Exercise 4 for 2022∼ 2023 USTC Course

‘Introduction to Quantum Information’

Jun-Hao Wei, Shu-Ming Hu and Kai Chen

Hefei National Research Center for Physical Sciences
at the Microscale and School of Physical Sciences,
University of Science and Technology of China, Hefei 230026, China

1. (1) Write down the communication process of BB84 quantum key distribution (QKD) protocol.

   (2) Write down the secure key rate formula of single-photon BB84 QKD and explain the relationship with entanglement purification protocol. (Hint: see Shor and Preskill’s security proof.)

   (3) Write down the GLLP formula of BB84 QKD and explain the meaning of each item in the formula.

   (4) Suppose in BB84 QKD Alice and Bob both choose their bases with uniform probability and we neglect photon losses and systematic errors, compute the mutual information of Alice and Bob $H(A:B)$ when there is no eavesdropping.

   (5) Describe the photon number splitting attack and the principle of decoy QKD protocol.

Answer: We only give the answer of question (4) here and refer to the lecture “QIP2022chapt_4_Kai Chen.pdf” for the rest.

(4) Denote the measurement basis of Alice and Bob as M and N. We use a to denote the bit that Alice wants to encode and b to denote the measurement result of Bob. Then,

$$p(ab|MN) = \frac{1}{4}, \forall\ a, b = 0, 1, \text{ if } M \neq N,$$

$$p(00|MN) = p(11|MN) = \frac{1}{2}, \text{ if } M = N,$$

where $p(ab|MN)$ is the conditional probability that Alice encodes her bit a and Bob gets measurement result b when Alice chooses basis M and Bob chooses basis N.

Since Alice and Bob both choose their bases with uniform probability, the probability that Alice chooses basis M and Bob chooses basis N is $p(MN) = 1/4$. Thus, one can see that the raw bit string of Alice and Bob are uniformly distributed,

$$p(a=0) = p(a=1) = \frac{1}{2},\ p(b=0) = p(b=1) = \frac{1}{2}\ \Rightarrow H(A) = H(B) = 1.$$

Furthermore, the joint probability is

$$p(ab=00) = p(ab=11) = \frac{1}{2}\times\frac{1}{4} + \frac{1}{2}\times\frac{1}{4} + \frac{1}{4}\times\frac{1}{4} + \frac{1}{4}\times\frac{1}{4} = \frac{3}{8},$$

$$p(ab=01) = p(ab=10) = \frac{1}{4}\times\frac{1}{4} + \frac{1}{4}\times\frac{1}{4} = \frac{1}{8}.$$

Thus, the joint entropy is $H(A,B) = -\sum_{a,b} p(ab)\log_2 p(ab) = -\frac{3}{4}\log_2\frac{3}{8} - \frac{1}{4}\log_2\frac{1}{8}$. Therefore, the mutual information of Alice and Bob's *raw key* is $H(A:B) = H(A) + H(B) - H(A,B) = 1 + 1 + \frac{3}{4}\log_2\frac{3}{8} + \frac{1}{4}\log_2\frac{1}{8} = \frac{3}{4}\log_2 3 - 1 = 0.189$. While after basis sifting, it is obvious that the mutual information of Alice and Bob is 1, i.e. they have identical bit strings.

2. The action of creation operator $a^\dagger$ and annihilation operator a on Fock states $|n\rangle$ is as follows,

$$a\,|n\rangle = \sqrt{n}\,|n-1\rangle\,,\ a^\dagger\,|n\rangle = \sqrt{n+1}\,|n+1\rangle\,,$$

where n denotes the number of particles and is a non-negative integer. The coherent state is defined as the unique eigenket of the annihilation operator a,

$$a\,|\alpha\rangle = \alpha\,|\alpha\rangle\,,$$

where α is a complex number.

(1) Prove that the coherent state $|\alpha\rangle$ can be expanded in Fock basis as

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,.$$

(2) Prove that the photon number statistics of coherent state follows Poisson distribution, i.e.,

$$\Delta^2 n \equiv \langle n^2\rangle - \langle n\rangle^2 = \langle n\rangle,$$

where $\langle n\rangle = \langle\alpha|\, a^\dagger a\, |\alpha\rangle\,, \langle n^2\rangle = \langle\alpha|\, a^\dagger a a^\dagger a\, |\alpha\rangle\,.$

(3) Prove that the phase randomized coherent state $\int_0^{2\pi} \frac{1}{2\pi} |e^{i\theta}\sqrt{\mu}\rangle \langle e^{i\theta}\sqrt{\mu}|\, \mathrm{d}\theta$ is a mixture of Fock states with Poisson distribution, where μ is a positive real number.

