An experimental comparison of BB84 and SARG04 quantum key distribution protocols

2014 Laser Phys. Lett. 11 095201

(http://iopscience.iop.org/1612-202X/11/9/095201)

IOP Publishing | Astro Ltd
Laser Physics Letters
Laser Phys. Lett. **11** (2014) 095201 (4pp)
doi:10.1088/1612-2011/11/9/095201

An experimental comparison of BB84 and SARG04 quantum key distribution protocols

Youn-Chang Jeong, Yong-Su Kim[1] and Yoon-Ho Kim

Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790–784, Korea

E-mail: w31400@gmail.com and yoonho72@gmail.com

Received 6 June 2014, revised 9 June 2014
Accepted for publication 10 June 2014
Published 27 June 2014

Abstract

SARG04 uses the same quantum states and the same measurement bases with BB84 protocol, but SARG04 can generate secret keys from two-photon pulses when BB84 cannot. We report the implementation of BB84 and SARG04 protocols using a polarization-encoded weak coherent pulse with an optical fiber quantum channel. We have experimentally investigated the secret key rate of BB84 and SARG04 protocols, and BB84 gave a higher secret key rate than SARG04.

Keywords: quantum key distribution, BB84 protocol, SARG04 protocol, quantum cryptography

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum key distribution (QKD) enables Alice (a transmitter) and Bob (a receiver) to share a key while keeping it secret from an eavesdropper (Eve), and thereby offers the promise of unconditional security [1, 2]. Since the first QKD protocol, known as BB84, was proposed in 1984 [3], various QKD protocols have been proposed: such as, B92 [4], E91 [5], differential phase shift [6], coherent one-way [7], and so on.

BB84 [3] is the most widely-used QKD system; it uses two sets of non-orthogonal basis states of a single photon. Unconditional security of the BB84 protocol has been proven by many different techniques [8–11], but one of its key requirements is a single-photon source. However, a highly efficient single-photon source, suitable for quantum cryptography applications, does not currently exist [12].

As an alternative photon source for a QKD system, weak laser pulses with average photon numbers per pulse $\mu < 1$ could be used [13–17] to encode bits, because these pulses are easy to implement in a QKD system. However, weak laser pulses are not ideal single photon states, so they are vulnerable to photon number splitting (PNS) attack [13, 18]. Although weak laser pulses are mostly either empty or consist of only one photon, the probability that they consist of two or more photons is always non-zero: so Eve can implement her PNS attack for multi-photons and extract some of the shared key bits without being detected.

Many efforts have been made to base QKD on weak laser pulses, which would make it robust against PNS attack. The decoy state method [19] and the SARG04 protocol [20] are good examples of these efforts. In the decoy state method, Alice generates several different intensities of photon states that are called decoy states and signal states, and sends them to Bob. Since Eve cannot distinguish whether a photon state is from a signal or a decoy, if she attempts a PNS attack, the yield of signal and decoy states becomes different [19, 21, 22]. Then, Alice and Bob can detect the PNS attack by comparing them. Although this is a good defense against the PNS attack, the effort and cost to implement the decoy state method increase because Alice must send several different intensities of the photon state.

However, the SARG04 protocol [20] defends against the PNS attack, without extra work and cost, in a QKD system based on BB84. In the BB84 protocol, Alice and Bob use two non-orthogonal polarization bases Z ($|V\rangle$, $|H\rangle$) and X ($|45°\rangle$, $|-45°\rangle$). Alice randomly sends one of the four non-orthogonal polarization states ($|V\rangle$, $|H\rangle$, $|45°\rangle$, and $|-45°\rangle$). After quantum communication is finished, Alice and Bob each reveal their basis. However, the SARG04 protocol uses four sets: $s_1 = (|V\rangle, |45°\rangle)$, $s_2 = (|V\rangle, |-45\rangle)$, $s_3 = (|H\rangle, |45°\rangle)$,

