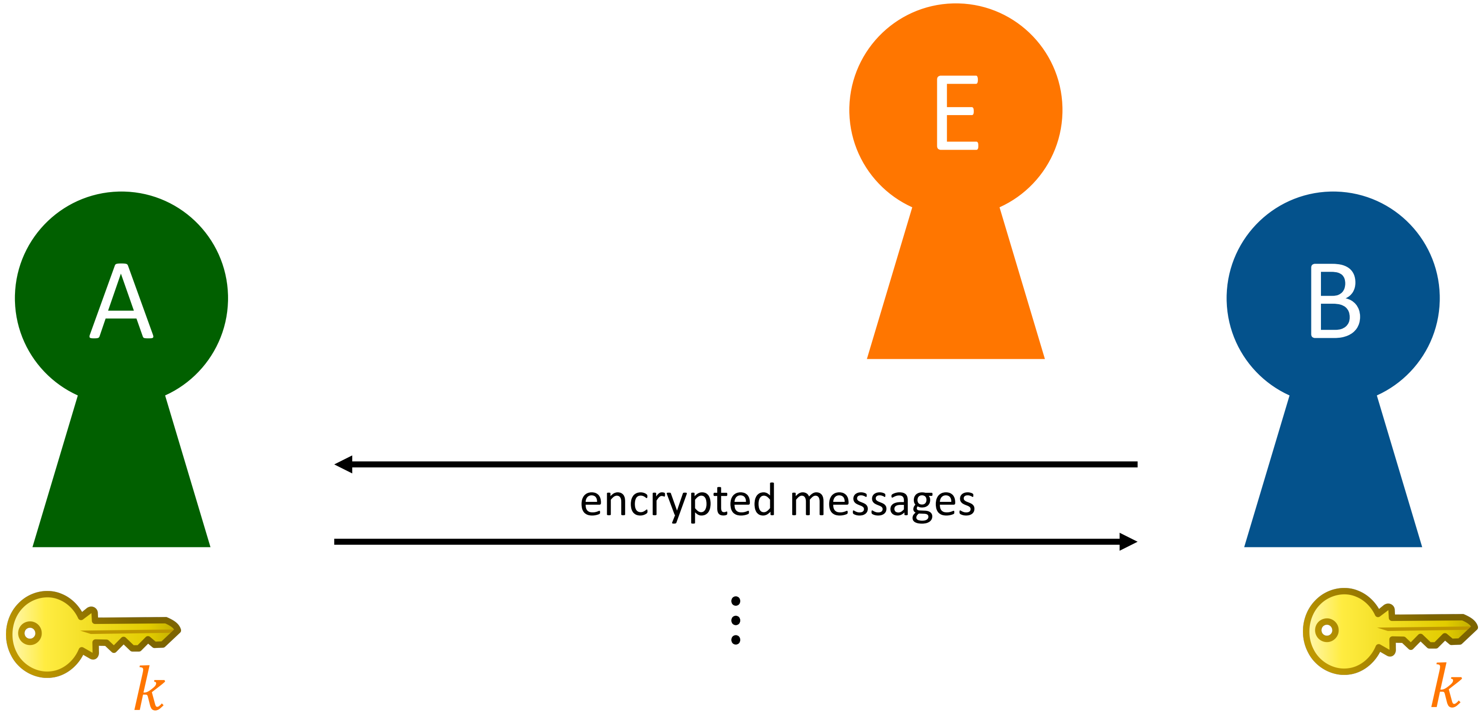
1. BB84
2. Decoy
3. Measurement Device Independent
4. Device Independent

