ISSN 1054-660X, Laser Physics, 2011, Vol. 21, No. 8, pp. 1438–1442.

Effects of Depolarizing Quantum Channels on BB84 and SARG04 Quantum Cryptography Protocols[1]

Y.-C. Jeong, Y.-S. Kim, and Y.-H. Kim*

Department of Physics, Pohang University of Science and Technology (POSTECH), Pohang, 790-784, Korea
*e-mail: yoonho72@gmail.com

Received December 9, 2010; in final form February 24, 2011; published online July 4, 2011

Abstract—We report experimental studies on the effect of the depolarizing quantum channel on weak-pulse BB84 and SARG04 quantum cryptography. The experimental results show that, in real world conditions in which channel depolarization cannot be ignored, BB84 should perform better than SARG04 under the most general eavesdropping attack.

DOI: 10.1134/S1054660X11150126

1. INTRODUCTION

In quantum cryptography or quantum key distribution (QKD), the goal is to establish shared secret keys between two communicating parties, Alice and Bob [1–3]. One of the key components of the original BB84 quantum cryptography protocol [4] is the single-photon source, but the lack of efficient single-photon sources resulted experimental implementations with weak pulses of light [5, 6]. The weak pulse implementations are practical but is susceptible to the photon number splitting (PNS) attack [5, 7]. It, nevertheless, has been shown that secret keys can be extracted from the weak pulse implementations of the BB84 protocol if certain conditions are met [8, 9].

There also exist quantum cryptography protocols which are inherently more secure against the PNS attack when implemented with weak pulses. One is the decoy state method [10] and the other is the SARG04 protocol [11]. The decoy state method, while very robust against the PNS attack, requires additional physical resources which could introduce further vulnerabilities to the system [12–14]. The SARG04 protocol, on the other hand, offers more robustness against the PNS attack than the BB84 protocol implemented with weak pulses, while using the same hardware as that of the BB84 protocol [15, 16].

One important problem in practical quantum cryptography is the systems' behaviors under the presence of disturbances or quantum noise (e.g., the depolarization effect, the phase error, damping, etc.) in the quantum channel connecting Alice and Bob. The depolarization effect in a quantum channel, specifically, is an important type of quantum noise [17] and has been studied in a variety of contexts in quantum communication [18–20]. In free-space quantum cryptography, the depolarization effect in the quantum channel might come from changing weather conditions and, in fiber-based quantum cryptography, it can be caused by uncontrolled polarization and phase changes in a long optical fiber. Also, any imperfections of the optical components can give rise to the effective depolarization effect. Since all types of errors in the quantum channel should be assumed to be caused by an eavesdropper, it is important to consider how the depolarization effect affects the performance of a quantum cryptography system.

In particular, it is of importance to compare the performances for the BB84 and SARG04 quantum cryptography systems as they differ only in the classical key sifting procedures [21–23]. In this paper, we investigate experimentally how the depolarization effect in the quantum channel affects the secret key generation performances for the weak-pulse BB84 and SARG04 quantum cryptography systems.

2. THEORY

In the BB84 and the SARG04 quantum cryptography protocols, the qubit $|\Psi\rangle$ is often encoded in the polarization state of a single-photon pulse or a weak pulse of light and is sent to Bob via a free-space [13, 24–26] or a fiber quantum channel [14, 27–29]. The effect of depolarization in the quantum channel on the qubit $|\Psi\rangle$ can be described as $\varepsilon[|\Psi\rangle]$ and is given by [21]

$$\varepsilon[|\Psi\rangle] = F|\Psi\rangle\langle\Psi| + D|\Psi^{\perp}\rangle\langle\Psi^{\perp}|, \quad (1)$$

where $|\Psi^{\perp}\rangle$ is the state orthogonal to $|\Psi\rangle$, F is the fidelity of the quantum channel, and D quantifies the disturbance in the quantum channel. The values F and D depend on the quantum channel visibility V as $F = (1 + V)/2$ and $D = (1 - V)/2$, respectively [21]. Note that $F + D = 1$.