Answer:

(1) Suppose $|\alpha\rangle = \sum_n C_n |n\rangle$. Premultiply $a|\alpha\rangle = \sum_n C_n a|n\rangle = \sum_n C_n\sqrt{n}\,|n-1\rangle$ with $\langle m-1|$, then

$$\alpha\,\langle m-1|\alpha\rangle = \sum_n C_n\sqrt{n}\,\langle m-1|n-1\rangle \Rightarrow \alpha C_{m+1} = C_m\sqrt{m} \Rightarrow C_n = \frac{\alpha^n}{\sqrt{n!}}\cdot C_0.$$

Consider normalization,

$$\langle\alpha|\alpha\rangle = \sum_{n,n'} \frac{\alpha^{*n'}\alpha^n}{\sqrt{n'!n!}}\cdot C_0^* C_0 \left\langle n'|n\right\rangle = \sum_n \frac{|\alpha|^{2n}}{n!}\,|C_0|^2 = e^{|\alpha|^2}\cdot|C_0|^2 = 1 \Rightarrow C_0 = e^{-|\alpha|^2/2}.$$

Therefore, we have

$$|\alpha\rangle = e^{-|\alpha|^2/2}\sum_n \frac{\alpha^n}{\sqrt{n!}}\,|n\rangle\,.$$

(2) Note that $aa^\dagger|n\rangle = (n+1)|n\rangle\,, a^\dagger a|n\rangle = n|n\rangle\,.$ Due to the completeness of Fock basis, we have $[a,a^\dagger] = I$. Thus, $a^\dagger a a^\dagger a = a^\dagger a^\dagger a a + a^\dagger[a,a^\dagger]a = a^\dagger a^\dagger a a + a^\dagger a$. Since the Hermitian conjugate of $a|\alpha\rangle = \alpha|\alpha\rangle$ is $\langle\alpha|\, a^\dagger = \langle\alpha|\,\alpha^*$, we have

$$\begin{aligned}\Delta^2 n &= \langle\alpha|\, a^\dagger a a^\dagger a\,|\alpha\rangle - (\langle\alpha|\, a^\dagger a\,|\alpha\rangle)^2\\ &= \langle\alpha|\, a^\dagger a^\dagger a a\,|\alpha\rangle + \langle\alpha|\, a^\dagger a\,|\alpha\rangle - (\langle\alpha|\, a^\dagger a\,|\alpha\rangle)^2\\ &= |\alpha|^4 + |\alpha|^2 - (|\alpha|^2)^2 = |\alpha|^2 = \langle\alpha|\, a^\dagger a\,|\alpha\rangle = \langle n\rangle.\end{aligned}$$

(3)

$$\int_0^{2\pi} \frac{1}{2\pi} |e^{i\theta}\sqrt{\mu}\rangle \langle e^{i\theta}\sqrt{\mu}|\,\mathrm{d}\theta = \frac{1}{2\pi}\int_0^{2\pi} \sum_{n,n'} \frac{(e^{i\theta})^{n-n'}\sqrt{\mu}^{n+n'}}{\sqrt{n'!n!}}\,|n\rangle\langle n'| = \sum_{n=0}^{\infty} \frac{e^{-\mu}\mu^n}{n!}\,|n\rangle\langle n|\,,$$

where we used $\frac{1}{2\pi}\int_0^{2\pi} e^{i(n-m)\theta}\mathrm{d}\theta = \delta_{nm}$.

3. Quantum teleportation is a process by which quantum information can be transmitted from one location to another, with the help of quantum entanglement.

   (1) Suppose the initials states are $|\psi\rangle_1 = \alpha\,|0\rangle_1 + \beta\,|1\rangle_1\,, |\psi^-\rangle_{23} = \frac{1}{\sqrt{2}}(|0\rangle_2\,|1\rangle_3 - |1\rangle_2\,|0\rangle_3)$. Show that particle 3 can be projected onto the same state as particle 1 by some local operators after Bell state measurement on particle 1 and 2.

   (2) Suppose the initials states are $|\psi\rangle_1 = \alpha\,|0\rangle_1 + \beta\,|1\rangle_1\,, |GHZ\rangle_{234} = \frac{1}{\sqrt{2}}(|0\rangle_2\,|0\rangle_3\,|0\rangle_4 + |1\rangle_2\,|1\rangle_3\,|1\rangle_4)$. Show that particle 4 can be projected onto the same state as particle 1 by some local operators after Bell state measurement on particle 1 and 2 and local X measurement on particle 3.

