JEAS | Journal of Economics and Administrative Sciences
E-ISSN: 2148-1792 P- ISSN: 1302-2024
Volume 5, Supplement Issue 2
www.jeasweb.org

Design of high-dimensional quantum keys to increase security between transmitter and receiver and transfer more information

Mohammad Hadi Mohammadi[*]
PhD student in Gravitation and Cosmology
Bu Ali University of Hamadan

Dr. Abbas Mobasheri
Assistant Professor of Physics - Condensed Matter
Faculty of Basic Sciences. Imam Ali Officer University

Dr. Amir Hamzeh Farajollahi
Assistant Professor of Aerospace Engineering - Major Aerodynamics and Propulsion
Faculty of Basic Sciences. Imam Ali Officer University

ABSTRACT

The encoding of information in the position of single photons has no definite limitations due to unlimited sources. By using a split single-photon source and a space light module (SLM), we direct single photons to specific locations in a virtual network in a large area that solves the photon count detector (ICCD). We experimentally show the selective addressing of each location (symbol) on a 9072 size grid (alphabetically) to achieve 10.5 bits of mutual information per photon detected between transmitter and receiver. Our results can be useful for processing very large quantum information.
Keywords: Decoy mode - Quantum key - HDQKD protocol.

Introduction

This study intends to establish a secure connection between two people that a third person cannot hear or access the information exchanged between the parties. These days, the enemy easily controls communications (through the Internet and eavesdropping). In this research, we present a quantum connection that, when the enemy wants to eavesdrop on the connection or measure it, its measurement is disrupted according to Heisenberg's uncertainty principle. In this research, the transmitter and receiver are called Alice and Bob, and the listener is called Eve. In this study, we can measure the amount of this information in case of information leakage.

Section 1

Problem description:

We first define quantum cryptography. The act of hiding information is called cryptography, which aims to transfer information securely. One way to create security in message transmission is to use shared keys. Current cryptography can be divided into classical and modern, apart from traditional cryptography. Classical cryptography does not mean obsolete cryptography. Classical cryptographic methods include methods that use algorithms such as DES. These algorithms can be decoded due to the mathematical dependence of the keys on each other. IT researchers have successfully demonstrated that the principles of quantum physics and quantum cryptography in optical networks can better protect communications. Wiesner Stephen first introduced quantum cryptography in the 1970s. In 1991, Ekert Arthur, a doctoral student at Oxford University, proposed another method for quantum cryptography. It should be noted that quantum cryptography is only used to generate and distribute keys, and this method does not apply to information encryption and transmission. To study quantum cryptography in detail and get acquainted with the basic terms and concepts, we will first briefly study electromagnetic and quantum waves; then, we will take a deeper look at quantum cryptography and key generation and distribution in this cryptography. [1,2]

Electromagnetic waves

Electromagnetic waves are a series of waves with the following characteristics: Electromagnetic waves have the same nature and speed. There is no gap in the spectrum of electromagnetic waves, meaning that any frequency can be generated. These waves do not need a material environment to propagate. Electromagnetic waves are transverse waves. Ground sources of electromagnetic waves include telephone relay device waves, lights, etc.

Photon

A photon is a fundamental particle that is a quantum unit of light or any type of electromagnetic radiation. Each photon has a certain amount of energy, motion magnitude, and angular or spin magnitude.

Polarization

Polarization is one of the properties of an electromagnetic wave, such as light. Huygens first discovered the polarization of light in 1960. Polarization can be used extensively, for example, in quantum cryptography. In the following, this issue will be discussed in more detail.

Principles of quantum cryptography

As mentioned, electromagnetic waves can be polarized. Polarization is contractually defined as the direction of an electric field in which either the direction of the electric field fluctuations is constant or varies in a certain way. If the polarization process is accurate enough, the process of generating photons can be positioned so that photons with vertical and horizontal polarizations are always generated. A polarizer is a device that only allows light to pass through a specific polarization direction. So if the light is not completely polarized, only half of it passes through the polarizer. As mentioned, each photon has the size of an angular motion or spin. In this theory, the photon, regardless of whether it has an initial

polarization or is passed through the polarizer, but if it does, it aligns with the polarizer axis. Uncertainty principle Heisenberg's quantum theory is based more on the premise that some of the quantities considered continuous in classical physics are quantum or discrete. In short, there are only two types of descriptions for a material particle or a photon: One is a wave description, and the other is a particle description. Thus, a particle can be attributed to both material properties (motion and location) and wave properties (wavelength and frequency). Electromagnetic radiation shows both wave and particle aspects. Heisenberg's uncertainty theory can be expressed in two ways: 1. Suppose we express electromagnetic radiation in the language of particles and determine a photon's location at any given moment with complete accuracy. In that case, the uncertainty in space and time becomes zero, but on the other hand, the uncertainty in what is attributed to the photon wave (such as wavelength) is infinitely large. 2. On the other hand, if we can determine exactly what is attributed to the photon wave, then the uncertainty in the photon wave will be zero, and the location of the photon will be unknown.

Quantum cryptography

In this section, we come to the main part of the discussion. As mentioned earlier, quantum cryptography is only used to generate and distribute keys. This key can be used in the next steps with any encryption algorithm to convert the message into a password or vice versa. Quantum cryptography allows both parts of the connection to communicate their password through a completely secure private channel. The following protocols can be used to generate and distribute quantum keys:

- BB84
- T12 protocol
- Decoy state protocol: A practical QKD scheme using imperfect single-photon sources, such as weak coherent state sources
- SARG04
- six-state protocol
- E91 protocol: entanglement protocol
- B92 protocol: protocol using only two nonorthogonal states by Charles Bennett
- BBM92 protocol: entanglement protocol
- MSZ96 protocol
- COW protocol: coherent one-way protocol by Gisin
- DPS protocol: differential phase shift by Yamamoto
- KMB09 protocol: High Error-rate QKD protocol by Khan et al.
- HDQKD: High-dimensional Quantum Key Distribution

HDQKD protocol

This research uses the HDQKD protocol to increase security and noise tolerance and increase the information exchanged. To use this protocol, we use the SPDC device. This device converts one high-energy photon into two low-energy photons, in which case more information is exchanged because each photon carries one qubit, and the dimensions of each qubit are more than 2. This protocol uses the decoy-

state protocol to determine whether Eve could access the parties' information. PNS ATTACK is an attack by a third party for accessing information that retrieves information from Alice and sends a copy to Bob, that this problem is partially solved with the decoy-state protocol. However, the main difference in the decoy-state of this protocol (HDQKD) with BB84 is that in BB84, we use Quantum bit error to find out how much information Eve has received, but in HDQKD, we reduce the measurement so that less information is disturbed to understand how much information is leaked.

