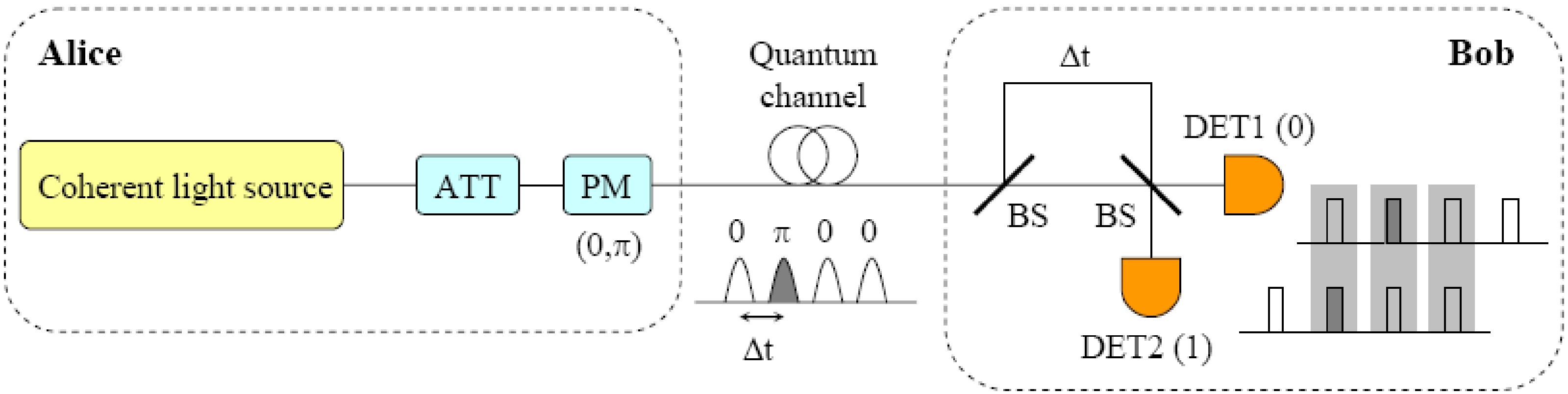
Unconditional security of differential phase shift quantum key distribution

Kai Wen, Yoshihisa Yamamoto

Ginzton Lab and Dept of Electrical Engineering

Stanford University

Basic idea of DPS-QKD



Protocol

1. Alice generates a sequence of attenuated pulses, e.g. the average photon number per pulse is 0.2. The number of pulses is N+1.
2. Alice picks a random *N*-bit key, encodes each bit into the phase difference between two consecutive pulses (DPSK).
3. Bob employs an unbalanced interferometer which delays the pulse sequence by 1 bit on one arm. He then measure the outcome by the interferometer to determine the phase shift and thus the encoded key.
4. On average, Alice and Bob can share 0.2 x *N* bits of the random key.
5. Finally, Alice and Bob apply error correction and privacy amplification to obtain a correct and secure key.

K. Inoue, E. Waks and Y. Yamamoto, Phys. Rev. A 68, 022317 (2003)

Security against eavesdropping

- Quantum uncertainty principle and non-cloning theorem
- Channel bit error rate and channel efficiency binds Eve's capability of eavesdropping.
- Against intercept-and-resend attack:
  - Eve measures the pulse sequence similar to Bob.
  - Once she obtain one result, she reconstructs the two consecutive pulses with the resulting phase shift.
  - In these two pulses, Bob has 1/4 chances get an error.
- Against beam-splitting attack:
  - Eve uses a beam-splitter to split the pulses into two parts. She sends one part to Bob and keeps the other part. She then measures the other part similar to Bob to obtain a part of Alice's random key.
  - Bound by the channel efficiency η, Eve can only keep $0.2N(1-\eta)$ photons.
  - Because the pulses are attenuated, there is still significant chance that Bob obtains the phase shifts in timeslots in which Eve doesn't get.

Unconditional security proof

- Suppose Eve has ultimate computation power and techniques allowed by physics.
- Find the capability of Eve’s eavesdropping, given bit error rate and channel efficiency.
- Apply theoretical bound of error correction and privacy amplification to make sure Eve’s mutual information is exponentially small with a security parameter.

