Soliton modeling of public key algorithm security

Chan Myae Hein and T F Kamalov
Moscow Institute of Physics and Technology (State University), 9 Institutskiy per.,
Dolgoprudny, Moscow Region, 141701, Russian Federation

Abstract. Quantum key distribution protocols and problems of their protection were studied with the soliton model of entangled photons. There were estimated mutual influences between legitimate users and for any types of cracker attack. For example, BB84 protocol is shown to be unconditional security protocols using photon polarization between outlying channels. Secret keys share quantum state between spatially separated (removed or remote) legitimate users. A simple method of generating a dichotomy signal has also been accomplished. In fact, this method can open the way of probabilistic quantum states. We argue that quantum cryptographic systems can be partially simulated on a classical computer with entangled soliton model. The quantum entanglement is a basic tool of communication and processing of the information.

1. Introduction
This study analyzes and demonstrates the ability of a bait state to allow QKD systems to detect PNS attacks. PNS attacks are detected with a high degree of confidence. On the possibility of determining the state of a single photon Eve can be seen as follows. Quantum cryptography is a field in which the laws of quantum physics are directly used to give a significant advantage in information processing [1–5]. But the eavesdropper can use the same laws of quantum physics. In the entanglement scheme, the eavesdropper uses the carrier particle in conjunction with its own quantum system, called the probe, so that the particles and the probe remain entangled, and subsequent measurement of the probe provides the necessary information. The scheme under consideration is based on “indirect copying” using the property of quantum non-locality. According to this scheme, the eavesdropper can obtain information transmitted between legal users without being detected with a sufficiently high probability determined using the uncertainty relation [6]. In the BB84 protocol, there are four non-commuting \( |0\rangle, |\pi/2\rangle, |\pi/4\rangle, |3\pi/4\rangle \) Linearly polarized states \( |0\rangle, |\pi/2\rangle \) and circular polarized states \( |\pi/4\rangle, |3\pi/4\rangle \) are orthogonal respectively. The quantum states \( |\pi\rangle \) and \( |\pi/2\rangle \) are measured by the so-called rectilinear type of measurement. Representing this straightforward measuring type as \( L \), we have:

\[
L|0\rangle = \lambda_1|0\rangle \\
L|\pi/2\rangle = \lambda_2|\pi/2\rangle
\]

Where \( \lambda_i, i=1, 2 \) are eigenvalues. Since the states form the base in Hilbert, an arbitrary quantum state can be expanded by this base, i.e.

\[
|\psi\rangle = C_1|0\rangle + C_2|\pi/2\rangle
\]
From (3),

\[ |\pi/4\rangle = \frac{\sqrt{2}}{2} |0\rangle + \frac{\sqrt{2}}{2} |\pi/2\rangle, \]

(4)

\[ |3\pi/4\rangle = \frac{\sqrt{2}}{2} |0\rangle - \frac{\sqrt{2}}{2} |\pi/2\rangle, \]

(5)

Own auxiliary quantum state has the form

\[ |\alpha\rangle = \frac{3}{2} |0\rangle + \frac{1}{2} |\pi/2\rangle, \]

(6)

The product of the auxiliary quantum state \( |\alpha\rangle \) and basic quantum state gives

\[ \langle \alpha |0\rangle = \frac{3}{2} \rightarrow m_1 = \frac{3}{4} = 0.75, \]

(7)

\[ \langle \alpha |\pi/2\rangle = \frac{1}{2} \rightarrow m_2 = \frac{1}{4} = 0.25, \]

(8)

\[ \langle \alpha |3\pi/4\rangle = \frac{\sqrt{6} - 2}{4} \rightarrow m_4 = \frac{(\sqrt{3} - 1)^2}{8} = 0.07, \]

(9)

Here \( m_J, J = 1, 2, 3, 4 \) corresponds only to the ground quantum state, \( k = 1, 2, 3, 4 \). It follows that the BB84 protocol is sufficiently reliable and the risks of decryption by its Eve are rather low.

2. Soliton simulation of entangled state

The generation of several dichotomous random signals with a controlled cross-correlation coefficient was realized from one continuous random process (Kamalov, 2006).

\[ L = \frac{1}{4} \left( 2\varepsilon_0 E^2 + \varepsilon_1 E^4 - 2 B^2 \right), \]

(10)

Let us define a function

\[ \varphi = \frac{1}{\sqrt{2}} \left( \nu \vec{A} + \frac{i}{\nu} \vec{\pi} \right), \quad \vec{\pi} = -\varepsilon \vec{E}, \]

(11)

where \( \nu \) is a constant,

\[ h = \int dz |\varphi|^2, \]

(12)

\( h \) is the Planck constant. We introduce the function \( \psi_N \)

\[ \psi_N(t, z) = (hN)^{-1/2} \sum_{j=1}^{N} \varphi_j(t, z), \]

(13)

Classically observed \( A_j \) parameter with test index \( j \) is represented as a soliton particle.

\[ \psi_N(t, z) = (hN)^{-1/2} \sum_{j=1}^{N} \varphi_j(t, z), \]

(14)

where \( \pi_j \) is the generalized momentum and \( \phi_j \) is the generalized coordinates.
Here φ_j is expressed through A_j and π_j is expressed through \( \vec{\pi}_j = -\varepsilon \vec{E}_j \). The values can be written as:

\[
E(A) = \frac{1}{N} \sum_{j=1}^{N} A_j = \frac{1}{N} \sum_{j=1}^{N} \int d^3x \varphi_j^* \hat{M}_A \varphi_j = \int d^3x \Psi_N^* \hat{A} \Psi_N,
\]

(15)

Here \( \hat{A} = \hbar \hat{M}_A \) is the Hermitian operator.