[1] Present address: Center for Nano & Quantum Information, Korea Institute of Science, Technology (KIST), Seoul, 136–791, Korea

and $s_4 = (|H\rangle, |-45°\rangle)$. Alice randomly sends one of the two non-orthogonal polarization states in the randomly selected set; Bob uses either the Z basis or the X basis to measure the photon. After quantum communication is finished, Alice and Bob exchange the information of Alice's selected set and Bob's measuring basis. Thus, quantum communication in SARG04 is identical to the BB84 protocol; only the classical key sifting procedure is modified. At that time, SARG04 is secure for two-photon pulses. For example, if Alice sends $|V\rangle$ with two-photon pulses and reveals $s_1 = (|V\rangle, |45°\rangle)$, then Eve gets $|V\rangle$ by the Z basis and measures $|45°\rangle$ or $|-45°\rangle$ with 50% probability by the X basis. Eve cannot discriminate the state from her measurement in two-photon pulses. As a result, SARG04 generates a secret key from one-photon and two-photon pulses, whereas BB84 generates a secret key from one-photon pulses [23].

In this letter, we report an experimental comparison of BB84 and SARG04 in the same QKD system. We implemented both protocols for several average photon numbers and quantum channel distances, and experimentally compared the secret key rates of BB84 and SARG04 protocols in the same QKD system.

2. Theory

Theoretically, the lower bounds of the secret key rates of BB84 $\left(r^{\mathrm{L}}_{\mathrm{BB84}}\right)$ and SARG04 $\left(r^{\mathrm{L}}_{\mathrm{SARG04}}\right)$ at a given μ can be estimated from the quantum bit error rate (QBER, Q_μ) and the sifting rate (R_μ), the latter being defined as the ratio of sifted bits to the total number of Alice's raw bits.

The BB84 protocol is secure in the single-photon state and the lower bound of the secret key rate of BB84 is given as [24]

$$r_{\mathrm{BB84}} \geqslant r^{\mathrm{L}}_{\mathrm{BB84}} = R_1^{\min}[1 - H(Q_1^{\max})] - R_\mu H(Q_\mu), \quad (1)$$

where H denotes the Shannon entropy, R_1 is the sifting rate of single-photon states, and Q_1 is the QBER of single-photon states. R_1 and Q_1 of BB84 are constrained as

$$\begin{aligned} R_1 &\leqslant \tfrac{1}{2} p_1, \\ R_1 &\geqslant R_\mu - \tfrac{1}{2}\sum_{n \geqslant 2} p_n, \\ R_1 Q_1 &\leqslant R_\mu Q_\mu, \end{aligned} \quad (2)$$

where $p_n = \dfrac{e^\mu \mu^n}{n!}$ is the probability that a pulse consists of n photons. The minimum of the sifting rate of the single photon state is $R_1^{\min} = R_\mu - \frac{1}{2}\sum_{n\geqslant 2} p_n$. If $R_1^{\min} \leqslant 0$, then $r_{\mathrm{BB84}} \leqslant 0$, so Alice and Bob must abort the whole sifted key.

The SARG04 protocol can generate the secret key even when a pulse contains two photons, because Eve cannot get full information of Alice's key from the two-photon pulse [23]. From this fact, the lower bound of the secret key rate of SARG04 is [24]

$$\begin{aligned} r_{\mathrm{SARG}} \geqslant r^{\mathrm{L}}_{\mathrm{SARG}} = \inf_{\{R_1, Q_1, R_2, Q_2\}} & R_1 S_1^{\mathrm{SARG}}(Q_1) \\ & + R_2 S_2^{\mathrm{SARG}}(Q_2) - R_\mu H(Q_\mu), \end{aligned} \quad (3)$$

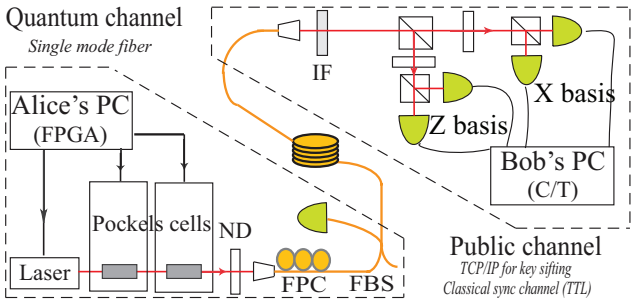

Figure 1. QKD experimental setup. Alice: attenuated laser pulses are polarization-encoded using two Pockels cells. A fiber non-polarizing beam splitter (FBS) is used to check the average photon number per pulse μ. Alice's laser and two Pockels cells are controlled by a field-programmable gate array card (FPGA) and three delay generators (not shown). Bob: a beam splitter (BS) is used to randomly direct the incoming photon to either X or Z measurement basis. Bob's detection events are recorded using a PC-based counter/timer (C/T).