   (3) Explain why we can't use quantum teleportation to achieve superluminal communication.

Answer:

(1) The joint state of the three particles can be rewritten as following,

$$
\begin{aligned}
|\psi\rangle_1\,|\psi^-\rangle_{23} &= (\alpha\,|0\rangle_1 + \beta\,|1\rangle_1)\frac{1}{\sqrt{2}}(|0\rangle_2\,|1\rangle_3 - |1\rangle_2\,|0\rangle_3) \\
&= \frac{1}{\sqrt{2}}(\alpha\,|001\rangle_{123} - \alpha\,|010\rangle_{123} + \beta\,|101\rangle_{123} - \beta\,|110\rangle_{123}) \\
&= \frac{1}{\sqrt{2}}\left[\alpha\frac{1}{\sqrt{2}}(|\phi^+\rangle_{12} + |\phi^-\rangle_{12})\,|1\rangle_3 - \alpha\frac{1}{\sqrt{2}}(|\psi^+\rangle_{12} + |\psi^-\rangle_{12})\,|0\rangle_3\right. \\
&\left. +\beta\frac{1}{\sqrt{2}}(|\psi^+\rangle_{12} - |\psi^-\rangle_{12})\,|1\rangle_3 - \beta\frac{1}{\sqrt{2}}(|\phi^+\rangle_{12} - |\phi^-\rangle_{12})\,|0\rangle_3\right] \\
&= \frac{1}{2}\left[|\phi^+\rangle_{12}\,(\alpha\,|1\rangle_3 - \beta\,|0\rangle_3) + |\phi^-\rangle_{12}\,(\alpha\,|1\rangle_3 + \beta\,|0\rangle_3)\right. \\
&\left. - |\psi^+\rangle_{12}\,(\alpha\,|0\rangle_3 - \beta\,|1\rangle_3) - |\psi^-\rangle_{12}\,(\alpha\,|0\rangle_3 + \beta\,|1\rangle_3)\right] \\
&= \frac{1}{2}\left[|\phi^+\rangle_{12}\,X_3Z_3(\alpha\,|0\rangle_3 + \beta\,|1\rangle_3) + |\phi^-\rangle_{12}\,X_3(\alpha\,|0\rangle_3 + \beta\,|1\rangle_3)\right. \\
&\left. - |\psi^+\rangle_{12}\,Z_3(\alpha\,|0\rangle_3 + \beta\,|1\rangle_3) - |\psi^-\rangle_{12}\,(\alpha\,|0\rangle_3 + \beta\,|1\rangle_3)\right].
\end{aligned}
$$

Bell measurements on the first two particles would project the state of particle 3 into the same form as $|\psi\rangle_1$ up to a local Pauli operator.

(2) The joint state of the four particles can be rewritten as following,

$$
\begin{aligned}
|\psi\rangle_1 |GHZ\rangle_{234} &= (\alpha |0\rangle_1 + \beta |1\rangle_1)\frac{1}{\sqrt{2}}(|000\rangle_{234} + |111\rangle_{234}) \\
&= \frac{1}{\sqrt{2}}(\alpha |0000\rangle_{1234} + \alpha |0111\rangle_{1234} + \beta |1000\rangle_{1234} + \beta |1111\rangle_{1234}) \\
&= \frac{1}{\sqrt{2}}\left[\alpha\frac{1}{\sqrt{2}}(|\phi^+\rangle_{12} + |\phi^-\rangle_{12}) |00\rangle_{34} + \alpha\frac{1}{\sqrt{2}}(|\psi^+\rangle_{12} + |\psi^-\rangle_{12}) |11\rangle_{34}\right. \\
&\left.+\beta\frac{1}{\sqrt{2}}(|\psi^+\rangle_{12} - |\psi^-\rangle_{12}) |00\rangle_{34} + \beta\frac{1}{\sqrt{2}}(|\phi^+\rangle_{12} - |\phi^-\rangle_{12}) |11\rangle_{34}\right] \\
&= \frac{1}{2}\left[|\phi^+\rangle_{12} (\alpha |00\rangle_{34} + \beta |11\rangle_{34}) + |\phi^-\rangle_{12} (\alpha |00\rangle_{34} - \beta |11\rangle_{34})\right. \\
&\left.+ |\psi^+\rangle_{12} (\alpha |11\rangle_{34} + \beta |00\rangle_{34}) + |\psi^-\rangle_{12} (\alpha |11\rangle_{34} - \beta |00\rangle_{34})\right].
\end{aligned}
$$

