Generalized Approach for Analysing Quantum Key Distribution Experiments

Arpita Maitra and Suvra Sekhar Das
C R Rao AIMSCS & Indian Institute of Technology Kharagpur

December 18, 2019

Outline of the Talk

- Preliminaries
  - Physical Representation of Qubit
  - Fock State Basis
  - Quantum Description of
    - Beam Splitter
    - Phase Retarder
- Brief Description of the Algorithm
- Importance in Cryptology
- Concluding Remarks
  - Caveat
  - Summary

Preliminaries: Qubit and Its Different Representation

- Bit (0 or 1): basic element of a classical computer
- The quantum bit (called the qubit): the main mathematical object in the quantum paradigm (physical counterpart is a photon)

Physical support	Name	Information support	$\|0\rangle$	$\|1\rangle$
Photon	Polarization encoding	Polarization of light	Horizontal	Vertical
	Number of photon	Fock state	Vacuum	Single photon state
	Time bin encoding	Time of arrival	Early	Late
Electrons	Electronic spin	Spin	Up	Down
	Electron number	Charge	No electron	One electron

Jones Matrix vs. Fock State Representation

- Any optical device can be represented by a $2^n \times 2^n$ matrix called Jones Matrix, where, n is the number of particles
- The size of the matrix increases exponentially with the number of particles
- Hence, as the number increases, it becomes difficult to handle the matrices
- Alternate solution; Fock State Representation of Photon

Fock State Representation

- In Fock State Basis, the states are represented by integers
- Each integer signifies the number of photon presented in input-output signal
- For example, $|0\rangle$ means no photon present in the signal, $|1\rangle$ implies presence of a single photon, $|2\rangle$ stands for two photons in the signal etc.

Fock State Representation Contd.

- Any state $|n\rangle$ can be written as

$$|n\rangle = \frac{1}{\sqrt{n!}}(a^\dagger)^n |0\rangle$$

where, $a^\dagger$ is creation operator, i.e, each operation of this operator generates a single photon. Precisely,

$$\begin{aligned}
|1\rangle &= a^\dagger |0\rangle \\
|2\rangle &= \frac{1}{\sqrt{2}} a^\dagger |1\rangle \\
&= \frac{1}{\sqrt{2.1}} a^\dagger a^\dagger |0\rangle \\
&= \frac{1}{\sqrt{2!}} (a^\dagger)^2 |0\rangle \\
&\vdots \\
|n\rangle &= \frac{1}{\sqrt{n!}} (a^\dagger)^n |0\rangle
\end{aligned}$$

Fock State Representation Contd.

- Here, we will deal with two modes of a photon. One is polarization and another is number of photon in a signal
- The Fock state representation will be $|n_H, n_V\rangle$, where n_H represents the number of horizontally polarized photons and n_V represents vertically polarized photons with $n_H + n_V = n$.
- The basis state can be written in terms of annihilation and creation operator as follows.

$$|n_H, n_V\rangle = \frac{(a_H^\dagger)^{n_H}(a_V^\dagger)^{n_V}}{\sqrt{n_H! n_V!}} |0\rangle .$$

Fock State Representation Contd.

- Any n photon state can be expressed as the superposition of the basis states. That is any n photon state can be written as

$$|\psi^n\rangle = \sum_{n_H=0}^{n} C_{n_H} |n_H, n_V\rangle |_{n_V=n-n_H}$$

  where, $\sum_{n_H=0}^{n} |C_{n_H}|^2 = 1$.
- Consider, a single photon state $|\psi^1\rangle$ with 45° angle polarization.
- Such state can be expressed as equal superposition of Horizontal and Vertical polarization. That is we can write

$$|\psi^1\rangle = \frac{1}{\sqrt{2}}(|1_H, 0_V\rangle + |0_H, 1_V\rangle)$$

Beam Splitter

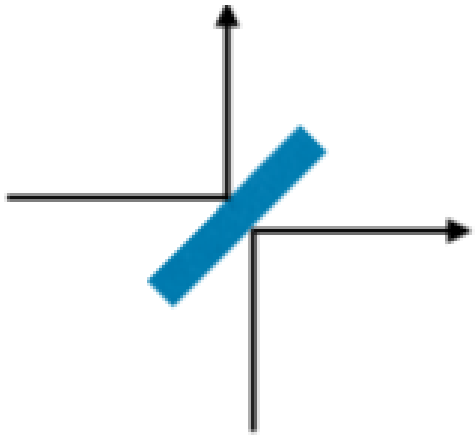

Figure: Figure shows the schematic diagram of a beam splitter. Here, incoming ray which is projected on the beam splitter through port 1 is reflected through port 4 (vertical arrow) and transmitted through port 3 (horizontal arrow). The incoming ray which is projected on the beam splitter through port 2 is reflected through port 3 (horizontal arrow) and transmitted through port 4 (vertical arrow).