Two soliton singlet states provided that the spin and momentum are equal to zero (the index \( L \) describes the left polarization and \( R \) the right polarization):

\[
\varphi^{(12)}(t, z_1, z_2) = \frac{1}{\sqrt{2}} \left[ \varphi_L(t, -z_1) \otimes \varphi_R(t, z_2) - \varphi_R(t, -z_1) \otimes \varphi_L(t, z_2) \right]
\]

(16)

A normalization results in:

\[
\int dz_1 \int dz_2 \varphi^{(12)*} \varphi^{(12)} = \hbar^2
\]

(17)

Two solitons in the singlet entangled states have the form:

\[
\Psi_N(t, z_1, z_2) = (\hbar^2 N)^{-1/2} \sum_{j=1}^{N} \varphi_j^{(12)}
\]

(18)

Here functions \( \varphi_j^{(12)} \) describe entangled solitons, and \( j \) is the test number.

If \( \phi_j \) is a random phase, then the probability of finding the center of the soliton is

\[
\left| \int d^3x \varphi_j^{(k)}(t, \vec{r}) \varphi_j^{(k)*}(t, \vec{r} - \vec{d}_j^{(k)}) \right| \rightarrow \text{max}
\]

(19)

The random phase has the form:

\[
\Phi_j = \sum_{k=1}^{n} \text{arg} \int d^3x \varphi_j^{(k)}(t, \vec{r}) \varphi_j^{(k)*}(t, \vec{r} - \vec{d}_j^{(k)})
\]

(20)

Then we get the dichotomous function

\[
f_s(\theta) = \text{sign} \left[ \cos(\Phi_j + \theta_s) \right], s = 1, K
\]

(21)

For two particles we have

\[
E(f_1 f_2) = 1 - \frac{2}{\pi} |\Delta \theta|
\]

(22)

\[
b(\alpha, t) = \text{sign} \{ \cos(\Phi(t) + \alpha) \}.
\]

(23)

Where, \( \alpha \) is an arbitrary parameter and \( \phi(t) \) is a random variable satisfied by \( \langle \phi(t) \rangle \). We want to emphasize that in Kamalov’s random dichotomous functions defined by equation (1), it was not explicitly mentioned that there are an infinite number of degrees of freedom, although, of course, such functions contain them (Avila, 2011). In fact, it is stated here that “the phases are arbitrarily fixed.” It should be noted that an infinite number of signals in equation (1) is quantized in accordance with the expression:

\[
B_n = \text{sign} \{ \cos(\Psi(t) + \alpha + n\pi/2) \}.
\]

(24)

Then the correlation coefficient for each \( n = 0, \pm 1, \pm 2, \pm 3... \) is equal.

\[
M(\Delta \alpha) = \langle x(\alpha)x(\alpha + \Delta \alpha) \rangle = 1 - \frac{2|\Delta \alpha|}{\pi}
\]

(25)
Note that for a pair of phases \( a_1 = a + (n + 1)\pi/2 \) and \( a_2 = a + n\pi/2 \), the correlation is calculated by the formula (Kamalov, 2006):

\[
M(\Delta \alpha) = 1 - \frac{2|\Delta \alpha|}{\pi} = 0.
\] (26)

In the light of the fact that the operator corresponds to the twice angular momentum operator \([9]\), one should calculate the following expression

\[
P'(a, b) = M \int d^3x_1 \int d^3x_2 \psi_N^+ 2(J_1 a) \otimes 2(J_2 b) \psi_N,
\] (27)

where \( M \) stands for the averaging over the random phases of the solitons. Now it is not difficult to find the expression for the stochastic wave function for the singlet two-solitons state:

\[
P'(a, b) = -\hbar^{-2} (ab) \left( \int_0^\infty dr r^2 (f^2 + g^2) \right)^2 = -(ab)
\] (28)

That is the solitonian model satisfies the EPR–correlation criterium.

3. Conclusion
Soliton simulation of quantum cryptographic process has been shown experimentally that it is possible to improve the quantum key distribution protocols and the questions of their protection were studied with the soliton model of entangled photons. In fact, this method can open the way of probabilistic quantum states. We argue that quantum cryptographic systems can be partially simulated on a classical computer with entangled soliton model.

References
[1] Rybakov Y P and Kamalov T F 2016 Int. J. Theoret. Phys. 55 4075
[2] Chen W K 1993 Linear Networks and Systems (Belmont CA: Wadsworth)
[3] Kamalov T F 2009 Nanotechn. Nanomater. B 324
[4] Rybakov Y P and Kamalov T F 2006 Quantum comput. and comput. 6 125
[5] Kamalov T F 2001 J. of the Russian Laser Research 475
[6] Griffiths R B and Niu C S 1997 Phys. Rev. L. 1173