Device-Independent Quantum Key Distribution Protocol Based on Hyper-Entanglement

Yan Chang[1, *], Shibin Zhang[1], Lili Yan[1], Xueyang Li[1], Tian Cao[1] and Qirun Wang[2]

Abstract: The secure key rate of quantum key distribution (QKD) is greatly reduced because of the untrusted devices. In this paper, to raise the secure key rate of QKD, a device-independent quantum key distribution (DIQKD) protocol is proposed based on hyper-entangled states and Bell inequalities. The security of the protocol is analyzed against the individual attack by an adversary only limited by the no-signaling condition. Based on the formalization of Clauser-Horne Shimony-Holt (CHSH) violation measurement on local correlation, the probability of a secure secret bit is obtained, which is produced by a pair of hyper-entangled particles. By analyzing the secure secret bit, it is proven that, when both the polarization mode and the path mode contains entangled-states, the DIQKD protocol gets a better secure key rate than common Bell states.

Keywords: Hyper-entangled states, device-independent, QKD, secure key rate.

1 Introduction

Security and channel capacity are two key problems that need to be solved urgently in quantum cryptographic [Liu, Xu, Zhang et al. (2019)] systems. In previous studies, the security of quantum cryptographic protocols [Acín, Gisin and Masanes (2006); Barrett, Linden, Massar et al. (2005); Masanes, Acin and Gisin (2006); Scarani, Gisin and Brunner (2006); Wang, Gao, Liu et al. (2019)] is guaranteed by the principle of quantum mechanics. The devices for preparing and measuring quantum states are considered perfect. However, in reality, it is difficult to achieve the perfect devices; therefore, there may be various security risks in real quantum cryptography systems. Currently, there are many attack schemes against the imperfection of devices, such as "time shift attack", "dead time attack" and "blind attack by strong light", etc. In other words, many quantum cryptographic protocols [Liu, Gao, Liu et al. (2019); Liu, Xu, Yang et al. (2019)], which are absolutely secure in theory, may not be secure in practice. Therefore, it's meaningful to study quantum cryptographic protocols on the premise that devices cannot be trusted. In addition, because the devices are not trusted, the secure key rate is greatly reduced. If the secure key rate is too low, the practical quantum cryptographic system will not be realized.

[1] College of Information Security Engineering, Chengdu University of Information Technology, Chengdu, China.

[2] School of Engineering and Technology, University of Hertfordshire, Hertford, UK.

[*] Corresponding Author: Yan Chang. Email: cyttkl@cuit.edu.cn.

Received: 06 February 2020; Accepted: 03 May 2020.

CMC. doi:10.32604/cmc.2020.010042 www.techscience.com/journal/cmc

Most of the quantum hacker attacks are implemented by using the non-ideal devices in QKD systems. In order to solve these security problems fundamentally, device independent (DI) protocols [Acín, Gisin and Masanes (2006); Scarani, Gisin and Brunner (2006); Chang, Xiong, Gao et al. (2018); Umesh and Thomas (2014); Ge, Liu, Xia et al. (2019)] have been studied. The device-independent approach to QKD aims to establish a secret key between two or more parties with untrusted devices, potentially under full control of a quantum adversary.

On the theoretical side, the security of DIQKD has been proven against increasingly powerful eavesdroppers [Acín, Brunner and Gisin (2007); Pironio, Acín, Brunner et al. (2009)] But experimental DIQKD still faces many challenges [Mattar, Kolodynski, Skrzypczyk et al. (2018)]. The first challenge is the stringent Bell test that requires the whole measurement process meets the requirements of Loophole-free Bell Test (LFBT), which makes most of the attack schemes invalid. The second challenge is the detection efficiency for observing a Bell violation of the CHSH [Clauser, Horne, Shimony et al. (1969)] inequality, which can be as low as 2/3 [Eberhard (1993)], while, a DIQKD protocol based on CHSH requires an efficiency of 90% [Mattar, Kolodynski, Skrzypczyk et al. (2018)]. Many studies have been made to resolve the above two problems. The first Bell experiments closing the detection loophole used massive particles [Rowe, Kielpinski, Meyer et al. (2001); Matsukevich, Maunz, Moehring et al. (2008); Hensen, Bernien, Dreau et al. (2015); Qu, Li, Xu et al. (2019)]. Progress has also been made in photo-detection efficiency, which allowed for the first loophole-free photonic Bell inequality violations over short distances [Giustina, Mech, Ramelow et al. (2013); Lynden, Evan, Bradley et al. (2015)].

The performance of a QKD protocol can be quantified by the secret key rate, which can be lower-bounded via the violation of an appropriate Bell-inequality in a setup with untrusted devices [Holz, Kampermann and Bru (2018)]. However, the rates of key distribution they could provide are seriously limited owing to the measurements involved that, despite allowing for near unit efficiency, take significant time [Mattar, Kolodynski, Skrzypczyk et al. (2018); Alejandro, Jonatan and Antonio (2013)]. Holz et al. [Holz, Kampermann and Bru (2018)] studied secret key rates in the device-independent scenario for long-distance scheme using quantum repeater setups. Mattar et al. [Mattar, Kolodynski, Skrzypczyk et al. (2018)] introduced novel photonic protocols for DIQKD exploiting single-photon sources and heralding-type architectures. The use of single-photon sources for entanglement distribution instead of standard entangled-pair generation schemes, provides significant improvements on the attainable key rates [Mattar, Kolodynski, Skrzypczyk et al. (2018)].

Some novel methods are proposed to reduce the difficulty of security proof of quantum cryptography protocol. A framework for graphical security proof is proposed to reprove a recent result from DI quantum cryptography: any linear randomness expansion protocol can be converted into an unbounded randomness expansion protocol [Breiner, Miller and Ross (2018)]. Fine [Fine (1982)] proposed that the following statements about a quantum correlation experiment are mutually equivalent. (1) There is a deterministic hidden-variables model for the experiment. (2) There is one joint distribution for all observables of the experiment, returning the experimental probabilities. (3) There are well-defined, compatible joint distributions for all pairs and triples of commuting and noncommuting observables. (4) The Bell inequalities hold. Based on Fine et al. [Fine (1982); Acín, Gisin and Masanes (2006); Scarani, Gisin and Brunner (2006)] proposed DI QKD protocols and proved its security against any individual attack by an adversary only limited by the no-signaling condition.

In this paper, to raise the secure key rate of QKD, a DIQKD protocol is proposed based on hyper-entangled states and Bell inequalities. We analyzed the security against any individual attack by an adversary only limited by the no-signaling condition. By analyzing the secure secret bit, it is proved that, when both the polarization mode and the path mode contains entangled-states, the DIQKD protocol gets a better security key rate than that distributes common Bell states.

