Passive decoy state SARG04 quantum-key-distribution with practical photon-number resolving detectors*

Xu Fang-Xing(许方星), Wang Shuang(王 双),
Han Zheng-Fu(韩正甫)†, and Guo Guang-Can(郭光灿)

Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, *China*

(Received 25 March 2010; revised manuscript received 11 May 2010)

SARG04 protocol has its advantages in defending photon number splitting attack, benefited from two-photon pulses part. In this paper, we present a passive decoy state SARG04 scheme combining with practical photon number resolving (PNR) detectors. Two kinds of practical detectors, transition-edge sensor and time-multiplexing detector, are taken into consideration. Theoretical analysis shows that both of them are compatible with the passive decoy state SARG04. Compared with the original SARG04, two detectors can boost the key generation rate and maximal secure distance obviously. Meanwhile, the result shows that quantum efficiency and dark count of the detector influence the maximal distance slightly, which indicates the prospect of implementation in real quantum key distribution system with imperfect practical PNS detectors.

Keywords: quantum key distribution, photon-number-resolving detector

PACC: 0367, 4230Q, 4250

1. Introduction

Quantum key distribution (QKD) for the secure communication as the earliest practical application of quantum mechanism is well developed, and different QKD protocols are derived in this decade. Some of them with frank security in principle,[1−3] are used to supply unconditional secure communications. Some of them have obvious specific advantages in key generation rate, modulation speed, complexity of establishment and other aspects,[4−7] suitable for wide promotion in practice, even though their security proofs are not sufficient. The eternal goal is to find a scheme with nice performances in use and perfect security guarantee, especially under the most-concerned photon number splitting (PNS) attack[8−10] as long as a perfect single photon source lacks in practice. We have to presume that only one-photon pulses in the signal sequence are immune to Eve's splitting and safe to distill secure keys.[11] For BB84 protocol, the lower bound of final secure key generation rate ($R^{\rm L}_{\rm BB84}$) is given by

$$R \geq R^{\rm L}_{\rm BB84} = -Q_\mu f(E_\mu) H_2(E_\mu) + Q_1[1 - H_2(e_1)], \quad (1)$$

where $f(E_\mu)$ represents the bidirectional error correction efficiency, and $H_2(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary Shannon entropy. The gain Q_n is defined as the joint probability that Alice sends an n-photon state and Bob obtains a detection event. The overall gain $Q_\mu = \sum_n Q_n$ stands for the counting rate on Bob's side for the source with intensity of μ. And e_n is the bit error rate of n-photon state, while E_μ is the overall error rate. To defend the PNS attack and improve QKD performance, people applied the decoy state method.[12−15] and better photon sources, such as the modified coherent state,[16] the triggered parametric down-conversion (PDC) source (also known as an HSPS, heralded single-photon source).[17−21] The former is to give a tight estimation of the portion of single photon pulses emitted from the source by using decoy state pulses, and the latter is to replace the photon number distribution with a sub-Poisson distribution which has a larger portion of single photon pulses compared with a Poisson distribution. Several groups also implement the passive decoy method combined with HSPS and decoy method to improve the QKD system.[22]

There is another attempt to combat the PNS attack, named Scarani–Acin–Ribordy–Gisin (SARG04)

*Project supported by the National Basic Research Program of China (Grant No. 2006CB921900), the National Natural Science Foundation of China (Grant Nos. 60537020 and 60621064) and the Innovation Funds of the Chinese Academy of Sciences.

†Corresponding author. E-mail: zfhan@ustc.edu.cn

© 2010 Chinese Physical Society and IOP Publishing Ltd

protocol.[23] With its principle the two-photon pulses can contribute to the final key generation as well. The lower bound of final secure key generation rate ($R^{\rm L}_{\rm SARG04}$) is shown as follows:[24,25]

$$\begin{aligned} R \geq R^{\rm L}_{\rm SARG04} = & -Q_\mu f(E_\mu) H_2(E_\mu) \\ & + Q_1[1 - H_2(Z_1|X_1)] \\ & + Q_2[1 - H_2(Z_2|X_2)], \end{aligned} \tag{2}$$

where Z_n (X_n) is a random variable corresponding to the phase (bit) error for the n-photon state. Compared to the key rate for BB84 in Eq. (1), the third term is the contribution from two-photon pulses to make SARG04 protocol act better, while the first term for the error correction and the second term achieved from one-photon pulses are the same as those for BB84. Recently, SARG04 schemes using HSPS sources and heralded pair-coherent state sources are considered for discussing the potential of SARG04 protocol.[26,27] Actually, a better photon number distribution can be gained if we use a photon-number resolving (PNR) detector instead of a threshold single photon detector in the passive decoy state QKD, which will benefit the SARG04 scheme as the portions of both the one-photon part and two-photon part are increased simultaneously.