However, the main purpose of this research is to measure parameters such as noise and decoy states (detecting the amount of leaked information or PNS attack) that Alice and Bob can be in a secure connection in the form of HDQKD protocol which leads to increased security, more noise tolerance, increased information exchange and high data transfer speed. [3-4-5-6] I will deal with two similar works that have been done in this regard:

BB84 protocol:

This protocol was proposed by Bennett and Brassard in 1984 and is based on the Heisenberg uncertainty principle. According to this principle, For example, without knowing the initial state of a photon, if we choose the vertical direction to measure the polarization of a photon, the photon passes through the polarizer with vertical polarization, and the horizontal polarization does not pass at all. Now, if we make another measurement at an angle of 45 degrees from the first measurement, the probability of the photon passing through the second polarizer is exactly 0.5, so we say that the first polarizer makes the measurement of the second polarizer completely random. Therefore, the direction of this polarization can be determined if a polarizer with zero to 90 degrees is selected because a 45 or 135-degree polarizer also gives an output with the same polarization. According to the description, the transmitter uses the source to send one of the four modes of high polarization (zero, 45, 90, 135) to the receiver. The receiver, on the other hand, is used to measure polarization. The receiver stores the measurement result. The receiver then uses the public channel to specify the type of Rectilinear and Diagonal measurement filters. In all these steps, the measurement result is kept secret by the receiver then the sender informs the receiver about which receiver filter was correct. Only if the transmitter and receiver used the same measurement type can we be sure that the measurement was correct. The key is made by using common measurements between the transmitter and receiver and eventually converting them to bits. [7]

E91 protocol:

In 1991, Ekert Arthur proposed a new protocol for key distribution based on quantum correlation. This protocol uses a quantum channel and a single-photon source. The function of this protocol is that two correlation pairs are separated from each other, and each transmitter and receiver are received one of the two pairs. Each uses a filter to measure its input in detail according to this protocol. Like the BB84 protocol in its second functional part, this protocol exchanges in the classical channel to determine the measurement filters on both sides. Finally, for every measurement that the transmitter and receiver use the same filter, they should expect conflicting results according to the laws of quantum correlation. This means that both sides of the exchange interpret their measurements as before, except that the bit string of each is a complementary binary to the other. If one of the parties reverses its key, a secret key is shared between the two. [8]

Section 2

Concepts

Communication means exchanging information through speaking and writing or any other media. In this project, information is passed between Alice and Bob that Alice is the transmitter and Bob the receiver, but unfortunately, a third person named Eve hears or observes this connection. If Alice and Bob want to prevent Eve from being spotted, they must encrypt their connection. Encryption involves communication in which the transmitted information is encrypted. The most direct encoding is the disposable pad, in which the message is encoded by random bit strings that act as keys. Random bit strings are refined by the logical XOR operator (an operator that compares two input bits and generates one output bit) to encode or decrypt the message. This method has been proven to be a safe method [9]. In the project, random bit strings are the key generated from the information exchanged between Alice and Bob. To do this, we need to define the quantity of information. One way to do this is to define the entropy of the information described below:

Information entropy

Information entropy can be used to measure the average of the information in the *X* alphabet, in which *'x'* is a discrete variable and *'P(X)'* its probability is defined as follows [10]:

$$H(X)=\sum_{x}P(x)\log_2\frac{1}{P(x)'}$$

This entropy is also called *X* uncertainty, generally using the base two logarithms. Thus the entropy of information can be interpreted by yes and no questions, which one of them is the answer that leads to the identification of information.

Mutual Information

Here we are dealing with information that is transmitted between two actors, which is why we define entropy as follows:

$$H(X,Y)=\sum_{x,y}P(x,y)\log_2\frac{1}{P(x,y)'}$$

$$I(X;\gamma)=H(X)+H(\gamma)-H(X,\gamma)=H(\gamma)-H(\gamma|X)=H(X)-H(X|\gamma) \quad \text{(q)}$$

The entropy *x* with the condition γ is as follows:

$$H(X|\gamma)=\sum_{y}P(y)\left[\sum_{x}P(x|y)\log_2\frac{1}{P(x|y)}\right]=\sum_{x,y}P(x,y)\log_2\frac{1}{P(x,y)'} \quad \text{(qq)}$$

According to Bayes's theorem, we have

$$P(x,y)=P(x)P(y|x)=P(y)P(x|y)$$

Therefore, according to the (qq) equation and the Bayes's theorem, the entropy is equal to:

$$H(X|\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(y)}{P(y|x)P(x)}=$$

$$=\sum_{x,y}P(x,y)\log_2\frac{1}{P(x)}+\sum_{x,y}P(x,y)\log_2\frac{P(y)}{P(y|x)}$$

Therefore, according to equation (q), **Mutual Information** is equal to:

$$I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$$

Measurement operator

So far, we have talked about classical information theory. To understand quantum mechanics in information theory, we must choose a strategy that can measure quantum states [11]. Quantum measurement is described by quantum operators $[M_m]$ that apply to the following equation:

$$\sum_m M_m^+ M_m = 1$$

For each special case, $|\psi\rangle$ the measurement load *m* occurs with the following probability:

$$p(m)=\langle\psi|M_m^+M_m|\psi\rangle \qquad (1)$$

() the operator is special hermetic and has a positive expectation value ($\langle\psi|E_m|\psi\rangle\geq 0$). If the operator is a hermetic measure and has this condition $M_m M_{m'}=\delta_{m,m'}M_{m'}$ is called the measurement of the projection that we have already encountered in optics. The special positive expected value is called PVOM.

State discrimination

The simplest example of state discrimination is the distinction between two qubits. A qubit is a two-dimensional quantum state $a|0\rangle+b|1\rangle$ $(a,b\in\square,|a|^2+|b|^2=1)$ in which special vectors are $|0\rangle,|1\rangle$ perpendicular to each other. Since Bob can distinguish between special cases, the special cases are orthogonal or perpendicular. For example, when Alice prepares two-mode specials $|\psi_1\rangle=|1\rangle,|\psi_2\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)$ to send to Bob, she decides which special mode Bob will receive. The

projection measurement defines two properties of the asymmetric state $|\varphi_1\rangle, |\varphi_2\rangle$ that are not angular $|\psi_1\rangle$, $|\psi_2\rangle$ which $|\varphi_1\rangle$ covers a greater angle than $|\psi_1\rangle$. The projection is performed by operators $|\varphi_1\rangle\langle\varphi_1|$ و , and its probability of success is $|\psi_1\rangle$ we guess will result $|\varphi_1\rangle$. If the system is thrown at, $|\varphi_2\rangle\langle\varphi_2|$ calculated as follows:

$$P_{GUESS} = \frac{1}{2} + \frac{1}{2}(1 - |\langle\psi_1|\psi_2\rangle|^2)^{\frac{1}{2}}) = \frac{1+\sqrt{2}}{2\sqrt{2}} \approx 0.85$$

Obviously, by calculating this probability, an error occurs in detecting states. However, there is a way to distinguish between the two modes. Sometimes, this method is called unambiguous state discrimination [12]. The first scenario is for Bob to measure the projection on the special orthogonal states. For half of the measurement time, Bob operates on the operator $|\psi_1\rangle\langle\psi_1|$ (in pin 1), and the other half of $|\psi_1^T\rangle\langle\psi_1^T|$ و the measurement time acts on (in pin 2). Suppose Bob performs a projection $|\psi_2^T\rangle\langle\psi_2^T|$ و $|\psi_2\rangle\langle\psi_2|$ measurement at base 1. If the system is thrown after measurement $|\psi_1^T\rangle$, Bob knows that our case is because components $|\psi_2\rangle$ are in the direction of $|\psi_1^T\rangle$. If the system is thrown after the measurement, it will not result because it has components in direction $|\psi_1\rangle$.

$$P_{proj} = \frac{1 - |\langle\psi_1|\psi_2\rangle|^2}{2} = \frac{1}{4}$$

Quantum information and Holevo range

The Mutual Information section includes measuring the information shared between Alice and Bob. Unlike the two classical states, the quantum measurement is not always able to distinguish between quantum states. This amount of information that can be considered about a quantum system is called accessible information [11]. In the case of quantum states, this available information is a measure of the information shared between Alice and Bob. There may be no known formula for calculating; however, high ranges like Holevo give us this inequality. Suppose Alice prepares a possible state mixed with the *ρx* density operator where *X = 1, .., d* with probabilities *p1, p2,... pd* that Bob makes this measurement by *PVOM = {E1. .., Em}* mentioned in the measurement operator section, in which case, with the result of measuring $^{\gamma}$ for each measurement, the Holevo range states that:

$$I(X;Y) \leq S(\rho) - \sum_x \rho_x S(\rho_x)$$

That is the above equation $\rho = \sum_x p_x \rho_x,$ and $S(\rho) = -Tr(\rho \log_2 \rho)$ which is Newman entropy. The maximum information for mixed quantum states is obtained $\rho = \sum_n \frac{1}{d}|n\rangle\langle n|$ with orthogonal bases $\{|n\rangle\}$ containing the same probabilities for each special state ($p_1, \ldots p_d = \frac{1}{d}$). Because Alice can block an

unlimited amount of information, but Bob only has access to this ($\log_2 d$) in the orthogonal system, quantum information and classical information are equal. However, we are interested in quantum information because limited information can be less than information prepared by Alice.