Bell measurements on the first two particles would project the state of particle 3 and 4 into $\alpha |00\rangle_{34} + \beta |11\rangle_{34}$ or one of the other three terms. For example, if particle 3 and 4 are projected into $\alpha |11\rangle_{34} - \beta |00\rangle_{34}$, then

$$
\begin{aligned}
\alpha |11\rangle_{34} - \beta |00\rangle_{34} &= \alpha\frac{1}{\sqrt{2}}(|+\rangle_3 - |-\rangle_3) |1\rangle_4 - \beta\frac{1}{\sqrt{2}}(|+\rangle_3 + |-\rangle_3) |0\rangle_4 \\
&= \frac{1}{\sqrt{2}} |+\rangle_3 (\alpha |1\rangle_4 - \beta |0\rangle_4) - \frac{1}{\sqrt{2}} |-\rangle_3 (\alpha |1\rangle_4 + \beta |0\rangle_4) \\
&= \frac{1}{\sqrt{2}} |+\rangle_3 X_4 Z_4(\alpha |0\rangle_4 + \beta |1\rangle_4) - \frac{1}{\sqrt{2}} |-\rangle_3 X_4(\alpha |0\rangle_4 + \beta |1\rangle_4).
\end{aligned}
$$

Thus, local X measurement on particle 3 would further project the state of particle 4 into the same form as $|\psi\rangle_1$ up to a local Pauli operator.

(3) Without the knowledge of the Bell measurement result, the state of particle 3 is $\rho_3 = \mathrm{tr}_{12}\,\rho_{123} = I/2$. So the owner of particle 3 cannot tell whether the owner of particles 1 and 2 did anything at all unless he receives the Bell measurement result sent by Alice. Thus, quantum teleportation must contain the classical communication, meaning that we cannot use it to communicate faster than light.

4. Consider the following 4-qubit state:

$$|\theta\rangle_{1234} = |\psi\rangle_1 \otimes \frac{1}{\sqrt{2}}(I_2 \otimes U) \left[(|00\rangle_{23} + |11\rangle_{23}) \otimes |\phi\rangle_4\right],$$

where $|\psi\rangle = a|0\rangle + b|1\rangle$ and $|\phi\rangle = c\,|0\rangle + d\,|1\rangle$ are arbitrary qubit states and U is a two-qubit unitary operator. After Bell state measurement on qubit 1 and 2 of $|\theta\rangle$, how can we make the state of qubit 3 and 4 be $U(|\psi\rangle \otimes |\phi\rangle)$?

Answer:

We have

$$
\begin{aligned}
|\theta\rangle &= (a|0\rangle_1 + b|1\rangle_1) \otimes \frac{1}{\sqrt{2}}(I_2 \otimes U)(|00\rangle_{23} + |11\rangle_{23}) \otimes |\phi\rangle_4 \\
&= \frac{1}{2}[|\phi^+\rangle U(a|0\rangle + b|1\rangle)|\phi\rangle + |\phi^-\rangle U(a|0\rangle - b|1\rangle)|\phi\rangle \\
&+ |\psi^+\rangle U(a|1\rangle + b|0\rangle)|\phi\rangle + |\psi^-\rangle U(a|1\rangle - b|0\rangle)|\phi\rangle]
\end{aligned}
$$

where the $|\phi^+\rangle, |\phi^-\rangle, |\psi^+\rangle$ and $|\psi^-\rangle$ are the four Bell states. Then we can perform a transform to obtain $U(|\psi\rangle \otimes |\phi\rangle)$ in the last two qubits as follows :

Bell state	Transform
$\lvert\phi^+\rangle$	$U(I \otimes I)U^\dagger$
$\lvert\phi^-\rangle$	$U(Z \otimes I)U^\dagger$
$\lvert\psi^+\rangle$	$U(X \otimes I)U^\dagger$
$\lvert\psi^-\rangle$	$U(ZX \otimes I)U^\dagger$

5. The polarization dependent beam splitter (PDBS), which has transmission rate T_H for horizontal polarization mode and transmission rate T_V for vertical polarization mode, can be used to construct controlled phase gate. In Fig. 1.(a), a PDBS performs the following transformation on input single photon with path mode a:

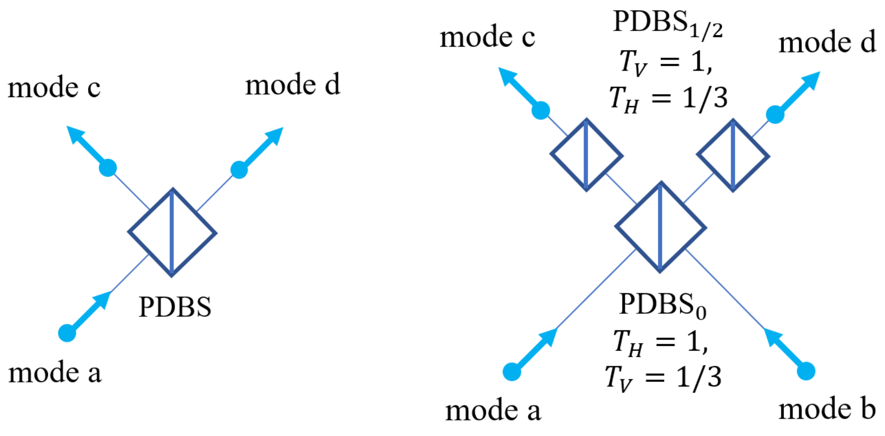
$$\alpha\,|H_a\rangle + \beta\,|V_a\rangle \longrightarrow \alpha(\sqrt{T_H}\,|H_d\rangle + i\sqrt{1-T_H}\,|H_c\rangle) + \beta(\sqrt{T_V}\,|V_d\rangle + i\sqrt{1-T_V}\,|V_c\rangle),$$

where $|H_d\rangle$ denotes horizontal polarized photon on path mode d and similar for the other terms.

In Fig. 1.(b), two input modes a and b are overlapped at PDBS$_0$, with a PDBS$_{1/2}$ on each of its output mode. Show that, conditioned on the coincidence detection of output modes c and d, the setup in figure (b) can implement the controlled phase gate perfectly,

$$
\begin{aligned}
&c_{HH}\,|H_a H_b\rangle + c_{HV}\,|H_a V_b\rangle + c_{VH}\,|V_a H_b\rangle + c_{VV}\,|V_a V_b\rangle \\
\longrightarrow\ &c_{HH}\,|H_d H_c\rangle + c_{HV}\,|H_d V_c\rangle + c_{VH}\,|V_d H_c\rangle - c_{VV}\,|V_d V_c\rangle\,.
\end{aligned}
$$

Calculate the probability to obtain a coincidence in the outputs.



(a)PDBS

(b)Setup for the controlled phase gate

FIG. 1. Linear optics controlled phase gate.

Answer:

$$\begin{aligned}
&c_{HH}\left|H_aH_b\right\rangle + c_{HV}\left|H_aV_b\right\rangle + c_{VH}\left|V_aH_b\right\rangle + c_{VV}\left|V_aV_b\right\rangle\\
\xrightarrow{PDBS_0}\,&c_{HH}\left|H_dH_c\right\rangle + c_{HV}\left|H_d\right\rangle\left(\sqrt{\frac{1}{3}}\left|V_c\right\rangle + i\sqrt{\frac{2}{3}}\left|V_d\right\rangle\right)\\
&+c_{VH}\left(\sqrt{\frac{1}{3}}\left|V_d\right\rangle + i\sqrt{\frac{2}{3}}\left|V_c\right\rangle\right)\left|H_c\right\rangle\\
&+c_{VV}\left(\sqrt{\frac{1}{3}}\left|V_d\right\rangle + i\sqrt{\frac{2}{3}}\left|V_c\right\rangle\right)\left(\sqrt{\frac{1}{3}}\left|V_c\right\rangle + i\sqrt{\frac{2}{3}}\left|V_d\right\rangle\right)\\
&=c_{HH}\left|H_dH_c\right\rangle + \sqrt{\frac{1}{3}}c_{HV}\left|H_dV_c\right\rangle + i\sqrt{\frac{2}{3}}c_{HV}\left|H_dV_d\right\rangle + \sqrt{\frac{1}{3}}c_{VH}\left|V_dH_c\right\rangle\\
&+i\sqrt{\frac{2}{3}}c_{VH}\left|V_cH_c\right\rangle - \frac{1}{3}c_{VV}\left|V_dV_c\right\rangle + i\sqrt{\frac{2}{3}}c_{VV}(\left|V_cV_c\right\rangle + \left|V_dV_d\right\rangle)\\
\xrightarrow{Post-selection}\,&c_{HH}\left|H_dH_c\right\rangle + \sqrt{\frac{1}{3}}c_{HV}\left|H_dV_c\right\rangle + \sqrt{\frac{1}{3}}c_{VH}\left|V_dH_c\right\rangle - \frac{1}{3}c_{VV}\left|V_dV_c\right\rangle\\
\xrightarrow{PDBS_{1/2}}\,&\frac{1}{3}(c_{HH}\left|H_dH_c\right\rangle + c_{HV}\left|H_dV_c\right\rangle + c_{VH}\left|V_dH_c\right\rangle - c_{VV}\left|V_dV_c\right\rangle),
\end{aligned}$$