Future Work

1. Finite Key Analysis
2. Security Proof of RRDPS

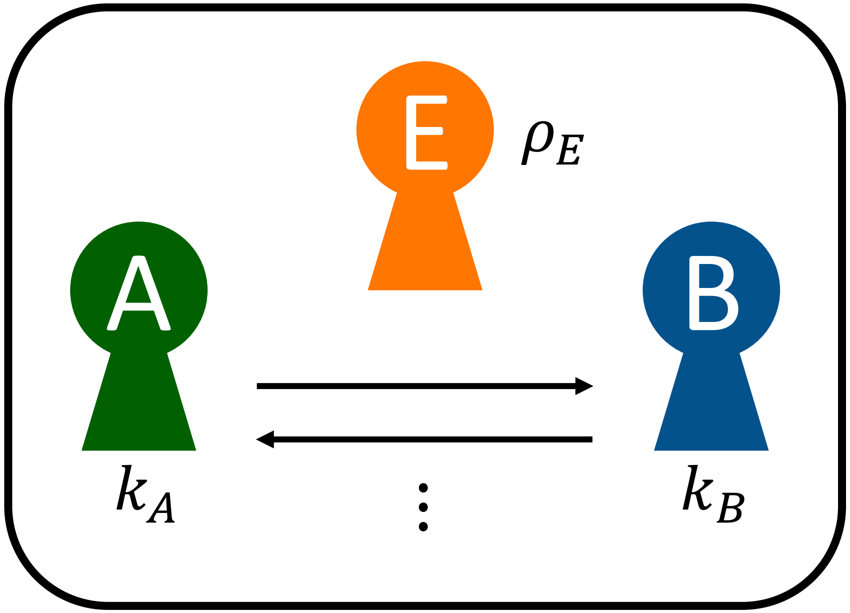
Key Distribution

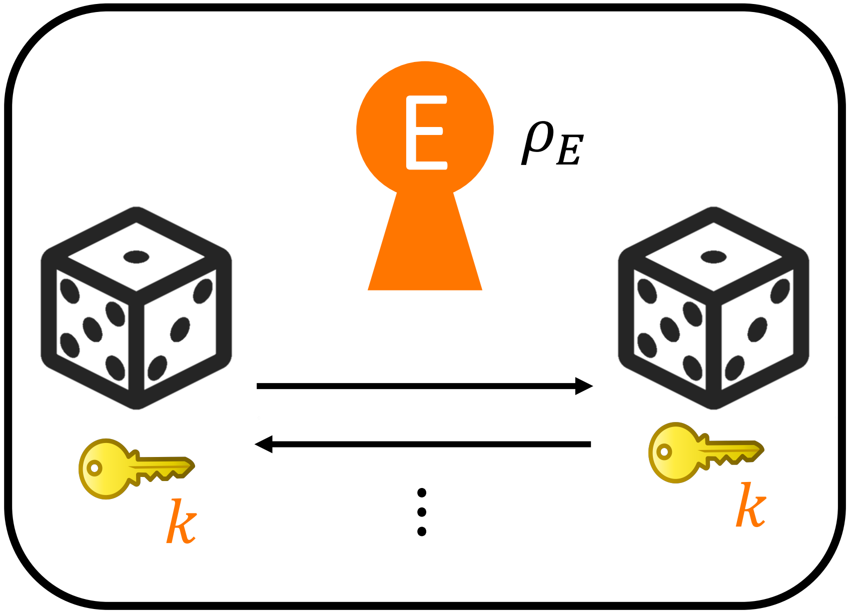
To enable efficient secure encrypted communication,
Alice & Bob need to share a uniform key k against adversary Eve.
How do they establish such a shared key k?



Security Definition

"Simulation paradigm": secure if the real protocol outcome is "indistinguishable" to an "ideal protocol" outcome in trace distance





$$\rho_{\text{real}} \approx \rho_{\text{ideal}}$$

- Trace distance: right distance measure for security
- Real protocol is "as secure as" the ideal protocol

Main Structure of QKD protocol

Encoding

Alice encodes information in some quantum signals and send them to Bob.

Parameter Estimation

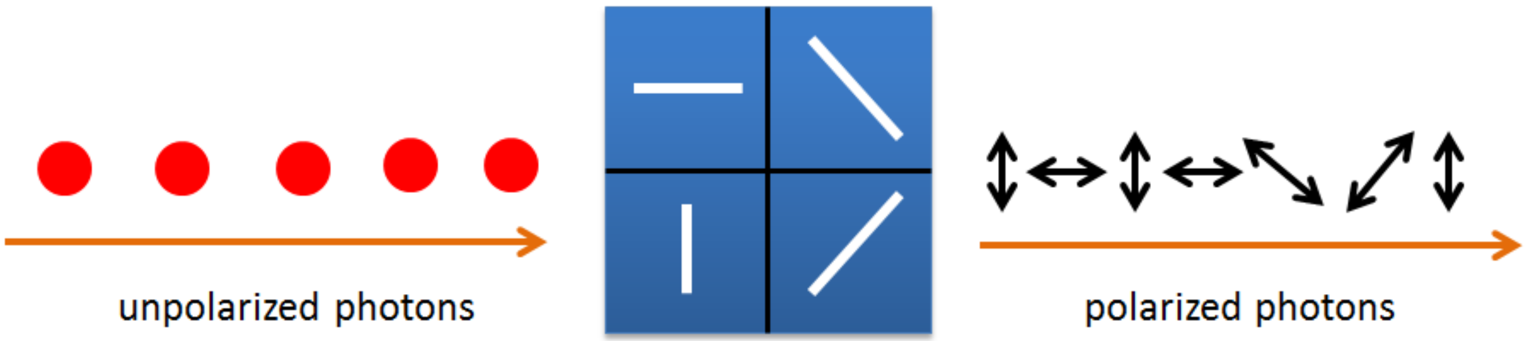
Alice and Bob do measurements on quantum signals and discuss over the classical channel in order to estimate the error rate.

Information Reconciliation and Privacy Amplification

Alice and Bob apply some algorithm depending on error rate so that they can have a shared secret key.

Encoding of BB84

1. Alice sends polarized photons. Each photon polarizes at one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ randomly. Alice need to record what she sent.



Parameter Estimation of BB84

1. Bob measures the photons using a random choice of two bases and records the results.
2. Bob tells Alice which basis he applied for each photons in public channel.
3. Alice tells Bob which photons are measured correctly. Those photons are called "sifted photons" and other photons are aborted.
4. Among the sifted photons, they choose a subset of the photons and compare the measurement results. If more than δ portion are different, they abort the protocol.

Information Reconciliation and Privacy Amplification

Now, let the remaining sifted key at Alice side be S_A and at Bob side be S_B.