Let us first consider how the channel depolarization will affect the quantum bit error rate (QBER, Q), which is the ratio of the number of error bits in the sifted key to the total number of sifted keys, in the case of single-photon pulse. In the BB84 protocol, a sifted

[1] The article is published in the original.

key bit is generated when Alice and Bob happen to choose the same basis and, thus, the error bit in the sifted key is dependent on the disturbance D in the quantum channel. Since the probabilities for generating the error bit and the correct bit in the BB84 protocol are given as $p_e = D$ and $p_c = F$, respectively, QBER can be written as [21]

$$Q^{\mathrm{BB84}} = \frac{p_e}{p_c + p_e} = \frac{D}{F + D} = \frac{1 - V}{2}.$$

In the SARG04 protocol, the situation is a bit different. Consider, for example, Alice sends $|V\rangle$ and announces publicly $S_0 \equiv \{|V\rangle, |45°\rangle\}$. On Bob's side, out of four possible outcomes, only the $|-45°\rangle$ outcome is a conclusive one [11]. When depolarization in the quantum channel is considered,

$$\begin{aligned}\varepsilon[|V\rangle] &= F|V\rangle\langle V| + D|H\rangle\langle H| \\ &= \frac{1}{2}|+45°\rangle\langle +45°| + \frac{1}{2}|-45°\rangle\langle -45°| \\ &+ \frac{F-D}{2}|45°\rangle\langle -45°| + \frac{F-D}{2}|-45°\rangle\langle 45°|.\end{aligned}$$

Thus, the probability of the correct bit is $p_c = 1/2$ and is independent of the channel visibility V. The error bit probability, however, depends on the disturbance factor D in the quantum channel, $p_e = D$. QBER is thus given as [21]

$$Q^{\mathrm{SARG04}} = \frac{D}{\frac{1}{2} + D} = \frac{1 - V}{2 - V}.$$

In the weak-pulse implementations of BB84 and SARG04 QKD, QBER depends additionally on the dark count probability p_d, the average photon number per pulse μ, the length l and the attenuation coefficient α (dB/km) of the quantum channel, and Bob's detection efficiency η_d [21]. In the limit of $p_d \ll 1$ and $\mu\eta \ll 1$, QBER for the BB84 protocol is given as

$$Q_\mu^{\mathrm{BB84}} \approx \frac{\frac{1}{2}D\mu\eta + \frac{p_d}{2}}{\frac{1}{2}D\mu\eta + \frac{p_d}{2} + \frac{1}{2}F\mu\eta + \frac{p_d}{2}},$$

and, for the SARG04 protocol, it can be written as

$$Q_\mu^{\mathrm{SARG04}} \approx \frac{\frac{1}{2}D\mu\eta + \frac{p_d}{2}}{\frac{1}{4}\mu\eta + \frac{p_d}{2} + \frac{1}{2}D\mu\eta + \frac{p_d}{2}},$$

where $\eta = \eta_d t$ with the transmission factor $t = 10^{-\alpha l/10}$. Usually in experiment, $p_d \ll D\mu\eta$ and under this condition, QBER in the weak-pulse implementations of BB84 and SARG04 approach those of the single-photon case

$$Q_\mu^{\mathrm{BB84}} \approx \frac{D}{F + D}, \tag{2}$$

$$Q_\mu^{\mathrm{SARG04}} \approx \frac{D}{\frac{1}{2} + D}. \tag{3}$$

The total sifting rate R_μ, which is the sifted key rate per bit, for the weak-pulse BB84 and the SARG04 protocols are given as [23]

$$R_\mu^{\mathrm{BB84}} = \frac{1}{2}[1 - \bar{p}_d^2 \exp(-\mu\eta)], \tag{4}$$

$$\begin{aligned}R_\mu^{\mathrm{SARG04}} = \frac{1}{2}\Bigg[1 + \frac{\bar{p}_d}{2}\exp(-\mu F\eta) \\ - \frac{\bar{p}_d}{2}\exp(-\mu D\eta) - \bar{p}_d^2\exp(-\mu\eta)\Bigg],\end{aligned} \tag{5}$$

where $\bar{p}_d = 1 - p_d$.

Note that $R_\mu = \sum_n R_n = \sum_n Y_n \exp(-\mu)\mu^n/n!$, where Y_n is the probability for Bob to have a conclusive result for the n-photon pulse sent from Alice. It is interesting to point out that the sifting rate for BB84, Eq. (4), is independent of the channel visibility V while that of SARG04, Eq. (5), varies with V. For BB84, sifted keys are generated whenever Alice and Bob happen to choose the same basis. Since the bases choices are random and are independent of the channel visibility, the sifted key rate of BB84 is independent of the channel visibility V or depolarization $D = (1 - V)/2$. For SARG04, however, the situation is different as all detections at Bob that are interpreted as conclusive form the sifted key and the probability of a conclusive outcome at Bob depends on the channel visibility V.