where we dropped the terms like $\left|H_dV_d\right\rangle$ since they would not give coincidence detection on output modes c and d. The probability to obtain a coincidence is 1/9.

6. We can construct a nondestructive CNOT gate by polarizing beam splitters (PBS), half-wave plates (HWP), and an ancilla entangled photon pair $\left|\phi^+\right\rangle_{ab} =$

$\frac{1}{\sqrt{2}}(|00\rangle_{ab}+|11\rangle_{ab})$ shown as Fig. 2. Consider an arbitrary input state of the form $|\psi\rangle_{2'3'}=\alpha_1|H_{2'}H_{3'}\rangle+\alpha_2|H_{2'}V_{3'}\rangle+\alpha_3|V_{2'}H_{3'}\rangle+\alpha_4|V_{2'}V_{3'}\rangle$, with control photon in mode $2'$ and target photon in mode $3'$. Prove that one can implement the CNOT operation between photons $2'$ and $3'$ when detecting a $|+\rangle$ photon in mode c and a $|H\rangle$ photon in mode d.

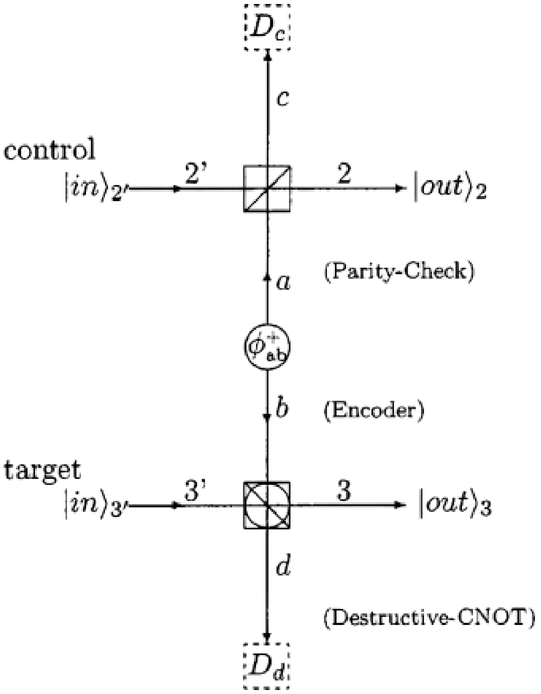


FIG. 2. The nondestructive CNOT gate constructed by polarizing beam splitters (PBS), half-wave plates (HWP), and an ancilla entangled photon pair $|\phi^+\rangle_{ab}$. The PBS with a circle, which performs the same action as ordinary PBS in the ±45° basis, is accomplished by inserting one HWP oriented at 22.5° with respect to the horizontal direction in each of the two inputs ($3'$ and b) and two outputs (3 and d) of an ordinary PBS.

Answer: The initial state is :

$$\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{ab}\otimes(\alpha_1|HH\rangle+\alpha_2|HV\rangle+\alpha_3|VH\rangle+\alpha_4|VV\rangle)_{2'3'},$$

and then

$$\xrightarrow{HWP}\frac{1}{\sqrt{2}}(|0+\rangle+|1-\rangle)_{ab}(\alpha_1|H+\rangle+\alpha_2|H-\rangle+\alpha_3|V+\rangle+\alpha_4|V-\rangle)_{2'3'}$$

$$\xrightarrow{PBS} \frac{1}{2\sqrt{2}}(|HH\rangle_{cd} + |HV\rangle_{c3} + |VH\rangle_{2d} - |VV\rangle_{23})\otimes$$