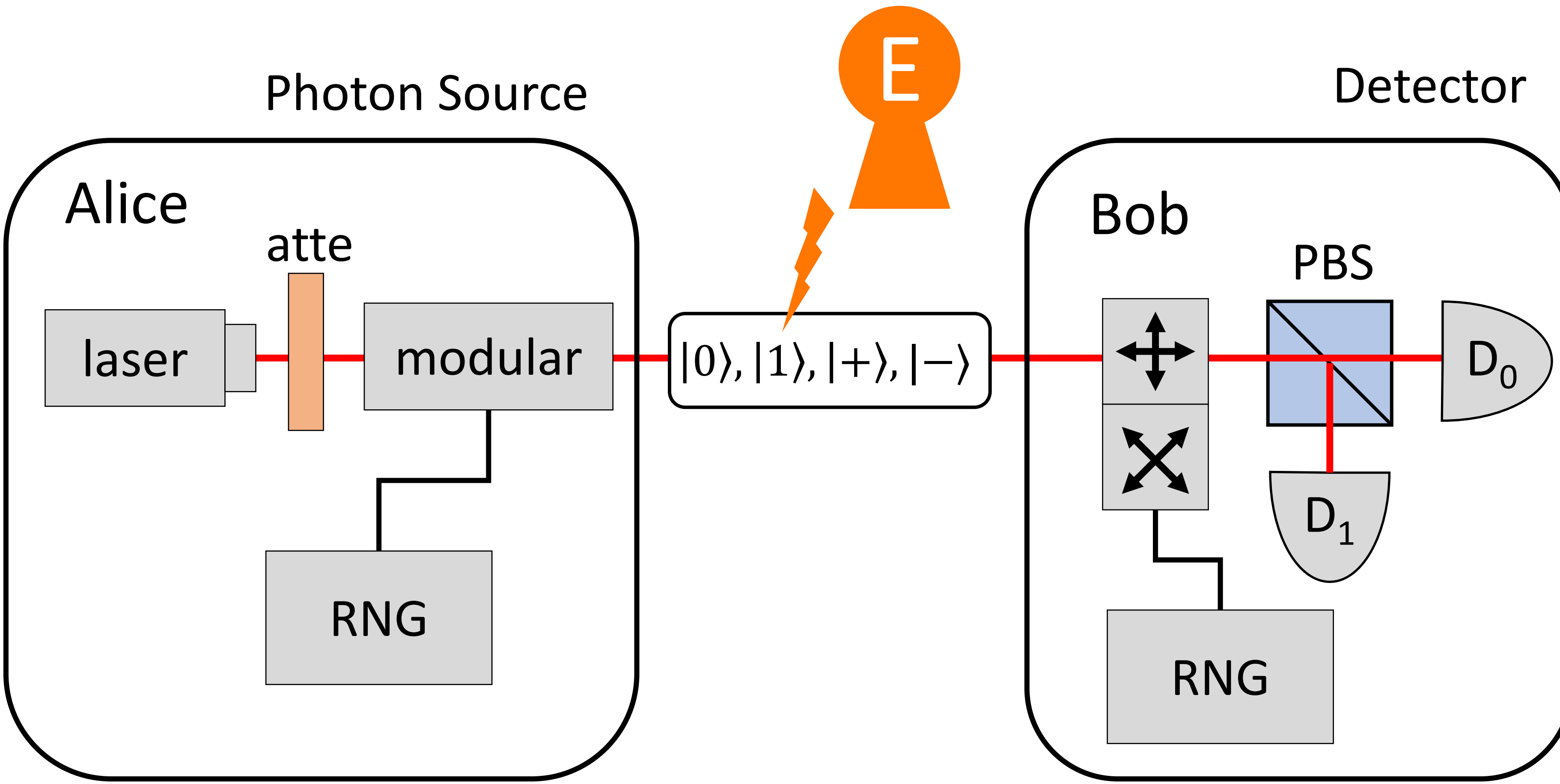
1. Alice sends $x = synd(S_A)$ to Bob.
2. Bob computes $S_B' = corr(x, S_B)$.

Note that if $d(S_A, S_B) < \frac{d-1}{2}$, the error correction code guarantee that

$$S_A = S_B'.$$

3. Alice computes $K_A = H_{PA}(S_A)$ and Bob computes $K_B = H_{PA}(S_B')$, where H_{PA} is a hash function chosen from a family of 2-universal hash functions.

QKD Setup



RNG: random number generator
PBS: polarizing beamsplitter
atte: attenuator

Intuition that why QKD is secure

The properties of quantum mechanics:

No-cloning theorem:

- Two non-orthogonal quantum states could not be copied.

Uncertainty Principle:

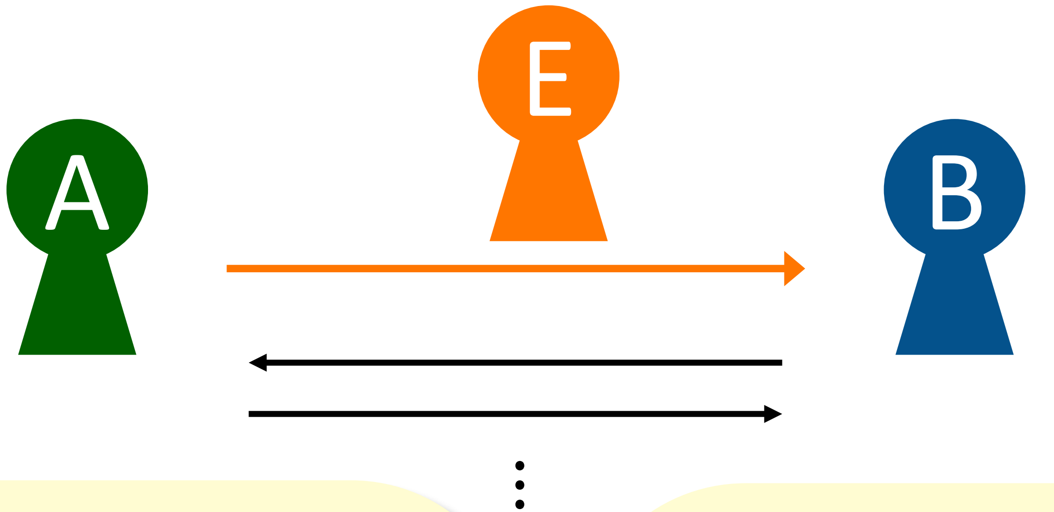
- One could not measure a quantum state without changing the state.

The eavesdropper must resend a new photon after measuring the old one.

The eavesdropper must "guess" the basis.

However, what if we don't have a perfect single photon source?

Security Model of [LC99,SP00] for BB84



Assumptions:

Perfect RNG & auth. classical msgs

Perfect single-photon source

Perfect detector

Threats:

Eve fully control quantum channel, see all classical messages (but not modify), no access to RNG.

No access to source and detector

What's wrong with multi-photon?

- Security proof: IF we have perfect devices, then BB84 is secure!
- However, perfect single-photon source is not realistic
  - Weak coherent sources: photon # follows Poisson distribution
  - Multi-photon pulses give Eve "cloned copies" for free
- Photon-number-splitting (PNS) attack
  - Block all single-photon pulses & steal one photon from all multi-photon pulses.
  - Eve can learn the final key without detected by Alice & Bob

Solution 1: Take multi-photon into account

In 2004, Gottesman et al. gave a security proof for BB84 if knowing the ratio of multi-photon Δ.

Idea: Can we quantify how much information that Eve learns?

Gottesman et al. showed that if Δ is low enough, we can remove all the information that Eve has by sacrificing some key bits.