PNR detectors can distinguish the photon number in the incoming pulses directly, which helps much in the field of quantum computation and quantum detection. At present, for the urgent need of this technique PNR detectors with different principles have been demonstrated by several groups. One kind of practical PNR detectors is the tungsten transition-edge sensor (TES), which is based on the temperature dependence of the resistance at the superconducting transition of tungsten.[28,29] The energy resolution of TES is nearly 0.088 eV that can guarantee the success of resolving photon numbers. Moreover, using a resonant cavity can make the quantum efficiency of TES η increase up to 82%.[29]

Another widely-used PNR detector is the time-multiplexed single photon detector (TMD).[30] By using k balanced beam splitters and fibre loops, this set can divide the incident pulse of n photons into a time sequence of N weaker pulses. Provided that $N = 2^k \gg n$, TMD can calculate the photon number with cascade method from the measurement result by normal avalanche photon diode (APD) which usually give only one output regardless of the incident photon number n. With refined commercial apparatus of Si APD, InGaAs APD and recent superconducting single photon detector (SSPD), TMD techniques can behave well in practical use for different scenarios.

Recently schemes with a single InGaAs APD for photon number resolving have been proposed successfully,[31,32] nevertheless its physical model is still missing. Some theoretical studies have been done about improving BB84 QKD with PNR detectors[33−36] as well. Here we give a SARG04 scheme with PNR detector using passive decoy state method. In this paper, we will focus on TES and TMD, investigate the advantage of these PNR detectors in this SARG04 scheme, and check the improvement in the QKD performance.

2. Proposal

In this scheme, we use a PDC process by pumping a Type-II crystal and generate photon pairs so that the state of photons in two spatial modes is

$$\begin{aligned} |\Psi\rangle_{si} &= \sum_{n=0}^{\infty} \sqrt{p_n} |n\rangle_s |n\rangle_i \\ &= \sum_{n=0}^{\infty} \sqrt{\mu^n/(1+\mu)^{n+1}} |n\rangle_s |n\rangle_i, \end{aligned} \tag{3}$$

where μ is the average photon number, and $p_n = \mu^n/(1+\mu)^{n+1}$ is the photon number distribution in each mode of the PDC source. Alice measures photons of each pulse in the idle mode with a PNR detector and implements the SARG04 modulation on the photons of the corresponding pulse in the signal mode. After the encoding process, she sends all the pulses to Bob and separates pulse sequence into several subsets according to her measurement results with PNR detectors: "one-click" events are assigned to signal state pulses μ-part, "non-click" and "two-clicks" events assigned to decoy state pulses Z-part and ν-part respectively, and "more than two-clicks" events treated as the useless part. This decoy method, named 3-intensity passive decoy, can pass over the steps to actively switch pulses intensity on Alice's side that is necessary for the conventional decoy method, and keep the system secure and easy to demonstrate.[22] Assuming the response function of the PNR detector is $P(l|n)$, which means the probability of l counts for n incident photons, we can follow the analysis about triggered QKD in Ref. [10] and neglect the coincidence between dark counts and detection events, and subsequently deduce the distribution for each subset of the

signal pulse sequence with a similar method in such mixture states[36]

$$\rho^Z = \frac{1}{A^Z}\left[\frac{1-d_{\rm A}}{1+\mu}|0\rangle_s\langle 0| + \sum_{n=1}^{\infty} P(0|n)p_n|n\rangle_s\langle n|\right],$$
$$\rho^\mu = \frac{1}{A^\mu}\left[\frac{d_{\rm A}}{1+\mu}|0\rangle_s\langle 0| + \sum_{n=1}^{\infty} P(1|n)p_n|n\rangle_s\langle n|\right],$$
$$\rho^\nu = \frac{1}{A^\nu}\left[\sum_{n=2}^{\infty} P(2|n)p_n|n\rangle_s\langle n|\right]. \quad (4)$$

Here the normalization factors for the three states are $A^Z = N^Z/N, A^\mu = N^\mu/N, A^\nu = N^\nu/N$ respectively, supposed that N is the pulse number in total; $d_{\rm A}$ is the dark count of Alice's PNR detector, and it is assumed that it only appears as a one-photon event. For two-click events, the probability (without normalization) of non-darkcount event is $\sum_{n=2}^{\infty} P(2|n)p_n$ and that of event with-darkcount is $d_{\rm A}\sum_{n=1}^{\infty} P(1|n)p_n + d_{\rm A}^2\sum_{n=0}^{\infty} P(0|n)p_n$. Considered that $P(i|n) \sim O(\eta^i)$, for a practical PNR detector with efficiency η larger than 1% and $d_{\rm A}$ less than 10^{-6}, the ratio between darkcounts and two-photon clicks is $O(10^{-4})$, which makes it reasonable to ignore the darkcounts in this subset.