2 Brief introduction of research methods

2.1 No-signaling principle

There are two experimental facts in physics: one is that no signal can carry information over the speed of light, the other is that there is a nonlocal correlation which violates the Bell inequality. At present, in physics, the principle of quantum mechanics can satisfy the above two experimental facts at the same time. However, the principle of quantum mechanics is not the only one that satisfies the above two experimental facts at the same time. There is a more nonlocal correlation in the no-signaling correlation than in the quantum mechanics principle.

(1) Basic definition

Suppose the *n*-party user-Alice, Bob, Charlie, etc., each party has a physical system (quantum state) that can be measured with different measurement inputs. x_k represents the measurement input of the *k*th party user, and the a_k represents the corresponding measurement output. Then, $P(a_1,......,a_n\,|\,x_1,......,x_n)$ represent the joint conditional probability distribution of the *n* party users. $P(a_1,......,a_n\,|\,x_1,......,x_n)$ are no-signaling, when the marginal probability distribution of each subset $\{a_{k1},......,a_{km}\}$ of measurement results depend only on its corresponding input, i.e., $P(a_{k1},......,a_{km}\,|\,x_1,......,x_n)$ = $P(a_{k1},......,a_{km}\,|\,x_{k1},......,x_{km})$ [Masanes, Acin and Gisin (2006)]. The principle of no-signaling is a basic prerequisite for DI quantum communication.

(2) The monogamy of nonlocal correlations

Unlike classical correlations, quantum correlations cannot be shared by many parties. This phenomenon is called the monogamy of nonlocal correlations (entanglement). The monogamy of nonlocal correlations is a basic characteristic of no-signaling principle.

The result of Barrett et al. [Barrett, Linden, Massar et al. (2005)] shows that the maximum violation of all Bell inequalities consistent with the no-signaling principle can be obtained by a unique probability distribution, which has a single matching constraint. Let us assume that we have a Bell inequality Ë with the single largest violation of P_{max}. If Alice and Bob maximum violate this inequality Ë (P (a, $b|x$, y))=1, then Alice and Charlie are completely irrelevant.

It can also be considered that if a probability distribution violates the Bell class inequality, the probability distribution can realize a nonlocal correlation. Because of the singularity of the nonlocal correlation, this probability distribution allows for the distribution of secret information that is absolutely secure. Of course, at present, in physics, only the probability distribution of entangled states can violate Bell class inequalities.

2.2 Hyper-entanglement

Hyper-entanglement is a state simultaneously entangled in multiple degrees of freedom. Photons have a variety of quantum degrees of freedom and each degree of freedom can define a quantum bit under suitable conditions. Theoretically these different degrees of freedom can also form entanglement called hyper-entanglement. A hyper-entangled Bell state with polarization and path mode degrees of freedom can be described as:

$$\left|\Phi^{+}_{AB}\right\rangle_{PS} = \frac{1}{\sqrt{2}}(\left|00\right\rangle + \left|11\right\rangle)_{AB} \otimes \frac{1}{\sqrt{2}}(\left|ll\right\rangle + \left|uu\right\rangle)_{AB} \tag{1}$$

where $\left|0\right\rangle$ and $\left|1\right\rangle$ denote the horizontal and vertical polarization of the photon respectively. Subscript A and B denote two photons in the hyper-entangled state. *l* and *u* represent different path modes of photons A and B. Subscript P denotes polarization degree of freedom and subscript S denotes path mode degree of freedom. An ultraviolet light pump pulse passing through a barium borate crystal (BBO) will produce an interrelated photonic pair in mode *u*, and a related pair of photons in mode *l* when a second reflection through the crystal.

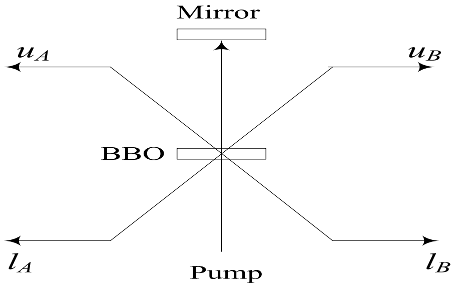

Figure 1: Principle diagram of hyper-entangled Bell state source under polarization mode and path mode

A two-photon hyper-entangled Bell quantum system with polarization and path mode degrees of freedom has 16 Bell states, which can be expressed as:

$$\left|\Gamma_{AB}\right\rangle_{PS} = \left|\Theta\right\rangle_{P} \otimes \left|\Xi\right\rangle_{S} \tag{2}$$

where $\left|\Theta\right\rangle_{P}$ denotes one of the four Bell states with polarization degrees of freedom:

$$\left|\Psi^{\pm}\right\rangle_{P} = \frac{1}{\sqrt{2}}(\left|00\right\rangle \pm \left|11\right\rangle)_{AB} \tag{3}$$

$$\left|\Sigma^{\pm}\right\rangle_{P} = \frac{1}{\sqrt{2}}(\left|01\right\rangle \pm \left|10\right\rangle)_{AB} \tag{4}$$

And $|\Xi\rangle_S$ denotes one of the four Bell states with path mode degrees of freedom:

$$|\Lambda^{\pm}\rangle_S = \frac{1}{\sqrt{2}}(|ll\rangle \pm |uu\rangle)_{AB} \tag{5}$$

$$|\Omega^{\pm}\rangle_S = \frac{1}{\sqrt{2}}(|lu\rangle \pm |ul\rangle)_{AB} \tag{6}$$

Two non-orthogonal measurement bases under polarization degrees of freedom can be selected as follows:

$Z^P = \{|0\rangle, |1\rangle\}$ and $X^P = \{|+\rangle_P = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)\ , |-\rangle_P = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\}$. Two non-orthogonal measurement bases under path mode degrees of freedom can be selected as follows: $Z^S = \{|l\rangle, |u\rangle\}$ and $X^S = \{|+\rangle_S = \frac{1}{\sqrt{2}}(|l\rangle + |u\rangle),\ |-\rangle_S = \frac{1}{\sqrt{2}}(|l\rangle - |u\rangle)\}$.

3 The protocol

3.1 The CHSH inequality and principle of sharing secret bits.

Defining CHSH inequality:

$$I_{CHSH} = P(a_0 = b_0) + P(a_0 = b_1) + P(a_1 = b_0) + P(a_1 \neq b_1) \leq 3 \tag{7}$$

where

$$P(a_j = b_k) = P(a = b = 0l \mid x = j, y = k) + P(a = b = 0u \mid x = j, y = k)$$
$$+P(a = b = 1l \mid x = j, y = k) + P(a = b = 1u \mid x = j, y = k) \tag{8}$$

The meaning of violation of inequality $I_{CHSH} = P(a_0 = b_0) + P(a_0 = b_1) + P(a_1 = b_0)$ $+P(a_1 \neq b_1) \leq 3$ is that: when the value of *x* and *y* is 00, 01 and 10, *a* equals to *b*, called positive correlation; when the value of *x* and *y* is 11, *a* does not equals to *b*, called inverse correlation. Therefore, if Alice publishes her input value *x*, Bob can use his input value *y* to determine when the measurement results are positively correlated and when they are inversely correlated. In this protocol, Alice and Bob use the above principle to share secret bits.