Beam Splitter Contd.

The input-output relationship of Quantum Non-Polarized Beam Splitter (NBS) is as follows.

$$\begin{pmatrix} c^\dagger \\ d^\dagger \end{pmatrix} = \begin{pmatrix} t_0 & r_1 \\ r_0 & t_1 \end{pmatrix} \cdot \begin{pmatrix} a^\dagger \\ b^\dagger \end{pmatrix}$$

where, where t_0 (resp. t_1) is the transmission coefficient of port 1 (resp. port 2) and r_0 (resp. r_1) is the reflection coefficient of port 1 (resp. port 2). And $c^\dagger, d^\dagger$ are creation operator at port 3 and 4 respectively and $a^\dagger, b^\dagger$ are the creation operator at the input ports 1 and 2 respectively.

Beam Splitter Contd.

Based on the construction of the BS, the sign of the coefficients is determined. The conventional choice for a BS cube is $\arg(r_0) = \arg(r_1) = \arg(t_0) = 0$, but $\arg(t_1) = \pi$.

Set $r_0 = r_1 = \sqrt{\eta}$ and $t_0 = t_1 = \sqrt{1-\eta}$, then one may write,

$$\begin{aligned} c^\dagger &= \sqrt{1-\eta}a^\dagger + \sqrt{\eta}b^\dagger, \\ d^\dagger &= \sqrt{\eta}a^\dagger - \sqrt{1-\eta}b^\dagger \end{aligned}$$

Alternatively, we can write

$$\begin{aligned} a^\dagger &= \sqrt{1-\eta}c^\dagger + \sqrt{\eta}d^\dagger, \\ b^\dagger &= \sqrt{\eta}c^\dagger - \sqrt{1-\eta}d^\dagger \end{aligned}$$

Beam Splitter Contd.

- If we consider polarization along with the photon number, then an extra index has to be added with the operators
- Instead of $a^\dagger$ (resp. $b^\dagger$) we use $a_j^\dagger$ (resp. $b_k^\dagger$), where j, k each indicates either horizontal or vertical polarization.
- Hence, the input-output relationship becomes

$$a_j^\dagger = \sqrt{1-\eta}\, c_j^\dagger + \sqrt{\eta}\, d_j^\dagger,$$
$$b_k^\dagger = \sqrt{\eta}\, c_k^\dagger - \sqrt{1-\eta}\, d_k^\dagger$$

Polarization Beam Splitter

In case of Polarizing Beam Splitter (PBS), Horizontal polarization is transmitted completely where as Vertical polarization is completely reflected.

$$\begin{aligned} a_H^\dagger &= c_H^\dagger, \\ b_H^\dagger &= d_H^\dagger \end{aligned}$$

Similarly, we can write

$$\begin{aligned} a_V^\dagger &= d_V^\dagger, \\ b_V^\dagger &= c_V^\dagger \end{aligned}$$

Phase Retarder

A schematic diagram of a phase retarder is given below.

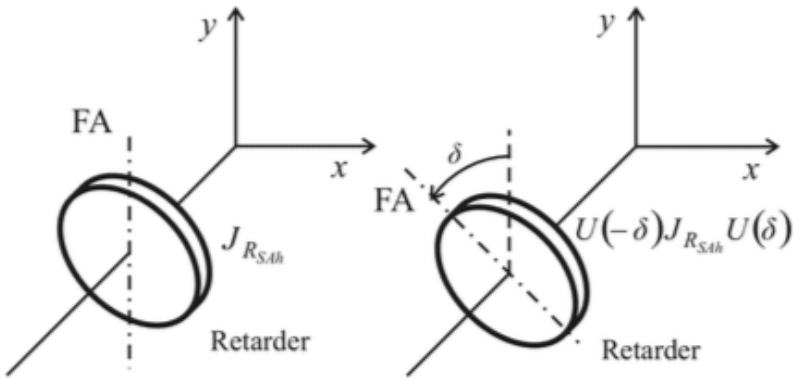

Figure: Figure shows the schematic diagram of a phase retarder. The left one shows Fast axis parallel to conventional Y axis whereas the right one shows Fast axis making an angle δ with conventional Y axis.

Phase Retarder Contd.

In case of quantum PR, the input-output relational matrix is as follows.

$$\begin{pmatrix} a_x'^{\dagger} \\ a_y'^{\dagger} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & e^{-i\theta} \end{pmatrix} \cdot \begin{pmatrix} a_x^{\dagger} \\ a_y^{\dagger} \end{pmatrix}$$

where, $a_x'^{\dagger}$ (resp. $a_y'^{\dagger}$) is the creation operator at output port along X (resp. Y) axis and $a_x^{\dagger}$ (resp. $a_y^{\dagger}$) is the creation operator at input port along X (resp. Y) axis.