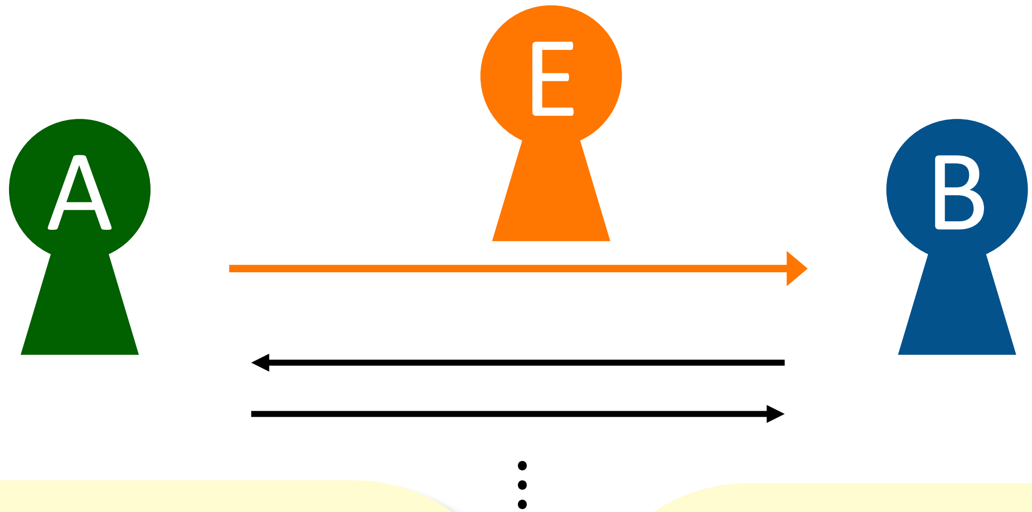
Precisely, we can have secure key bits if $\Delta < 0.0289$.

However,

① the key rate is very low

② it still need nearly perfect single photon source

Security Model of [GLLP04]



Assumptions:
Perfect RNG & auth. classical msgs

Weak coherent source
- almost single photon pulses

Perfect detector and channel
(when no attack)

Threats:
Eve fully control quantum channel, see all classical messages (but not modify), no access to RNG.

No access to source and detector

Discussion: Key Idea of [GLLP04] and Main Issue

- Key idea: single-photon pulses *received by* Bob can be used to distill secure key, even though there are multi-photon pulses and we don’t know where are the single-photon pulses

- Main issue: lower bound single-photon pulses *received by* Bob. Pessimistic estimation needed if no further information.

  - E.g., most pulses are single-photon and received by Bob

  - Need almost perfect source, channel, and detector

- Solution: Decoy-state QKD

  - A clever way to lower bound single-photon pulses received by Bob by exploiting additional *physics assumptions* on the source

Solution 2: Decoy Method

In 2003, Hwang proposed the idea of decoy state.

Idea: If we do not know the ratio Δ in advance,
can we estimate it by some "decoy?"

Hwang modeled the source as Poissonian distribution

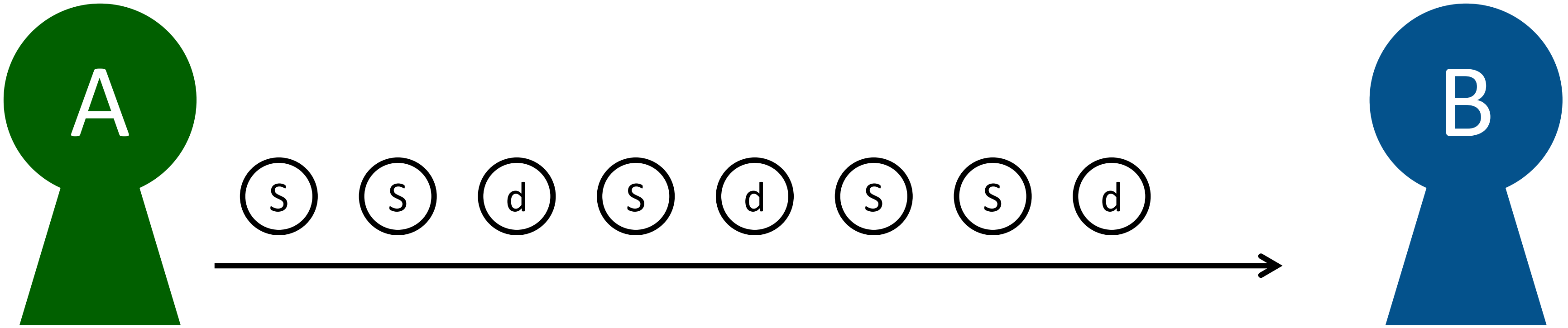
$$\rho_\mu = \sum_n \frac{e^{-\mu}\mu^n}{n!} |n\rangle\langle n|,$$

which is a reasonable model for laser.

In reality, we can adjust the intensity μ of the laser.

Encoding of Decoy

1. Alice sends the signal states ($\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) and the decoy states ($\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) with different intensity.



Here we assume that Eve can distinguish # of photons in each pulse.

However, Eve given # of photons, Eve cannot distinguish it is signal state or decoy state.

Adversary Model

We define Y_n to be the conditional probability that Bob detects an event, given that an n-photon signal is emitted by Alice.

We define e_n to be the bit error probability that Alice and Bob do a measurement and get $Z \otimes Z = -1$ condition on that Alice emits an n-photon pulse.

Since decoy state and signal state have the same properties except the # photon distribution, the only information available to Eve is the number of photons in a signal.

Thus,

$$Y_n(signal) = Y_n(decoy) = Y_n;$$
$$e_n(signal) = e_n(decoy) = e_n.$$

Variables

- Q_μ: the true probability that Bob detects an event condition on the intensity μ over the channel $\mathcal{N}$.

$$Q_\mu = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n \,,$$

which is defined by Y_n and $\mathcal{N}$.

- E_μ: true bit error rate condition on the intensity μ over the channel $\mathcal{N}$

$$Q_\mu E_\mu = e^{-\mu} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} Y_n e_n \,,$$

which is defined by Y_n, e_n and $\mathcal{N}$.

Empirical Estimation for Variables

- $\widetilde{Q_\mu}$: the empirical probability that Bob calculates in the protocol such that

$$\widetilde{Q_\mu} = \frac{D_\mu}{N_\mu},$$

where N_μ is the total # pulses with intensity μ and D_μ is # detect event with intensity μ.