Quantum cryptography:

One way to use the quantum nature of light to generate a key between Alice and Bob is to use a quantum key distribution or QKD [13]. Bennett et al. developed the first QKD protocol in 1984 by Bennett et al. [14]. Alice has a single-photon light source. She encodes a bit of information with 0 or 1 at a two-dimensional polarization according to the bases of the photons. She encodes horizontal and vertical bases according to Pauli matrices $\sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$ or diagonal or non-diagonal bases with $\sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$ that in this way, Alice and Bob can change their bases. By rotating the PBS at a 45-degree angle, Alice and Bob adjust the device to each other and encode the qubits.

Intercept resend attack

The most direct attack strategy by Eve is called intercept resend. Eve tracks photons through a quantum channel and measures scattering as Bob does. Because Alice and Bob alone generate the key that Bob receives, Eve needs to resend the same photon. There are two scenarios here. The first is that Alice and Eve randomly choose the same bases (same Pauli matrix). So by measurement, the photon state does not change, so Eve has the information sent by Alice, and there is no error in it. The second scenario is that Alice and Eve choose unequal bases, which means that the information sent by Alice will not be revealed.

Mass attacks

Mass attacks cause Eve to have no quantum memory. She can hold her attack equipment for as long as she wants and make the best measurement, according to her knowledge, a collective measure. The covert measurement of this attack was performed by Devetak-Winter [15].

$$\lim_{N\to\infty} r = S(X|E) - H(X|\gamma)$$

$$S(X|E) = S(X,E) - S(E)$$

That these relationships are established $H(X|\gamma) = H(X,\gamma) - H(\gamma)$

Coding

In this research, the position of photons is coded transversely, which was first done by Walbourne [16]. If $f(r)$ the detection range is on page *x,y* then:

$$|\psi\rangle = \int |r\rangle\langle r|d^2r|\psi\rangle = \int f(r)|r\rangle d^2r \quad (3)$$

This is a special single-photon mode on this page *x,y*. Now the location of $|\psi\rangle$ the special state of this single-photon is measured. On the other hand, we have the completion rule for the measurement operator:

$$\int |r'\rangle\langle r'| d^2 r' = 1$$
$$\langle r'|r\rangle = \delta^2(r'-r)$$

According to Equation (1), the probability of detecting a photon in space r' is equal to:

$$p(r') = \langle\psi|r'\rangle\langle r'|\psi\rangle = |f(r')|^2$$

The single-photon wave function can be defined in *k* space using the evolution equation:

$$|\psi\rangle = \int f(r)|r\rangle d^2 r = \iint f(r)\langle k|r\rangle|k\rangle d^2 r d^2 k = \int \frac{1}{2\pi}\int f(r) e^{-ik.r} d^2 r |k\rangle d^2 k$$

In the above equation, the wave function and the Fourier transform amplitude are as follows:

$$\langle k|r\rangle = \frac{1}{2\pi} e^{-ik.r}$$
$$\mathcal{F}(f(r))[k] = \frac{1}{2\pi}\int f(r) e^{-ik.r} d^2 r$$

For a two-dimensional Gaussian function at the point $r_0 = (x_0, y_0)$ with variance Δx, the amplitude is as follows:

$$f(r) = f(x,y) = \frac{1}{\sqrt{2\pi\Delta r^2}} \exp(-\frac{(x-x_0)^2 + (y-y_0)^2}{4\Delta r^2})$$

Therefore, according to the above two equations, the amplitude in space *k* is as follows:

$$\mathcal{F}(f(x,y))[k_x, k_y] = \frac{2\Delta r}{\sqrt{2\pi}} \exp(-\Delta r^2(k_x^2 + k_y^2)) \exp(-i(x_0 k_x + y_0 k_y))$$

Since the variance in space *k* is $\Delta k = \frac{1}{2\Delta r}$, the amplitude in space *k* is as follows:

$$\mathcal{F}(f(x,y))[k_x, k_y] = \frac{1}{\sqrt{2\pi\Delta k^2}} \exp(-\frac{(k_x^2 + k_y^2)}{4\Delta k^2}) \exp(-i(x_0 k_x + y_0 k_y))$$

The variance of these two conditions estimates the uncertainty [17].

$$\Delta k \Delta r = \frac{1}{2}$$

Now the probability can be calculated according to Equation 1:

$$p(k') = \left|\mathcal{F}(f(x,y))[k_x, k_y]\right|^2 = \frac{1}{2\pi\Delta k^2} \exp(-\frac{(k_x^2 + k_y^2)}{2\Delta k^2})$$

It should be noted that the probability does not depend on the center of the Gaussian point. Measurements in space *k* give us no information about the center of a point in space *x* and vice versa. Space *x* and space *k* are Fouriers of each other. Due to limitations, basic vectors $|k\rangle \ |r\rangle$ can not be used for coding. The limit of Equation (3) $f(r)$ has a non-zero expansion, which $\langle a_i | b_j \rangle = \frac{1}{d}$ makes the difference between theoretical and observational values. A discrete detector measures the position of the photons.

Section 3

High limit on mutual information

Until now, it has been assumed that the information content of individual photons is limited only by choice of encoded quantum states, as seen in the Concepts section. If someone considers the connection between the line of sight of free space and light, it has to deal with several sources of noise [18, 19]. Another source of atmospheric turbulence is wind and temperature gradients [20]. Under real circumstances, the detection efficiency of the detectors and their dark number must also be considered. The information capacity of encoded photons has been analyzed spectrally [21] and temporally [22]. This paper investigates the high level of information that space-encoded photons can transmit. Examination of the maximum information encoded in a single pulse begins with introducing the multi-photon effect in the first section. The second part focuses on the contribution of detector noise. Finally, the final section adds transverse beam propagation by noise transmission channels.

Methodology:

High level of data encryption

In this section, a high limit for the content of transmitted information can be translated under soundless conditions. The number of photons per pulse of the *Np* signal can be greater than one. Several *Nd* (orthogonal) detectors are used to read the signal. Detectors cannot count the number of photons. The simultaneous entry of several photons results in only one detector, just like a single photon. For this reason, we assume that each detector has only one single photon event, and a two-factor coefficient gives the number of recognizable symbols.

$$N_s = \binom{N_d}{N_p} = \frac{N_d!}{N_p!(N_d - N_p)!} \quad (3.1)$$

This number reaches its maximum when the number of symbols equals half the number of detectors.

The upper limit includes detector noise

Inspired by a more accurate description, the effect of tracker noise should be analyzed. As in the previous section, signal pulses with a maximum of one photon per detection region are considered. Recognition of these signals requires a special class of sensitive single-photon cameras. Their high sensitivity is costly, and the possibilities are limited. Symbols in relation (3.1): *Np* Number of photons in a signal pulse and *Nd* Number of detectors. If the number of detector clicks does not match the number of photons in the signal pulse, this measurement will be ignored, as this is an undeniable sign of a noise event. For previous detectors, four separate events are possible. There are two ideal states, true negative and true

positive: no photons sent and no photons sent. The measurement is sent with a probability K_{00} or a photon and causes the detector to click with the probability K_{11}. Two unintended events are positive and false. Negative: No photons are sent, but the detector is sent with a probability K_{01} or one photon, but it is not likely to be diagnosed with the probability K_{10}.