The secret key rates (the lower bound) in the presence of depolarization in the quantum channel can then be determined with the total sifting rates R_μ and the average QBER $Q_\mu \equiv \sum_n Q_n R_n / R_\mu$ (Q_n denotes the QBER for the n-photon pulse) using experimental obtained parameters [23].

3. EXPERIMENTAL SETUP

To experimentally test the effects of depolarization in the quantum channel on the performance of weak-pulse BB84 and SARG04 quantum cryptography protocols, we have built a fiber-based quantum cryptography system schematically shown in Fig. 1. Alice's setup consists of a diode laser which emits a train of 3 ns long 780 nm laser pulses at 1 MHz repetition rate, two RTP Pockels cells for polarization encoding, and FPGA-based electronics for controlling and storing the data. Polarization-encoded laser pulses are then

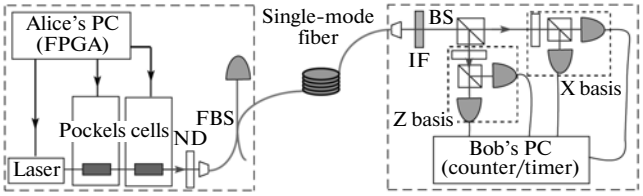

Fig. 1. Schematic of experimental setup. *Z*-basis detects $|H\rangle$ and $|V\rangle$ polarized photons and *X*-basis detects photons polarized at $|45°\rangle$ and $|-45°\rangle$ polarizations. See text for details.

attenuated with a neutral density (ND) filter set and coupled into a fiber beamsplitter (FBS). A silicon single-photon detector connected to one end of FBS is used to measure the average photon number per pulse so that $\mu < 1$ and the other end of FBS is connected to the quantum channel, a 1.27 km long single-mode fiber spool. The attenuation coefficient of the fiber at 780 nm is $\alpha = 3$ dB/km and the initial channel visibility of the fiber quantum channel is measured to be $V_i = 0.954 \pm 0.002$. Bob's setup consists of a 3 nm bandpass filter (IF), a 50/50 beam splitter for random selecting between *Z*-basis ($|H\rangle$ and $|V\rangle$) and *X*-basis ($|45°\rangle$ and $|-45°\rangle$), four silicon single-photon detectors and a PC with a counter/timer PCI card for data collection and storage. Bob's detection efficiency (including optics and the detector) and the dark count probability are measured to be $\eta_d = 0.4$ and $p_d = (3.3 \pm 0.6) \times 10^{-5}$, respectively. Alice and Bob's setups are synchronized with the 1 MHz clock signal over a BNC cable and the key sifting is done over the internet.

Since depolarization in the quantum channel is related to the channel visibility as $D = (1 - V)/2$, it is necessary to vary the channel visibility V to observe the effect of depolarizing quantum channels oh BB84 and SARG04 protocols. Rather than actually introducing additional fiber-based polarization controllers to the setup to decrease the channel visibility from the initial value $V_i = 0.954$, we use the effective method described as follows. Note that the effect of quantum channel depolarization is to flip the qubit $|\Psi\rangle$ to the orthogonal one $|\Psi^{\perp}\rangle$ with the probability D. Thus, to effectively implement channel depolarization, we simply flip the stored bit information at Alice with probability D determined by the desired channel visibility value. For example, to achieve the effect of channel visibility $V = 0.9$, D must be 0.05 so that 5% of Alice's stored bits are randomly selected and flipped. Note that, in this case, since the initial channel visibility is 0.954, we are in fact achieving the channel visibility $0.9 \times V_i = 0.859$.

4. RESULTS AND DISCUSSION

Figure 2 shows QBER as a function of channel visibility for the BB84 and the SARG04 protocols in the case of average photon number per pulse $\mu = 0.189$.

