The attack strategy for a quantum key distribution protocol based on Bell’s theorem

Chan Myae Hein¹ and T F Kamalov¹,²
¹Department of Theoretical Physics, Moscow Institute of Physics and Technology (State University), 9 Institutskiy per., Dolgoprudny, Moscow Region, 141701, Russia
²Moscow Region State University MRSU, Very Voloshinoy str., 24, Mytishi, 141014, Russia

E-mail: chanmyaehein3@gmail.com

Abstract. A new eavesdropping strategy is proposed for the Quantum Key Distribution (QKD) protocol. This scheme represents a new kind of intercept/resend strategy based on Bell’s theorem. Quantum key distribution (QKD) provides the foremost reliable form of secure key exchange, using only the input-output statistics of the devices to realize information-theoretic security. In this paper, we present an improved QKD protocol that can simultaneously distribute the quantum secret key. We are already using the QKD protocol with simulated results matched completely with the theoretical concepts.

1. Introduction
The security of quantum key distribution (QKD) is predicated on a fundamental characteristic of quantum mechanics: measuring a quantum system violates it. Thus, an interceptor attempting to intercept quantum exchange will inevitably leave visible traces. Legitimate exchangers can prefer to either discard the corrupted information or nullify the data available to the eavesdropper by extracting a shorter key. The first (QKD) protocol was proposed in 1984 by Charles H. Bennett and Gilles Brassard [1]. QKD protocols may be classified in keeping with the principle used. These are the Heisenberg uncertainty principle, quantum entanglement, and public and private key cryptography. The aim of quantum key distribution (QKD) and classical key distribution is that the same; the only difference is in how they’re implemented. The quantum key distribution [2] relies on the principle of quantum physics, where both the persons are initially unaware of the keys before sharing, and the secret key’s determined by matching the basis used at both ends, which is completely random in nature. A communication system will be implemented using quantum entanglement or quantum superposition and transmission of information in quantum states that detect eavesdropping. An important goal of this research is the analysis of the types of attacks that eavesdropper can make on quantum key distribution protocol (QKD).

2. The Heisenberg Uncertainty Principle
The recent results in (QKD) are related to the Heisenberg uncertainty principle in quantum mechanics and EPR effects. This principle plays a critical role in preventing the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. For any two observable
properties linked together like A and B, if the corresponding operators \( \hat{A} \), \( \hat{B} \) satisfy

\[
[\hat{A}, \hat{B}] = \hat{A}\hat{B} - \hat{B}\hat{A}
\]

(1)

\[
\langle \Delta A \rangle \langle \Delta B \rangle \geq \frac{1}{2} \| \langle [A, B] \rangle \|
\]

(2)

where \( \langle \Delta A \rangle \) and \( \langle \Delta B \rangle \) are average value of operators \( \Delta \hat{A} \) and \( \Delta \hat{B} \), respectively. Thus, \( \langle \Delta A \rangle \) and \( \langle \Delta B \rangle \) are variances that measure the uncertainty of the observed. For observables A and B such that \( [A, B] \neq 0 \), decreasing the uncertainty \( \langle \Delta A \rangle \) of A forces the uncertainty \( \langle \Delta B \rangle \) of B to increase, and vice versa. Thus, observables A and B cannot be simultaneously measured with arbitrary precision. The Heisenberg Uncertainty Principle can be applied to design a fully secure channel in quantum cryptographic key distribution protocols that transmit random binary sequences (i.e. keys) with automatic interception detection. An example is the uncertainty in the polarization of light, which is widely used in a coding system. This coding system uses 4 non-orthogonal polarization states identified as horizontal, vertical, 45°, and 135°. This system works with the sending side (Alice) sending polarized qubits to the receiving side (Bob) through the quantum channel. However, the 4 non-orthogonal states of polarization cannot be distinguished due to the limitation of the uncertainty principle. Rectilinear and diagonal polarizations are complementary properties in the sense that measuring one property necessarily randomizes another.

3. Quantum Key Distribution (QKD) based on Bell’s theorem

EPR effect plays an important role in quantum information processing. This happens when a spherically symmetric atom emits two photons in opposite directions towards two observers, Alice and Bob. Two photons are produced in an initial state of indefinite polarization. For example, if Alice and Bob both measure rectilinear polarization, they are each equally likely to capture either 0 (horizontal polarization) or 1 (vertical polarization), but if Alice gets 0, Bob will get 1 and vice versa. Of course, the EPR effect may occur on various particles, and not only on photons. Einstein, Podolsky and Rosen (EPR) in their famous 1935 paper [3] challenged the foundations of quantum mechanics by pointing out a ”paradox”.