Model of DPS-QKD

- Pulse block
  - Contains n pulses and m photons.
  - Alice encodes (n-1)-bit random key inside a block.
  - In the worst case, each photon is of the same quantum state (m copies of the state).
  - Due to high channel loss, at most 1 photon can arrive at Bob's side. Actually, Bob can count the photon number of each block arriving at his side and discard those with more than 1 photons.
  - We call it [m, n] DPS-QKD

Preparation of the initial state

- Pulses in a block represents an *n*-dimensional Hilbert space in quantum mechanics.
  - Each pulse is one base vector

$$|i\rangle = (\underbrace{0 \quad \cdots \quad 0}_{i} \quad 1 \quad \underbrace{0 \quad \cdots \quad 0}_{n-i-1})^{\mathrm{T}}, i = 0 \cdots n-1$$

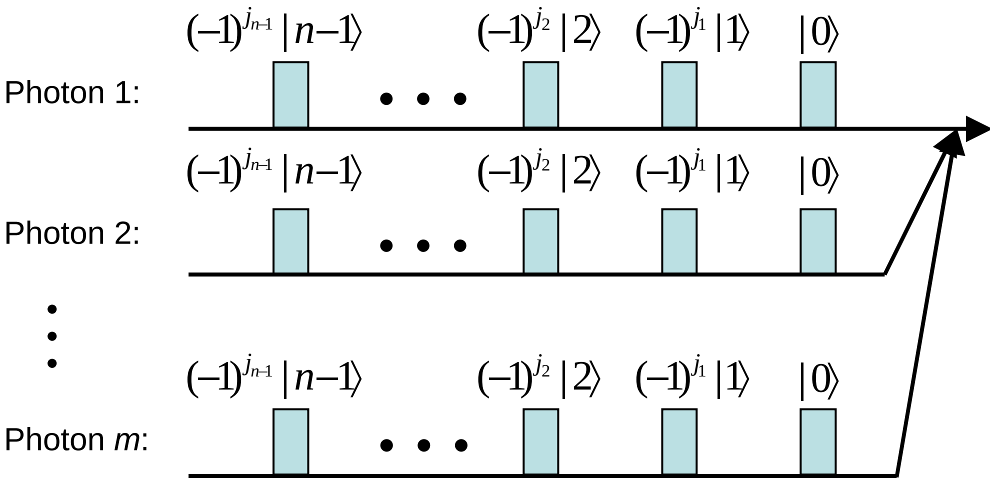
  - Encode the (*n*-1)-bit key into the pulse state of each photon

$$|\phi_j\rangle_B = \frac{1}{\sqrt{n}}\left(|0\rangle + \sum_{k=1}^{n-1}(-1)^{j_k}|k\rangle\right)$$

$$j = (j_{n-1} j_{n-2} \cdots j_1)_2$$

  - Prepare the initial entangled state

$$|\phi\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=0}^{2^{n-1}-1}\left(|j_1 \cdots j_{n-1}\rangle_A \otimes |\phi_j\rangle_B^{\otimes m}\right)$$



    - The state labeled with A is the state of n-1 2-dim qubits
      $|0\rangle_A = (1 \quad 0)^{\mathrm{T}}, |1\rangle_A = (0 \quad 1)^{\mathrm{T}}$
    - Example [2,3] DPS-QKD

$$|\phi\rangle_{[2,3]} = \frac{1}{2}\left\{|00\rangle_A \otimes \left[\frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle + |2\rangle\right)\right]_B^{\otimes 2} + |01\rangle_A \otimes \left[\frac{1}{\sqrt{3}}\left(|0\rangle + |1\rangle - |2\rangle\right)\right]_B^{\otimes 2}\right.$$

$$\left. + |10\rangle_A \otimes \left[\frac{1}{\sqrt{3}}\left(|0\rangle - |1\rangle + |2\rangle\right)\right]_B^{\otimes 2} + |11\rangle_A \otimes \left[\frac{1}{\sqrt{3}}\left(|0\rangle - |1\rangle - |2\rangle\right)\right]_B^{\otimes 2}\right\}$$

Description of eavesdropping

- When Alice sends the photons labeled with B to Bob through the quantum channel, Eve can measure, transform or do other operations allowed by physics.
- In general, we can treat that the channel is totally controlled by Eve.
- Any Eve's operation can be described as a POVM (Positive Operator Valued Measure), in the following matrix form:

$$M_E = \left(a_{i,j}\right)_{(n^m)\times(n^m)}$$

  where every matrix element a_{ij} is an arbitrary complex number and $|a_{ij}| <= 1$.
- In quantum mechanics, the final state through the channel is

$$|\phi'\rangle = (I_{2^{n-1}} \otimes M_E)|\phi\rangle = \frac{1}{\sqrt{2^{n-1}}} \sum_{j=0}^{2^{n-1}-1} \left(|j_1 \cdots j_{n-1}\rangle_A \otimes M_E |\phi_j\rangle_B^{\otimes m} \right)$$