$$[(\alpha_1 + \alpha_2)|HH\rangle_{23} + (\alpha_1 - \alpha_2)|HV\rangle_{2d} + (\alpha_3 + \alpha_4)|VH\rangle_{c3} + (\alpha_3 - \alpha_4)|VV\rangle_{cd}]$$

$$\xrightarrow{HWP} \frac{1}{2\sqrt{2}}(|H+\rangle_{cd} + |H-\rangle_{c3} + |V+\rangle_{2d} - |V-\rangle_{23})\otimes$$

$$[(\alpha_1 + \alpha_2)|H+\rangle_{23} + (\alpha_1 - \alpha_2)|H-\rangle_{2d} + (\alpha_3 + \alpha_4)|V+\rangle_{c3} + (\alpha_3 - \alpha_4)|V-\rangle_{cd}]$$

when detecting a $|+\rangle$ photon in mode c and a $|H\rangle$ photon in mode d, the state in mode $2, 3$ is :

$$\alpha_1|HH\rangle_{23} + \alpha_2|HV\rangle_{23} + \alpha_3|VV\rangle_{23} + \alpha_4|VH\rangle_{23},$$

which is equal to implement the CNOT operation between photons $2'$ and $3'$.

7. Alice and Bob prepare phase randomized weak coherent pulses (WCPs) in a different BB84 polarization state which is selected, independently and at random for each signal, by means of a polarization modulator (Pol-M). Decoy states are generated using an intensity modulator (Decoy-IM). Inside the measurement device, signals from Alice and Bob interfere at a $50 : 50$ beam splitter (BS) that has on each end a polarizing beam splitter (PBS) projecting the input photons into either horizontal (H) or vertical (V) polarization states (see Fig. 3). Four single-photon detectors are employed to detect the photons. A successful Bell state measurement corresponds to the observation of precisely two detectors (associated to orthogonal polarizations) being triggered. Successful detection events and the corresponding measurement results are publicly announced

   (1) Which state are the two photons projected into when there is a click in D_{1H} and D_{2V}, or in D_{1V} and D_{2H}?

   (2) Which state are the two photons projected into when there is a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}?

   (3) Alice and Bob post-select the events where the relay outputs a successful result and they use the same basis in their transmission. To guarantee that their bit strings are correctly correlated, either Alice or Bob has to apply a bit flip to her or his data. Please give a protocol which make their bit strings correctly correlated.

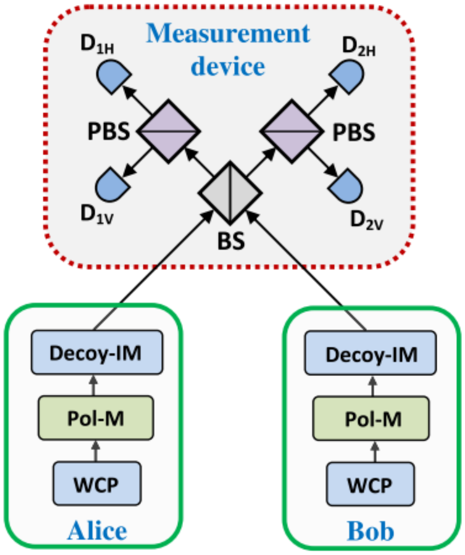


FIG. 3. Basic setup of a MDI-QKD protocol.

Answer:

(1) A click in D_{1H} and D_{2V}, or in D_{1V} and D_{2H} indicates a projection into the Bell state $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$.

(2) A click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V} indicates a projection into the Bell state $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$.

(3) Alice and Bob should apply a bit flip to her/his data according to their basis and the BSM results as follows :

TABLE I. Successful Bell state measurements

BSM results	$\|\psi^-\rangle$	$\|\psi^+\rangle$
Rectilinear basis	Bit flip	Bit flip
Diagonal basis	Bit flip	No bit flip

8. Consider the MDI-QKD with one entangled photon source in the middle (see Fig. 4). Each of Alice and Bob prepares phase-randomized weak coherent pulses (WCP) in one of the four BB84 polarization states randomly and independently. Meanwhile, an untrusted source, Charles, prepares polarization entangled photon pairs using a singlet $|\psi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$. All three parties send quantum signals to two untrusted relays, David and Ethan, each

of whom is supposed to perform a Bell state measurement that projects the incoming signals into a Bell state. In the classical communication phase, both of David and Ethan use classical channels to broadcast their successful measurement results. Alice and Bob keep the successful events and discard the rest, then post-select the events where they use the same basis. Either Alice or Bob can apply a bit flip to her/his data according to their basis and the BSM results. Please give a protocol which make their bit strings correctly correlated.