When D_μ is large enough, $\widetilde{Q_\mu} \approx Q_\mu$.

- $\widetilde{E_\mu}$: the empirical bit error rate that Alice and Bob perform random sampling test.

We can get Q_μ and E_μ experimentally.
But what we really care are Y_1 and e_1.

Estimation of e_1

Solve the linear equations.

$$Q_\mu e^\mu = \sum_{i=0}^{\infty} Y_i \frac{\mu^i}{i!}$$

$$E_\mu Q_\mu e^\mu = \sum_{i=0}^{\infty} e_i Y_i \frac{\mu^i}{i!}$$

$$Q_{\nu_1} e^{\nu_1} = \sum_{i=0}^{\infty} Y_i \frac{\nu_1^i}{i!}$$

$$E_{\nu_1} Q_{\nu_1} e^{\nu_1} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_1^i}{i!}$$

$$Q_{\nu_2} e^{\nu_2} = \sum_{i=0}^{\infty} Y_i \frac{\nu_2^i}{i!}$$

$$E_{\nu_2} Q_{\nu_2} e^{\nu_2} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_2^i}{i!}$$

$$\cdots$$

$$Q_{\nu_m} e^{\nu_m} = \sum_{i=0}^{\infty} Y_i \frac{\nu_m^i}{i!}$$

$$E_{\nu_m} Q_{\nu_m} e^{\nu_m} = \sum_{i=0}^{\infty} e_i Y_i \frac{\nu_m^i}{i!}$$

Estimation of e_1

We can get the following bound for the empirical parameters just use 2 different decoy states with intensities μ_1 and μ_2.

$$\widetilde{Y_0^L} \coloneqq \max\left[\frac{\mu_1 \widetilde{Q_{\mu_2}} e^{\mu_2} - \mu_2 \widetilde{Q_{\mu_1}} e^{\mu_1}}{\mu_1 - \mu_2}, 0\right]$$

$$\widetilde{Y_1^L} \coloneqq \frac{\mu_0}{\mu_0\mu_1 - \mu_0\mu_2 - \mu_1^2 + \mu_2^2}\left[\widetilde{Q_{\mu_1}} e^{\mu_1} - \widetilde{Q_{\mu_2}} e^{\mu_2} - \frac{\mu_1^2 - \mu_2^2}{\mu_0^2}\left(\widetilde{Q_{\mu_0}} e^{\mu_0} - \widetilde{Y_0}\right)\right]$$

$$\widetilde{e_1^U} \coloneqq \frac{\widetilde{E_{\mu_1}} \widetilde{Q_{\mu_1}} e^{\mu_1} - \widetilde{E_{\mu_2}} \widetilde{Q_{\mu_2}} e^{\mu_2}}{(\mu_1 - \mu_2)\widetilde{Y_1}}$$

Parameter Estimation of Decoy

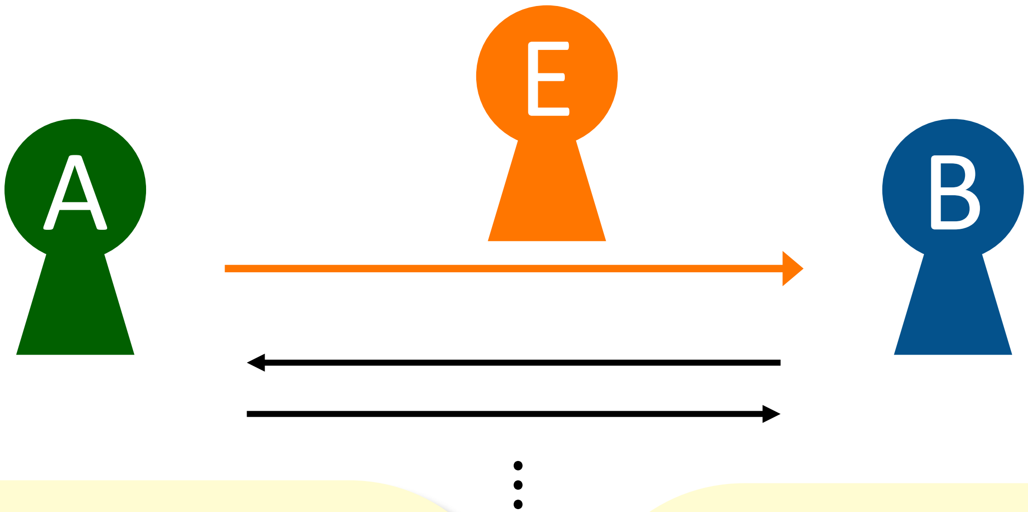
1. Alice and Bob compare ”all” the measurement results of decoy states and they get $\widetilde{E_{\mu_1}}, \widetilde{E_{\mu_2}}$. Note that they don’t compare the result of signal states now.
2. Alice and Bob perform random sampling test and get the empirical bit error rate $\widetilde{E_{\mu_0}}$ of signal pulses.
3. If $\widetilde{E_{\mu_0}} + \epsilon_{err} \geq \delta_{err}$ or $\widetilde{e_1} + \epsilon_{amp} \geq \delta_{amp}$, Alice and Bob abort the protocol, where $\delta_{err}, \epsilon_{err}, \delta_{amp}, \epsilon_{amp}$ are pre-determined parameters.

   Otherwise, they do the next step.

Information Reconciliation and Privacy Amplification

The information reconciliation and privacy amplification of decoy are the same as BB84!

Security Model of Decoy-state QKD [LMC05]



Assumptions:

Perfect RNG & auth. classical msgs

Weak coherent source

- Know distribution of photon #
- Indistinguishable pulses with the same photon #

Detector with "benign error" (indep. of the secret msg)

Threats:

Eve fully control quantum channel, see all classical messages (but not modify), no access to RNG.