Bob's side

- Measure only 1 photon in each block by channel loss or discarding multiple-photon blocks
  - Partial trace
  - Symmetry -> Bob measure the first photon

$$\mathrm{Tr}_{B_2 \cdots B_m} |\phi'\rangle$$

- The 1-bit delayed interferometer is described by an (2(n+1) x n)-dimensional matrix M_{DPS}

$$M_{DPS} = \left(b_{i,j}\right)_{(2(n+1))\times(n)}$$

$$\forall j = 1 \cdots n, b_{2j-1,j} = \frac{1}{2}, b_{2j,j} = -\frac{1}{2}, b_{2j+1,j} = \frac{1}{2}, b_{2j+2,j} = \frac{1}{2}$$

$$otherwise, b_{i,j} = 0$$

- The final state arrives before Bob's detectors:

$$|\phi''\rangle = (I_{2^{n-1}} \otimes M_{DPS}) Tr_{B_2 \cdots B_m} |\phi'\rangle$$

Detection

- After the interferometer, the pulses in a block are split into 2(*n*+1) pulses in *n*+1 timeslots, namely, *l*=0,…,*n*. Each timeslot has two pulses, representing the two values of one key bit.
- Only the results in the middle 2(*n*-1) timeslots are conclusive. Otherwise, Bob should discard the results of the timeslot 0 and timeslot *n*.
- After Bob reports the timeslot *l*, if *l*>1, Alice should apply the following operation to her qubits labeled A, so that Alice and Bob can obtain the same bit value.

$$CNOT(l-1,l) = \left(c_{i,j}\right)_{2^{n-1}\times 2^{n-1}}$$

$$= \underbrace{I_2 \otimes \cdots \otimes I_2}_{l-2} \otimes \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix} \otimes \underbrace{I_2 \otimes \cdots \otimes I_2}_{n-1-l}$$

  - The resulting state is

$$|\phi_l\rangle = (CNOT(l-1,l) \otimes I_m)\,|\phi''\rangle$$

Error rates and channel efficiencies

- In quantum mechanics, there are two different types of errors
  - Bit error rate of timeslot 0 < *l* < n

$$M_l^{bit} = \frac{I_{2^{n-1}m} - I_{2^{l-1}} \otimes (|0\rangle\langle 0| - |1\rangle\langle 1|) \otimes I_{2^{n-l-1}} \otimes \left(|2l+1\rangle\langle 2l+1| - |2l+2\rangle\langle 2l+2|\right)}{2}$$

$$P_l^{bit} = \langle \phi_l | M_l^{bit} | \phi_l \rangle, \forall l \in \{1, \cdots, n-1\}$$

  - Total bit error rate in a block $P^{bit} = \sum_{l=1}^{n-1} P_l^{bit}$
  - Phase error rate of timeslot 0 < *l* < n

$$M_l^{ph} = \frac{I_{2^{n-1}m} - I_{2^{l-1}} \otimes (|0\rangle\langle 1| + |1\rangle\langle 0|) \otimes I_{2^{n-l-1}} \otimes \left(|2l+1\rangle\langle 2l+2| + |2l+2\rangle\langle 2l+1|\right)}{2}$$

$$P_l^{ph} = \langle \phi_l | M_l^{ph} | \phi_l \rangle, \forall l \in \{1, \cdots, n-1\}$$

  - Total phase error rate in a block $P^{ph} = \sum_{l=1}^{n-1} P_l^{ph}$

- Channel efficiency of timeslot 0 < *l* < n

$$M_l^{eff} = I_{2^{n-1}} \otimes \left(|2l+1\rangle\langle 2l+1| + |2l+2\rangle\langle 2l+2|\right)$$

$$P_l^{eff} = \langle \phi_l | M_l^{eff} | \phi_l \rangle, \forall l \in \{1, \cdots, n-1\}$$

  - Total channel efficiency in a block $P^{eff} = \sum_{l=1}^{n-1} P_l^{eff}$

Security

- The unconditional secure key generation rate of quantum key distribution is given by

$$R = 1 - H\left(P^{bit} / P^{eff}\right) - H\left(P^{ph} / P^{eff}\right)$$

$$H(x) = -x \log_2 x - (1-x)\log_2(1-x)$$

- In experiment, we can only measure and obtain bit error rates and channel efficiencies.