3.2 Protocol for DIQKD based on hyper-entanglement

In this section we proposed a DI protocol for QKD using hyper-entangled Bell states. The hyper-entangled Bell states can be denoted as:

$$|\Phi^{+}_{AB}\rangle_{PS} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \otimes \frac{1}{\sqrt{2}}(|ll\rangle + |uu\rangle)_{AB} \tag{9}$$

where subscript A and B denote two photons in the hyper-entangled state. $|0\rangle$ and $|1\rangle$ denote the horizontal and vertical polarization of the photon respectively. *l* and *u* represent different path modes of photons A and B. Subscript P denotes polarization degree of freedom and subscript S denotes path mode degree of freedom.

Step 1: Eve prepares some hyper-entangled Bell states $\left|\Phi_{AB}^{+}\right\rangle_{PS}$, and then distributes each particle A to Alice and each particle B to Bob for the next communication.

Step 2: Alice and Bob test for the hyper-entanglement properties of quantum systems A and B.

Alice randomly selects the measurement inputs $x \in \{0,1\}$ to measure each particle A, where x=0 means $Z^{S}=\{|l\rangle,|u\rangle\}$ basis measurement first and $Z^{P}=\{|0\rangle,|1\rangle\}$ basis measurement second, and x=1 means $X^{S}=\{\frac{1}{\sqrt{2}}(|l\rangle+|u\rangle),\frac{1}{\sqrt{2}}(|l\rangle-|u\rangle)\}$ basis measurement first and X^{P} = $\{\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\}$ basis measurement second. Bob randomly selects the measurement inputs $y \in \{0,1\}$ to measure each particle B, where y=0 means $(Z^{S}+X^{S})/\sqrt{2}$ basis measurement first and $(Z^{P}+X^{P})/\sqrt{2}$ basis measurement second, and y=1 means $(Z^{S}-X^{S})/\sqrt{2}$ basis measurement first and $(Z^{P}-X^{P})/\sqrt{2}$ basis measurement second. The measurement results of Alice and Bob are expressed as a and $b \in \{0l,0u,1l,1u\}$ respectively.

Alice and Bob select some particles computing conditional probabilities $P(a,b\,|\,x,y)$ and determine whether the CHSH inequality is violated or not. If it is violated, the particles distributed to Alice and Bob are hyper-entangled, and the greater the violation is, the stronger the nonlocal correlation is.

Step 3: Alice and Bob get shared secret bits.

Alice publishes her input value *x*. Bob can use his input value *y* to determine when the measurement results are positively correlated and when they are inversely correlated. If Alice publishes her input value *x*=0, then Alice and Bob know that their output is the same (*a*=*b*). If Alice publishes her input value *x*=1, and Bob's input is *y*=0, Bob knows that his output is the same with Alice (*a*=*b*). If Alice publishes her input value *x*=1, and Bob's input is *y*=1, then Bob knows that his output is exactly the opposite of that of Alice， so Bob flips his bit. Therefore, by reversing the result of the inverse correlation, a pair of DI secret key can be shared between Alice and Bob securely.

Based on one hyper-entangled Bell state, theoretically, Alice and Bob can share two secure secret bits (0*l*, 0*u*, 1*l*, or 1*u*). However, because the maximum violation of CHSH inequality is often difficult to reach, the secure key rate is usually unable to achieve the theoretical value.

It should be noted that, according to the monogamy of the nonlocal correlation and no-signaling principle, if Eve prepares a nonlocal correlation, even if Alice publishes *x*, Eve cannot know *y*, *a*, and *b*.

Step 4: Classical processing. Alice and Bob use error correction and privacy amplification to make the key of Alice and Bob basically the same, while reducing the key information known to eavesdroppers to close to zero.

4 Security analysis

In this section, we analyze the security of the DIQKD protocol based on hyper-entanglement against any individual attack by an adversary only limited by the no-signaling condition. Firstly, we analyze the eavesdropping strategies of Eve, and propose the optimal eavesdropping strategy for Eve. Here, the eavesdropping strategies belong to individual attack, and Eve is an adversary only limited by the no-signaling condition. Then, we give the formalization of CHSH violation measurement on local correlation, which can help us to estimate the amount of information obtained by Eve. Based on the monogamy of the nonlocal correlation under no-signaling principle and the formalization of CHSH violation measurement on local correlation, we obtain the probability that each pair of hyper-entangled particles distributed to Alice and Bob produces a secure secret bit. By analyzing the secure secret bit, we prove that, when both the polarization mode and the path mode contains entangled-states, the DIQKD protocol gets a better security key rate than that distributes common Bell states.

4.1 Eve's eavesdropping strategy

DIQKD has a limitation on Eve, that is, "no-signaling principle". In order to estimate the amount of information obtained by Eve, it is necessary to investigate the eavesdropping strategy of Eve. The eavesdropping strategy of Eve should satisfy some kind of "causal independence": the eavesdropping strategy of Eve does not affect the probability of the results of Alice and Bob in the "average" sense [Guo, Li, and Peng (2016)]. This assumption, commonly referred to as "no-signaling principle", is mathematically formulated as follows [Guo, Li, and Peng (2016)]:

$$\sum_{e} P(a,b,e\,|\,x,y,z) = P(a,b\,|\,x,y) \ \ (\forall z) \tag{10}$$

In the formula: x, y is the measurement choice of Alice and Bob; a, b is the corresponding measurement output; z is the eavesdropping strategy of Eve; e is Eve's information on a and b under strategy z. The significance of this formula is that for any eavesdropping strategy z of Eve, the sum of the probabilities of eavesdropping results is invariant [Guo, Li and Peng (2016)].

The individual attack of Eve using the untrusted devices can be the preparation of pseudo quantum states or the setting of hidden variables on the measurement devices of Alice and Bob. Preparing quantum states with local correlation (non-entangled) can help Eve to obtain the outputs of Alice and Bob. However, if only the localized quantum states were prepared, $P(a,b\,|\,x,y)$ will be affected, and the CHSH inequality cannot be violated. Thus eavesdropping was discovered. To avoid that, Eve must prepare nonlocal correlations (entangled states). Therefore, the best strategy for Eve is to prepare mixed states of nonlocal correlation and local correlation satisfying $I_{CHSH} = 3$. As studied in Scarani et al. [Scarani, Gisin and Brunner (2006)], a CHSH violation measurement on quantum states with local correlation can be reproduced with local hidden variables, which produces the same probability distribution. However, the measurement on nonlocal correlation cannot be reproduced with shared hidden variables.