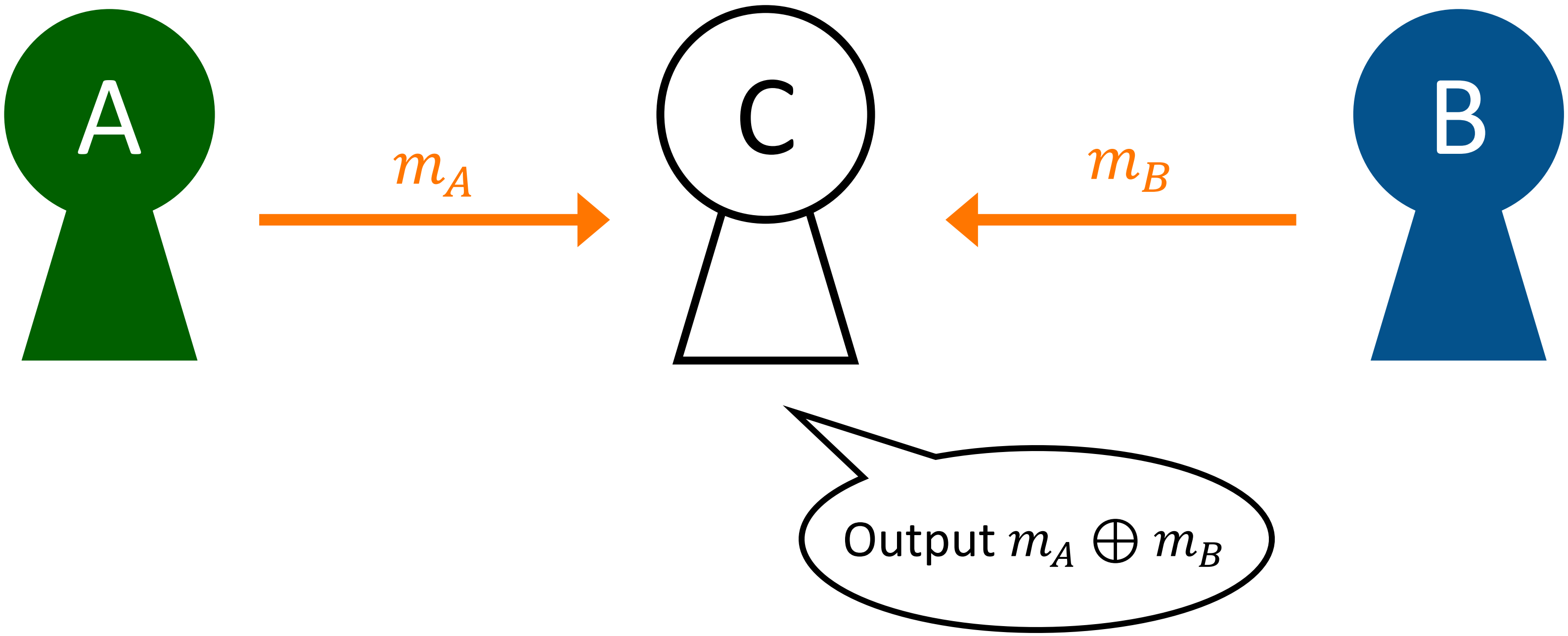
No access to source and detector

Key Idea of Decoy-state QKD & Attack on Detector

- Key idea: use sources with different intensities, which are indistinguishable by Eve, to estimate the single-photon pulses received by Bob
  - E.g., in PNS attack, when Eve block all single-photon pulses, the distribution of received photons will be skewed and detected!
- Next issue: attack on measurement-device!
  - Receive external pulses controlled by Eve, vulnerable to attack.
  - E.g., time-shift attack & detector blinding attack
- Solution: measurement-device independent (MDI) QKD
  - Remove all assumptions on the detector

Measurement device independent QKD

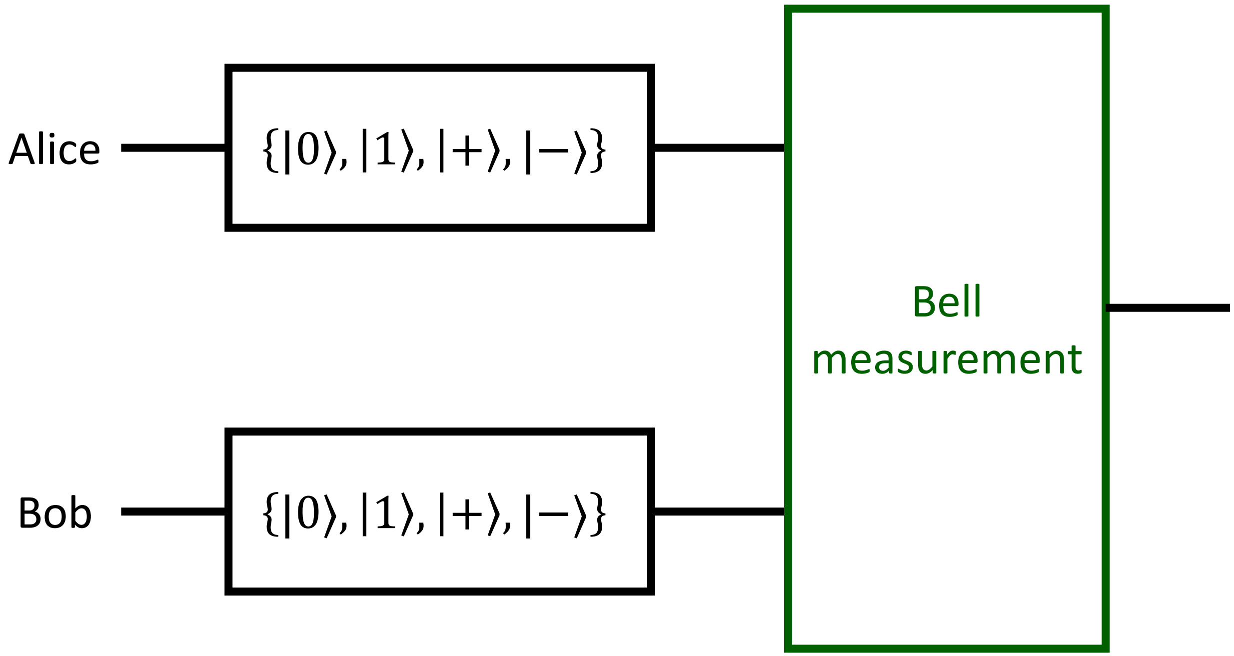
Both Alice and Bob send quantum signal to the untrusted third party.



