Quantum Physics Letters
An International Journal

http://dx.doi.org/10.18576/qpl/070301

Optimization of Measurement Device Independent Scarani-Acín-Ribordy-Gisin Protocol

C. Tannous [1,*] *and J. Langlois*[2]

[1] Laboratoire des Sciences et Techniques de l'Information, de la Communication et de la Connaissance, UMR-6285 CNRS, Brest Cedex3, FRANCE
[2] Laboratoire OPTIMAG, EA938, Brest Cedex3, FRANCE

Received: 2 Sep. 2018, Revised: 22 Nov. 2018, Accepted: 28 Nov. 2018
Published online: 1 Dec. 2018

Abstract: The measurement device independent (MDI) Quantum Key Distribution (QKD) is a practically implementable method for transmitting secret keys between distant partners performing quantum communication. SARG04 (Scarani-Acín-Ribordy-Gisin 2004) is a protocol tailored to struggle against photon number splitting (PNS) attacks by eavesdroppers. Considering its decoy implemented MDI-QKD version, we analyse its performance from secret key bitrate versus communication distance point of view. Among several factors such as error correction function, dark counting rate (DCR) and quantum efficiency, considered for achieving the largest key bitrate versus longest communication distance, we infer that the most promising for MDI-QKD SARG04 protocol is the DCR representing a challenge to optical material scientists.

Keywords: Quantum communications; Quantum cryptography; Quantum information and processing

1 Introduction

While Classical cryptography uses two types of keys to encode and decode messages (secret or symmetric and public or asymmetric keys), Quantum cryptography uses QKD for transmitting secret keys between partners allowing them to encrypt and decrypt their messages over the forthcoming Quantum Internet [1]. QKD main characteristic is its practical implementability since it has already been deployed commercially by several quantum communication providers such as SeQureNet in France, ID Quantique in Switzerland, MagiQ Technologies in the USA and QuintessenceLabs in Australia. The second main feature of QKD is that it allows communicating parties to detect online eavesdroppers in a straightforward fashion.

In principle, QKD is unconditionally secure nevertheless its practical implementation has many loopholes and consequently has been attacked by many different ways exploiting some intermediate operation or another, during secret key processing, such as time-shift [2,3], phase-remapping [4], detector blinding [5,6], detector dead-time [7], device calibration [8], laser damage [9]...

Fortunately a number of methods [10] have been developed in order to improve QKD security since its main weakness originates from the assumption of perfect implementation from theory to experiment. Side-channel attacks exploit discrepancies between theoretical and experimental implementation and efficient protection from these attacks has been suggested by Braunstein *et al.* [10] who use virtual channels in order to place detectors and processing tools inside inaccessible private spaces.

This work is about performance analysis of SARG04 [11] protocol in its MDI-QKD [12] version designed to fend off photon number splitting (PNS) attacks by examining the impact of important factors such as error correction function types, detector DCR and quantum efficiency. It is organized as follows: after reviewing the original four-state SARG04 protocol, we discuss its MDI version and describe the effects of various parameters on communication distance and secret key bitrate.

* Corresponding author e-mail: tannous@univ-brest.fr

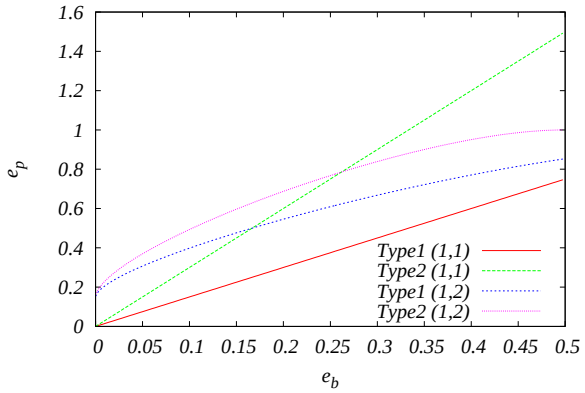

Fig. 1: (Color on-line) Phase error probability e_p versus bit error probability e_b for Type1 and Type2 with different number of photons (m,n) emitted by Alice and Bob.