where $S_1^{\mathrm{SARG}}(Q_1)$ and $S_2^{\mathrm{SARG}}(Q_2)$ are Eve's uncertainty on the one-photon and two-photon pulses respectively [24, 25], R_2 is the sifting rate of two-photon states, and Q_2 is the QBER of two-photon states. To be compatible with R_μ and Q_μ, R_1, R_2, Q_1 and Q_2 are constrained as [24]

$$\begin{aligned} & R_1(1-Q_1) \leqslant \tfrac{1}{4} p_1, \\ & R_2(1-Q_2) \leqslant \tfrac{1}{4} p_2, \\ & R_1(1-Q_1) + R_2(1-Q_2) \geqslant R_\mu(1-Q_\mu) - \tfrac{1}{4}\sum_{n\geqslant 3} p_n, \\ & R_1 Q_1 + R_2 Q_2 \leqslant R_\mu Q_\mu. \end{aligned} \quad (4)$$

We can obtain $R_1^{\min}$ and $Q_1^{\max}$ of BB84 using equation (2) from the sifting rate and the QBER of BB84. Hence, we can estimate $r^{\mathrm{L}}_{\mathrm{BB84}}$ from the average photon number, the sifting rate and QBER of BB84. We can also estimate $r^{\mathrm{L}}_{\mathrm{SARG}}$ using equations (3) and (4) from the experimental results.

Theoretically, the sifting rate and QBER are calculated from the average photon number and the QKD system parameters: such as, the dark-count rate, the transmittance of a quantum channel, and Bob's detection probability. Hence, we can also use equations (1)–(4) to calculate the theoretical secret key rate of BB84 and SARG04 in the QKD system [24].

3. Experiments

To implement BB84 and SARG04 protocols, we built a fiber-based QKD system (figure 1). It consists of a transmitter (Alice), a receiver (Bob), a quantum channel that is a single mode fiber spool (attenuation coefficient is $\alpha = 3$ dB km^{-1}) at 780 nm wavelength, and the public channel coaxial cables and the TCP/IP.

Alice's setup consists of a 780 nm pulsed diode laser (Coherent, CUBE 785-40C) that generates a train of 3 ns laser pulses at 1 MHz repetition rate, a variable attenuator, two high-speed Pockels cells (Leysop, RTP-3-20) for polarization encoding, and a personal computer with a PCI field-programmable

gate array card (FPGA; National Instruments PCI-7813) and three delay generators. Polarization-encoded laser pulses are strongly attenuated by using neutral density filters (ND), so that $\mu < 1$; the pulses are coupled into a fiber non-polarizing beam splitter (FBS), which splits the beam into two to allow checking of μ, and to allow launching to the quantum channel that is connected to Bob's setup. The polarization-encoded laser pulses are transmitted to Bob through a single-mode fiber. Note that the polarization transmission, via an optical fiber, requires efforts to keep the polarization stable; this can be done with a fiber polarization controller (FPC). In practical QKD systems, it can be achieved by active compensation techniques [26].

Bob's setup consists of a 3 nm interference filter (IF), a 50/50 beam splitter for randomly selecting either Z basis ($|V\rangle$, $|H\rangle$) or X basis ($|45°\rangle$, $|-45°\rangle$), four single-photon detectors, and a personal computer with two counter/timer (National Instruments PCI-6602). The single-photon detector has a detection efficiency (η_{det}) of ~ 0.6 at 780 nm wavelength and dark-count probability $(3.3\pm0.6)\times10^{-5}$. The efficiency of optical components is $\eta_{\mathrm{opt}} = 0.72$, so overall Bob's detection efficiency is $\eta_{\mathrm{Bob}} = \eta_{\mathrm{opt}}\,\eta_{\mathrm{det}} \approx 0.40$.

BB84 and SARG04 use different methods to allow Alice and Bob to generate shared sifted keys. In the BB84 protocol they announce their basis information to each other. In SARG04, Alice sends her basis set information to Bob via TCP/IP; he uses this information to sift his raw keys to establish a set of shared sifted key bits. Bob informs Alice whether he got a conclusive result for each signal and Alice uses this information to sift her raw keys. After generating the sifted key, we estimate the secret key rate from the sifting rate and the QBER of Alice and Bob.