The passive decoy method can guarantee that the signal states and decoy states are indistinguishable in each degree of freedom so that eavesdroppers cannot manipulate them differently. Hence the n-photon pulses' yield keeps the same for both signal pulses and decoy pulses. This denotes the conditional probability that Bob obtains a click event when Alice sends an n-photon state, which is $Y_n^\mu = Y_n^\nu = Y_n^Z = Y_n$. Quantum bit error rate (QBER) runs similarly $e_n^\mu = e_n^\nu = e_n^Z = e_n$. The overall gain Q and QBER E are given as

$$Q^{(x)} = \sum_{n=0}^{\infty} Q_n^{(x)} = \sum_{n=0}^{\infty} P_n^{(x)} Y_n,$$
$$Q^{(x)}E^{(x)} = \sum_{n=0}^{\infty} Q_n^{(x)} e_n = \sum_{n=0}^{\infty} P_n^{(x)} Y_n e_n, \quad (5)$$

where $x = \mu$, ν, and Z stand for μ-part, ν-part, and Z-part respectively. Therefore, we have

$$A^\mu Q^\mu = d_{\rm A}p_0Y_0 + \sum_{n=1}^{\infty} P(1|n)p_nY_n,$$
$$A^\mu Q^\mu E^\mu = d_{\rm A}p_0Y_0e_0 + \sum_{n=1}^{\infty} P(1|n)p_nY_ne_n,$$
$$A^\nu Q^\nu = \sum_{n=2}^{\infty} P(2|n)p_nY_n,$$
$$A^\nu Q^\nu E^\nu = \sum_{n=2}^{\infty} P(2|n)p_nY_ne_n,$$
$$A^Z Q^Z = (1-d_{\rm A})p_0Y_0 + \sum_{n=1}^{\infty} P(0|n)p_nY_n,$$
$$A^Z Q^Z E^Z = (1-d_{\rm A})p_0Y_0e_0 + \sum_{n=1}^{\infty} P(0|n)p_nY_ne_n. \quad (6)$$

Apparently, Y_0 and e_0 come from the vacuum state. In the asymptotic case with infinite number of decoy states, which indicates the limit potential of the protocol, we can substitute the background influences of the QKD setup into them. For SARG04 scheme, the non-orthogonal basis set Bob measured will give inclusive results that need to be discarded. Thus the yield and error rate for vacuum states should be

$$Y_0 = p_{\rm dark}/2, \quad e_0 = 1/2, \quad (7)$$

where $p_{\rm dark}$ is the dark count of Bob's detector. It is also consistent with the general formulas for the yield and QBER.[25] Combining the "one-click" part and "non-click" part and defining a function $F(n) = P(1|n)P(0|1) - P(0|n)P(1|1)$, we have

$$A^\mu Q^\mu P(0|2) - A^Z Q^Z P(1|2) = p_0Y_0[d_{\rm A}P(0|2) - (1-d_{\rm A})P(1|2)] - p_1Y_1F(2) + \sum_{n=3}^{\infty} p_nY_n[P(1|n)P(0|2) - P(0|n)P(1|2)]. \quad (8)$$

To obtain the lower bound of Y_1, we have made use of the following inequalities (9) as Condition 1

$$F(2) \geq 0, \quad P(1|n)P(0|2) \geq P(0|n)P(1|2), \quad (\text{when } n \geq 3), \quad (9)$$

and resolved from Eq. (10)

$$Y_1 \geq \underline{Y_1} = \frac{1}{p_1F(2)}\{A^Z Q^Z P(1|2) - A^\mu Q^\mu P(0|2) + p_0Y_0[d_{\rm A}P(0|2) - (1-d_{\rm A})P(1|2)]\}, \quad (10)$$

that the gain of single-photon states in the "μ" part is given as

$$Q_1^\mu \geq \underline{Q_1^\mu} = P_1^\mu \underline{Y_1} = \frac{p_1 P(1|1)\underline{Y_1}}{A^\mu}. \tag{11}$$

An upper bound of e_1 can be obtained as well

$$e_1 \leq \overline{e_1} = \frac{(1-d_{\rm A})A^\mu Q^\mu E^\mu - d_{\rm A}A^Z Q^Z E^Z}{p_1 \underline{Y_1}\left[(1-d_{\rm A})P(1|1) - d_{\rm A}P(0|1)\right]}. \tag{12}$$