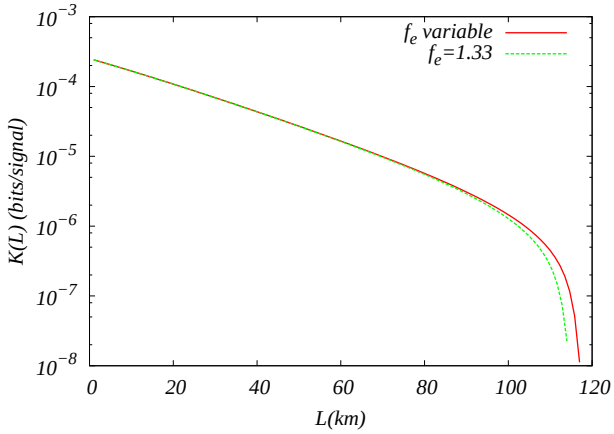

Fig. 2: (Color on-line) Key rate $K(L)$ for Type 1 events, in bps versus distance L using the same parameters as in Ref. [15] η=0.045, $d = 8.5\times10^{-7}$, $\alpha = 0.21$ for different error correction function.

2 MDI version of the four-state SARG04 protocol

SARG04 protocol has been developed to combat PNS attacks that are targeted toward intercepting photons present in weak coherent pulses (WCP) that are used for communication. This stems from the fact, it is not possible presently to commercially exploit single photons in a pulse. However, progress in developing large scale methods targeted at using single photons in a pulse is advancing steadily [13].

Mizutani *et al.* [14] modified the original SARG04 protocol by including an intermediate experimental setup run by Charlie, at mid-distance between Alice and Bob, consisting of Bell correlation measurements. The setup contains a half beam-splitter, two polarization beam-splitters to simulate photonic Hadamard and CNOT gates in order to produce Bell states, as well as photodiode detectors. This additional step will help discard non perfectly anti-correlated photons and thus reduce transmission error rates. In addition, Alice and Bob not only choose photon polarization randomly, they also use WCP amplitude modulation to generate decoy states in order to confuse the eavesdropper.

The protocol runs as follows:

–Charlie performs Bell measurement on the incoming photon pulses and announces to Alice and Bob over the public channel whether his measurement outcome is adequate or not. When the outcome is satisfactory, he announces the adequate events as being of Type1 or Type2. Type1 is coincidence detection events of AT and BR or BT and AR. Type2 is coincidence detection events of AT and AR or BT and BR where AT, BT stand for detecting transmitted (T) photon events from Alice (A) or Bob (B) linearly polarized at 45° whereas AR, BR are for detecting reflected (R) photon events at -45° .

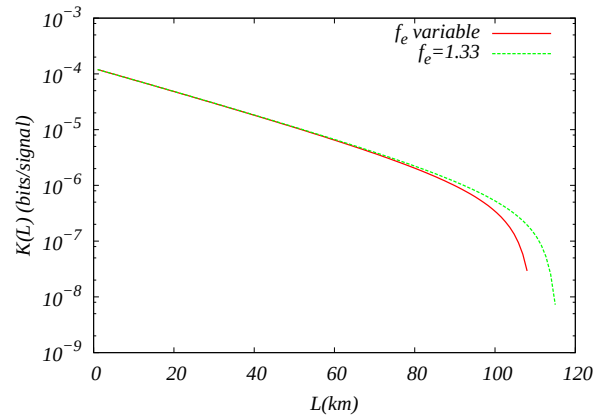

Fig. 3: (Color on-line) Key rate $K(L)$ for Type 2 events, in bps versus distance L using the same parameters as in Ref. [15] η=0.045, $d = 8.5\times10^{-7}$, $\alpha = 0.21$ for different error correction function.