In the DIQKD protocol, Eve can prepare any state, but if Eve makes quantum states at will, the CHSH inequality violation test will not be successful, so the protocol cannot be carried out. Therefore, Eve must obtain information on *a* and *b* under the constraint condition that CHSH inequality violated successfully. Eve can prepare the localized quantum states satisfying $I_{CHSH}=3$ in addition to the entangled states, where $I_{CHSH}=3$ are the extreme points of CHSH inequality. Eve's best eavesdropping strategy is to prepare mixed states ρ_{AB} of the following states: $\left|\Phi_{AB}^{+}\right\rangle_{PS}$、$\left|\phi_1\right\rangle$、$\left|\phi_2\right\rangle$、$\left|\phi_3\right\rangle$、$\left|\phi_4\right\rangle$、$\left|\phi_5\right\rangle$, $\left|\phi_6\right\rangle$, $\left|\phi_7\right\rangle$, $\left|\phi_8\right\rangle$.

$$\begin{aligned}\rho_{AB}=&\,p_1p_2\left|\Phi_{AB}^{+}\right\rangle_{PS}\left\langle\Phi_{AB}^{+}\right|+\frac{p_1(1-p_2)}{2}\left|\phi_1\right\rangle\left\langle\phi_1\right|+\frac{p_1(1-p_2)}{2}\left|\phi_2\right\rangle\left\langle\phi_2\right|+\frac{p_2(1-p_1)}{2}\left|\phi_3\right\rangle\left\langle\phi_3\right|\\&+\frac{p_2(1-p_1)}{2}\left|\phi_4\right\rangle\left\langle\phi_4\right|+\frac{(1-p_1)(1-p_2)}{4}\left|\phi_5\right\rangle\left\langle\phi_5\right|+\frac{(1-p_1)(1-p_2)}{4}\left|\phi_6\right\rangle\left\langle\phi_6\right|\\&+\frac{(1-p_1)(1-p_2)}{4}\left|\phi_7\right\rangle\left\langle\phi_7\right|+\frac{(1-p_1)(1-p_2)}{4}\left|\phi_8\right\rangle\left\langle\phi_8\right|\end{aligned}\tag{11}$$

$$\left|\Phi_{AB}^{+}\right\rangle_{PS}=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)_{AB}\otimes\frac{1}{\sqrt{2}}(\left|ll\right\rangle+\left|uu\right\rangle)_{AB}\tag{12}$$

$$\left|\phi_1\right\rangle=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)_{AB}\otimes\left|ll\right\rangle_{AB}\tag{13}$$

$$\left|\phi_2\right\rangle=\frac{1}{\sqrt{2}}(\left|00\right\rangle+\left|11\right\rangle)_{AB}\otimes\left|uu\right\rangle_{AB}\tag{14}$$

$$\left|\phi_3\right\rangle=\frac{1}{\sqrt{2}}(\left|ll\right\rangle+\left|uu\right\rangle)_{AB}\otimes\left|00\right\rangle_{AB}\tag{15}$$

$$\left|\phi_4\right\rangle=\frac{1}{\sqrt{2}}(\left|ll\right\rangle+\left|uu\right\rangle)_{AB}\otimes\left|11\right\rangle_{AB}\tag{16}$$

$$\left|\phi_5\right\rangle=\left|00\right\rangle_{AB}\otimes\left|ll\right\rangle_{AB}\tag{17}$$

$$\left|\phi_6\right\rangle=\left|00\right\rangle_{AB}\otimes\left|uu\right\rangle_{AB}\tag{18}$$

$$\left|\phi_7\right\rangle=\left|11\right\rangle_{AB}\otimes\left|ll\right\rangle_{AB}\tag{19}$$

$$\left|\phi_8\right\rangle=\left|11\right\rangle_{AB}\otimes\left|uu\right\rangle_{AB}\tag{20}$$

Here p_1 is the probability of preparing entangled state in polarization mode, and $1-p_1$ is the probability of preparing local correlations (localized quantum states) in polarization mode. p_2 is the probability of preparing entangled state in path mode, and $\mathbf{1}-\boldsymbol{p}_{\mathbf{2}}$is the probability of preparing local correlations in path mode.

Eve does not need to save any quantum states for eavesdropping. When Eve prepares hyper-entangled states $\left|\Phi_{AB}^{+}\right\rangle_{PS}$, even if Alice publishes her measurement inputs, Eve will not know any outputs of both Alice and Bob because of the monogamy of nonlocal correlations. When Eve prepares $|\phi_1\rangle, |\phi_2\rangle$ (nonlocal in polarization mode, but local in path mode), after Alice announces her measurement input, Eve can obtain Alice's path mode output and partial output of Bob in path mode according to her strategy of preparing local states. When Eve prepares $|\phi_3\rangle, |\phi_4\rangle$ (nonlocal in path mode, but local in polarization mode), after Alice announces her measurement input, Eve can obtain Alice's polarization mode output and partial output of Bob in polarization mode. When Eve prepares $|\phi_5\rangle$, $|\phi_6\rangle$, $|\phi_7\rangle$, $|\phi_8\rangle$(local both in path mode and in polarization mode), after Alice announces her measurement input, Eve can obtain Alice's output and partial output of Bob in both modes. Therefore, in Eve's eavesdropping strategy, Eve does not need to save any quantum states.

4.2 Formalization of CHSH violation measurement on local correlation

In Eve's eavesdropping strategy, Eve acquires information by preparing local quantum states that satisfy equation $I_{CHSH} = 3$. To satisfy CHSH violation tests, Eve uses local hidden variables to formalize CHSH measurements of local states, which produces the same probability distribution.

In this section, with local hidden variables, we formalize the CHSH violation measurement on localized quantum states (measuring localized quantum states in CHSH violation bases), which produces the same probability distribution.

First, let's review the formalization idea of the Bell-type experiments in Scarani et al. [Scarani, Gisin and Brunner (2006)]. Local hidden variables might be hidden in Alice's and Bob's laboratories, in the devices that Eve has provided to them. The bounded region, which contains all probability distributions that can be obtained by shared randomness, forms the local polytope. The vertices of the local polytope are the points corresponding to deterministic strategies, that is, strategies in which a=a(x) and b=b(y) with probability one. If a point, representing a Bell type experiment, lies within the polytope (such as the measurement on a local state), then there exists a strategy with shared randomness that produces the same probability distribution. On the contrary, if a point lies outside the local polytope (such as the measurement on an entangled state), then the experiment cannot be reproduced with shared randomness. The local polytope correspond to Bell's inequalities [Scarani, Gisin and Brunner (2006)].

According to the results of Scarani et al. [Scarani, Gisin and Brunner (2006)], the probability distribution $P(a,b|x,y)$ of a localized quantum state lies in the local polytope and can be reproduced with local hidden variables.