With two of these probabilities, the probability of correct measurement of the symbol can be calculated as follows:

$$R = K_{00}^{N_d - N_p} K_{11}^{N_p} \quad (3.2)$$

In this case, all *Np* detectors click with radiant photons, while $N_d - N_p$ the number of darkness does not occur. The probability of recognizing a wrong symbol is not $1-R$ because measurements whose number of detection events is not equal to the number of Np radiation photons are discarded, and an accurate count is not the same as a correct measurement on any detector. A dark count must compensate any photons that do not cause the detector to click from a false count detector for a fixed and correct number of detection events. Therefore, the probability of wrong clicks *k* is given by the following relation:

$$W = K_{00}^{N_d - N_p - k} K_{11}^{N_p - k} K_{01}^{k} K_{10}^{k} \quad (3.3)$$

Here, $N_p - k$ detectors click with radiant photons, while dark states do not occur at times. To fulfill the terms of the general *Np* click framework, *k* detectors that do not click with K_{01} probability, *k* detectors that do not click with K_{10} probability. No dark counting above the number required for *Np*, $k = 0$, $W_0 = R$, to calculate the error W, the W_k probability must be multiplied by the number of permutations. This leads to:

$$W = \sum_{k=1}^{\min(N_p, N_d - N_p)} W_k \binom{N_d - N_p}{k} \binom{N_p}{k} \quad (3.4)$$

The average probability of measurement is the symbol of $\frac{W}{N_s - 1}$ error. Common probability is defined as follows:

$$P(x, y) = \frac{R}{N_s (R + W)} \qquad \forall x = y \quad (3.5)$$

$$P(x, y) = \frac{W}{N_s (N_s - 1)(R + W)} \qquad \forall x \neq y \quad (3.6)$$

Probabilities can be used to calculate mutual information using the $I(X;\gamma) = \sum_{x,y} P(x,y) \log_2 \frac{P(x,y)}{P(x)P(y)}$ equation. As a result, the final equation equals:

$$I(X;Y)=\frac{R}{R+W}\log_2(\frac{N_sR}{R+W})+\frac{W}{R+W}\log_2(\frac{\frac{N_s}{N_s-1}W}{R+W}) \quad (3.7)$$

Now, if $a=\frac{W}{R}$ we have:

$$I(X;Y)=\frac{1}{1+a}\log_2(\frac{N_s}{1+a})+\frac{a}{1+a}\log_2(\frac{\frac{N_s}{N_s-1}a}{1+a})=\log_2(N_s)+\log_2(\frac{1}{1+a})+\frac{a}{1+a}\log_2(\frac{a}{N_s-1})$$

(3.8)

As expected, mutual information increases for smaller ratios $a=\frac{W}{R}$. The higher the probability of recognizing the correct symbol *R* and the less likely it is to measure the incorrect symbol *W*, the greater the mutual information. In addition, as seen in the previous section, the mutual information increases with the number of symbols.

In this section, the number of detection events was considered equal to the number of signal photons. As a result of this limitation, signal loss is associated with events in which these numbers are unequal. This leads to total loss, which considers all events not recognized as false or true symbols. This dissipation measures polynomials in the number of detectors and signal photons. In this model, Nd detectors with efficiency detect an Np photon wave state. If the number of darknesses is N_{dark}, the probability of an observer for darkness is $\frac{N_{dark}}{N_d}$, so the fidelity of finding the right symbol is equal to:

$$F=\frac{N_p(\eta+\frac{N_{dark}}{N_d})}{N_p(\eta+\frac{N_{dark}}{N_d})+(N_d-N_p)\frac{N_{dark}}{N_d}}=\frac{N_p(\eta+\frac{N_{dark}}{N_d})}{N_p\eta+N_{dark}} \quad (3.9)$$

Fidelity can be placed in the formula of mutual information:

$$I(X;Y)=\log_2(N_s)+F\log_2(F)+(1-F)\log_2(\frac{1-F}{N_s-1}) \quad (3.10)$$

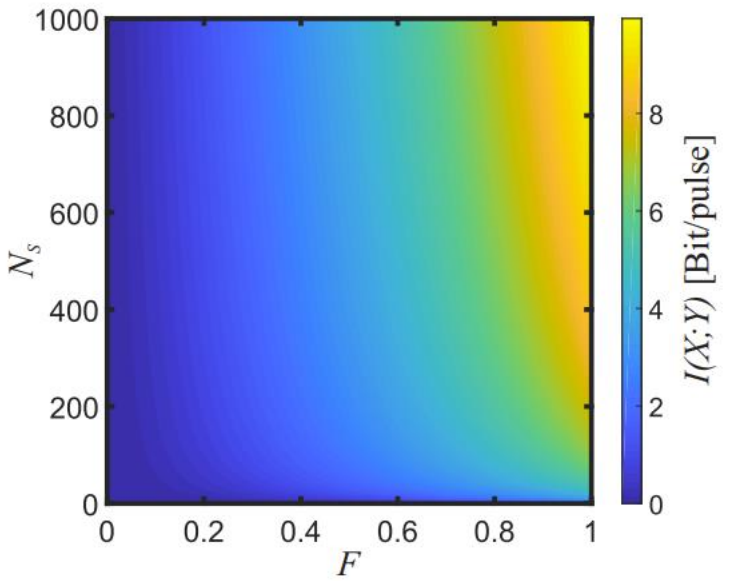

Figure 1: $I(X;Y)$ as a function of the number of symbols N_s and the fidelity F

Figure 1 shows that :

Surface plot of the upper bound on the mutual information $I(X;Y)$ as a function of the number of symbols N_s and the fidelity F. The influence of the fidelity on the mutual information is shown in figure 1. The information per pulse increases with the fidelity and reaches its maximum at a fidelity of one which corresponds to the noise-free case with a mutual information of log2 (N_s).

High-limit level diagrams on cross-information $I(X;Y)$ function the number of *NS* and Fidelity *F* symbols.

The effect of accuracy on mutual information is shown in the figure above. The information of each pulse increases with accuracy and reaches its maximum accuracy, which is related to $\log_2(N_s)$ a noise-free state.

The upper limit includes channel noise

As discussed in the previous section, if someone wants to increase the mutual formation of photons effectively, they must consider a single photon on a large number of detectors. This is why this section limits the number of photons to one photon per signal pulse. The detectors are arranged in a two-dimensional detection array, and the photon is routed to a specific detector. Channel noise in the form of $F(x-x_0, y-y_0, \sigma)$ function amplitude of focus with a width of σ around the center: (x_0, y_0). It is assumed that the overall probability of a dark count is small compared to the detector's performance, which makes it possible to simplify the analysis only by considering single-photon detection. Due to the amplitude of the photon and the two-dimensional arrangement of the detectors, the interaction between the detectors becomes noticeable. The size of the detectors can be increased to minimize the exchange, but in realistic scenarios with limited diaphragms, this is not possible. The other end will be a range of focus on many detectors, which minimizes mutual information. To calculate the mutual information from this relation:

$I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$, the common probability distribution $P(X;Y)$ must be known. $P(X;Y)$ Participates in two places: the first in the simulated signal of the $F(x-x_0,y-y_0,\sigma)$ function with η efficiency and the second in the counting of dark states. To describe these two states, we have to make a formulation and define it with an icon, which shape it is $M(X,Y)$. For each *x*-symbol, this statistical function can be calculated by integrating reflecting the intensity of the focus on the detectors being identified.