By uncertainty principle, Charlie can only know whether m_A and m_B are the same by Bell measurement.
Otherwise, he will be caught.

Encoding of MDI QKD

1. Both Alice and Bob send n pulses to the untrusted third party, Charlie, where each pulse is in $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.
2. Charlie announces his Bell measurement result.



$$|\Phi^+\rangle = \frac{|00\rangle + |11\rangle}{\sqrt{2}}$$

$$|\Phi^-\rangle = \frac{|00\rangle - |11\rangle}{\sqrt{2}}$$

$$|\Psi^+\rangle = \frac{|01\rangle + |10\rangle}{\sqrt{2}}$$

$$|\Psi^-\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

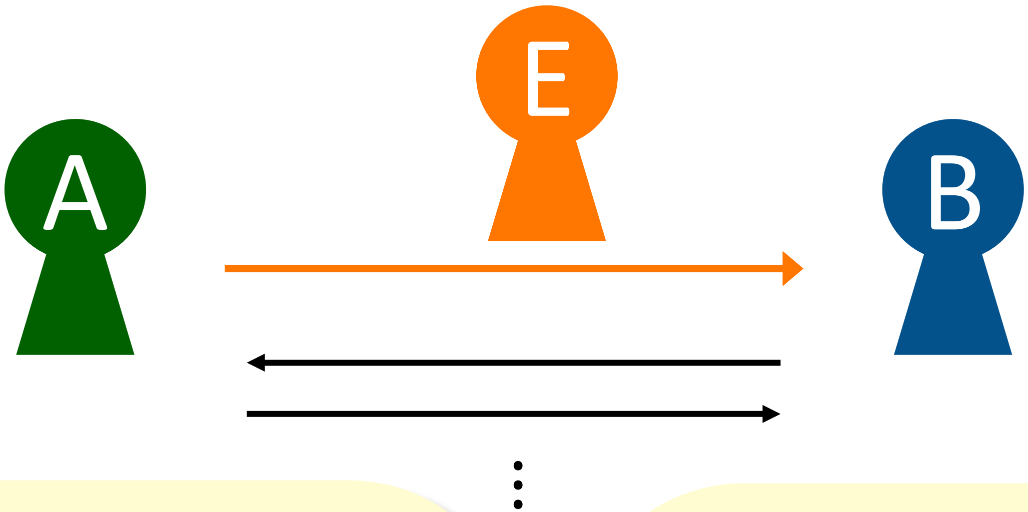
Parameter Estimation

1. Alice and Bob discuss the basis they use before and they discard all the pulses that they encode in different basis.
2. Among the sifted key, only Alice does the bit flip on her sending record if Charlie's Bell measurement result is $|\Psi^+\rangle$ or $|\Psi^-\rangle$ for the pulses encoded in Z basis.
3. Alice does the phase flip on her sending record if Charlie's Bell measurement result is $|\Phi^-\rangle$ or $|\Psi^-\rangle$ for the pulses encoded in X basis.
4. They choose a subset of the photons and compare the measurement results. If more than δ portion are different, they abort the protocol.

Information Reconciliation and Privacy Amplification

The information reconciliation and privacy amplification of decoy are the same as BB84!

Security Model of Decoy-state MDI-QKD [LCQ12]



Assumptions:
Perfect RNG & auth. classical msgs
Weak coherent source
- Know distribution of photon #
- Indistinguishable pulses with the same photon #

No assumption on detector!

Threats:
Eve fully control quantum channel, see all classical messages (but not modify), no access to RNG.

No access to source

Fully control detector!

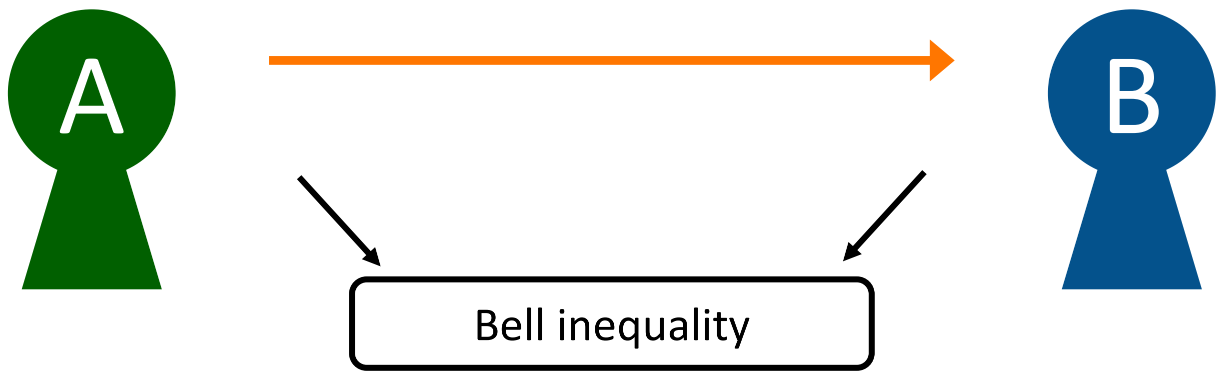
Brief Discussion on MDI-QKD & Fully DI-QKD

- MDI-QKD requires a very different protocol
  - Require Bell measurement on two independent photon sources
  - Harder to implement and lower key rate
- Can we also remove assumptions on the source?
- Fully device-independent (DI) QKD
  - Remove assumptions on all devices
  - But require violating Bell inequality with very high efficiency
  - Beyond current technology

Future

Can we even remove the assumptions of the source?

Yes, the solution is fully device independent QKD.