In the case of binary inputs and outputs, under no-signaling, the local polytope [Acín, Gisin and Masanes (2006); Scarani, Gisin and Brunner (2006); Fine (1982)] has eight nontrivial facets, which are all equivalent to $I_{CHSH} \le 3$. On each facet lie eight out of the sixteen ($2^2\times2^2$) deterministic strategies; these are said to give $I_{CHSH} = 3$. For the hyper-entangled Bell states, because of the entanglement characteristics of both the polarization mode and the path mode, each mode has eight deterministic strategies can give $I_{CHSH} = 3$, which are linearly independent from one another.

Under no-signaling principle Barrett et al. [Barrett, Linden, Massar et al. (2005)], in polarization mode, the 8 extreme points of the local correlation can be expressed in the following form:

$$L_1^{(P,w)}: a_0(x) = w\,;\ b_0(y) = w \tag{21}$$

$$L_2^{(P,w)}: a_0(x) = x + w\,;\ b_0(y) = w \tag{22}$$

$$L_3^{(P,w)}: a_0(x) = w\,;\ b_0(y) = y + w \tag{23}$$

$$L_4^{(P,w)}: a_0(x) = x + w\,;\ b_0(y) = y + w + 1 \tag{24}$$

In path mode, the 8 extreme points of the local correlation can be expressed in the following form:

$$L_1^{(S,v)}: a_1(x) = v\,;\ b_1(y) = v \tag{25}$$

$$L_2^{(S,v)}: a_1(x) = x + v\,;\ b_1(y) = v \tag{26}$$

$$L_3^{(S,v)}: a_1(x) = v\,;\ b_1(y) = y + v \tag{27}$$

$$L_4^{(S,v)}: a_1(x) = x + v\,;\ b_1(y) = y + v + 1 \tag{28}$$

Here $w \in (0,1)$; $v \in (l,u)$; $a = a_0a_1$ and $b = b_0b_1$ are binary outputs of Alice and Bob respectively; $x \in (0,1)$ and $y \in (0,1)$ are binary inputs of Alice and Bob respectively.

Suppose Eve transmits deterministic local correlations $L_j^{(P,w)}$ with probability $p(L_j^{(P,w)})$, where $\sum_{w,j} p(L_j^{(P,w)}) = 1 - p_1$, *j*=1,2,3,4.

Suppose Eve transmits deterministic local correlations $L_j^{(S,v)}$ with probability $p(L_j^{(S,v)})$, where $\sum_{v,j} p(L_j^{(S,v)}) = 1 - p_2$, *j*=1,2,3,4.

4.3 The secure key rate

In this section, based on the formalization of CHSH violation measurement on local correlation, we first analyze the probability distribution of input and output data of Alice, Bob, and Eve's information on *a* and *b*, under different eavesdropping strategies of Eve. Then, by calculating the qubit error rate of Alice and mutual information between Alice and Eve, we obtain the probability that each pair of hyper-entangled particles produces a secure secret bit.

In our protocol, when Alice and Bob randomly select measurement inputs $x \in (0,1)$ and $y \in (0,1)$ for measurement, Eve has the greatest uncertainty, so the probability that *x* and *y* take values 0 and 1 is 1/2.

Table 1: The probability distribution of *a*, *b* and Eve's information on *a* and *b* when Eve prepares hyper-entangled states $\left|\Phi_{AB}^{+}\right\rangle_{PS}$

$x=0$	$b=0l$	$b=0u$	$b=1l$	$b=1u$
$a=0l$	$p(e=??,??)$			
$a=0u$		$p(e=??,??)$		
$a=1l$			$p(e=??,??)$	
$a=1u$				$p(e=??,??)$

Here, $p(e=??,??)$ means the probability that Eve does not know Alice's and Bob's measurement results.

Table 2: The probability distribution of *a*, *b* and Eve's information on *a* and *b* when Eve prepares $\left|\phi_1\right\rangle,\left|\phi_2\right\rangle$ (nonlocal in polarization mode, but local in path mode)

$x=0$	$b=0l$	$b=0u$	$b=1l$	$b=1u$
$a=0l$	$p(e=?l,?l)$ $p(e=?l,??)$	$p(e=?l,??)$		
$a=0u$	$p(e=?u,??)$	$p(e=?u,?u)$ $p(e=?u,??)$		
$a=1l$			$p(e=?l,?l)$ $p(e=?l,??)$	$p(e=?l,??)$
$a=1u$			$p(e=?u,??)$	$p(e=?u,?u)$ $p(e=?u,??)$

Here, $p(e=?l,?l)$ means the probability that Eve knows a_1 and b_1 of each *a* and *b* ($a=a_0a_1$ and $b=b_0b_1$); $p(e=?l,??)$ means the probability that Eve only knows a_1 of each *a* and *b*.

Table 3: The probability distribution of *a*, *b* and Eve's information on *a* and *b* when Eve prepares $\left|\phi_3\right\rangle,\left|\phi_4\right\rangle$ (nonlocal in path mode, but local in polarization mode)

$x=0$	$b=0l$	$b=0u$	$b=1l$	$b=1u$
$a=0l$	$p(e=0?,0?)$ $p(e=0?,??)$		$p(e=0?,??)$	

$a=0u$		$p(e=0?,0?)$ $p(e=0?,??)$		$p(e=0?,??)$
$a=1l$	$p(e=1?,??)$		$p(e=1?,1?)$ $p(e=1?,??)$	
$a=1u$		$p(e=1?,??)$		$p(e=1?,1?)$ $p(e=1?,??)$

Table 4: The probability distribution of *a*, *b* and Eve's information on *a* and *b* when Eve prepares $|\phi_5\rangle$, $|\phi_6\rangle$, $|\phi_7\rangle$, $|\phi_8\rangle$ (local both in path mode and in polarization mode)

$x=0$	$b=0l$	$b=0u$	$b=1l$	$b=1u$
$a=0l$	$p(e=0l,0l)$ $p(e=0l,??)$ $p(e=0l,0?)$ $p(e=0l,?l)$	$p(e=0l,??)$ $p(e=0l,0?)$	$p(e=0l,?l)$ $p(e=0l,??)$	$p(e=0l,??)$
$a=0u$	$p(e=0u,??)$ $p(e=0u,0?)$	$p(e=0u,0u)$ $p(e=0u,??)$ $p(e=0u,0?)$ $p(e=0u,?u)$	$p(e=0u,??)$	$p(e=0u,??)$ $p(e=0u,?u)$
$a=1l$	$p(e=1l,?l)$ $p(e=1l,??)$	$p(e=1l,??)$	$p(e=1l,1l)$ $p(e=1l,??)$ $p(e=1l,1?)$ $p(e=1l,?l)$	$p(e=1l,??)$ $p(e=1l,1?)$
$a=1u$	$p(e=1u,??)$	$p(e=1u,??)$ $p(e=1u,?u)$	$p(e=1u,??)$ $p(e=1u,1?)$	$p(e=1u,1u)$ $p(e=1u,??)$ $p(e=1u,1?)$ $p(e=1u,?u)$

