Symmetric encryption algorithm using “twisted” light

S. A. Burlov[1], A. V. Gorokhov[1]

[1]*Samara National Research University, 34, Moskovskoye shosse, Samara, 443086, Russia*

Abstract

An algorithm for applying a ”twisted” light for constructing an encryption scheme is described. Our approach is founded on famous classical symmetric permutation algorithm based on NP-full task for ”Knapsack Problem” with changes taken into account the quantum origin of the information carrier. As a measuring device for selection of pure states from a mixed one, the Mach-Zehnder interferometer cascade is supposed to use, which allows sorting the parity of the mixed state of the orbital angular momentum (OAM) of photons.

Keywords: quantum cryptography, encryption algorithm, orbital angular momentum of photons, “twisted” light

1. Introduction

The modern bit cryptography is developing rapidly due to the active development of information storage and transmission devices. The search for good algorithms among algebraic structures leads to the known problems of discrete logarithm and factorization, which have a large history of applications in cryptanalysis.

The quantum cryptography was appeared, potentially having unlimited information capacity, huge transmission speed and stability, based on the laws of quantum physics. Among the types of algorithms for quantum cryptography are known only a schemes of key distribution and their using is considered mainly as an auxiliary position. The possibilities of quantum encryption are not yet fully disclosed, but steps to this are done every day. At present widely used the quantum two-dimensional systems based on the particles spin states and polarization states of photons. The main goal of this paper consist in the use for encryption a potentially infinite-dimensional quantum systems based on the states of orbital angular momentum of photons [1].

2. Orbital angular momentum of photon

The light beams with an azimuthal phase that depends on a complex factor $exp(-il\phi)$ carry an orbital angular momentum. The angle ϕ is the azimuthal coordinate in the cross section of the beam, and l can be any integer number. The value of l indicates the amount of twist of the spiral phase front. The value OAM is equal to $L = l \cdot \hbar$ per photon [1].

Many researches of this phenomenon are connected with a certain type of light beam - the Laguerre-Gaussian mode. In works [2, 3] showed the modification scheme of the quantum key distribution (QKD), the transmission of information with superposition of states with non-zero OAM values of photons [4]. Many works are related to the generation of the light beams with OAM [5, 6, 7, 8]. The main difficulty in the practical use of this phenomenon consist in the problem of measurement the OAM value of a photon and in search of the appropriate transmission medium for such beams. Some methods have been developed, which allows to measure OAM value of a photons: the measurement method with generating hologram [9], the sorting method using the Mach-Zehnder interferometers cascade [10, 11, 12], the method of optical geometric transformation [13, 14] and etc.

In this paper we offer to use a method that uses generating holograms and cascade of Mach-Zehnder interferometers. It is proposed to construct a measurement scheme in a such way as to minimize the uncertainty of the receiving beam. The absence of photons at the output of the detector is also an useful unambiguos information for the process.

It is well known that when studying the states of photons with an orbital angular momentum, we get to an infinite-dimensional Hilbert space, which is formed from the set of eigenstates of the operator $\widehat{L_z}$:

$$\widehat{L_z} = i\frac{\partial}{\partial\phi} \tag{1}$$

In principle, states with an arbitrary OAM value may be generated in an experiment. In the paper [15] it is shown the possibility of continuous beam generation with various values of OAM using computer-controlled holograms.

3. Merkley’s scheme

The basis of algorithm of the Merkley’s scheme is a secret super-growing sequence of the natural numbers

$$A = \{a_1, a_2, ..., a_k\}, \quad where \quad a_j \geq \sum_{i=1}^{j-1} a_i, \tag{2}$$

which distributed between the subscribers of the network (Alice, Bob, $\cdots$) and pair of numbers n and w

$$n, w \in N, n > 2 \cdot a_k, \quad GCD(n, w) = 1. \tag{3}$$

Here GCD(n,w) means the greatest common divisor of the numbers n, w, and the number n is greater than the sum of elements of the sequence (2) [16]. Next, the numbers n and w create the new sequence according to the rule:

$$G = \{g_1, g_2, ..., g_k\}, \quad where \quad g_j = a_j \cdot w(mod \quad n). \tag{4}$$