Similarly, from Eq. (6) we can calculate the yield and QBER of two-photon states,

$$\begin{aligned} Y_2 \geq \underline{Y_2} = & \frac{1}{p_2\left[F(2)P(2|3) - F(3)P(2|2)\right]} \\ & \times \{A^\mu Q^\mu P(0|1)P(2|3) \\ & - A^Z Q^Z P(1|1)P(2|3) \\ & - A^\nu Q^\nu F(3) - p_0 Y_0 P(2|3)[d_{\rm A}P(0|1) \\ & - (1-d_{\rm A})P(1|1)]\}, \end{aligned} \tag{13}$$

$$Q_2^\mu \geq \underline{Q_2^\mu} = P_2^\mu \underline{Y_2} = \frac{p_2 P(1|2)\underline{Y_2}}{A^\mu}, \tag{14}$$

$$e_2 \leq \overline{e_2} = \frac{A^\nu Q^\nu E^\nu}{p_2 \underline{Y_2} P(2|2)}, \tag{15}$$

under Condition 2

$$\begin{aligned} & F(2)P(2|3) \geq F(3)P(2|2), \\ & F(3)P(2|n) \geq F(n)P(2|3) \quad (\text{when} \ \ n \geq 4). \end{aligned} \tag{16}$$

Consequently, by using a PNS detector, that satisfies Condition 1 and Condition 2 and a suitable PDC source, legal users can achieve lower bounds of yield for both single-photon states and two-photon states with Eqs. (10) and (13), and upper bounds of QBER with Eqs. (12) and (15). Subsequently one can use Eq. (2) to work out the key generation rate as

$$\begin{aligned} R \geq R^{\rm L}_{\rm SARG04} = & -Q_\mu f(E_\mu)H_2(E_\mu) \\ & + \underline{Q_1^\mu}[1 - H_2(\overline{e_1})] \\ & + \underline{Q_2^\mu}[1 - H_2(\overline{e_{p,2}})], \end{aligned} \tag{17}$$

where $e_{p,2} = e_2$ is the phase error rate of two-photon states.

This is the general procedure of the passive decoy method for SARG04 protocol with PNR detectors. The response function $P(l|n)$ varies from the PNR detector used in the scheme. Whether we can use such a PNR detector in this proposal, depends on whether its response function obeys the constraint conditions in Eqs. (9) and (16). Thus, in the following section we have to calculate separately for different kinds of detector.

2.1. Passive SARG04 with TES detector

For a TES detector, the probability $P(l|n)$ is given by[28]

$$P(l|n) = \binom{n}{l}\eta^l(1-\eta)^{n-l}, \tag{18}$$

and

$$F(n) = (n-1)\eta(1-\eta)^n. \tag{19}$$

Normalization factors for the states of μ-part, ν-part, and Z-part are derived from Eq. (6)

$$\begin{aligned} A^\mu &= d_{\rm A}p_0 + \sum_{n=1}^{\infty} P(1|n)p_n = \frac{d_{\rm A}}{1+\mu} + \frac{\eta\mu}{(1+\eta\mu)^2}, \\ A^\nu &= \sum_{n=2}^{\infty} P(2|n)p_n = \frac{\eta^2\mu^2}{(1+\eta\mu)^3}, \\ A^Z &= (1-d_{\rm A})p_0 + \sum_{n=1}^{\infty} P(0|n)p_n \\ &= \frac{1-d_{\rm A}}{1+\mu} + \frac{\mu(1-\eta)}{(1+\mu)(1+\eta\mu)}. \end{aligned} \tag{20}$$

The two constraint conditions (9) and (16) can be verified for this case, given $\eta \in [0,1]$.

Proof See Appendix A.

The above result can guarantee the success of using a TES in this scheme. Substituting Eqs. (18) and (19) into the general calculation formula (17), we can obtain the final secure key generation rate for SARG04 with TES detector.

2.2. Passive SARG04 with TMD

Defining the three auxiliary parameters $a = 1-\eta$,$b = 1-\eta+\eta/N$, $c = 1-\eta+2\eta/N$ so that $a < b < c$, then for a TMD the probability $P(l|n)$ is expressed as[30]

$$P(l|n) = \binom{N}{l}\sum_{j=0}^{l}(-1)^j\binom{l}{j}\left[(1-\eta) + \frac{(l-j)\eta}{N}\right]^n \tag{21}$$

and

$$F(n) = N(1-\eta)\left[\left(1 - \frac{N-1}{N}\eta\right)^n - (1-\eta)^n\right] - \eta(1-\eta)^n = (ab^n - a^n b). \tag{22}$$

Normalization factors for the states of μ-part, ν-part, and Z-part are calculated from Eq. (6) as

$$\begin{aligned} A^{\mu} &= \frac{d_{\rm A}}{1+\mu} + N\left\{\frac{1}{1+\mu-b\mu} - \frac{1}{1+\mu-a\mu}\right\}, \\ A^{\nu} &= \frac{N(N-1)}{2}\left\{\frac{1}{1+\mu-a\mu} + \frac{1}{1+\mu-c\mu} - \frac{2}{1+\mu-b\mu}\right\}, \\ A^{Z} &= \frac{1-d_{\rm A}}{1+\mu} + \frac{a\mu}{(1+\mu)(1+\mu-a\mu)}. \end{aligned} \tag{23}$$

Detector efficiency $\eta \in [0,1]$ can also guarantee the constraint conditions (9) and (16) verified for this case with a TMD.