According to Tabs. 1 to 4, the qubit error rate of Alice is obtained:

$$\begin{aligned}Q&=2\times\frac{1}{2}p(e=?u,??)+2\times\frac{1}{2}p(e=?l,??)+2\times\frac{1}{2}p(e=0?,??)+2\times\frac{1}{2}p(e=1?,??)\\&+\frac{1}{2}[p(e=0l,??)+p(e=0l,0?)]+\frac{1}{2}[p(e=0l,?l)+p(e=0l,??)]+p(e=0l,??)\\&+\frac{1}{2}[p(e=0u,??)+p(e=0u,0?)]+\frac{1}{2}[p(e=0u,?u)+p(e=0u,??)]+p(e=0u,??)\\&+\frac{1}{2}[p(e=1l,??)+p(e=1l,1?)]+\frac{1}{2}[p(e=1l,?l)+p(e=1l,??)]+p(e=1l,??)\\&+\frac{1}{2}[p(e=1u,??)+p(e=1u,1?)]+\frac{1}{2}[p(e=1u,?u)+p(e=1u,??)]+p(e=1u,??)\\&=\frac{2-p_1-p_2}{8}\end{aligned}\tag{29}$$

The mutual information between Alice and Eve is:

$$\begin{aligned}I(A:E)&=2\times\frac{1}{2}p(e=?l,?l)+2\times\frac{1}{2}p(e=?u,?u)+2\times\frac{1}{2}p(e=0?,0?)+2\times\frac{1}{2}p(e=1?,1?)\\&+p(e=0l,0l)+2\times\frac{1}{2}p(e=0l,0?)+2\times\frac{1}{2}p(e=0l,?l)\\&+p(e=0u,0u)+2\times\frac{1}{2}p(e=0u,0?)+2\times\frac{1}{2}p(e=0u,?u)\\&+p(e=1l,1l)+2\times\frac{1}{2}p(e=1l,1?)+2\times\frac{1}{2}p(e=1l,?l)\\&+p(e=1u,1u)+2\times\frac{1}{2}p(e=1u,1?)+2\times\frac{1}{2}p(e=1u,?u)\\&=\frac{2-p_1-p_2}{4}\end{aligned}\tag{30}$$

The probability that each qubit produces a secure secret bit is:

$$r_0\geq I(A:B)-I(A:E)=1-h(\frac{2-p_1-p_2}{8})-\frac{1}{4}\left(2-p_1-p_2\right)\tag{31}$$

Each pair of hyper-entangled particles distributed to Alice and Bob, allows Alice and Bob to share two qubits (polarization mode and path mode), respectively, so, the probability that each pair of hyper-entangled particles produces a secure secret bit is:

$$r\geq 2[1-h(\frac{2-p_1-p_2}{8})-\frac{1}{4}\left(2-p_1-p_2\right)]\tag{32}$$

When $p_1=p_2=p$,

$$r\geq 1-2h(\frac{1-p}{4})+p\tag{33}$$

When $p_1=0$, $p_2=p$, or $p_2=0$, $p_1=p$

$$r' \geq 1-2h(\frac{2-p}{8})+\frac{p}{2} \tag{34}$$

As studied in Acín et al. [Acín, Gisin and Masanes (2006)], the common Bell states distributed to Alice and Bob, allows Alice and Bob to share only one qubit, respectively, so, the probability that each pair of common Bell states particles produces a secure secret bit is:

$$r1 \geq 1-h(\frac{1-p}{4})-\frac{1}{2}(1-p) \tag{35}$$

Obviously, If Eve prepares hyper-entangled states $\left|\Phi^{+}_{AB}\right\rangle_{PS}$ (that is $p_1 = p_2 = p = 1$), because of the monogamy of nonlocal correlations, Alice and Bob can share two secure secret bits for each distribution of a pair of hyper-entangled particles. If Eve prepares the mixed state of $\left|\Phi^{+}_{AB}\right\rangle_{PS}$, $|\phi_1\rangle$, $|\phi_2\rangle$, $|\phi_3\rangle$, $|\phi_4\rangle$, $|\phi_5\rangle$, $|\phi_6\rangle$, $|\phi_7\rangle$ and $|\phi_8\rangle$ (that is $0.32 < p_1 = p_2 = p < 1$), Alice and Bob always get a better security key rate than $r1$. Moreover, with the increase of p, the advantage becomes more obvious. If Eve prepares the mixed state of $|\phi_1\rangle$ and $|\phi_2\rangle$ (that is $p_2 = 0$, $p_1 = p = 1$), or the mixed state of $|\phi_3\rangle$ and $|\phi_4\rangle$ (that is $p_1 = 0$, $p_2 = p = 1$), Alice and Bob get a positive secure key rate 0.41. If Eve prepares the mixed state of $|\phi_1\rangle$, $|\phi_2\rangle$, $|\phi_5\rangle$, $|\phi_6\rangle$, $|\phi_7\rangle$ and $|\phi_8\rangle$, or the mixed state of $|\phi_3\rangle$, $|\phi_4\rangle$, $|\phi_5\rangle$, $|\phi_6\rangle$, $|\phi_7\rangle$ and $|\phi_8\rangle$, when $p > 0.63$, Alice and Bob can get a positive secure key rate less than 0.41.

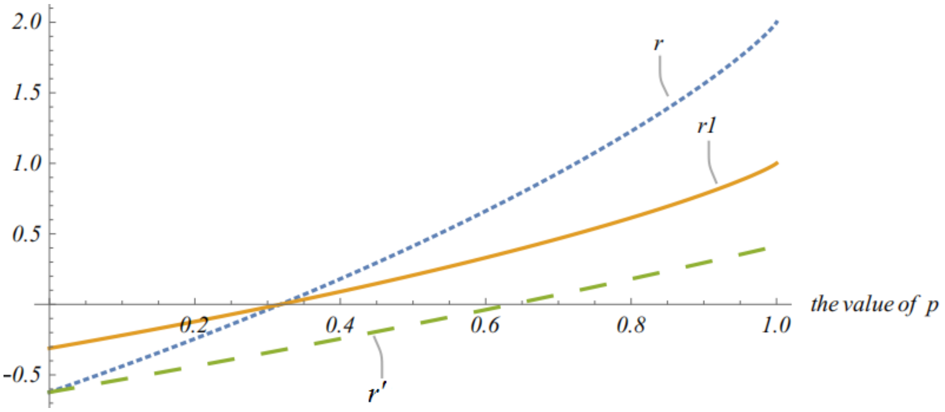

Figure 2: The secure key rate comparison between DIQKD based on hyper-entangled states and common Bell states

5 Conclusion

In the actual QKD protocol, eavesdroppers may use the imperfectness of devices to obtain the distributed secret key. Therefore, the secure key rate of QKD is greatly reduced. To raise the secure key rate of QKD, DIQKD protocol should be considered based on hyper-entangled states and Bell inequalities and the eavesdropper should be given a more powerful eavesdropping capability without violating the principle of no-signaling in the security analysis. By analyzing, the secure key rate based on hyper-entangled states is found improved obviously, comparing with the similar DIQKD scheme based on Bell states.