An original message is divided into blocks of bits of length k

$$M = \{m_1,\ m_2,\ ... m_n\}, j \in \overline{1..n} \Rightarrow \{M_i\} = \{m_{i1},\ m_{i2} ... m_{ik}\}, i \in \overline{1..[\frac{n}{k}]}. \tag{5}$$

After it the corresponding sum is calculated

$$c_i = \sum_{j=1}^{k} g_j \cdot m_{ij}. \tag{6}$$

This number is a block of encrypted text that is transmitted to another subscriber of a network. In its turn, the receiver calculates the value f_i from the obtained value c_i given by expression (6).

$$f_i = c_i \cdot w^{-1}(mod \quad n) \tag{7}$$

This number is decomposed on the sequence (2) basis and as result the original message is obtained. These actions are performed for all blocks. The reliability and validity analysis of this scheme can be found, for example, in the article [17].

4. Adapted Merkley's schemes

Let the secret sequence (2) and secret numbers (3) are distributed between subscribers of the network. The permutation sequence T is formed by the sequence (4)

$$T = \sigma(G) = \{g_{j1}, g_{j2}, ..., g_{jk}\}, \quad where \quad g_{j1} < g_{j2} < ... < g_{jk} \tag{8}$$

using the substitution

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & k \\ j1 & j2 & \cdots & jk \end{pmatrix}. \tag{9}$$

The control device for spatial light modulator (SLM) is being configured to generate laser beams with OAM photon projection only for values from the set T. The generation of target beams can be realized, for example, using computer-controlled holograms of diffraction gratings according to Refs [9].

The opentext is converted to a bit string. Each block is processed separately. The i-th iteration is performed as follows:

$$B_i = \sigma(M_i) = \{b_{i1}, b_{i2}, ..., b_{ik}\}. \tag{10}$$

Schematically, the design of the sender and receiver of the encryption process is shown in Fig. 1.

The digital-to-analog converter (DAC) specify SLM to generate the required beam type. Below are two versions of the encrypted text generation that correspond to light rays with OAM of different types. The measurement block is also different for each option, but the result of his work is the same: we get a list of values, which were laid in the ciphertext. This data is transferred to the computer and deciphered by computing of expression (7). The resulting number is decomposed based on the sequence (2).

4.1. Variant I

Here, in order to encrypt the transmitted text, it is suggested to use a mixed state, which corresponds to superposition

$$|\Psi\rangle = \sum_{i=1}^{k} a_i \cdot b_i \cdot \left|OAM = g_{ji}\right\rangle, \tag{11}$$

here factors a_i are given by the sender and factors b_i are calculated in accordance to the bit decomposition (10), and

$$f_i = c_i \cdot w^{-1}(mod \quad n). \tag{12}$$

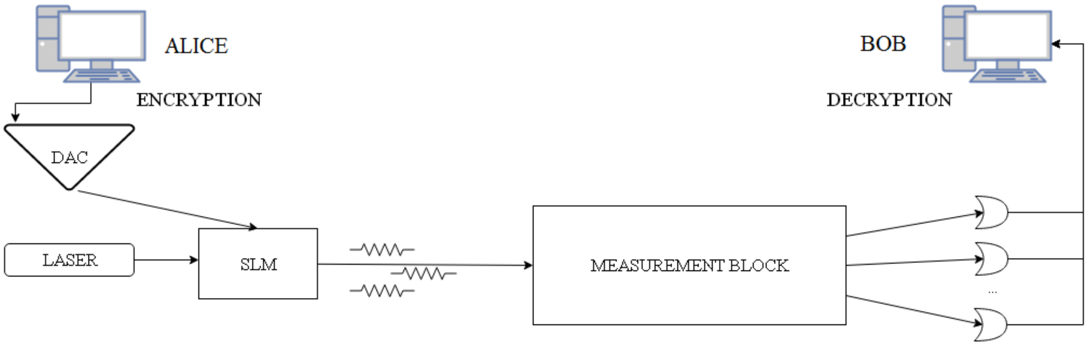

Figure 1: Scheme of the process of formation, transmission and measurement of packages