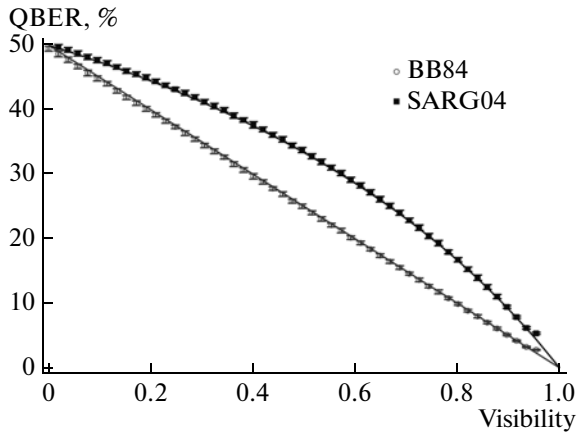

Fig. 2. QBER vs. channel visibility. Experiments are done for $\mu = 0.189 \pm 0.001$. The solid lines are due to Eqs. (2) and (3). The critical visibility values are 0.89 for BB84 and 0.90 for SARG04.

The experimental results shown in Fig. 2 agree well with Eqs. (2) and (3). Note that, for BB84 and SARG04 protocols, there exist critical QBER values below which no secret key can be generated. Since QBER is related to the quantum channel visibility, the BB84 and SARG04 protocols have critical channel visibility values below which no secret keys can be generated. For the experimental conditions reported in Fig. 2 ($\mu = 0.189$), the critical visibility values are 0.89 and 0.90 for BB84 and SARG04 protocols, respectively.

Although no secret keys can be generated if the channel visibility is below the critical visibility values at a given μ value, investigating the QBER and the sifted key rate behaviors as functions of the channel visibility is useful for experimentally studying their general relations to the channel visibility. We have also repeated the QBER vs. channel visibility measurement for various values of the average photon number per pulse, $\mu \approx 0.033$–0.283, and they show similar results as in Fig. 2. The SARG04 protocol, therefore, is shown to be more sensitive than the BB84 protocol for the depolarization effect in the quantum channel.

How the sifted key rates are affected by the depolarizing effect in the quantum channel for BB84 and SARG04 protocols are shown in Fig. 3. The experimental results shown in Fig. 3 reveal that the sifted key rate for the BB84 is independent on the channel visibility, but the SARG04 protocol exhibits channel visibility dependent sifted key rates. It is also worth while to mention that, as evident from Fig. 3, the BB84 protocol always generates more sifted keys than the SARG04 protocol. Note that Fig. 3 shows small discrepancies between the experimental results and the theoretical results due to Eqs. (4) and (5). These discrepancies suggest that there are slight systematic errors in estimating the average photon number per

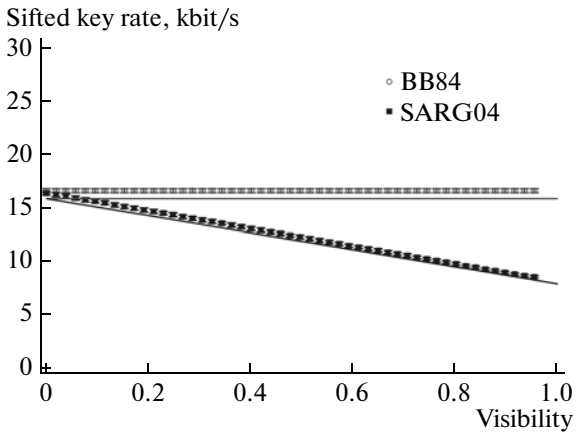

Fig. 3. Sifted key generating rate vs. quantum channel visibility. Experiments are done for $\mu = 0.189 \pm 0.001$. The solid lines are from the theoretical results of Eqs. (4) and (5). As in Fig. 2, the critical visibility values are 0.89 for BB84 and 0.90 for SARG04.

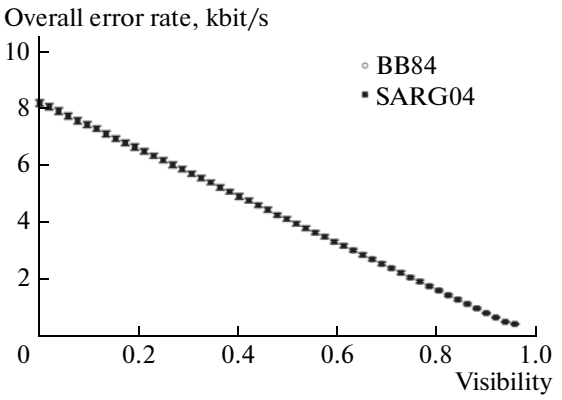

Fig. 4. Overall error rate vs. channel visibility. Experiments are done for $\mu = 0.189 \pm 0.001$. Note that the overall rate rates for the BB84 and SARG04 protocols are the same as predicted in Eq. (6). As in Fig. 2 and Fig. 3, the critical visibility values are 0.89 for BB84 and 0.90 for SARG04. The overall error rate is shown to decrease linearly as the visibility of the quantum channel is increased.

pulse μ, the detection efficiencies, and the dark counts. These errors, however, are small enough so that they do not affect the secret key generation rates (the lower bound) significantly, see Fig. 5.