$$M(X,Y)=\eta\int_{floor(\frac{y}{\sqrt{N_d}})}^{floor(\frac{y}{\sqrt{N_d}})+1}\int_{(y \bmod\sqrt{N_d})-1}^{y \bmod\sqrt{N_d}}F(k-floor(\frac{x}{\sqrt{N_d}})-0.5l-x \bmod\sqrt{N_d}+0.5\sigma)dkdl+\frac{N_{dark}}{N_d}$$

(3.11)

On the other hand, we have in the Gaussian function:

$$F(x-x_0,y-y_0,\sigma)=\frac{1}{2\pi\sigma^2}\exp(-\frac{(x-x_0)^2+(y-y_0)^2}{2\sigma^2}) \quad (3.12)$$

Finally, we use the following condition to normalize the probability:

$$\sum_{x\in X,y\in Y}P(x,y)=1 \quad (3.13)$$

So we have:

$$P(x,y)=\frac{M(x,y)}{\sum_{x\in X,y\in Y}M(x,y)}\approx\frac{M(x,y)}{N_d(\eta+N_{dark})} \quad (3.14)$$

The maximum state of mutual information sent and received is equal to $P(X)=P(Y)=\frac{1}{N_s}$. With this data, we can obtain reciprocal information from the relation: $I(X;\gamma)=\sum_{x,y}P(x,y)\log_2\frac{P(x,y)}{P(x)P(y)}$. The upper bound is the mutual information between a transmitter and a receiver for a particular model. The first part provides an expression for the maximum amount of information that can be encrypted. A single-photon must be encoded at each signal pulse to maximize information per photon. The next section introduces the detector noise within the design range. Detector noise reduces mutual information per photon.

Section 4

Transmit data over 10 bits with a single photon

The encoding of information in the position of single photons has no definite limitations concerning unlimited sources. Using a split single-photon source and a space light module (SLM), we direct individual photons to specific locations in a virtual network in a large area that solves the photon count detector (ICCD). We experimentally show the selective addressing of each location (symbol) on a 9072 size grid

(alphabetically) to achieve 10.5 bits of mutual information per photon detected between transmitter and receiver. Our results can be useful for processing very large quantum information.

Its poor interaction with the environment makes the light ideal for sharing information between remote parties. For this reason, light is used to transmit information around the world. With single-photon sources, a new class of applications has emerged. Due to their quantum properties, single photons are used for attack angle quantum systems or quantum cryptography [23]. A well-known example is the Quantum Key Distribution (QKD) using the BB84 protocol [24] to create a shared secret key between Alice and Bob. The security of this method is based on the non-simulation theorem [25], which prohibits the copying of quantum states. The standard implementation of the BB84 protocol uses a two-dimensional polarization basis to encode information in photons. Thus the alphabet contains only the two symbols "0" and "1", which limits the content of information in each photon to one bit. Increasing the base dimension using a large alphabet increases each photon's information content and improves security [26, 27, 28]. This motivation is to use larger alphabets using the force of orbital angular motion [29, 30], temporal buffing [31, 32] or spatial translation [33, 34]. Among the spatial encryption schemes, Orbital Angle Rotation (OAM) modes have been proposed for encrypting high-dimensional information [35]. In a practical scenario, however, assuming a transmitter-receiver configuration with finite-sized diaphragms, a limited diffraction point that translates into space or the Gaus-Logger material has a higher capacity limit than a subset of pure OAM modes [36, 37]. This spatial positioning of light, or equivalently, tilting the plane waves, provides an ideal way to increase the information content per photon.

Interestingly, there is no high limit to information content transmitted by single photons due to unlimited sources. For example, using one mole of ideally positioned single-photon detectors results in 79-bit information content per photon detected. This is out of reach in a practical situation. So a very relevant question is what can be achieved experimentally. In this chapter, we report our experiment in which we definitively encode more than 10 bits of information into one photon. We used 2 to 3 times more space encryption than before, which reported 7 bits per photon as the highest value for random keys [34] and is comparable to that obtained in temporal coding and polarization [38].

Methodology:

Method of operation

The setup

The setup is shown in Figure (4.1). We use the spontaneous parametric method to generate a conversion source to produce photon pairs [39]. A locked Piscond laser with 790 nm mode with a pulse repetition rate of 76 MHz in an LBO crystal doubles the frequency to 395 nm. The double-frequency light is concentrated in a crystal of polarized photons of the potassium-tectyl phosphate (PPKTP) period, which automatically produces pairs of vertically polarized photons at 790 nm. Photon pairs stuck in a divider and a narrow, polarizing beam are separated into two states of single photons. One of these photons is sent to a single photon counting module that acts as a herald; the second photon, on the other hand, is routed to the encryption settings via a 28.5-meter single-mode fiber with 47% operating power. To communicate freely, one needs a coder device in the sender position and the other a decoder device in the receiver position. As an encoder, we use a space light modulator to adjust the wavefront of single photons. By writing a glowing grid on the SLM, we change the reflection angle to 0.8 angles in the vertical and horizontal directions with a refractive index of 76% in the first instance. The Fourier transform SLM is imaged with a 1m focal length lens configured in f2 on a large space photon-counting detector. A bandpass filter in 800 ± 40 nm is placed in front of the detector to block stray light.

Detector

The decoder must measure the entry of a photon in a single image over a large area. One of the technologies that can achieve this goal is the device equipped with a charge-coupling [40, 41]. ICCDs provide a nanosecond on light option, which significantly reduces the amount of darkness, and it enables such an ICCD to measure explicitly and reduces the number of darkness to one per thousand readings. The dark number of ICCDs originates in the thermal electrons released by the ICCD photocathode. In addition, the remaining gas atoms can be ionized by electron avalanche inside the microchannel plate (MCP) of the amplifier. These ions accelerate to the photocathode at MCP bias voltage and release secondary electron beams. The effect of ions is to generate many more electrons than the input photons. This increases the local signal in the ICCD, which is brighter than the signal produced by a photon. Therefore, these fake ion signals can be filtered in post-processing. Our model (Andor iStar A334 – DH - 3u – A18T) has a photocathode quantum efficiency of 5%. Each photon selected from the SPDC source opens the ICCD gate for 2 nm. Figure 4.2 is taken with an exposure time of 0.1 seconds. Single-photon events were analyzed using threshold photon count [41], with a threshold level set above the CCD camera readout noise. According to the SPDC, at the 400 kHz herald rate, we measured an average of 7.3 photon detections per symbol. FWHM of focus, with a fixed phase pattern in SLM and integration of more than 1000 photon detection events, was found to be 7.9 ± 0.3 pixels horizontally and 7.4 ± 0.2 pixels vertically.