Proof See Appendix A.

The final key generation rate $R_{\rm SARG+TMD}$ can be calculated by combining Eq. (17) with Eqs. (21) and (22).

3. Numerical simulation

In a real QKD experiment with decoy method, we can measure the overall gain Q, QBER E, and the pulse ratio A for each subset in $\{\mu,\nu,Z\}$ directly, which are used for the error correction and classic privacy amplification to distill the final secure key. Nevertheless, using a set of typical experimental parameters in Table 1 and simulating experiment outputs can still infer the performance of the scheme.

Table 1. Typical QKD setup parameters from GYS experiments;[37] α is the loss coefficient for commercial communication fibres, $p_{\rm dark}$ is the darkcount of Bob's threshold detector, $\eta_{\rm B}$ is the transmittance in Bob's side, including the internal transmittance of optical components and detector efficiency, and $e_{\rm det}$ is the intrinsic error rate due to the imperfect interference.

	λ/nm	α/dB·km^{-1}	$p_{\rm dark}$	$\eta_{\rm B}$	$e_{\rm det}$
GYS	1550	0.21	1.7×10^{-6}	0.045	0.033

For SARG04 protocol, the yield and error rate of n-photon pulses are[25]

$$Y_n = \eta_n\left(\frac{e_{\rm det}}{2}+\frac{1}{4}\right) + \frac{1}{2}(1-\eta_n)p_{\rm dark}, \tag{24}$$

$$e_n = \left[\frac{e_{\rm det}}{2}\eta_n + \frac{1}{4}(1-\eta_n)p_{\rm dark}\right]/Y_n. \tag{25}$$

Here η_n is the transmittance of the n-photon states with respect to the channel loss between users that $t_{\rm AB} = {\rm e}^{-\alpha L}$ and $\eta_n = 1-(1-t_{\rm AB}\eta_{\rm B})^n$. Thus, the pulse ratio A^x, the overall gain Q^x and the overall QBER E^x ($x=\mu,\nu,Z$) can be derived from Eqs. (6), (20), and (23) for respective response functions (18) and (21) of different PNR detectors. With these simulated experimental outputs, we can calculate the lower bound of key generation rate following the analysis in Section 2. On the other hand, for studying the potential limitation of the scheme, we substitute Eqs. (24) and (25) into Eqs. (5) and (17) to achieve the performance of the perfect decoy method (the asymptotical case) with infinite number of decoy states.

In Fig. 1, we show key generation rates versus transmission distance for different SARG04 schemes: original one with a weak coherent pulse (WCP) source, passive SARG04 with a TES detector, and passive SARG04 with TMD. Results of most popular schemes that BB84 protocol with a WCP source and the passive decoy BB84 are given in contrast as well. For simulation, typical QKD setup parameters are borrowed from GYS experiment[37] in Table 1 and

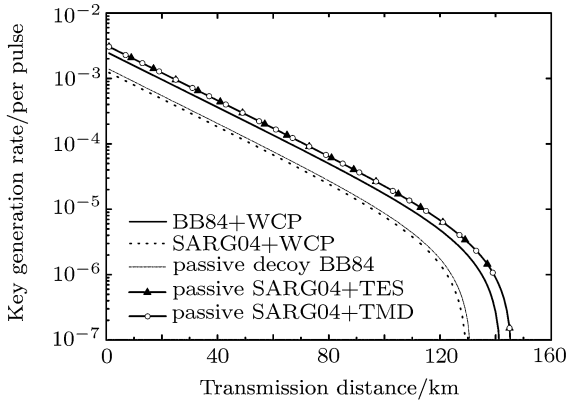


Fig. 1. Key generation rates versus transmission distance. Asymptotical cases for five QKD schemes are taken into consideration to indicate the limit potential of protocols: decoy SARG04 using a WCP source, passive SARG04 with a TES detector and passive SARG04 with a TMD, compared with decoy BB84 using a WCP source and the passive decoy BB84. The maximal secure distances are 129, 146, 145, 141, and 130 km respectively. Two lines for TES and TMD are very close and the gap between maximum distances is 1 km in this simulation.

key rates are calculated in asymptotical cases with an optimal photon number μ selected via exhaust search which is shown in Fig. 2. Compared with the limited

distances of the original SARG04 with decoy method as 129 km, TMD with $N = 4$ commercial InGaAs APD[37] can extend the distance for modified SARG04 to 145 km and a TES with efficiency 82%[29] can extend it to 146 km. Both of the PNR detectors can increase the key generation rate per pulse twice compared with the original SARG04. Even that of the original or passive decoy BB84, the raise of key rate and extension of distance is obvious.