Phase Retarder Contd.

Thus, we can write

$$\begin{aligned} a_x'^{\dagger} &= a_x, \\ a_y'^{\dagger} &= e^{-i\theta} a_y \end{aligned}$$

where, θ is the angle made by the PR with its fast axis.

If we assume Horizontal polarization is along X axis and Vertical polarization is along Y axis, then the above equation can be rewritten as

$$\begin{aligned} a_H'^{\dagger} &= a_H^{\dagger}, \\ a_V'^{\dagger} &= e^{-i\theta} a_V^{\dagger} \end{aligned}$$

Motivation of the Algorithm

- Optical set-up of any QKD protocol requires photon source, optical fibre, beam splitter (Non-Polarized as well as Polarized), Phase Retarder and Time Controller
- Input state depends on the source
- Time controller is used to synchronize emission and detection of the photon
- Optical fibre is used as quantum channel
- Beam Splitter and Phase Retarder are responsible for the modification of the input state, i.e, introducing phases, changing the polarization etc.
- In current effort, we describe a disciplined methodology to capture such modification of the input signal

Motivation of the Algorithm Contd.

- Our methodology may open up an avenue for automation where given an optical circuit and an initial state, the generated output will combine all optical operations that the photon passes through
- In other words, the generated output will carry the information about the paths it travels
- The motivation behind this is to build up a simulator which replace the optical laboratory set-up
- This approach can be extended towards any optical experiment

Proposed Algorithm

1. Inputs: initial photon state, circuit diagram.
2. Represent the initial photon state in Fock state basis, i.e., in terms of

$$|n_H, n_V\rangle = \frac{(a_H^\dagger)^{n_H}(a_V^\dagger)^{n_V}}{\sqrt{n_H! n_V!}} |0\rangle . \tag{1}$$

3. If the photon passes through a BS, then for
   - port 1 and Horizontal polarization H, write $a^{\dagger}{}_H = \sqrt{1-\eta}c_H^\dagger + \sqrt{\eta}d_H^\dagger$, where η is reflection coefficient and $c_H^\dagger$ and $d_H^\dagger$ represent outer ports of the BS.
   - port 2 and Horizontal polarization H, write $b_H^\dagger = \sqrt{\eta}c_H^\dagger - \sqrt{1-\eta}d_H^\dagger$.
   - port 1 and Vertical polarization V, write $a_V^\dagger = \sqrt{1-\eta}c_V^\dagger + \sqrt{\eta}d_V^\dagger$, where $c_V^\dagger$ and $d_V^\dagger$ represent outer ports of the BS.
   - port 2 and Vertical polarization V, write $b_V^\dagger = \sqrt{\eta}c_V^\dagger - \sqrt{1-\eta}d_V^\dagger$.

Proposed Algorithm Contd.

1. If the photon passes through PBS, then for
   - H polarization,
     - write $a_H^\dagger = c_H^\dagger$
     - write $b_H^\dagger = d_H^\dagger$
   - V polarization,
     - write $a_V^\dagger = d_V^\dagger$
     - write $b_V^\dagger = c_V^\dagger$
2. If the photon passes through a PR making an angle θ with its fast axis, then for
   - H polarization, write $a_H^\dagger = c_H^\dagger$
   - V polarization write $a_V^\dagger = e^{-i\theta} c_V^\dagger$,
     where a stands for input port and c stands for output port.
3. Output: resultant state

Connection with Cryptology

- The conditional probability for the coincident events can be calculated from the resultant state

- Consider the initial state in 6-4 Reference Frame Independent QKD

$$|\psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|1_H, 0_V\rangle_A |0_H, 1_V\rangle_B + e^{-i\phi} |0_H, 1_V\rangle_A |1_H, 0_V\rangle_B)$$

where, the subscript A stands for Alice and subscript B stands for Bob

Connection with Cryptology Contd.