- So we should know the maximal phase error rate from arbitrary Eve's POVM matrix M_E, so as to find the lower bound of the unconditional secure key generation rate.

$$R \geq 1 - H\left(P^{bit} / P^{eff}\right) - H\left(P^{ph}_{\max}(P^{bit}_l, P^{eff}_l)\right)$$

$$P^{ph}_{\max}(P^{bit}_l, P^{eff}_l) = \max\left(\sum_{l=1}^{n-1} P^{ph}_l / P^{eff}\right)$$

  - The protocol is unconditional secure if this lower bound is positive.

Optimization Problem

- Variables: the elements in Eve's matrix

$$M_E = \left(a_{i,j}\right)_{(n^m)\times(n^m)}$$

- Goal: the maximal total phase error rate in a block

$$P_{\max}^{ph} = \max\left(\sum_{l=1}^{n-1} P_l^{ph} / P^{eff}\right)$$

- Constraints:
  - Matrix requirements $|a_{i,j}| \leq 1$
  - Channel efficiency in every time slot is $\eta/(n\text{-}1)$

$$P_l^{eff} = \eta/(n-1), \forall l \in \{1,\cdots,n-1\}$$

  - Bit error rate in every time slot is e_b

$$P_l^{bit} / P_l^{eff} = e_b, \forall l \in \{1,\cdots,n-1\}$$

Optimization Range

- Typical values for our optimization
  - m = 2~4
  - n = 8~20
  - e_b = 1%~4%
  - η = 1e-2~1e-5
- Calculation takes an order of $2^n n^m$

Analytical Result for [1,n] DPS-QKD

- Bit error rates:

$$
\begin{aligned}
p_l^{bit} = \frac{1}{4n}[&|a_{l-1,l-1} - a_{l,l}|^2 + |a_{l-1,l} - a_{l,l-1}|^2 + \\
&(|a_{l-1,1}|^2 + \cdots + |a_{l-1,l-2}|^2 + |a_{l-1,l+1}|^2 + \cdots + |a_{l-1,n}|^2) + \\
&(|a_{l,1}|^2 + \cdots + |a_{l,l-2}|^2 + |a_{l,l+1}|^2 + \cdots + |a_{l,n}|^2)],
\end{aligned}
$$

- Phase error rates:

$$
p_l^{ph} = \frac{1}{2n}[|a_{l,1}|^2 + \cdots + |a_{l,l-1}|^2 + |a_{l-1,l}|^2 + \cdots + |a_{l-1,n}|^2]
$$

- The relation between two types:

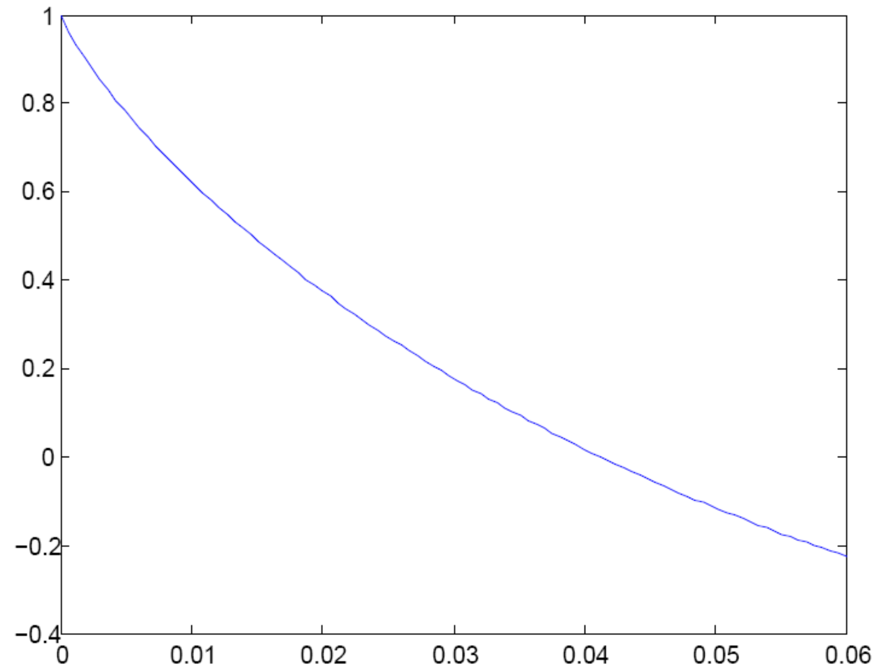
$$
P^{ph} \leq (3+\sqrt{5})P^{bit}
$$

- Secure key generation rate:

$$
R \geq 1 - H(e_b) - H\left((3+\sqrt{5})e_b\right)
$$

  - Unconditional secure if e_b <= 4.12%

- Observe the expressions
  - Both constraints and goals are quadratic.
  - Non-convex problem.
  - Variables can be reduce to real numbers.