Although the sifted key rates for the BB84 and the SARG04 protocols behave differently in the presence of depolarization in the quantum channel, the overall error rates per bit $R_\mu Q_\mu$ are calculated to be the same for a given channel visibility [23],

$$R_\mu^{\mathrm{BB84}} Q_\mu^{\mathrm{BB84}} = R_\mu^{\mathrm{SARG04}} Q_\mu^{\mathrm{SARG04}}$$
$$= \frac{1}{4}[(1 + \bar{p}_d \exp(-\mu F \eta) - \bar{p}_d \exp(-\mu D \eta) \qquad (6)$$
$$- \bar{p}_d^2 \exp(-\mu \eta)].$$

We have directly measured the overall error rates, which are the total error key rates, i.e., the error key per second in the sifted key, in the experiment and compared the experimental results with the overall error rates determined using the experimental data shown in Figs. 2 and 3. The experimentally measured overall error rates of BB84 and SARG04 are shown in Fig. 4 and they overlap almost completely, confirming the relation in Eq. (6).

Finally, we study the secret key generation rates (the lower bound) for the BB84 and the SARG04 protocols in the presence of depolarization in the quantum channel. As mentioned earlier, the secret key rates are calculated from the experimentally obtained QBER, sifted key rates, and parameters of the experimental setup [23]. Figure 5 shows the secret key generation rates (the lower bound) for the two protocols as functions of the channel visibility. Note that each data point in Fig. 5 corresponds the maximum value of the secret key rate (the lower bound) for the range of average photon number per pulse, $0.033 \leq \mu \leq 0.283$, for the given channel visibility. In other words, each data point in Fig. 5 is obtained with the optimum value of μ. We also note that the optimum value of μ is shown to decrease monotonically (from $\mu = 0.189$ to 0.033 for both BB84 and SARG04 protocols) as the quantum channel visibility is reduced.

In addition, the experimental results in Fig. 5 show that the critical channel visibility values are 0.81 for BB84 and 0.86 for SARG04. The theoretical critical channel visibility values are 0.78 for BB84 and 0.87 for SARG04 [30]. Slight discrepancy for BB84 is due to the fact that, in our experiment, the average photon

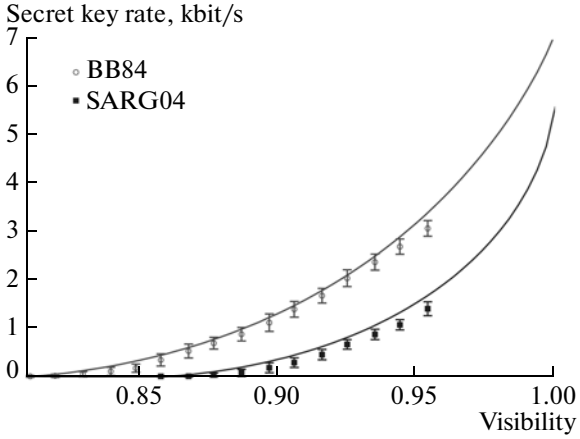

Fig. 5. Secret key generation rate (the lower bound) vs. channel visibility. The BB84 protocol is shown to generate more secret keys than the SARG04 protocol under the most general attack in the presence of depolarization in the quantum channel. The solid lines are theoretical plots using the parameters of the experimental setup. See [23, 32].

number per pulse was limited to $0.033 \le \mu \le 0.283$. If we had used even smaller for lower channel visibility, we would have been able to approach the theoretical critical visibility value of 0.78. The experimental results in Fig. 5, therefore, show that, although the SARG04 protocol has been known to be more robust against the PNS attack than the BB84 protocol, the latter performs better in real-world conditions, i.e., limited detection efficiency [31], non-zero dark count probability, and, most importantly, the quantum channel subject to depolarization effects [32].

5. CONCLUSIONS

We have demonstrated experimentally the effect of depolarization in the quantum channel on weak-pulse BB84 and SARG04 quantum cryptography protocols. The experimental results show that the SARG04 protocol is more susceptible to the depolarization effect in the quantum channel than the BB84 protocol. In real-world quantum cryptography applications in which the quantum channel cannot be assumed to be perfect, therefore, the BB84 protocol appears to provide better performance than the SARG04 protocol.