It is necessary to obtain a mixed state with the density matrix ρ. In general, the density matrix has k^2 elements, but for a mixed state only the diagonal elements can differ from zero, which correspond to the elements of the sequence (4).

$$\rho = \begin{pmatrix} \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & \alpha_1^2 & \cdots & 0 & \cdots & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & 0 & \cdots & \alpha_2^2 & \cdots & 0 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ \cdots & 0 & \cdots & 0 & \cdots & \alpha_k^2 & \cdots \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \end{pmatrix}. \tag{13}$$

The SLM control unit generates a mixed state (11) and transmits it during the iteration period. In this case, the input measurement block should detect which states are participating in the generation of the mixed state. According to [10], the cascade of the Mach-Zehnder interferometers can “do this work”. But there is one important feature: to determine 2^p states, $2^p - 1$ interferometers required.

To optimize the measurement, it is proposed to use a short cascade. Optimization is based on the fact that for sorting out k values (knowing these values), each photon will pass no more than p interferometers. In total, we need a maximum of $k \cdot p$ interferometers. Therefore, when building a cascade, one can block empty paths, thereby greatly reducing the number of constituent elements.

Having received the statistics, one need to select those indicators that satisfy the specified threshold values, find their sum, which corresponds to (6), then calculate the expression (7) and get the source text.

4.2. Variant II

In this variant it is proposed to use a sequence of pure OAM photons states as an encryption text. The SLM control unit, before starting the transmission, gives the beamforming device a control signal for sending the zero Gaussian mode to the receiver. The receiver and the sender should be synchronized during the iteration period - v of the beams sequence transmission. When the sequence B_i' is obtained during the time interval $\tau = \frac{v}{k}$, depending on the value of 0 or 1, the SLM sends a pure state corresponding to g_{ij} or its inversion.

Reception is carried out after receiving the signal state, which can be a zero Gaussian mode, and during a time interval $\frac{v}{k}$ the detector perceives the beam with predetermined OAM value. If it is not detected, 0 is sent. Each iteration needs a time interval equal v. After the successful transfer of one packet the sum of indicators that are assumed to be equals to 1 is calculated.

$$c_j = \sum_{i=1}^{k} b_i' \cdot g_i. \tag{14}$$

Then, the expression (7) should be calculated and the resulting number is decomposed using a basis of the secret sequence (2). As result, the opentext block is obtained. Having received all the blocks and deciphering them, the recipient decrypts the transmitted message.

5. Conclusion

Described encryption scheme is symmetric scheme due to restrictions imposed earlier, so that for effective measurement it is necessary to minimize the uncertainty of the received signal for legal subscribers. This can be done primarily due to the fact that the legal subscriber knows what sequence and what physical signals should be received and the messages themselves are unknown a priori.

The persistence of the presented variant I is determined by the durability of the classical Merkley’s scheme. The reliability of the variant II schema is determined by a stability of the permutational interrelations, which are used to calculate the transmitted sequence: the probability of determining key is equal $\frac{1}{k!}$. Therefore the length of the original sequence should be optimal. Optimum in this case is understood as a weighting between the length of the cipher sequence (2) and the maximum index of the OAM of the beam, which will be detected with a minimum error. Based on the maximum "well" detectable value f of the beam orbital angular momentum, the length of the bit sequence can not exceed the value of $\log_2(f)$, whereas the maximum length is reached for the "bad" superincreasing sequence $\{1, 2, 4, 8, 16, 32, \cdots\}$.

For an eavesdropper, obtaining a stream without accurate detection does not provide any information about the signal being transmitted, because the zeros of the sequence are sent also by a non-zero OAM value. Negative sign of the projection of the orbital angular momentum also needs to be revealed, for this the eavesdropper will be given a very short time interval (therefore it is important that the carrier can not be uniquely stored).

References

[1] L. Allen, M. W. Beijersbergen, R. J. C. Spreeuw, J. P. Woerdman, Allen, L. Orbital angular momentum of light and the transformation of lagerre-gaussian laser modes, Phys. Rev. 45 (1992) 8185–8189.