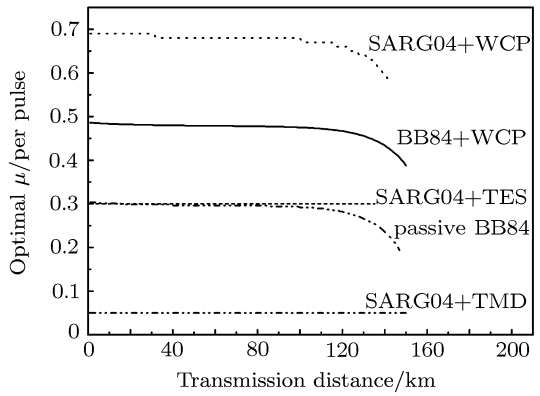


Fig. 2. Optimal μ of average photon number for different QKD schemes, which are selected numerically by exhausted research. Note that the optimal μ for SARG04 is larger than that for decoy BB84, nevertheless the optimal μ are much smaller for two passive SARG04 schemes which can still achieve a higher key rate per pulse. We also can learn that for QKD protocols, the optimal photon number in passive decoy protocol is smaller than the original one.

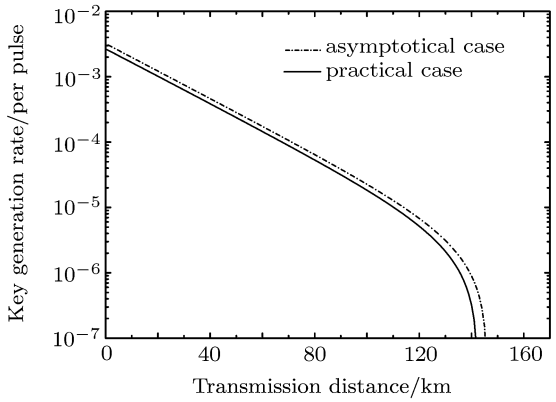


Fig. 3. Simulation for passive SARG04 with TES detector. Asymptotical cases for InGaAs PNR detector and tungsten PNR detector give two close curves in the upper side, which infers a maximal secure distance up to 185 km. Practical cases using four independent set of parameters give results that show the influence of detector's quantum efficiency and dark count.

Specifically, in Fig. 3 of the TES cases, we have calculated the limitations for the schemes (the asymptotical case with infinite decoy states) and the practical case with 3 decoy states using a tungsten PNR detector (η=82%, d.c.=10^{-2}/second, time window=1 ns).[29,38] The maximal distance are 146 and 141 km for respective cases. The small gap indicates that for passive decoy SARG04 protocol with TES, three-intensity decoy method acts quite well.

In Fig. 4, asymptotical calculations give the maximal distance of passive SARG04 with TMD to be 145 km. According to Ref. [35], the boost of the key rate is very small by increasing mode number N, $N = 4$ is assumed here for cases in practice. Si APD ($\eta_{\rm A} = 70\%$), InGaAs APD ($\eta_{\rm A} = 20\%$ and $\eta_{\rm A} = 10\%$, for different working conditions)[1)] are taken into consideration here for Alice's side. Both the quantum efficiency and dark count will influence the result, nevertheless the effect is slightly. As a result, in a practical case with three-intensity passive decoy SARG04 using commercial TMD, the limit secure distance is 139 km. Meanwhile, the gap between practical simulation and asymptotical calculation is small, indicating that the decoy method is suitable for this passive SARG04.

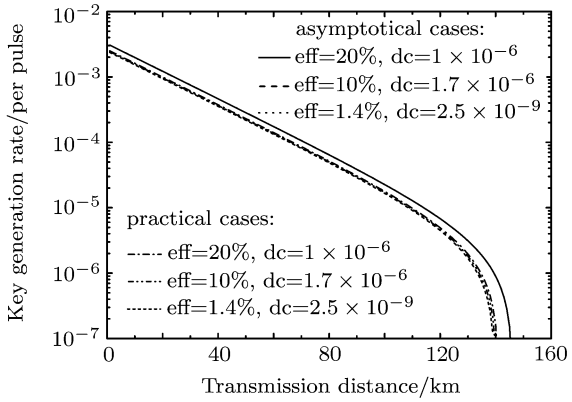


Fig. 4. Simulation for passive SARG04 with TMD. Asymptotical cases for TMD using Si APD and InGaAs APD also give two close curves, and the maximal secure distance is 145 km. Curves in practical cases are for implementing widely-used single photon threshold detectors, including commercial Si and InGaAs APDs. The gap between practical cases and asymptotical cases is slight, indicating that the estimation method of this passive SARG04 is efficient. In the figure, "eff" means efficiency and "dc" is the abbreviation for dark count.