–Alice and Bob broadcast, over the public channel, indices $k \in \{0,1,2,3\}$ and $k' \in \{0,1,2,3\}$ that are used for rotating states [14]. If the measurement outcome is acceptable with Type1 and $k = k' = 0,1,2,3$, they keep their initial bit values, and Alice flips her bit. If the measurement outcome is acceptable with Type2 and $k = k' = 0,2$, they keep their initial bit values. In all the other cases, they discard their bit values.

–After repeating the above operations several times, Alice and Bob perform error correction, privacy amplification and authentication as described previously.

In the ideal case (no transmission errors, no eavesdropping) Alice and Bob should discard results

pertaining to measurements done in different bases (or when Bob failed to detect any photon).

In QKD, Alice and Bob should be able to determine efficiently their shared secret key as a function of distance L separating them. Since, the secure key is determined after sifting and distillation, secure key rate is expressed in bps (bits per signal) given that Alice sends symbols to Bob to sift and distill with the remaining bits making the secret key.

For Type i event, we define $e_{i,p}^{(m,n)}$ as the phase error probability that Alice and Bob emits m and n photons respectively, and Charlie announces an adequate outcome with $Q_i^{(m,n)}$, the joint probability. Consequently the asymptotic key rate for Type i is given as a sum over partial private amplification terms of the form $Q_i^{(m,n)}[1-h_2(e_{i,p}^{(m,n)})]$ and one error correction term $Q_i^{tot} f(e_i^{tot}) h_2(e_i^{tot})$ related to total errors as [14,16]:

$$K_i(L) = Q_i^{(1,1)}[1-h_2(e_{i,p}^{(1,1)})] + Q_i^{(1,2)}[1-h_2(e_{i,p}^{(1,2)})] + Q_i^{(2,1)}[1-h_2(e_{i,p}^{(2,1)})] - Q_i^{tot} f(e_i^{tot}) h_2(e_i^{tot}). \quad (1)$$

The total probabilities $Q_i^{tot} = \sum_{m,n} Q_i^{(m,n)}$ and total error rates are given by $e_i^{tot} = \sum_{m,n} Q_i^{(m,n)} e_{i,b}^{(m,n)} / Q_i^{tot}$ where $e_{i,b}^{(m,n)}$ is the Type i bit error probability and h_2 is the binary Shannon entropy [17] given by $h_2(x) = -x\log_2(x) - (1-x)\log_2(1-x)$. Moreover, the above asymptotic key rate is obtained in the limit of infinite number of decoy states [14].

Phase error probabilities are determined from bit error probabilities as depicted in fig. 1 for Type 1 and 2 and depending on photons (m,n) emitted.

This validates our method of calculating the probabilities since our results agree with Mizutani *et al.* [14] work (see figure 3). Our method differs from Ma *et al.* [18] work who used a modified sifting technique to handle single-photon detector dead-time constraints without considering Type 1 and 2 bit error probabilities depending on photon emission.

Since Charlie is in the middle between Alice and Bob, the channel transmittance to Charlie from Alice is the same as that from Bob. Considering that L is the distance between Alice and Bob, the channel transmittance η_T is obtained by replacing L by $L/2$ resulting in: $\eta_T = 10^{-\alpha L/20}$.

3 Results

For the standard Telecom wavelength [17] $\lambda = 1.55\mu$m, the loss coefficient with distance is α=0.21 dB/km. The quantum efficiency and the dark counting probability (proportional to DCR) of the detectors are taken as $\eta = 0.045$ and $d = 8.5\times10^{-7}$, respectively as in the GYS [15] case.