[2] R. W. Boyd, A. Jha, M. Malik, C. O'Sullivan, B. Rodenburg, D. J. Gauthier, Boyd, R. W. Quantum key distribution in a high-dimensional state space: exploiting the transverse degree of freedom of the photon, Advances in Photonics of Quantum Computing, Memory, and Communication IV. Proc. of SPIE Vol. 7948. (2011) 79480L–1 79480L–6.

[3] M. Mirhosseini, O. S. Magana-Loaiza, M. N. O'Sullivan, B. Rodenburg, M. Malik, M. P. J. Lavery, M. J. Padgett, D. J. Gouthier, B. R. W., Mirhosseini, M. High-dimensional quantum cryptography with twisted light, New J. Phys. 17 (2015) 1–11.

[4] M. Krenn, R. Fickler, M. Fink, J. Handsteiner, M. Malik, T. Scheidl, R. Ursin, Z. A., Krenn, M. Communication with spatially modulated light through turbulent air across vienna, New Journal of Physics. 16 (2014).

[5] E. Abramochkin, V. V., Beam transformations and nontransformed beams, Opt. Commun. 83 (1991) 123–135.

[6] M. Beijersbergen, R. Coerwinkel, M. Kristensen, J. Woerdman, Beijersbergen, M. Helical-wavefront laser beams produced with a spiral phaseplate, Optics Communications. 112(5-6) (1994) 321327.

[7] N. Yoshida, H. Toyoda, Y. Igasaki, N. Mukohzaka, Y. Kobayashi, T. Hara, Yoshida, N. Nonpixellated electrically addressed spatial light modulator (slm) combining an optically addressed slm with a crt, Holographic Optical Elements and Displays. Proc. SPIE 2885 (1996) 132–136.

[8] L. Marrucci, C. Manzo, D. Paparo, Pancharatnam-berry phase optical elements for wave front shaping in the visible domain: switchable helical mode generation, Applied Physics Letters. 88 (2006).

[9] M. Padgett, J. Courtial, L. Allen, Light's orbital angular momentum, Phys. Today. 57 (2004) 35–40.

[10] J. Leach, M. J. Padgett, S. M. Barnett, J. Franke-Arnold, S. Courtial, Leach, J. Measuring the orbital angular momentum of a single photon, Phys. Rev. Lett. 88 (2002) 257901–1–257901–4.

[11] G. C. C. Berkhout, M. P. J. Lavery, J. Courtial, M. W. Beijersbergen, M. J. Padgett, Berkhout, G. C. C. Efficient sorting of orbital angular momentum states of light, Phys. Rev. Lett. 105 (2010) 153601–1–153601–4.

[12] J. Leach, J. Courtial, K. Skeldon, S. M. Barnett, S. Franke-Arnold, M. J. Padgett, Leach, J. Interferometric methods to measure orbital and spin, or the total angular momentum of a single photon, Phys. Rev. Lett. 92 (2004) 013601–1–013601–4.

[13] M. P. J. Lavery, G. C. C. Berkhout, J. Courtial, M. J. Padgett, Lavery, M. P. J. Measurement of the light orbital angular momentum spectrum using an optical geometric transformation, J. Opt. 13 (2011) 1–4.

[14] M. P. J. Lavery, D. Roberston, M. Malik, B. Robenburg, J. Courtial, R. W. Boyd, P. M. J., Lavery, M. P. J. The efficient sorting of light's orbital angular momentum for optical communications, Electro-Optical Remote Sensing, Photonic Technologies, and Applications VI. Proc. SPIE 8542 (2012) 85421R–1–85421R–7.

[15] J. Arlt, K. Dholakia, L. Allen, M. J. Padgett, Arlt, J. The production of multiringed laguerre-gaussian modes by computer-generated holograms, Mod. Opt. 45 (1998) 1231–1237.

[16] B. Schneier, Applied cryptography. Protocols, Algorithms and Source code in C., 2th ed., Triumf, M., 2002.

[17] A. Shamir, A polinomial-time algorithm for breaking the basic merkley-hellman cryptosystem, IEEE Transactions on informations theory. IT-30 (1984).