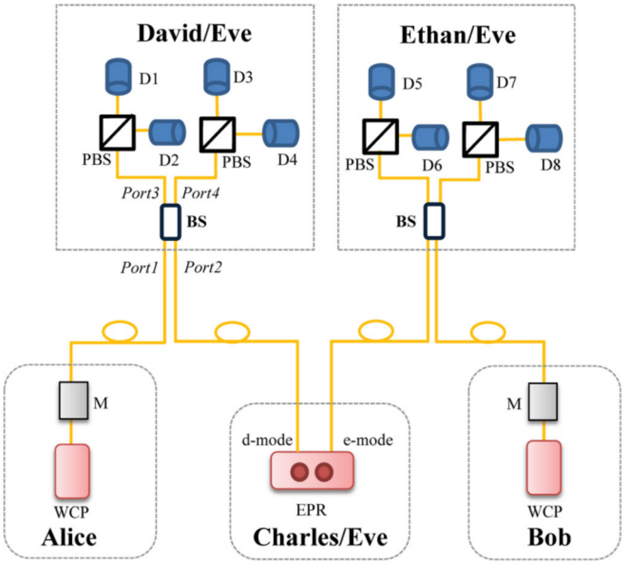


FIG. 4. MDI-QKD with one entangled photon source in the middle.

Answer:

Alice and Bob should apply a bit flip to her/his data according to their basis and the BSM results as follows :

TABLE II. Successful Bell state measurements

BSM results	$\lvert\psi^+\rangle\lvert\psi^+\rangle$	$\lvert\psi^-\rangle\lvert\psi^-\rangle$	$\lvert\psi^+\rangle\lvert\psi^-\rangle$	$\lvert\psi^-\rangle\lvert\psi^+\rangle$
Z-basis	Flip	Flip	Flip	Flip
X-basis	Flip	Flip	Non-flip	Non-flip

9. Suppose three EPR sources produce three pairs of entangled photons,

$$|\phi^+\rangle_{12} = \frac{|00\rangle_{12} + |11\rangle_{12}}{\sqrt{2}}, \ |\phi^+\rangle_{34} = \frac{|00\rangle_{34} + |11\rangle_{34}}{\sqrt{2}}, \ |\phi^+\rangle_{56} = \frac{|00\rangle_{56} + |11\rangle_{56}}{\sqrt{2}}.$$

Photons 2, 4, and 6 are projected to GHZ-state $\frac{|000\rangle-|111\rangle}{\sqrt{2}}$. Then, what is the state of the photons 1, 3 and 5?

Answer:

$$_{246}\langle GHZ|(|\phi^{+}\rangle_{12}\otimes|\phi^{+}\rangle_{34}\otimes|\phi^{+}\rangle_{56})\propto\frac{|000\rangle_{135}-|111\rangle_{135}}{\sqrt{2}}. \tag{1}$$

Therefore, the state of the photons 1, 3 and 5 is GHZ state $\frac{|000\rangle-|111\rangle}{\sqrt{2}}$.

10. The Schmidt number of a bi-partite pure state is the number of non-zero Schmidt components. Prove that the Schmidt number of a pure quantum state cannot be increased by local unitary transforms and classical communication.

Answer:

Suppose that a bi-partite state $|\phi^{AB}\rangle$ has Schmidt decomposition as

$$|\phi^{AB}\rangle=\sum_{i}^{n}\lambda_i|\psi_i^A\rangle|\psi_i^B\rangle,$$

where n is the Schmidt number,$\lambda_i>0$ for $i=1,2,\ldots,n$, and $|\psi_i^A\rangle(|\psi_i^B\rangle)$ form an orthonormal set. After local unitary transformation and classical communication, the state is changed to

$$|\tilde{\phi}^{AB}\rangle=\sum_{i}^{n}\lambda_iU^A|\psi_i^A\rangle U^B|\psi_i^B\rangle=\sum_{i}^{n}\lambda_i|\tilde{\psi}_i^A\rangle|\tilde{\psi}_i^B\rangle$$

Because U^A and U^B are local unitary operations, $|\tilde{\psi}_i^A\rangle$ and $|\tilde{\psi}_i^B\rangle$ still form two set of orthonormal vectors. Therefore, the above equation gives the Schmidt decomposed form of $|\tilde{\phi}^{AB}\rangle$ and the Schmidt number remains n.