There are spatially separated pairs of particles, hereinafter referred to as EPR pairs. EPR pairs can be pairs of particles separated over long distances. In 1964 Bell [4, 5] obtained the means to actually test the theories of local hidden variables. He proved that all such theories of local hidden variables must satisfy Bell’s inequality. Bell’s theorem provides a method for testing eavesdropping. Below we provide brief overviews. For convenience, we explain Bell’s theorem using pairs of particles with spin \( \frac{1}{2} \). Consider two measurable quantities A and B and denote the (discrete) possible values of A and B by \( \alpha_i \) and \( \beta_j \), the corresponding unit vectors are \( a_i \) and \( b_j \), respectively.

\[
E(a_i, b_j) = P_{++}(a_i, b_j) + P_{--}(a_i, b_j) - P_{-+}(a_i, b_j) - P_{+-}(a_i, b_j)
\]

(3)

where \( P_{\pm\mp}(a_i, b_j) \), denotes the probability that the result \( \pm 1 \) was obtained along \( a_i \) and \( \pm 1 \) along \( b_j \). The correlation coefficient \( S \) is obtained [6]

\[
S = \sum_{i,j} E(a_i, b_j)
\]

(4)

According to the rules of quantum

\[
E(a_i, b_j) = -a_i \cdot b_j
\]

(5)
Thus, quantum mechanics requires
\[ S = -2\sqrt{2}. \]

The eavesdropper intervention induces
\[ S = \int \rho(n_a, n_b)dn_a dn_b [\sqrt{2}n_a \cdot n_b], \tag{6} \]
where \( n_a \) and \( n_b \) are two unit vectors (for particles \( a \) and \( b \), respectively), \( \rho(n_a, n_b) \) is the probability of intercepting the spin component along a given direction for a specific measurement. In this case,
\[ -\sqrt{2} \leq S \leq 2 \]
When Alice connects Bob and exchanges information, Eva intercepts the quantum bit sequences. For each quantum bit in the sequence that Eva intercepted. By the correlation coefficients, a legitimate user can detect an interceptor (Eva) and Eva cannot escape the detection of Alice and Bob. So Eva’s work will be limited by the Bell’s theorem, her measurement disturbs the quantum state. From this it follows that the QKD is quite reliable and the risks of its decryption by Eva are quite low.

4. New Attack on QKD

With the development of technology, the implementation of a single photon source and quantum memory is just around the corner. Eve can use these new technologies and the new attack to eavesdrop and receive additional information. An important goal of this research is to find upper bounds on the amount of secret key information that may be eavesdropped by Eve.

In the QKD 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 straight forward measuring type as \( L \), we have:
\[ L|0\rangle = \lambda_1|0\rangle, \tag{7} \]
\[ L|\pi/2\rangle = \lambda_2|\pi/2\rangle, \tag{8} \]
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.
\[ |\psi\rangle = C_1|0\rangle + C_2|\pi/2\rangle, \tag{9} \]
\[ |\pi/4\rangle = \frac{\sqrt{2}}{2}|0\rangle + \frac{\sqrt{2}}{2}|\pi/2\rangle, \tag{10} \]
\[ |3\pi/4\rangle = \frac{\sqrt{2}}{2}|0\rangle - \frac{\sqrt{2}}{2}|\pi/2\rangle. \tag{11} \]

Own auxiliary quantum state has the form
\[ |\alpha\rangle = \frac{\sqrt{3}}{2}|0\rangle + \frac{1}{2}|\pi/2\rangle, \tag{12} \]
The product of the auxiliary quantum state and basic quantum state gives
\[ \langle \alpha|0\rangle = \frac{\sqrt{3}}{2} \rightarrow m_1 = \frac{3}{4} = 0.75, \tag{13} \]
\[ \langle \alpha | \pi/2 \rangle = \frac{1}{2} \rightarrow m_2 = \frac{1}{4} = 0.25, \]  
\[ \langle \alpha | \pi/4 \rangle = \frac{\sqrt{6} + \sqrt{2}}{4} \rightarrow m_3 = \frac{\left( \sqrt{3} + \sqrt{1} \right)^2}{8} \approx 0.933, \]  
\[ \langle \alpha | 3\pi/4 \rangle = \frac{\sqrt{6} - \sqrt{2}}{4} \rightarrow m_4 = \frac{\left( \sqrt{3} - \sqrt{1} \right)^2}{8} \approx 0.067, \]  

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

**Conclusions**

Quantum Key Distribution protocol has been showed theoretically that it is possible to improve the Bell’s theorem and QKD protocol is proven to be secure against eavesdropping attacks. The eavesdropper cannot obtain the information between the legitimate users without being detected. We used Bell’s theorem to implement the quantum key distribution protocol. It can prevent impersonation and middle attack. Of course, this can also be realized with non-orthogonal quantum states with the Heisenberg uncertainty principle. In the future, QKD protocol can be performed using the latest technology on Bell’s theorem to improve the accuracy of the results.

**References**

[1] C H Bennett and G Brassard 1984 Quantum cryptography: Public key distribution and coin tossing Proceedings of IEEE International Conference on Computers Systems and Signal Processing, Bangalore India (New York: IEEE,) pp 175-179.
[2] P W Shor and J Preskill 2000 Phys. Rev. L. 85 441.
[3] A Einstein, B Podolsky and N Rosen 1935 Phys. Rev. L. 47(777) 22
[4] J S Bell 1965 Physics (Long Island City, N.Y.) 1, 195.
[5] Yu P Rybakov and T F Kamalov 2016 Journal of Theoretical Physics 55(9) 4075–4080
[6] Yu P Rybakov and T F Kamalov 2007 Foundation of Probability and Physics 889 315-319