Differential-Phase-Shift Quantum Key Distribution

K. Inoue, H. Takesue, T. Honjo

Osaka University
NTT Basic Research Laboratories
JST CREST

Contents

(1) Setup & protocol
(2) Eavesdropping
(3) Modified protocol with decoy slots
(4) Requirement for light source
(5) Entanglement-based schemes
Setup

- Alice
  - Coherent pulse source
  - Phase mod.
  - {0, π}
  - att.

Bob

- Coherence time >> T

< 1 photon/pulse

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”

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 -

Alice \rightarrow [n \text{ photon/pulse}] \rightarrow Eve \rightarrow [\text{lossless}] \rightarrow [\text{receiver}] \rightarrow Bob

Passive receiver @ Eve

Coincident rate between Bob and Eve

\[ T_n \times (1 - T)n = (1 - T)Tn^2 \]

Fraction of leakage

\[ \frac{(1 - T)Tn^2}{Tn} = (1 - T)n \quad \Rightarrow \quad n \quad \text{for} \ T \ll 1 \]
Receiver with quantum memory

Eve
beam splitter
lossless

switch

(1-T)n (/pls.)

memory
memory
memory
memory

after detection-time disclosed

memory
memory
memory
memory

fraction of leakage

detection prob.

\[
\frac{2(1-T)n^2}{Tn} = 2(1-T)n \rightarrow 2n \quad \text{for } T \ll 1
\]
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.

key creation rate (log) vs. transmission loss (dB)

DPS
BB84 with laser

error
Differential-Phase-Shift QKD with Decoy Slots

Alice inserts vacant two pulses at random.

no click
Intercept & Resend attack is prohibited, provided that dark count rate is constant.
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.

\[
\Delta L
\]

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

\[
= \sin^2 \left[ \frac{\pi f}{FSR} \right]
\]

\[
FSR = \frac{\nu}{\Delta L} : \text{free spectrum range}
\]

Error rate

\[
\int_{-\infty}^{\infty} T(f) F(f) df
\]

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

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

(\(\delta f\): linewidth)
Three lasers are examined. 

Experimental setup

- cw-laser
- intensity mod.
- phase mod.
- waveguide interferometer

$\Delta L = 20 \text{ cm}$
$\text{FSR} = 1 \text{ GHz}$

$1 \text{ ns}$

Experimental setup

<table>
<thead>
<tr>
<th>Linewidth (MHz)</th>
<th>Bit error rate (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>5</td>
</tr>
<tr>
<td>20</td>
<td>10</td>
</tr>
</tbody>
</table>

Linewidth should be < 0.06 % of FSR.
future scheme for long distance

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

Entanglement source

coherent pulse source
parametric medium
filter

System length is double of photon transmission distance.
Source output:

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

\( t_j \): signal photon at time \( t_j \)
\( t_{j,i} \): idler photon at time \( t_j \)
\( \mu \): probability of one-pair generation
\( \phi_p \): pump phase

Interferometer output for coincident detection

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

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

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

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.

\[ \text{normal: } (1/2)\mu\eta^2 \]  \[ \text{eavesdropped: } (3/8)\mu\eta^2 \]  \( \eta \): line transmittance
Eavesdropping against Entanglement-Based DPS-QKD (2)  
- Source Replacement -

*Eve gets key information without inducing bit errors.*  
*However,....*
Quantum entanglement

Alice → Entanglement source → Bob

Bob’s detection

Entanglement source

Bob’s detection

μ pair/pls

η

Coincident rates

between time slots creating a key bit: $\mu \eta^2 / 2$

between shifted slots: $\mu \eta^2 / 4$

key creation

The eavesdropping is revealed from the coincident rates.

Classical entanglement

Alice → coherent source → Bob

Coincident rates are uniform between any time slots.

The eavesdropping is revealed from the coincident rates.
Experiment of entanglement-based QKD (A)

Entanglement generation

Laser
- Intensity mod.
  - Rep. rate: 1 GHz
  - Pulse width: 100 ps
- Opt. amp.
- Filter
- Fiber (500 m)
- Liq. Ni
- AWG filter
  - Signal (1551.6 nm)
  - Idler (1550.6 nm)

Four-photon mixing
- Pump
  - Signal
  - Idler

Waveguide interferometer
(ΔL = 20 cm)
- Phase mod.
- Time interval analyzer

(*)
Experimental results

Two photon interference

Waveguide temperature in Alice
Blue: $\Delta \theta_b = 0$, red: $\Delta \theta_b = \pi$.

Visibility $= 70\%$

Key creation rate $= 0.34$ bps with $8.6\%$ error

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