Note that for both kinds of PNR, the limitation is stable for different efficiency or dark count. That is reasonable because QKD setup's performance mainly depends on the schemes efficiency, the distribution of the source and the behaviour of Bob's detector. We can treat the PDC source and the PNR detection in the idle photons as a virtual source, and the efficiency

[1)] The simulation data come from the parameters for commercial products of the id Quantique and the Princeton Lightwave.

of PNR detector will mainly affect the system key generation speed instead of the distribution of this virtual source. Consequently, even though PNR techniques are still imperfect nowadays without high detection efficiency or high resolving precision, we can still implement the techniques for SARG04 scheme and achieve development of the QKD.

4. Conclusion

In this paper, we have studied the passive SARG04 scheme with practical PNR detectors. As the two-photon part can generate secure keys as well in SARG04 protocol, we have combined it with passive decoy method to achieve better QKD performance. The estimation method for this passive SARG04 scheme is presented in detail for two kinds of PNR detector respectively. The simulation results show that, as long as the detector fits two constraint conditions in Section 2, both TES and TMD can help to give a boost on the secure distance and key rate compared with the original SARG04. Meanwhile, estimation results with parameters of commercial PNR detectors indicate that, even using imperfect PNR detectors without high detection efficiency or high resolving precision, passive SARG04 scheme can still get benefit from their photon resolving abilities, which shows a prospect of implementation in real QKD system.

Appendix. Verifying the constraint conditions

This modified SARG04 has two constraint conditions (9) and (16) for applying the passive decoy method successfully. Here we will verify them in two cases with different PNR detectors.

Case 1 The case with TES detector

In this scenario, we have

$$P(l|n) = \binom{n}{l}\eta^l(1-\eta)^{n-l}, \tag{A1}$$

$$F(n) = (n-1)\eta(1-\eta)^n. \tag{A2}$$

Given that $\eta \in [0,1]$, Condition 1 can be transformed as

$$F(2) = \eta(1-\eta)^2 \geq 0,$$

and

$$P(1|n)P(0|2) - P(0|n)P(1|2) = (n-2)\eta(1-\eta)^{n+1} \geq 0$$

as long as $n \geq 3$.

Condition 2 can be written as

$$F(2)P(2|3) - F(3)P(2|2) = \eta^3(1-\eta)^3 \geq 0,$$

and

$$F(3)P(2|n) - F(n)P(2|3) = (n-1)(n-3)\eta^3(1-\eta)^{n+1} \geq 0,$$

as long as $n \geq 4$.

The two conditions are obviously true, which guarantees the applicability of TES in the passive SARG04 scheme.

Case 2 The case with TMD

In this scenario,

$$P(l|n) = \binom{N}{l}\sum_{j=0}^{l}(-1)^j\binom{l}{j}\left[(1-\eta)+\frac{(l-j)\eta}{N}\right]^n, \tag{A3}$$

$$F(n) = N(ab^n - a^n b). \tag{A4}$$

Given that $\eta \in [0,1]$, Condition 1 can be transformed as

$$F(2) = Nab(b-a) \geq 0.$$

and

$$P(1|n)P(0|2) - P(0|n)P(1|2) = Na^2b^2(b^{n-2} - a^{n-2}) \geq 0.$$

As long as $n \geq 3$, and $b > a$, Condition 1 is incidentally true.

Condition 2 can be written as

$$\begin{aligned} F(2)P(2|3) - F(3)P(2|2) &= \frac{N^2(N-1)}{2}ab(b-a)[-a^2b + 2ab^2 - ac^2 - bc^2 + c^3] \\ &= N^2(N-1)ab(b-a)(2b-a) \geq 0, \end{aligned}$$

and as long as $n \geq 4$,

$$F(3)P(2|n) - F(n)P(2|3) = \frac{N^2(N-1)}{2}\{a^3b^nc - a^nb^3c + ab^3c^n - ab^nc^3 + a^nbc^3 - a^3bc^n\} \geq 0. \tag{A5}$$

Here for simplicity, a new function $G(n)$ is defined as

$$G(n) = a^3b^nc - a^nb^3c + ab^3c^n - ab^nc^3 + a^nbc^3 - a^3bc^n. \tag{A6}$$

Subsequently, the condition turns out as

$$G(n) \geq 0, \quad (\text{when} \quad n \geq 4); \tag{A7}$$

which is proved with the following mathematical induction.

(i) When $n = 4$, the statement

$$G(4) = abc(b-a)(c-a)(c-b)(ab + ac + bc) \geq 0$$

is incidentally true as $a < b < c$.