4. Results and discussion

BB84 and SARG04 protocols were implemented in the same QKD system, and their secret key rate, sifted key rate (figure 2) were compared when signals with a range of average photon numbers through 1.27 km of single-mode fiber. The measured protocol efficiency (ration of sifted bits to the number of raw bits received) was 0.50 ± 0.01 for BB84 and 0.25 ± 0.01 for SARG04; these agree closely with the theoretical efficiencies of 0.5 for BB84 and 0.25 for SARG04. For that reason, the sifted key rate of BB84 was always about double that of SARG04 when they had the same number of raw bits. The sifted key rates of both protocols increased as the average photon number increased, but the QBER (BB84 $\sim$ 3% ; SARG04 $\sim$ 5%) did not change much when the dark-count contributions were subtracted (not shown in figure 2). As is well known theoretically and experimentally, the QBER of BB84 ($Q_{\mathrm{BB84}} = (1-V)/2$) is about half that of SARG04 ($Q_{\mathrm{SARG04}} = (1-V)/(2-V) \approx 1-V$) at the same visibility ($V = 0.954$) of the quantum channel [17, 27].

We estimated the lower bound of the secret key rate from the sifted key rate and the QBER of BB84 and SARG04 (figure 2). The sifted key rate increased consistently as the average photon number increased, but the secret key rate was

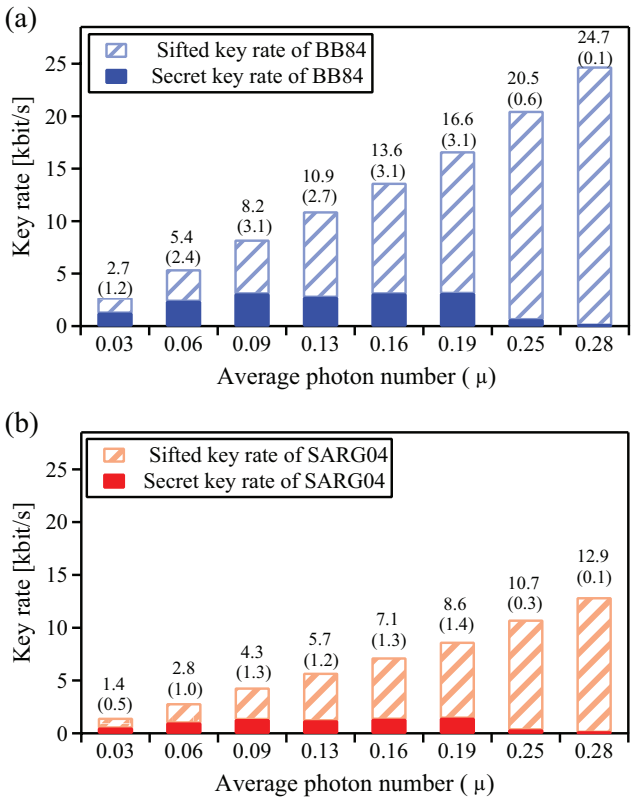

Figure 2. Key rates for (*a*) BB84 and (*b*) SARG04 versus μ in 1.27 km single-mode fiber. The key rate 2.7 (1.2) represents the secret key rate of 1.2 kbit s^{-1} generated from the sifted key rate of 2.7 kbit s^{-1}.

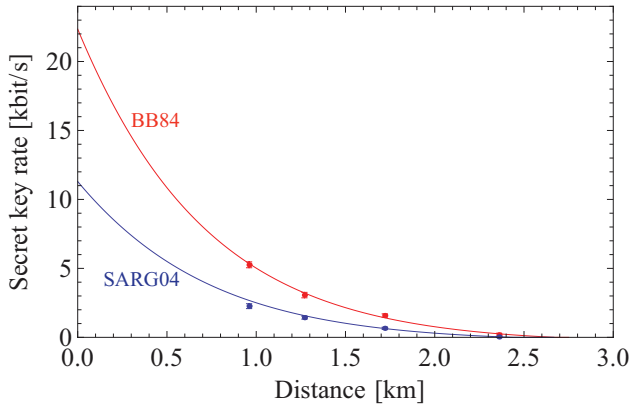

Figure 3. Experimental (points) and theoretical (lines) secret key rates for BB84 (red) and SARG04 (blue) versus distance at channel visibility $\sim$ 0.953.

highest at $\mu \approx 0.19$ on both BB84 and SARG04. The secret key rate of SARG04 was less than half that of BB84, and both had zero secret key when the average photon number was higher than $\mu \approx 0.3$ in the 1.27 km ($\alpha = 3$ dB km^{-1}) single-mode fiber.