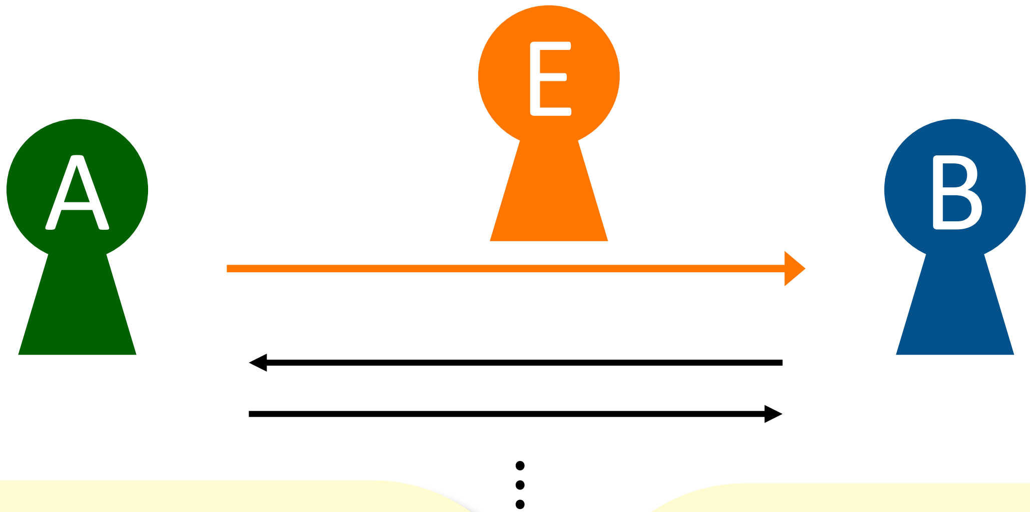
output key k

output key k

However, it need to compute Bell inequality.

There is no fully device independent QKD implementation for now.

Security Model of Fully Device-Independent QKD [LCQ12]



Assumptions:
Perfect RNG & auth. classical msgs

No assumption on all devices!

- Need no-signaling among device

Threats:
Eve fully control quantum channel, see all classical messages (but not modify), no access to RNG.

Eve prepare all devices

Outline

Assumptions of Different Protocols

1. BB84
2. Decoy
3. Measurement Device Independent
4. Device Independent

Future Work

1. Finite Key Analysis
2. Security Proof of RRDPS

Finite Key Analysis

Before 2012, most of the security proofs only deal with asymptotic case.

[TLGR12, HT12] gave a proof for BB84.

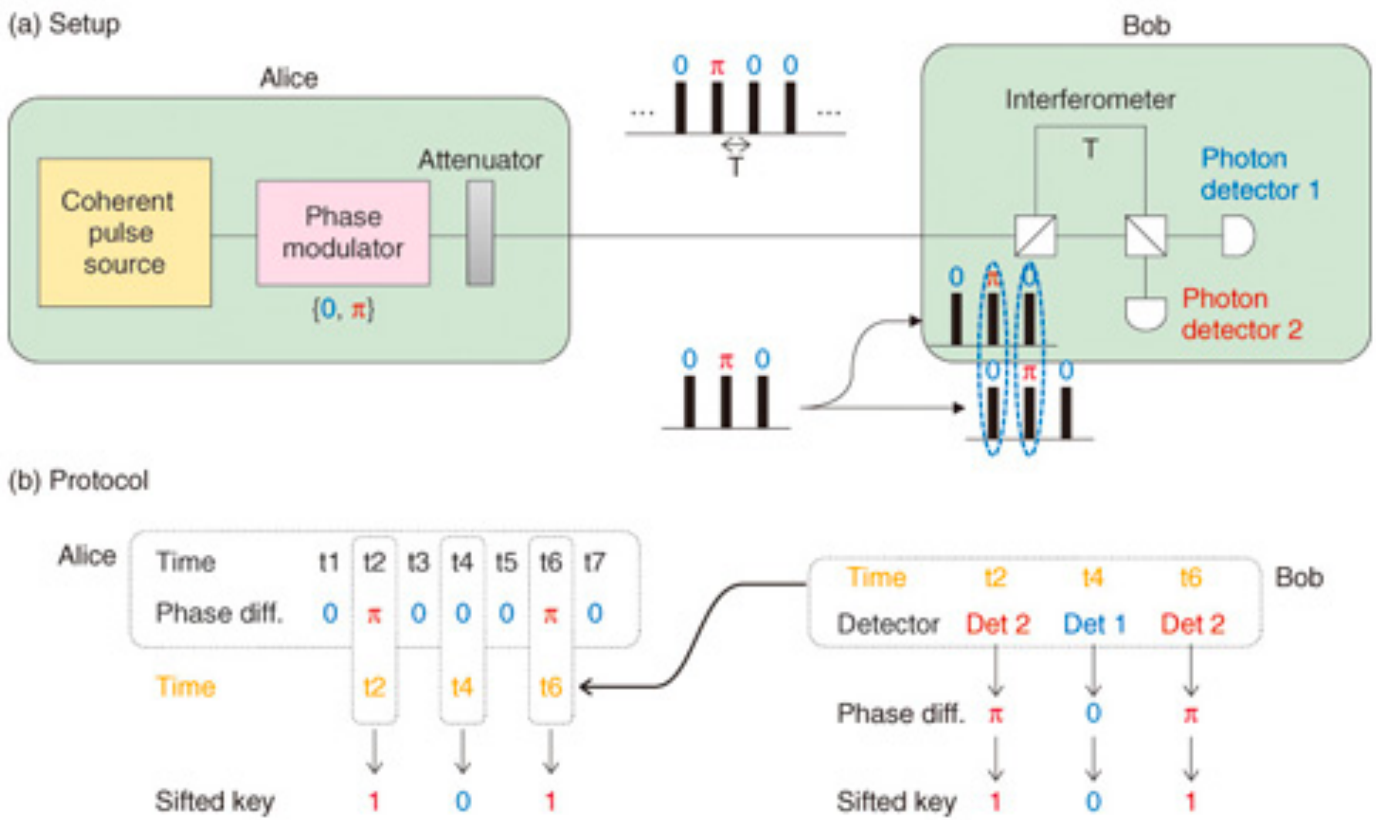
[HN14] gave a proof for decoy protocol.

[CXC+14] gave a proof for MDI QKD.

However, there are some room for the refinement of the key rate, which is important for the industry.

Differential Phase Shift (DPS) QKD

Other direction: protect the number of photon by uncertainty principle.



Round-Robin DPS QKD