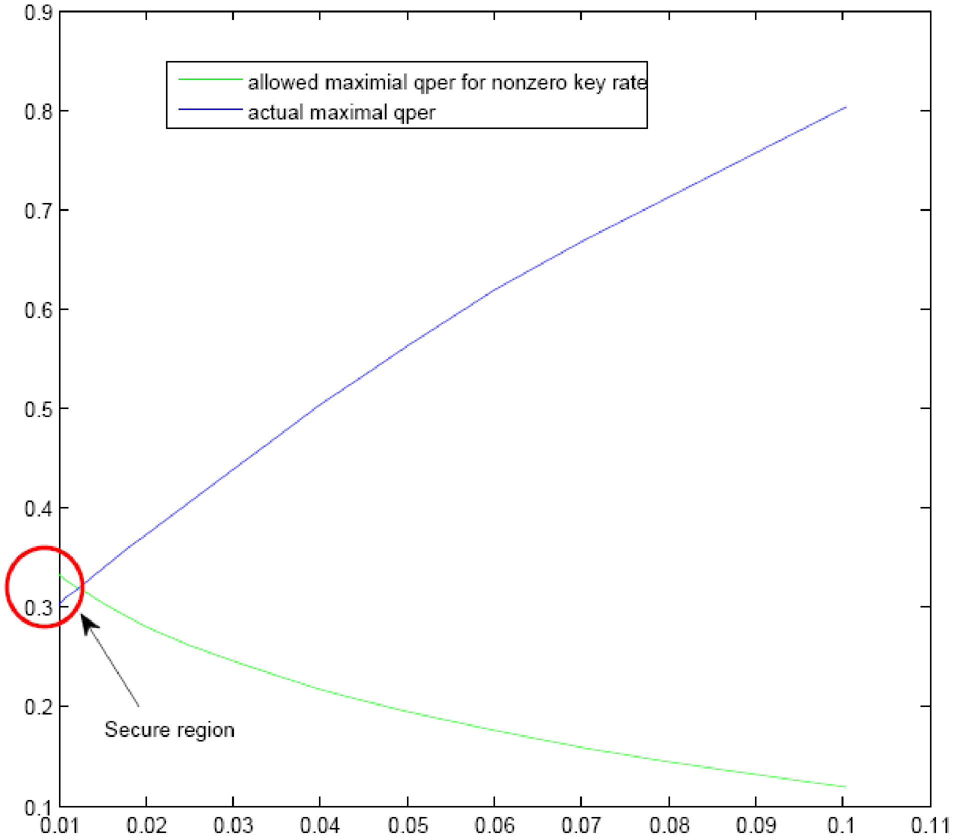
K. Wen, K. Tamaki and Y. Yamamoto, arXiv:0806.2684 (2008)

Multiple-photon cases

- Multiple-photon: $m>1$
- Nonlinear optimization, using optimization solver KNITRO on NEOS server
  - Only find the local maxima
- Reduce the dimension of the variables
  - Complex->Real variables (?)
  - Dimension of the matrix: n^m x n^m -> n x n^m
- Precalculate all the matrices and load them as the data file in AMPL.
- Use sparse matrices to reduce the memory consumption.

[2,8] DPS-QKD Result

- KNITRO output
  - dps_2_8_interp.txt
  - About 2-3 hours
- The properties of the result
  - P^{ph}/P^{eff} only depends on P^{bit}/P^{eff}, rather than the absolute values.
  - The maxima should be at the constraint boundary.
- Typical experiment has e_b >= 1%.



Difficulties and Further Research

- To calculate higher n and m.
  - Still much longer time to optimize higher n and m
    - Limitation of NEOS server,
      - Speed: [2,8] 3 hrs; [2,9] 5hrs; [2,10] exceeds the time limit of about 6hrs.
      - Space: Maximal size of the data file
  - Local Optimization vs Global Optimization
    - Use global optimization
      - Simulated Annealing
      - Genetic Algorithm
      - Monte Carlo
      - Others
- Our goals
  - Calculate up to [4,20] DPS-QKD. The total number of variables is 20^5=3.2M
  - Further tuning the program
    - Reduce the dimension
    - Distributed computing