Funding Statement: This work is supported by NSFC (Grant Nos. 61572086, 61402058), the Application Foundation Project of Sichuan Province of China (Grant No. 2017JY0168), the National Key Research and Development Program (No. 2017YFB0802302)，Sichuan innovation team of quantum security communication (No. 17TD0009), Sichuan academic and technical leaders training funding support projects (No. 2016120080102643), the Fund for Middle and Young Academic Leaders of CUIT (Grant No. J201511).

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S. et al. (2007): Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters*, vol. 98, no. 23, 230501.

Acín, A.; Gisin, N.; Masanes, L. (2006): From Bell's theorem to secure quantum key distribution. *Physical Review Letters*, vol. 97, no. 12, 120405.

Adlam, E.; Kent, A. (2015): Device-independent relativistic quantum bit commitment. *Physical Review A*, vol. 92, no. 1, 022315.

Alejandro, M.; Antonio, A. (2016): Implementations for device-independent quantum key distribution. *Physica Scripta*, vol. 91, no. 4, 043003.

Alejandro, M.; Jonatan, B. B.; Antonio, A. (2013): Device-independent quantum key distribution with spin-coupled cavities. *Physical Review Letters A*, vol. 88, no. 6, 062319.

Barrett, J.; Linden, N.; Massar, S.; Pironio, S.; Popescu, S. et al. (2005): Nonlocal correlations as an information-theoretic resource. *Physical Review A*, vol. 71, no. 2, 022101.

Breiner, S.; Miller, C. A.; Ross, N. J. (2018): Graphical methods in device-independent quantum cryptography. doi: 10.22331/q-2019-05-27-146.

Chang, Y.; Xiong, J. X.; Gao, X.; Zhang, S. B.; Yan, L. L. (2018): Quantum private query protocol based on EPR pairs. *Chinese Journal of Electronics*, vol. 27, no. 2, pp. 256-262.

Clauser, J. F.; Horne, M. A.; Shimony, A.; Holt, R. A. (1969): Proposed experiment to testlocal hidden-variable theories. *Physical Review Letters*, vol. 23, no. 1, pp. 880-884.

Eberhard, P. H. (1993): Background level and counter efficiencies required for a loophole-free Einstein Podolsky-Rosen experiment. *Physical Review A*, vol. 47, no. 1, pp. R747-R750.

Fine, A. (1982): Hidden variables, joint probability, and the Bell inequalities. *Physical Review Letters*, vol. 48, no. 5, pp. 291-295

Ge, C. P.; Liu, Z.; Xia, J.; Fang, L. M. (2019): Revocable identity-based broadcast proxy re-encryption for data sharing in clouds. *IEEE Transactions on Dependable and Secure Computing*.

Giustina, M.; Mech, A.; Ramelow, S.; Wittmann, B.; Kofler, J. et al. (2013): Bell violation using entangled photons without the fair-sampling assumption. *Nature*, vol. 497, no. 7448, pp. 227-257.

Guo, H.; Li, Z. Y.; Peng, X. (2016): *Quantum Cryptography*.

Hensen, B.; Bernien, H.; Dréau, A. E.; Reiserer, A.; Kalb, N. (2015): Loophole-free bell inequality violation using electron spins separated by 1.3 kilometers. *Nature*, vol. 526, no. 7575, pp. 682-688.

Holz, T.; Kampermann, H.; Bru, D. (2018): Device-independent secret-key-rate analysis for quantum repeaters. *Physical Review A*, vol. 97, no. 1, 012337.

Liu, W. J.; Gao, P. P.; Liu, Z. H.; Chen, H. W.; Zhang, M. J. (2019): A quantum-based database query scheme for privacy preservation in cloud environment. *Security and Communication Networks*.

Liu, W. J.; Xu, Y. S.; Zhang, M. J.; Chen, J. X.; Yang, C. N. (2019): A novel quantum visual secret sharing scheme. *IEEE Access*, vol. 7, no. 1, pp. 114374-114384.

Liu, W. J.; Xu, Y.; Yang, J. C. N.; Yu, W. B. (2019): Privacy-preserving quantum two-party geometric intersection. *Computers, Materials & Continua*, vol. 60, no. 3, pp. 1237-1250.

Lynden, K. S.; Evan, M. S.; Bradley, G. C.; Peter, B. (2015): Strong loophole-free test of local realism. *Physical Review Letters*, vol. 115, no. 25, 250402.

Maitra, A.; Paul, G.; Roy, S. (2017): Device-independent quantum private query. *Physical Review A*, vol. 95, no. 4, 042344.

Masanes, L.; Acin, A.; Gisin, N. (2006): General properties of nonsignaling theories. *Physical Review A*, vol. 73, no. 1, 012112.

Matsukevich, D. N.; Maunz, P.; Moehring, D. L.; Olmschenk, S.; Monroe, C. (2008): Bell inequality violation with two remote atomic qubits. *Physical Review Letters*, vol. 100, no. 15, 150404.

Mattar, A.; Kolodynski, J.; Skrzypczyk, P.; Woodhead, E.; Cavalcanti, D. et al. (2018): Device-independent quantum key distribution with single-photon sources. arXiv: 1803.07089v1.

Pironio, S.; Acín, A.; Brunner, N.; Gisin, N.; Massar, S. et al. (2009): Device-independent quantum key distribution secure against collective attacks. *New Journal of Physics*, vol. 11, no. 4, 045021.

Pitkanen, D.; Ma, X. F.; Wickert, R.; Loock, P. V.; Lutkenhaus, N. (2011): Efficient heralding of photonic qubits with applications to device independent quantum key distribution. *Physical Review A*, vol. 84, no. 2, 022325.

Qu, Z. G.; Li, Z. Y.; Xu, G; Wu, S. Y.; Wang, X. J. (2019): Quantum image steganography protocol based on quantum image expansion and Grover search algorithm. *IEEE Access*.

Rowe, M. A.; Kielpinski, D.; Meyer, V.; Sackett, C. A.; Itano, W. M. (2001): Experimental violation of a Bell's inequality with efficient detection. *Nature*, vol. 409, no. 1, pp. 791-794.

Scarani, V.; Gisin, N.; Brunner, N. (2006): Secrecy extraction from no-signaling correlations. *Physical Review A*, vol. 74, no. 1, 042339.