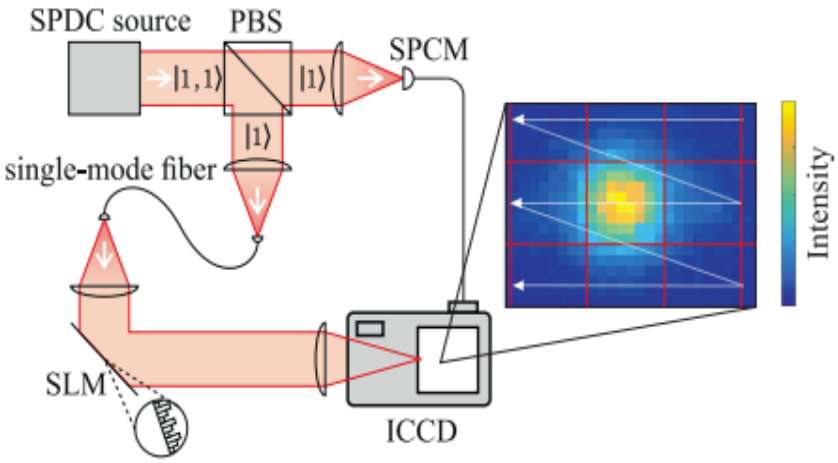

Figure 2: The schematic of Spontaneous Parametric Down-Conversion (SPDC)

Figure 2 shows that schematic representation of the layout. The spontaneous parametric decrement source of type II (SPDC) produces pairs of photons split by a polar beam splitter (PBS). A single-photon counting module (SPCM) detects one of the photons that acts as a signal for a sensitized CCD (ICCD). Another fiber photon is paired and occurs on a space light module (SLM). Its Fourier image is displayed on the ICCD. The focus position is carefully scanned according to the iron bars shown by the bow and arrow. The red lines indicate the 8*8 pixel mac of the symbols.

Encryption

The target position of the photon on the ICCD is determined by the horizontal and vertical diffraction angle of the network in the SLM. Although scanning mirrors can be used for spatial encryption, SLM is a more flexible tool. Through holography, the phase and amplitude of the wavefront can be manipulated, which allows the use of a complex wavefront. In addition, the path of light can be modified for disturbances using wavefront shaping methods [42]. SLM (pixel size: 20 µm, resolution: 800*600 pixels) with horizontal and vertical edges is programmed to scan at the ICCD detection level. The angular

range of the coded alphabets is small (0.33 o), and the grid step is more than 5 pixels, ensuring uniform and high diffraction performance for all symbols. In order to define the sent symbol, the position on the ICCD must be mapped to separate symbols.

For this reason, a network is defined on the ICCD. ICCD pixels are combined in 8*8 or 12*12 pixel recognition areas to form a 9072 or 4050 symbol alphabet. This ICCD-level rectangular map connects each identification area to a unique tag, numbered from left to right and from top to bottom.

Result

Spatial encryption of information takes place on a rectangular virtual network composed of the pixels of a camera. The maximum information is a bit if the entire camera chip is used. If we fill in our experimental parameters, the signal-to-dark ratio of 10.08 and the focus size of 8 pixels in each direction on the ICCD, this number will be reduced to 14.45 bits. In our experiment, we used a network with dimensions of 112*81 pixels, which are 9072 symbols of our alphabet. This value corresponds to the maximum $\log_2(9072) = 13.15$ bit information content. The light is directed to the distinctive symbols on the grid by scanning the focus using SLM as an ignited window. We assume that the sender uses the *X* alphabet and the receiver uses the *Y* alphabet. In this system, we examine the common probability distribution of P(X, Y), which indicates probabilities p(x, y) for distinguishing a particular y-symbol outside the Y-alphabet if an x-symbol is sent outside the X-alphabet. The result is shown in Figure 4.2. Applying a threshold to the measured signal reduces the ICCD noise to show only the amplified signal. A diagonal line in the graph of the sent symbol versus the received shows the maximum correlation. There is a strong correlation between the sent and received symbols set in graph (a), which shows the whole alphabet in a log-log diagram. Graph (b) shows a magnification of the first 200 of 9072 symbols. Due to the interference between the symbols, lines outside the diameter are visible, corresponding to the photons that hit the symbol above or below the target. The distance of 112 symbols between these lines and the diameter corresponds to the length of the network column written on the camera. The left and right diameter signal is obtained by interfering with the left and right symbols in the network. A dark ICCD count can also cause noise.

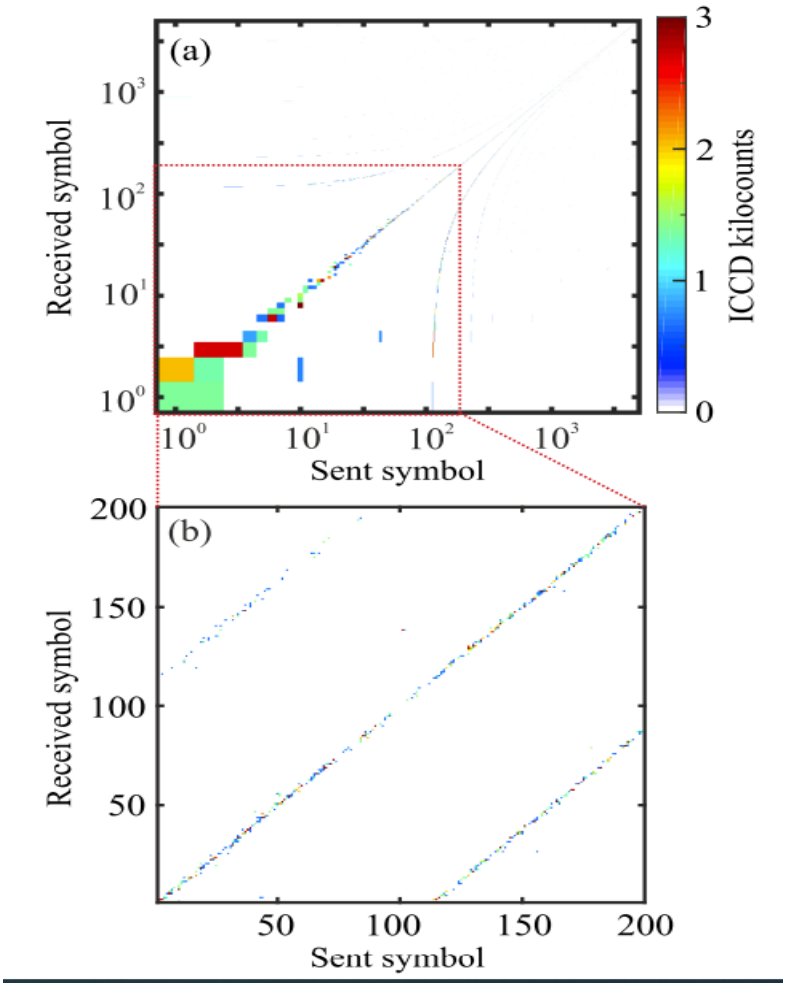

Figure 3 : The ICD measured symbols

Figure3 shows that the ICD measured in each of the measured symbols is counted as a function of the sent symbol with a macro size of 8*8 pixels. The exposure time for each symbol was 0.6 seconds. Graph (a) shows the correlation between all 9072 symbols in a log-log diagram. Figure (b) shows the measured correlation between the first 200 symbols in a line graph.