- After covering all the paths at Alice's as well as Bob's laboratory, the joint final state becomes

$$
\begin{aligned}
|\psi\rangle_{AB}^{PBS_A^2} &= \frac{1}{2}\left(\left(\frac{\alpha}{2}\left((DA^+ + DA^-)_2 + (RL^+ + RL^-)_3\right) + \beta(HV^+)_1\right)(HV^-)_1\right. \\
&+ \frac{1}{2}\left(\left(\frac{\alpha}{2}(RL^+ + RL^-)_3\right) + \beta(HV^+)_1\right)\frac{1}{\sqrt{2}}(DA^+ - DA^-)_2 \\
&+ \frac{1}{2}\left(\frac{\alpha}{2}\left((DA^+ - DA^-)_2 + (RL^+ - RL^-)_3\right) + \beta(HV^-)_1\right) \\
&\quad (HV^+)_1 + \frac{1}{2}\left(\frac{\alpha}{2}(RL^+ - RL^-)_3\right) + \beta(HV^-)_1\left)\left(\frac{1}{\sqrt{2}}(DA^+ + DA^-)_2\right.\right. \\
&+ \frac{\alpha}{2\sqrt{2}}(DA^+DA^+ + DA^-DA^-)_2
\end{aligned}
$$

The state is written in terms of some measurement bases used in the actual paper

R. Tannous, Polarization Entangled Photon Sources for Free-Space Quantum Key Distribution, Master Thesis, University of Waterloo, (2018)

Conditional Probability Table

Alice	Bob	$\Pr(A = +, B = +)$	$\Pr(A = +, B = -)$	$\Pr(A = -, B = +)$	$\Pr(A = -, B = -)$
$\{HA^+, HA^-\}$	$\{HA^+, HA^-\}$	0 0 0 0	0 $\frac{1}{4}\cdot\frac{1}{3}$ 0 0	0 0 $\frac{1}{4}\cdot\frac{1}{3}$ 0	0 0 0 0
$\{DA^+, DA^-\}$	$\{DA^+, DA^-\}$	$\frac{1}{8}\cdot\frac{2}{3}$ 0 0 0	0 0 0 0	0 0 0 0	0 0 0 $\frac{1}{8}\cdot\frac{2}{3}$
$\{HA^+, HA^-\}$	$\{DA^+, DA^-\}$	$\frac{1}{8}\cdot\frac{1}{3}$ 0 0 0	0 $\frac{1}{8}\cdot\frac{1}{3}$ 0 0	0 0 $\frac{1}{8}\cdot\frac{1}{3}$ 0	0 0 0 $\frac{1}{8}\cdot\frac{1}{3}$
$\{DA^+, DA^-\}$	$\{HA^+, HA^-\}$	$\frac{1}{16}\cdot\frac{2}{3}$ 0 0 0	0 $\frac{1}{16}\cdot\frac{2}{3}$ 0 0	0 0 $\frac{1}{16}\cdot\frac{2}{3}$ 0	0 0 0 $\frac{1}{16}\cdot\frac{2}{3}$
$\{RL^+, RL^-\}$	$\{HA^+, HA^-\}$	$\frac{1}{16}\cdot\frac{2}{3}$ 0 0 0	0 $\frac{1}{16}\cdot\frac{2}{3}$ 0 0	0 0 $\frac{1}{16}\cdot\frac{2}{3}$ 0	0 0 0 $\frac{1}{16}\cdot\frac{2}{3}$
$\{RL^+, RL^-\}$	$\{DA^+, DA^-\}$	$\frac{1}{16}\cdot\frac{2}{3}$ 0 0 0	0 $\frac{1}{16}\cdot\frac{2}{3}$ 0 0	0 0 $\frac{1}{16}\cdot\frac{2}{3}$ 0	0 0 0 $\frac{1}{16}\cdot\frac{2}{3}$

Connection with Cryptology Contd.

- Comparing the theoretical value with the observed one, one may calculate the noise in the channel
- In a QKD protocol any kind of noise is treated as the noise incorporated by the adversary due to extraction of the information
- From the noise model, one can estimate the amount of information extracted by the adversary
- Most importantly, based on the noise analysis, Error Correcting Code (ECC) and hash function are chosen in classical post-processing part

Caveat

- In the current initiative, we consider the pure states only
- We assume that the detectors are flawless and there is no noise in the channel without adversary
- Exploiting Stokes formalism (density matrix approach that includes mixed states), one may include the parameters for instrumental error.
- However, those are kept for future research

Summary

- Quantum computer: a real threat to RSA and ECC based cryptography
- Post Quantum Cryptography: Code based and Lattice based; believed to be hard in quantum domain
- Alternative solution: Quantum Cryptography
- Quantum key distribution has been proven secure
- QKD devices are available in the international market
- Schematic diagrams are available in literatures as well as white papers of the companies
- Step wise synthesis has been less explored

Summary Contd.

- For involved understanding of a circuit, step wise synthesis is necessary
- Proposed a methodology for step wise analysis of any optical experimental set up, specifically for QKD devices
- Paved an avenue towards automation where given an input state and a circuit, we will get back the output state
- Output state will preserve all the information about the path it has travelled
- This information is required for security analysis

Thank You