Umesh, V.; Thomas, V. (2014): Fully device independent quantum key distribution. *Physical Review Letters*, vol. 113, no. 14, 140501.

Wang, J.; Gao, Y.; Liu, W.; Wu, W. B.; Lim, S. J. (2019): An asynchronous clustering and mobile data gathering schema based on timer mechanism in wireless sensor networks. *Computers, Materials & Continua*, vol. 58, no. 3, pp. 711-725.

Wei, Z. H.; Sikora, J. (2017): Device-independent characterizations of a shared quantum state independent of any Bell inequalities. *Physical Review A*, vol. 95, no. 1, 032103.

Appendix

$$p(e=??,??)=\frac{p_1p_2}{4} \tag{36}$$

$$p(e=?l,?l)=\frac{p_1}{2}\left[p(L_1^{(S,l)})+p(L_2^{(S,l)})\right] \tag{37}$$

$$p(e=?l,??)=\frac{p_1}{2}\left[\frac{p(L_3^{(S,l)})}{2}+\frac{p(L_4^{(S,l)})}{2}\right] \tag{38}$$

$$p(e=?u,?u)=\frac{p_1}{2}\left[p(L_1^{(S,u)})+p(L_2^{(S,u)})\right] \tag{39}$$

$$p(e=?u,??)=\frac{p_1}{2}\left[\frac{p(L_3^{(S,u)})}{2}+\frac{p(L_4^{(S,u)})}{2}\right] \tag{40}$$

$$p(e=0?,0?)=\frac{p_2}{2}\left[p(L_1^{(P,0)})+p(L_2^{(P,0)})\right] \tag{41}$$

$$p(e=0?,??)=\frac{p_2}{2}\left[\frac{p(L_3^{(P,0)})}{2}+\frac{p(L_4^{(P,0)})}{2}\right] \tag{42}$$

$$p(e=1?,1?)=\frac{p_2}{2}\left[p(L_1^{(P,1)})+p(L_2^{(P,1)})\right] \tag{43}$$

$$p(e=1?,??)=\frac{p_2}{2}\left[\frac{p(L_3^{(P,1)})}{2}+\frac{p(L_4^{(P,1)})}{2}\right] \tag{44}$$

$$p(e=0l,0l)=\left[p(L_1^{(P,0)})+p(L_2^{(P,0)})\right]\left[p(L_1^{(S,l)})+p(L_2^{(S,l)})\right] \tag{45}$$

$$p(e=0l,??)=\left[\frac{p(L_3^{(P,0)})}{2}+\frac{p(L_4^{(P,0)})}{2}\right]\left[\frac{p(L_3^{(S,l)})}{2}+\frac{p(L_4^{(S,l)})}{2}\right] \tag{46}$$

$$p(e=0l,0?)=\left[p(L_1^{(P,0)})+p(L_2^{(P,0)})\right]\left[\frac{p(L_3^{(S,l)})}{2}+\frac{p(L_4^{(S,l)})}{2}\right] \tag{47}$$

$$p(e=0l,?l)=\left[\frac{p(L_3^{(P,0)})}{2}+\frac{p(L_4^{(P,0)})}{2}\right]\left[p(L_1^{(S,l)})+p(L_2^{(S,l)})\right] \tag{48}$$

$$p(e=1l,1l)=\left[p(L_1^{(P,1)})+p(L_2^{(P,1)})\right]\left[p(L_1^{(S,l)})+p(L_2^{(S,l)})\right] \tag{49}$$

$$p(e=1l,??)=\left[\frac{p(L_3^{(P,1)})}{2}+\frac{p(L_4^{(P,1)})}{2}\right]\left[\frac{p(L_3^{(S,l)})}{2}+\frac{p(L_4^{(S,l)})}{2}\right] \tag{50}$$

$$p(e=1l,1?)=\left[p(L_1^{(P,1)})+p(L_2^{(P,1)})\right]\left[\frac{p(L_3^{(S,l)})}{2}+\frac{p(L_4^{(S,l)})}{2}\right] \tag{51}$$

$$p(e=1l,?l)=\left[\frac{p(L_3^{(P,1)})}{2}+\frac{p(L_4^{(P,1)})}{2}\right]\left[p(L_1^{(S,l)})+p(L_2^{(S,l)})\right] \tag{52}$$

$$p(e=0u,0u)=\left[p(L_1^{(P,0)})+p(L_2^{(P,0)})\right]\left[p(L_1^{(S,u)})+p(L_2^{(S,u)})\right] \tag{53}$$

$$p(e=0u,??)=\left[\frac{p(L_3^{(P,0)})}{2}+\frac{p(L_4^{(P,0)})}{2}\right]\left[\frac{p(L_3^{(S,u)})}{2}+\frac{p(L_4^{(S,u)})}{2}\right] \tag{54}$$

$$p(e=0u,0?)=\left[p(L_1^{(P,0)})+p(L_2^{(P,0)})\right]\left[\frac{p(L_3^{(S,u)})}{2}+\frac{p(L_4^{(S,u)})}{2}\right] \tag{55}$$

$$p(e=0u,?u)=\left[\frac{p(L_3^{(P,0)})}{2}+\frac{p(L_4^{(P,0)})}{2}\right]\left[p(L_1^{(S,u)})+p(L_2^{(S,u)})\right] \tag{56}$$

$$p(e=1u,1u)=\left[p(L_1^{(P,1)})+p(L_2^{(P,1)})\right]\left[p(L_1^{(S,u)})+p(L_2^{(S,u)})\right] \tag{57}$$

$$p(e=1u,??)=\left[\frac{p(L_3^{(P,1)})}{2}+\frac{p(L_4^{(P,1)})}{2}\right]\left[\frac{p(L_3^{(S,u)})}{2}+\frac{p(L_4^{(S,u)})}{2}\right] \tag{58}$$

$$p(e=1u,1?)=\left[p(L_1^{(P,1)})+p(L_2^{(P,1)})\right]\left[\frac{p(L_3^{(S,u)})}{2}+\frac{p(L_4^{(S,u)})}{2}\right] \tag{59}$$

$$p(e=1u,?u)=\left[\frac{p(L_3^{(P,1)})}{2}+\frac{p(L_4^{(P,1)})}{2}\right]\left[p(L_1^{(S,u)})+p(L_2^{(S,u)})\right] \tag{60}$$

For all j, w and v, $L_j^{(P,w)}$ is linearly independent in polarization mode, therefore $p(L_j^{(P,w)})=\frac{1-p_1}{8}$, j=1,2,3,4, w=0, 1; $L_j^{(S,v)}$ is linearly independent in path mode, therefore $p(L_j^{(S,v)})=\frac{1-p_2}{8}$, j=1,2,3,4, v=l, u.