To quantify the information contained in each photon, we calculate the mutual information between the sender and receiver. Mutual information I (X: Y) is a measure to reduce the average uncertainty about a sent symbol set *X* obtained by learning the value of the received symbol set *Y;* or, conversely, the average amount of information that *X* conveys about *Y* [43]. The mutual information in each transmitter-receiver system detection event is mathematically displayed as follows:

$$I(X:Y) = \sum_{x \in X, y \in Y} P(x,y) \log_2 \frac{P(x,y)}{P(x)P(y)} \tag{4.1}$$

Where P (x, y) is the probability of receiving the symbol *y* when the symbol *x* is sent, P (Y) is the probability of measuring the symbol *y*, and P (x) is the probability that the sender encrypts the symbol *x*. Theoretically, the mutual information depends on the number of *N* symbols, which has a maximum of

$I_{\max} = \log_2(N)$, assuming $P(x) = \frac{1}{N}$ for each $x \in X$ symbol. In this paper, we guarantee the uniform probability of *x* for the maximum realization of the theory in the absence of noise. The limited CCD size limits the maximum number of symbols. Using the skin size of the 8*8 detection area, our theoretical limit is 13.15 bits. The interaction is limited not only by the number of symbols and the entropy of the sent alphabet but also by the interference between the symbols due to the diffraction focal points and the noise from the environment and the detector. In order to reduce the interference between the symbols, the macro size of the detection areas can be increased. However, this reduces the number of symbols given to a limited number of detection pixels. The blue circles in Figure 4.3 show the maximum interdependencies of the mutual information for the constructed symbols with different pixel sizes. Mutual information measured for 8*8 and 12*12 pixels are shown as red circles. The measured data are less than theoretical. This can be understood from the average collision probability, indicated by the green + markers. In addition, considering the signal-to-darkness ratio limited to between 10 and 100, which leads to the expected reciprocal information, it is shown as gray bars in the figure. As can be seen from the figure, there is maximum mutual information due to the physical limitations of interference and noise. For large bucket sizes with close to zero interference between symbols, very high mutual information of more than 9 bits per photon can be obtained. Given the FWHM dot size of approximately 8 pixels, we choose an 8*8 burning that achieves 10.5 bits of mutual information per photon detected. To calculate the mutual information in each transmitted photon, losses in our drivers must be considered. These include coupling losses in single-mode fibers 55%, failure losses in SLM 24%, spectral filters 30% and losses in detectors due to limited quantum efficiency 5%. This results in a channel capacity of 0.1 bits per photon.

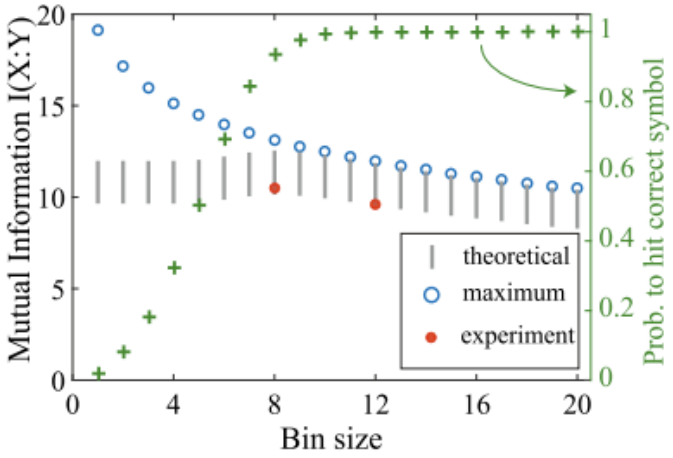

Figure 4: Mutual information I(X;Y) is function of size

Figure4 shows that interdependence of mutual information and the average probability of collision in the correct symbol as the skin of the detection areas are shown. The blue circles represent the I_{max} concept without any noise or interference. The red dots correspond to the mutual information for 8*8 and 12*12 pixels. Theoretical mutual information is shown in gray bars, modified for the ratio of photons with the number of signals to the darkness between 10 and 100. As shown in the figure, green + markers indicate the average collision probability in the correct area for a finite focal diameter with an FWHM of 8 pixels.

Discussion

For useful communication, incoming message errors must be corrected. An efficient method for error correction is value check (LDPC) [44]. All set symbols must be translated to a bit string to apply this error correction. So we encode our symbols' x and y positions independently, which each take-up half of the bits. Since the predominant noise expression is the interference between neighboring symbols, we use a gray code [45] for each direction. This causes a bit to be misdiagnosed by a neighboring symbol, either in the *x* or *y* direction. Figure 4.4 shows the bit error rate (BER) after error correction with LDPC versus BER of the received bit string. LDPC code was set on halved LDPC used in the digital television broadcast of standard DVD (2B-S). The washed vertical bars indicate the estimated error in the case of 8*8 and 12*12. Estimation takes into account the measured interference between symbols. Their left and right edges show the ratio of photons to the number of signals in darkness, 100 and 10, respectively. The ICCD used in this measurement is equal to 10.07. Other commercial ICCDs have ratios close to 100, which explains the choice of another limit. It is clear that a standard error correction code now allows for error-free practical communication with the current system.

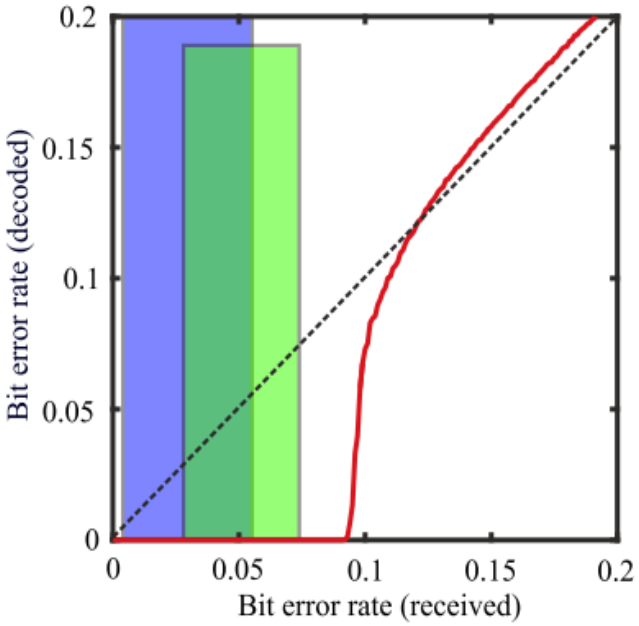

Figure 5: The decoded bit error has a relationship with the received bit error

Figure 5 shows that the bit error rate (BER) of the received bit string versus the BER of the bit string after performing the error correction is shown in the figure. The diagonal dashed line shows the result without error correction. The vertical bars represent the estimated error of our experiment in 8*8 (green) and 12*12 (blue). Their left and right edges show the ratio of photons to the number of signals in darkness, 100 and 10, respectively.

Conclusion

As a result, we show the high-dimensional encoding of single photons of up to 10.5 bits per photon. The capacity of this spatial encryption is limited only by the optics and the number of pixels in the detector. 0.1-bit channel capacity can be increased by reducing system losses. The main contribution of losses in our operation is due to the low quantum efficiency (5%) of ICCD, which can be improved up to 30% with different photocathode materials. This makes it possible to reach a signal ratio of 100 and bring the

measured values closer to their theoretical maximum. Our results are directly applicable to open space line communications. If the wavefront distortion in multimode fibers can be controlled [46, 47], a second and potentially stronger carrier for this high-dimensional encoding can be achieved. A promising way would be to implement a large encrypted spatial alphabet for distributing quantum keys or locking large quantum data [48, 49].

References

[1] Bennett C.H., Brassard G., Breidbart S., Wiesner S. (1983) Quantum Cryptography, or Unforgeable Subway Tokens. In: Chaum D., Rivest R.L., Sherman A.T. (eds) Advances in Cryptology. Springer, Boston, MA. https://doi.org/10.1007/978-1-4757-0602-4_26

[2] Artur K. Ekert," Quantum cryptography based on Bell's theorem", Phys. Rev. Lett. 67, 661 – Published 5 August 1991, DOI:https://doi.org/10.1103/PhysRevLett.67.661

[3] Darius Bunandar, Zheshen Zhang, Jeffrey H. Shapiro, and Dirk R. Englund," Practical high-dimensional quantum key distribution with decoy states", Phys. Rev. A 91, 022336 – Published 27 February 2015 DOI:https://doi.org/10.1103/PhysRevA.91.022336

[4] Ding, Y., Bacco, D., Dalgaard, K. *et al.* High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Inf* 3, 25 (2017). https://doi.org/10.1038/s41534-017-0026-2

[5] C. H. Bennett and G. Brassard, in Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing (IEEE, New York, 1984) pp. 175–179

[6]] W.-Y. Hwang, Phys. Rev. Lett. 91, 057901 (2003).