Quantum Error Correction Coding (QECC) is made with a function that has been experimentally determined from the CASCADE interactive algorithm developed by Brassard *et al.* [19] and given in an interpolative form by Enzer *et al.* [20] as: $f_e(x) = 1.1581 + 57.200x^3$. Usually $f_e(x)$ value depends on the error correction algorithm used, and is typically between 1 (where the number of error correction bits is equal to the ideal Shannon limit) and about 1.5. An average convenient value for $f_e(x)$ is 1.33. In the following we select either a freely variable $f_e(x)$ or a fixed f_e with an average value of 1.33.

In figs 2,3 secret key rates for Type 1 and Type 2 events are displayed versus distance when $f_e(x)$ function is considered as variable or fixed at a value of 1.33.

Improving detection quality means that dark counting must be substantially reduced in order to avoid false "clicks" (irrelevant event detection) of the detectors.

In figs 4,5 secret key rates for Type 1 and Type 2 events are displayed versus distance for different values of the DCR with error correction function $f_e(x)$ freely varying.

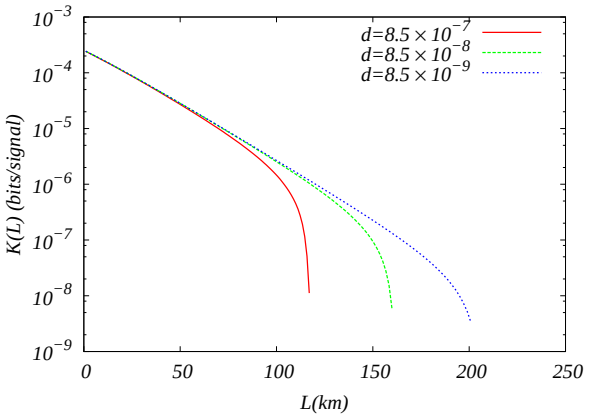

Fig. 4: (Color on-line) Key rate $K(L)$ for Type 1 events, in bps versus distance L using the same parameters as in Ref. [15] η=0.045, $\alpha = 0.21$ for different detector dark counting probability d and variable error correction function.

Quantum yield is an important parameter that plays a substantial role in quantum communications.

In figs 6,7 secret key rates for Type 1 and Type 2 events are displayed versus distance for different values of the quantum yield η with error correction function $f_e(x)$ freely varying. The value of η has been intentionally exaggerated in order to explore the range of communication distances covered by its variation. The values of the experimental parameters shows roughly a tenfold performance increase when we compare the 2004 GYS experiment [15] for which $\eta = 0.045$ and $d = 8.5\times10^{-7}$ to Tang *et al.* [21] parameters $\eta = 0.43$ and $d = 10^{-7}$ that were obtained 10 years afterwards. The rate of improvement is satisfactory when we additionally observe that the Quantum yields acts on communication

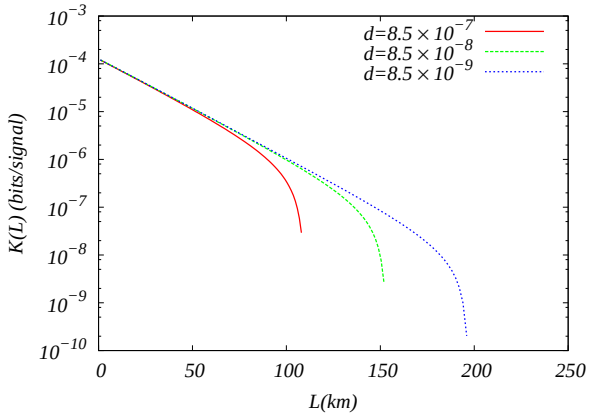

Fig. 5: (Color on-line) Key rate $K(L)$ for Type 2 events, in bps versus distance L using the same parameters as in Ref. [15] η=0.045, $\alpha = 0.21$ for different detector dark counting probability d and variable error correction function.