ACKNOWLEDGMENTS

This work was supported, in part, by the National Research Foundation of Korea (R01-2006-000-10354-0 and 2009-0070668). YSK acknowledges the support of the Korea Research Foundation (KRF-2007-511-C00004).

REFERENCES

1. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
2. F. A. A. El-Orany, M. R. B. Wahiddin, M.-A. Mat-Nor, N. Jamil, and I. Bahari, Laser Phys. **20**, 1210 (2010).
3. A. Yu. Khrennikov, Laser Phys. **19**, 346 (2009).
4. C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on the Computes, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
5. C. H. Bennett, F. Bessette, G. Brassard, L. Salvail, and J. Smolin, J. Cryptology **5**, 3 (1992).
6. Y.-S. Kim, Y.-C. Jeong, and Y.-H. Kim, Laser Phys. **18**, 810 (2008).
7. B. Huttner and N. Imoto, Phys. Rev. A **51**, 1863 (1995).
8. G. Brassard, N. Lutkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
9. N. Lutkenhaus, Phys. Rev. A **61**, 052304 (2000).
10. W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
11. V. Scarani, A. Acin, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
12. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, Phys. Rev. Lett. **96**, 070502 (2006).
13. T. Schmitt-Manderbach, H. Weier, M. Furst, R. Ursin, F. Tiefenbacher, T. Scheidl, J. Perdigues, Z. Sodnik, C. Kitrtsiefer, J. G. Rarity, A. Zeilinger, and H. Weinfurter, Phys. Rev. Lett. **98**, 010504 (2007).
14. C.-Z. Peng, J. Zhang, D. Yang, W.-B. Gao, H.-X. Ma, H. Yin, H.-P. Zeng, T. Yang, X.-B. Wang, and J.-W. Pan, Phys. Rev. Lett. **98**, 010505 (2007).
15. K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).
16. D. A. Kronberg, and S. N. Molotkov, Laser Phys. **19**, 884 (2009).
17. M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge Univ., Cambridge, 2000), ch. 8.
18. C. H. Bennett, D, P. DiVincenzo, and J. A. Smolin, Phys. Rev. Lett. **78**, 3217 (1997).
19. C. H. Bennett, P. W. Shor, J. A. Smolin, and A. V. Thapliyal, Phys. Rev. Lett **83**, 3081 (1999).
20. D. Brass, L. Faoro, C. Macchiavell, and G. M. Palma, J. Mod. Opt. **47**, 325 (2000).
21. C. Branciard, N. Gisin, B. Kraus, and V. Scarani, Phys. Rev. A **72**, 032301 (2005).
22. C.-H. F. Fung, K. Tamaki, and H.-K. Lo, Phys. Rev. A **73**, 012337 (2006).
23. B. Kraus, C. Branciard, and R. Renner, Phys. Rev. A **75**, 012316 (2007).
24. W. T. Buttler, R. J. Hughes, P. G. Kwiat, S. K. Lamoreaux, G. G. Luther, G. Morgan, J. E. Nordholt, C. G. Peterson, and C. M. Simmons, Phys. Rev. Lett. **81**, 3283 (1998).
25. W. T. Buttler, R. J. Hughes, S. K. Lamoreaux, G. L. Morgan, J. E. Nordholt, and C. G. Peterson, Phys. Rev. Lett. **84**, 5652 (2000).
26. R. J. Hughes, J. E. Nordholt, D. Derkacs and C. G. Peterson, New J. Phys. **4**, 43 (2002).
27. J. D. Franson and H. Ilves, Appl. Opt. **33**, 2949 (1994).
28. C. Gobby, Z. L. Yuan, and A. J. Shields, Appl. Phys. Lett. **84**, 3762 (2004).
29. P. A. Hiskett, D. Rosenberg, C. G. Peterson, R. J. Hughes, S. Nam, A. E. Lita, A. J. Miller, and J. E. Nordholt, New J. Phys. **8**, 193 (2006).
30. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
31. D. V. Strekalov, A. A. Savchenkov, A. B. Matsko, and N. Yu, Laser Phys. Lett. **6**, 129 (2009).
32. SARG04 could generate more secret keys than BB84 if $V \approx 1$ and $\eta \ll 1$. This condition, however, is difficult to satisfy, especially $V \approx 1$, in practice.