[7] Quantum Cryptography : On the Security of theBB84 Key-Exchange Protocol, Thomas Baign`eres

[8] Quantum Key Distribution Protocols and Applications, Sheila Cobourne, 8th March 2011

[9] C. E. Shannon, "Communication theory of secrecy systems," Bell Labs Tech. J. 28, 656–715 (1949).

[10] C. E. Shannon, "A mathematical theory of communication," Bell Syst. Tech. J. 27, 379–423 (1984).

[11] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University, 2010)

[12] I. D. Ivanovic, "How to differentiate between non-orthogonal states," Phys. Lett. A 123, 257–259 (1987)

[13] N. Gisin, G. Ribody, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. 74, 145–195 (2002).

[14] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984, (1984), pp. 175–179.

[15] I. Devetak and A. Winter, "Distillation of secret key and entanglement from quantum states," Proc. R. Soc. A 461, 2053, 207–235 (2005)

[16] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," Phys. Rev. Lett. 96, 090501 (2006).

[17] W. Heisenberg, "Über den anschaulichen Inhalt der quantentheoretischen Kinematik und Mechanik," Z. Phys. 43, 172–198 (1927).

[18] D. Korff, "Analysis of a method for obtaining near-diffraction-limited information in the presence of atmospheric turbulence," 2010 Int. Conf. Wirel. Commun. Sens. Comput. 63, 971–980 (1973)

[19] A. A. B. Raj, J. A. V. Selvi, and S. Raghavan, "Terrestrial free space line of sight optical communication (tfslsoc) using adaptive control steering system with laser beam tracking, aligning and positioning (atp)," 2010 Int. Conf. Wirel. Commun. Sens. Comput. 1–5 (2010).

[20] A. M. Oboukhov, "Some specific features of atmospheric tubulence," J. Fluid Mech. 13, 77–81 (1962)

[21] P. P. Rohde, J. F. Fitzsimons, and A. Gilchrist,"Information capacity of a single photon," Phys. Rev. A 88, 022310 (2013

[22] T. Brougham, C. F. Wildfeuer, S. M. Barnett, and D. J. Gauthier, "The information of high-dimensional time-bin encoded photons," Eur. Phys. J. D 70, 214 (2016).

[23] M. A. Nielsen and I. L. Chuang, Quantum computation and quantum information (Cambridge University, 2010

[24] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," in International Conference on Computers, Systems & Signal Processing, Bangalore, India, Dec 9-12, 1984, (1984), pp. 175–179

[25] W. K. Wootters and W. H. Zurek, "A single quantum cannot be cloned," Nature 299, 802–803 (1982).

[26] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," Rev. Mod. Phys. 81, 1301–1350 (2009)

[27] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, "Security of quantum key distribution using d-level systems," Phys. Rev. Lett. 88, 127902 (2002).

[28] H. Bechmann-Pasquinucci and W. Tittel, "Quantum cryptography using larger alphabets," Phys. Rev. A 61, 062308 (2000)

[29] M. Mirhosseini, O. S. Magaña-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gauthier, and R. W. Boyd, "Highdimensional quantum cryptography with twisted light," New J. Phys. 17, 033033 (2015).

[30] S. Gröblacher, T. Jennewein, A. Vaziri, G. Weihs, and A. Zeilinger, "Experimental quantum cryptography with qutrits," New J. Phys. 8, 75 (2
[31] I. Ali-Khan, C. J. Broadbent, and J. C. Howell, "Large-alphabet quantum key distribution using energy-time entangled bipartite states," Phys. Rev. Lett. 98, 060503 (2007)
[32] T. Zhong, H. Zhou, R. D. Horansky, C. Lee, V. B. Verma, A. E. Lita, A. Restelli, J. C. Bienfang, R. P. Mirin, T. Gerrits, "Photon-efficient quantum key distribution using time–energy entanglement with high-dimensional encoding," New J. Phys. 17, 022002 (2015).
[33] S. P. Walborn, D. S. Lemelle, M. P. Almeida, and P. H. S. Ribeiro, "Quantum key distribution with higher-order alphabets using spatially encoded qudits," Phys. Rev. Lett. 96, 090501 (2006).
[34] P. B. Dixon, G. A. Howland, J. Schneeloch, and J. C. Howell, "Quantum mutual information capacity for high-dimensional entangled states," Phys. Rev. Lett. 108, 143603 (2012).
[35] J. Wang, J-Y. Yang, I. M. Fazal, N. Ahmed, Y. Yan, H. Huang, Y. Ren, Y. Yue, S. Dolinar, M. Tur, and A. E. Willner, "Terabit free-space data transmission employing orbital angular momentum multiplexing," Nat. Photon. 6, 488- 496 (2012).
[36] N. Zhao, X. Li, G. Li, and J. M. Kahn, "Capacity limits of spatially multiplexed free-space communication
[37] J. M. Kahn, G. Li, X. Li, and N. Zhao, "To Twist or Not to Twist: Capacity Limits of Free-Space Channels," in "Advanced Photonics 2016 (IPR, NOMA, Sensors, Networks, SPPCom, SOF)" (2016), SpM4E.1
[38] D. J. Gauthier, C. F. Wildfeuer, H. Stipcevi´c, B. Christensen, D. Kumor, ˇ P. Kwiat, K. McCusker, T. Brougham, and S. M. Barnett, "Quantum Key Distribution Using Hyperentangled Time-Bin States," in "Proceedings of The Tenth Rochester Conference on Coherence on Quantum Optics (CQO10)," (2014), pp. 234–239.
[39] T. A. W. Wolterink, R. Uppu, G. Ctistis, W. L. Vos, K.-J. Boller, and P. W. H. Pinkse, "Programmable two-photon quantum interference in 10^3 channels in opaque scattering media," Phys. Rev. A 93, 053817 (2016).
[40] B. Jost, A. Sergienko, A. Abouraddy, B. Saleh, and M. Teich, "Spatial correlations of spontaneously down-converted photon pairs detected with a single-photon-sensitive ccd camera," Opt. Express 3, 81–88 (1998).
[41] R. Chrapkiewicz, W. Wasilewski, and K. Banaszek, "High-fidelity resolved multiphoton counting for quantum imaging applications," Opt. Lett. 39, 5090-5093 (2014).
[42] I. M. Vellekoop and A. P. Mosk, "Focusing coherent light through opaque strongly scattering media," Opt. Lett. 32, 2309–2311 (2007)
[43] D. J. C. MacKay, Information theory, inference and learning algorithms (Cambridge University, 2003).
[44] R. Gallager, "Low-density parity-check codes," IRE Transactions on information theory 8, 21–28 (1962).
[45] F. Gray, "Pulse code communication," (1953). US Patent 2,632,058.
[46] T. Cižmár and K. Dholakia, "Shaping the light transmission through a ˇ multimode optical fibre: complex transformation analysis and applications in biophotonics," Opt. Express 19, 18871–18884 (2011
[47] L. V. Amitonova, A. P. Mosk, and P. W. H. Pinkse, "Rotational memory effect of a multimode fiber," Opt. Express 23, 20569–20575 (2015).
[48] D. J. Lum, J. C. Howell, M. S. Allman, T. Gerrits, V. B. Verma, S. W. Nam, C. Lupo, and S. Lloyd, "Quantum enigma machine: Experimentally demonstrating quantum data locking," Phys. Rev. A 94, 022315 (2016).
[49] D. P. DiVincenzo, M. Horodecki, D. W. Leung, J. A. Smolin, and B. M. Terhal, "Locking classical correlations in quantum states," Phys. Rev. Lett. 92, 067902 (2004).