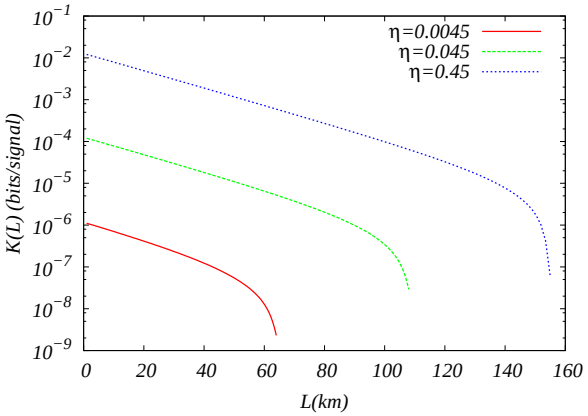

Fig. 7: (Color on-line) Key rate $K(L)$ for Type 2 events, in bps versus distance L using the same parameters as in Ref. [15] $d = 8.5 \times 10^{-7}$, $\alpha = 0.21$ and $f_e(x)$ variable for different values of the quantum yield parameter η.

distance and key bitrate simultaneously whereas DCR and error correction function changes affect solely communication distance.

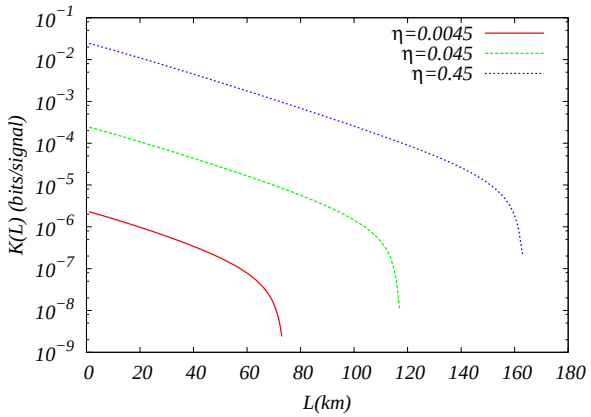

Fig. 6: (Color on-line) Key rate $K(L)$ for Type 1 events, in bps versus distance L using the same parameters as in Ref. [15] $d = 8.5 \times 10^{-7}$, $\alpha = 0.21$ and $f_e(x)$ variable for different values of the quantum yield parameter η.

4 Discussion and Conclusion

Communication distances and secret key bitrates obtained in this work can be improved when we vary the error correction function, DCR and quantum efficiency.

Our results show that the most sensitive way to increase communication distance substantially for the MDI-QKD SARG04 protocol is to decrease the DCR.

The least sensitive parameter is the error correction function $f_e(x)$ choice and in spite of exaggerating the values of the quantum efficiency in order to probe the largest possible range of communication distances, the DCR is still the most promising.

It is important to point out that our work being based on decoy-state MDI-QKD, it has been found by several workers such as Zhou *et al.* [22] that when communication resources are finite, MDI-QKD secret key rates are typically lower than that of standard decoy-state QKD. Nevertheless, a number of methods exist to circumvent this problem, such as proper basis choice along with intensity selection algorithms [22] in order to achieve longer distances.

Consequently, future research efforts along our line of work ought to be directed towards reducing DCR substantially. Statistically, progress in the experimental detector values is about one percent per year increase for the Quantum yield and about one percent per year decrease for the DCR. In order to substantially speed DCR decrease, special algorithms allowing to discriminate between different events impacting photodetector response should be urgently developed. Another challenging route for optical material scientists is to develop photo-sensitive materials possessing selective higher thresholds that would allow prevent accordingly false detection events.

References

[1] H. J. Kimble, Nature, The quantum internet **453**, 1023 (2008).
[2] B. Qi, C.-H. F. Fung, H.-K. Lo and X. Ma, Time-shift attack in practical quantum cryptosystems, Quantum Inf. Comput.**7**, 73 (2007).
[3] Y. Zhao, C.-H. F. Fung, B. Qi, C. Chen and H.-K Lo, Quantum hacking: Experimental demonstration of

time-shift attack against practical quantum-key-distribution systems Phys. Rev. A **78**, 042333 (2008).