To investigate the secret key rate of BB84 and SARG04 according to distance, we implemented the BB84 and SARG04 protocols on a quantum channel for several fiber lengths (figure 3). The measured optimal average photon number decreased as the distance of quantum channel increased. Theoretically, when $\alpha = 3$ dB km^{-1}, BB84 and SARG04 can generate the secret keys on our QKD system until 2.77 km and

2.44 km respectively. Although SARG04 is secure until the number of photons per pulse reaches two, and can generate more secret keys than BB84 under perfect quantum channel visibility and in particular situations [24], we experimentally showed that BB84 generates more secret keys than SARG04. In the real world devices are imperfect, and the quantum channel visibility at which SARG04 is more sensitive than BB84 is less than one. Therefore, even if the probabiiity that SARG04 can generate more secret keys than BB84 is less than one [24], BB84 is still more practical than SARG04 in the real world.

5. Conclusion

The BB84 and SARG04 QKD protocols were tested through single-mode fibers of different lengths. The setup was based on polarization encoding of an attenuated laser pulse. We checked the sifted key and the secret key rate according to average photon numbers per pulse in a fixed quantum channel distance. We found that BB84 is more suitable than SARG04 in the real world.

Acknowledgments

This work was supported in part by the National Research Foundation of Korea (Grant No. 2013R1A2A1A01006029 and 2011-0021452). Y-CJ acknowledges support from BK21 plus project.

References

[1] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145
[2] Scarani V, Bechmann-Pasquinucci H, Cerf N J, Dusek M, Lutkenhaus N and Peev M 2009 *Rev. Mod. Phys.* **81** 1301
[3] Bennett C H and Brassard G 1984 *Proc. of the IEEE Int. Conf. on the Computers, Systems, and Signal Processing (Bangalore, Dec. 1984)* (New York: IEEE) p 175
[4] Bennett C H 1992 *Phys. Rev. Lett.* **68** 3121
[5] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661
[6] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902
[7] Stucki D, Brunner N, Gisin N, Scarani V and Zbinden H 2005 *Appl. Phys. Lett.* **87** 194108
[8] Mayers D 2001 *J. ACM* **48** 351
[9] Lo H K and Chau H F 1999 *Science* **283** 2050
[10] Shor P W and Preskill J 2000 *Phys. Rev. Lett.* **85** 441
[11] Kraus B, Gisin N and Renner R 2005 *Phys. Rev. Lett.* **95** 080501
[12] Lounisand B and Orrit M 2005 *Rep. Prog. Phys.* **68** 1129
[13] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863
[14] Duligall J L, Godfrey M S, Harrison K A, Munro W J and Rarity J G 2006 *New J. Phys.* **8** 249
[15] Yuan Z L, Dizon A R, Dynes J F, Sharpe A W and Shields A J 2008 *Appl. Phys. Lett.* **92** 201104
[16] Kim Y S, Jeong Y C and Kim Y H 2008 *Laser Phys.* **18** 810
[17] Jeong Y C, Kim Y S and Kim Y H 2011 *Laser Phys.* **21** 1438
[18] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 *Phys. Rev. Lett.* **85** 1330
[19] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901
[20] Scarani V, Acin A, Ribordy G and Gisin N 2001 *Phys. Rev. Lett.* **92** 057901
[21] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503
[22] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504
[23] Tamaki K and Lo H K 2006 *Phys. Rev.* A **73** 010302
[24] Kraus B, Branciard C and Renner R 2007 *Phys. Rev.* A **75** 012316
[25] Fung C H F, Tamaki K and Lo H K 2006 *Phys. Rev.* A **73** 012337
[26] Liu Y *et al* 2010 *Opt. Express* **18** 8587
[27] Branciard C, Gisin N, Kraus B and Scarani V 2005 *Phys. Rev.* A **72** 032301