(ii) Assume that, for an arbitrary $k \geq 4$, $G(k) \geq 0$ is also true. We derive $G(k+1) \geq 0$ from this assumption. The differential coefficient of $G(k+1)$ is

$$\begin{aligned} G'(k+1) &= (k+1)(a^3b^kc - a^kb^3c + ab^3c^k - ab^kc^3 + a^kbc^3 - a^3bc^k) \\ &= (k+1)G(k) \geq 0. \end{aligned} \tag{A8}$$

It refers to that function $G(k)$ is monotonically increasing and subsequently becoming $G(k+1) \geq G(k) \geq 0$. Therefore, for arbitrary $n \geq 4$, $G(n) \geq 0$ is true, which also gives the verification that $F(3)P(2|n) - F(n)P(2|3) \geq 0$. Subsequently, TMD can be used for the passive decoy method in this scheme as well.

References

[1] Bennett C H and Brassard G 1984 *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE) pp. 175–179.

[2] Ekert A K 1991 *Phys. Rev. Lett.* **67** 661

[3] Gisin N, Ribordy G, Tittel W and Zbinden H 2002 *Rev. Mod. Phys.* **74** 145

[4] Braunstein S L and van Loock P 2005 *Rev. Mod. Phys.* **77** 2

[5] Inoue K, Waks E and Yamamoto Y 2002 *Phys. Rev. Lett.* **89** 037902

[6] Stucki D, Barreiro C, Fasel S, Gautier J D, Gay O, Gisin N, Thew R, Thoma Y, Trinkler P, Vannel F and Zbinden H 2009 *Opt. Express* **17** 13326

[7] Zhang J, Wang F Q, Zhao F, Lu Y Q and Liu S H 2008 *Acta Phys. Sin.* **57** 4941 (in Chinese)

[8] Huttner B, Imoto N, Gisin N and Mor T 1995 *Phys. Rev.* A **51** 1863

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

[10] Lütkenhaus N 2000 *Phys. Rev.* A **61** 052304

[11] Gottesman D, Lo H K, Lütkenhaus N and Preskill J 2004 *Quantum Information and Computation* **4** 325

[12] Hwang W Y 2003 *Phys. Rev. Lett.* **91** 057901

[13] Lo H K, Ma X F and Chen K 2005 *Phys. Rev. Lett.* **94** 230504

[14] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[15] Ma X F, Qi B, Zhao Y and Lo H K 2005 *Phys. Rev.* A **72** 012326

[16] Yin Z Q, Han Z F, Sun F W and Guo G C 2007 *Phys. Rev.* A **76** 014304

[17] Wang Q, Wang X B and Guo G C 2007 *Phys. Rev.* A **75** 012312
[18] Ma X F and Lo H K 2008 *New J. Phys.* **10** 073018
[19] Mi J L, Wang F Q, Lin Q Q and Liang R S 2008 *Chin. Phys.* B **17** 1178
[20] Liang R S, Lin Q Q, Liu S H, Mi J L and Wang F Q 2008 *Acta Phys. Sin.* **57** 678 (in Chinese)
[21] Hu H P, Huang Y X, Liu S H, Lu W and Wang J D 2010 *Acta Phys. Sin.* **59** 287 (in Chinese)
[22] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 *Phys. Rev. Lett.* **99** 180503
[23] Scarani V, Acin A, Ribordy G and Gisin N 2004 *Phys. Rev. Lett.* **92** 057901
[24] Tamaki K and Lo H K 2004 *arXiv: quant-ph/0412035*
[25] Fung C H F, Tamaki K and Lo H K 2006 *Phys. Rev.* A **73** 012337
[26] Zhang S L, Zou X B, Li K, Jin C H and Guo G C 2007 *Phys. Rev.* A **76** 044304
[27] Zhang S L, Ou X B, Jin C H and Guo G C 2008 *arXiv: quant-ph/0807.1760*
[28] Irwin K D 1995 *Appl. Phys. Lett.* **66** 1998
[29] Rosenberg D, Lita A E, Miller A, Nam S and Schwall R 2005 *IEEE Trans. Appl. Supercond.* **15** 575
[30] Fitch M, Jacobs B, Pittman T and Franson F 2003 *Phys. Rev.* A **68** 043814
[31] Kardynal B E, Yuan Z L and Shields A J 2008 *Nature Photonics* **2** 425
[32] Wu G, Jian Y, Wu E and Zeng H P 2009 *Opt. Express* **17** 18782
[33] Cai Q Y and Tan Y G 2006 *Phys. Rev.* A **73** 032305
[34] Mauerer W and Silberhorn C 2007 *Phys. Rev.* A **75** 050305
[35] Horikiri T and Kobayashi T 2006 *Phys. Rev.* A **73** 032331
[36] Xu F X, Han Z F and Guo G C 2008 *Proc. SPIE* **7278** 72780Y
[37] Gobby C, Yuan Z L and Shields A J 2004 *Appl. Phys. Lett.* **84** 3762
[38] Takesue H, Nam S W, Zhang Q, Hadfield R H, Honjo T, Tamaki K and Yamamoto Y 2007 *Nature Photonics* **1** 343