Quantum key distribution with floating bases and decoy states

Yu.V. Kurochkin, A.K. Fedorov, and V.L. Kurochkin

Russian Quantum Center, Skolkovo, Moscow 143025, Russia

Abstract

In view of breaking public-key encryption algorithms using quantum algorithms, the only way for privacy in communications is quantum key distribution. Significant efforts are focused on the increase of distance for secure key distribution (QKD). In this work, we study a novel approach to quantum key distribution protocol based on the combination of the floating bases and decoy states. Alice and Bob use a previously shared auxiliary key to generate secret additional rotations of BB84 bases as well as employ decoy states to avoid the photon number splitting (PNS) attack.

QKD provides an efficient method for two legal users — Alice and Bob — to share a private key, which can be used for the one-time pad encryption [1]. Importantly, privacy of a shared 'quantum' key is guaranteed not by limitations of eavesdropper's resources, but fundamental laws of physics.

The seminal QKD protocol, known as BB84, has been proposed by C.H. Bennet and G. Brassard in 1984 [2]. In this protocol, four states of photons in two conjugated bases are used:

$$\hat{\sigma}_y \equiv \{|{\uparrow}\rangle, |{\rightarrow}\rangle\}, \qquad \hat{\sigma}_x \equiv \{|{\nearrow}\rangle, |{\searrow}\rangle\}. \tag{1}$$

Fascinating feature of an unconditional security of communication with QKD has been verified on distances over 300 kilometers [3–5].

Privacy of a shared key in QKD is limited by the quantum bit error rate (QBER) and attacks on the channel. They are caused by imperfections of practical QKD systems. A curious example is using weak coherent states $|\mu \exp(i\theta)\rangle$ with the mean number $\mu = 0.1{-}0.5$ of photons per pulse are used instead of true single photons. According to the Poisson statistics, a non-negligible fraction of pulses contains more than one photon. This fact provides certain constrains for length of communication channels for QKD, which is limited by the photon number splitting (PNS) attack [6–8].

Towards overcome this challenge and improve characteristics of QKD systems several extensions of the BB84 protocol have been proposed. In the SARG protocol [9], Alice should encode each bit into a pair of nonorthogonal states belonging to two or more suitable sets. However, the key generation rate in the SARG protocol decreases.

Another promising approach is the decoy state protocol [10–14], in which Alice randomly sends some of laser pulses with a lower average photon number. These decoy states are used in the protocol to detect a PNS attack, because Eve has no way to verify is a pulse is signal and decoy. Decoy states based QKD protocol has been implemented in recent experimental studies [13,14].

Recently, a new QKD protocol with floating bases has been proposed [15]. In this method, Alice and Bob use a previously shared auxiliary key k_0 to generate secret additional rotations $\Delta\varphi$ of BB84 bases (1). In other words, for ith signal state, Alice uses k_0 and a random function to generate this shift as follows:

$$\Delta\varphi_i = \chi(i, k_0) \mod 2\pi. \tag{2}$$

It is important that function (2) with auxiliary key k_0 generates the uniform distribution over the circle.

Thus, the crucial idea of this protocol is avoiding of the fixed set bases, as it assumed in BB84 or SARG protocols, to floating bases:

$$\begin{aligned} \hat{\sigma}_{y+\Delta\varphi} &\equiv \{|\uparrow +\Delta\varphi\rangle, |\rightarrow +\Delta\varphi\rangle\}, \\ \hat{\sigma}_{x+\Delta\varphi} &\equiv \{|\nearrow +\Delta\varphi\rangle, |\searrow +\Delta\varphi\rangle\} \end{aligned} \tag{3}$$

However, for floating bases QKD protocol problems related with the PNS-attack are still a challenge.

We present a novel QKD protocol with floating bases [15] by combining this approach with the basic version of the decoy states protocol [10]. We suppose that Alice has, first, previously shared with Bob an initial key k_0, which being substituted in Eq. (2) gives the uniform distribution over the circle, and, second, a random sequence k_d for choosing type of transmitted state: (i) vacuum state with the mean number of photons μ_0, (ii) decoy state with the mean number μ_d, and (iii) signal state the mean number μ_s,

The protocol is organized as follows. Alice uses a random sequence k_d to choose the type of of transmitted state. As always, the signal source is used to distribute the key, whereas the decoy source is used to detect the PNS attack.

For ith signal state μ_s, Alice randomly choose the polarization bases (1) and employ function (2) to generate ith pair of floating bases (3). In other cases, *i.e.*, for vacuum μ_0 and decoy μ_d states, Alice generates a random additional shift to BB84 bases

$$\Delta\psi_j = \chi(j, k_i) \mod 2\pi. \tag{4}$$

Bob uses the key k_0 to generate floating bases (3) and randomly chooses them along the lines of the BB84 protocol. In the end, Alice announces chosen bases BB84 and numbers of signal bits. This strategy allows to generate a secret key for the one-time pad encryption.

We provide the security analysis of the suggested protocol and discuss its realization using current experimental tools.

References

[1] For a review, see N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002); V. Scarani, H. Bechmann-Pasquinucci, N.J. Cerf, M. Dušeket, N. Lütkenhaus, and M. Peev, *ibid.* **81**, 1301 (2009).

[2] C.H. Bennet and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Bangalore, India, December 9–12, 1984), p. 175.

[3] B. Korzh, C.C.W. Lim, R. Houlmann, N. Gisin, M.J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).

[4] Y. Kurochkin, V. Kurochkin, G. Goltsman, R. Ozhegov, M. Elezov, V. Kovalyuk, A. Divochiy, Y. Vakhtomin, and K. Smirnov, In press, (2015).

[5] H. Shibata, T. Honjo, and K. Shimizu, Opt. Lett. **39**, 5078 (2014).

[6] G. Brassard, N. Lütkenhaus, T. Mor, and B.C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).

[7] N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).

[8] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comp. **4**, 325 (2004).

[9] V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

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

[11] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[12] X. Ma, B.Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).

[13] Y. Zhao, B. Qi, X.Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).

[14] Z.L. Yuan, A.W. Sharpe, and A.J. Shields, Appl. Phys. Lett. **90**, 011118 (2007).

[15] Y.V. Kurochkin, SPIE Proc. **5833**, 213 (2005).