[4] F. Xu, B. Qi and H.-K. Lo, Experimental demonstration of phase-remapping attack in a practical quantum key distribution system, New J. of Phys. **12**, 113026 (2010).

[5] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination. Nature Photon. 4, 686 (2010).

[6] I. Gerhardt, Q. Liu, A. Lamas-Linares, J. Skaar and C. Kurtsiefer, Full-field implementation of a perfect eavesdropper on a quantum cryptography system. Nature Commun. 2, 349 (2011).

[7] H. Weier, H. Krauss, M. Rau, M. Fürst, S. Nauerth and H. Weinfurter, Quantum eavesdropping without interception: an attack exploiting the dead time of single-photon detectors New J. Phys. 13, 073024 (2011).

[8] N. Jain, C. Wittmann, L. Lydersen, C. Wiechers, D. Elser, C. Marquardt, V. Makarov, and G. Leuchs, Device calibration impacts security of quantum key distribution. Phys. Rev. Lett. 107, 110501 (2011).

[9] A. N. Bugge, S. Sauge, A. M. M. Ghazali, J. Skaar, L. Lydersen and V. Makarov, Laser damage helps the eavesdropper in quantum cryptography Phys. Rev. Lett. 112, 070503 (2014).

[10] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum Key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[11] V. Scarani, A. Acín, G. Ribordy and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004); see also: V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus and M. Peev, Rev. Mod. Phys. "The security of practical quantum key distribution" **81**, 1304 (2009).

[12] H-K Lo, M. Curty and B. Qi, Measurement-device-independent quantum key distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[13] N. Abe, Y. Mitsumori, M. Sadgrove and K. Edamatsu, Dynamically unpolarized single-photon source in diamond with intrinsic randomness, Sci. Rep. 7, 46722; doi: 10.1038/srep46722 (2017).

[14] A Mizutani, K Tamaki, R Ikuta, T Yamamoto and N Imoto, Measurement-device-independent quantum key distribution for Scarani-Acin-Ribordy-Gisin 04 protocol, Sci. Rep. 4, 5236, doi: 10.1038/srep05236 (2014).

[15] C. Gobby, Z. L. Yuan and A. J. Shields, Quantum key distribution over 122 km of standard telecom fiber, App. Phys. Lett. **84**, 3762 (2004).

[16] H-K Lo, X. Ma and K. Chen, Decoy state quantum key distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[17] A. B. Carlson and P. B. Crilly *Communication systems: An Introduction to Signals and Noise in Electrical Communication*, 5th Edition, McGraw-Hill, New York (2010).

[18] X. Ma and M. Razavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[19] G. Brassard and L. Salvail, Secret-Key Reconciliation by Public Discussion, *Advances in Cryptology-Eurocrypt 1993*, edited by T. Helleseth, Lecture Notes in Computer Science Vol. 765 Springer, Berlin, p. 410 (1994).

[20] D. G Enzer, P. G Hadley, R. J Hughes, C. G Peterson and P. G Kwiat, Entangled-photon six-state quantum cryptography, New Journal of Physics **4**, 45 (2002).

[21] Y-L Tang, H-L Yin,S-J Chen, Y. Liu, W-J Zhang, X. Jiang, L. Zhang, J. Wang, L-X You, J-Y Guan, D-X Yang, Z. Wang, H. Liang, Z. Zhang, N. Zhou, X. Ma, T-Y Chen, Q. Zhang, and J-W Pan, Measurement-Device-Independent Quantum Key Distribution over 200 km, Phys. Rev. Lett. **113**, 190501 (2014).

[22] C. Zhou, W-S Bao, H-L Zhang, H-W Li, Y Wang, Y. Li and X. Wang, Biased decoy-state measurement-device-independent quantum key distribution with finite resources, Phys. Rev. A **91**, 022313 (2015).