Finite-key analysis for the 1-decoy state QKD protocol

Rusca, Davide; Boaron, Alberto; Grünenfelder, Fadri; Martin, Anthony; Zbinden, Hugo

How to cite

RUSCA, Davide et al. Finite-key analysis for the 1-decoy state QKD protocol. In: Applied Physics Letters, 2018, vol. 112, n° 17, p. 171104. doi: 10.1063/1.5023340

This publication URL: https://archive-ouverte.unige.ch/unige:107046
Publication DOI: 10.1063/1.5023340

Finite-key analysis for the 1-decoy state QKD protocol

Davide Rusca, Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden

Citation: Appl. Phys. Lett. **112**, 171104 (2018); doi: 10.1063/1.5023340
View online: https://doi.org/10.1063/1.5023340
View Table of Contents: http://aip.scitation.org/toc/apl/112/17
Published by the American Institute of Physics

Finite-key analysis for the 1-decoy state QKD protocol

Davide Rusca,[a] Alberto Boaron, Fadri Grünenfelder, Anthony Martin, and Hugo Zbinden
Group of Applied Physics, University of Geneva, Chemin de Pinchat 22, CH-1211 Geneva 4, Switzerland

(Received 23 January 2018; accepted 11 April 2018; published online 23 April 2018)

It has been shown that in the asymptotic case of infinite-key length, the 2-decoy state Quantum Key Distribution (QKD) protocol outperforms the 1-decoy state protocol. Here, we present a finite-key analysis of the 1-decoy method. Interestingly, we find that for practical block sizes of up to 10^8 bits, the 1-decoy protocol achieves for almost all experimental settings higher secret key rates than the 2-decoy protocol. Since using only one decoy is also easier to implement, we conclude that it is the best choice for QKD, in most common practical scenarios. *Published by AIP Publishing.*
https://doi.org/10.1063/1.5023340

Quantum Key Distribution (QKD) has been originally designed to work with true single-photons.[1] However, more than 30 years later, suitable deterministic single-photon sources are still not available. Therefore, in most experimental setups, convenient weak coherent laser pulses are used.[2,3] Weak coherent pulses are vulnerable to the so-called photon number splitting (PNS) attack exploiting multi-photon pulses.[4,5] This attack can be mitigated using small average photon numbers μ or particular protocols which are more resistant by design.[6–8] However, arguably the most efficient counter-measure is the so-called decoy-method.[9,10] In this method, Alice chooses randomly the average photon number among different levels μ_i and analyses statistically the probabilities of detection at Bobs in order to detect a possible PNS attack.

The decoy state protocol was proposed by Hwang,[9] and the first complete security proof of the decoy-method was given in 2005 by Lo *et al.*[10] for an infinite amount of intensities. Wang[11] showed, instead, that it was possible to employ the decoy method with only three intensities, i.e., two decoys and one signal state. Later, Ma *et al.*[12] demonstrated that in the optimal configuration, one of the two decoys must be set close to the vacuum state (vacuum + weak decoy state protocol). In the same work, a simpler method with only two intensities was presented as well, i.e., a signal and a decoy state. Its security was proved, but the achieved secret key rates (SKR) was slightly below the 2-decoy protocol. However, the analysis did not take into account the statistical correction due to a finite-key length. This was first done by Hayashi and Nakayama[13] and then by Lim *et al.*,[14] using a simpler approach, but still only for the 2-decoy configuration.

In this paper, we compare the performance of 1-decoy and 2-decoy level approaches, following the method used by Lim *et al.* in 2014. Taking into account finite size effects, we show that, interestingly, for most experimental settings, the use of only 1-decoy level is advantageous.

The previous finite-key analysis of the 2-decoy method bounded the secret key length of the protocol to the quantity[14]

$$l \leq s^l_{Z,0} + s^l_{Z,1}(1 - h(\phi^u_Z)) - \lambda_{EC} \\ -a\log_2(b/\epsilon_{sec}) - \log_2(2/\epsilon_{cor}), \tag{1}$$

where $s^l_{Z,0}$ is the lower bound on the vacuum events ($s_{Z,0}$); those events where Bob had a detection and the pulse sent by Alice contained no photons, $s^l_{Z,1}$ is the lower bound on the single-photon events ($s_{Z,1}$), defined by the number of detections at Bob side when the pulse sent by Alice contained only one photon, ϕ^u_Z is the upper bound on the phase error rate (ϕ_Z), λ_{EC} is the number of disclosed bits in the error correction stage, ϵ_{sec} and ϵ_{cor} are the secrecy and correctness parameters, and a and b depend on the specific security analysis taken into account ($a = 6$ and $b = 21$ for the 2-decoy approach and $a = 6$ and $b = 19$ for the 1-decoy protocol, see supplementary material for details).

The main contribution to the secret key is given by the single-photon events, estimated by the following formula:

$$s_{Z,1} \geq s^l_{Z,1} := \frac{\tau_1\mu_1}{\mu_1(\mu_2-\mu_3)-\mu_2^2+\mu_3^2} \\ \times\left(n^-_{Z,\mu_2} - n^+_{Z,\mu_3} + \frac{(\mu_2^2-\mu_3^2)}{\mu_1^2}\left(\frac{s_{Z,0}}{\tau_0} - n^+_{Z,\mu_1}\right)\right), \tag{2}$$

where τ_n is the total probability to send an n-photon state and $n^{\pm}_{Z,k}$ is the finite-key correction, obtained by using Hoeffding's inequality,[15] of the number of detections in the Z basis due to the state of intensity $k \in \{\mu_1, \mu_2, \mu_3\}$

$$n^{\pm}_{Z,k} := \frac{e^k}{p_k}\left(n_{Z,k} \pm \sqrt{\frac{n_Z}{2}\log\frac{1}{\varepsilon_1}}\right). \tag{3}$$

In order to find the lower bound on this expression, another lower bound on the vacuum events $s_{Z,0}$ is needed. This is easily obtained by applying the decoy state analysis.[14]

Here, we continue on the same path and apply the finite-key analysis to the 1-decoy protocol (see supplementary material for more details). Our analysis results in a secret key length bound of the same form of Eq. (1). The main difference is given by the estimation of the single-photon events. In fact, without a third intensity level, the lower bound of this quantity changes to the form

$$s_{Z,1} \geq s^l_{Z,1} := \frac{\tau_1\mu_1}{\mu_2(\mu_1-\mu_2)}\left(n^-_{Z,\mu_2} - \frac{\mu_2^2}{\mu_1^2}n^+_{Z,\mu_1} - \frac{(\mu_1^2-\mu_2^2)}{\mu_1^2}\frac{s^u_{Z,0}}{\tau_0}\right). \tag{4}$$

[a]davide.rusca@unige.ch

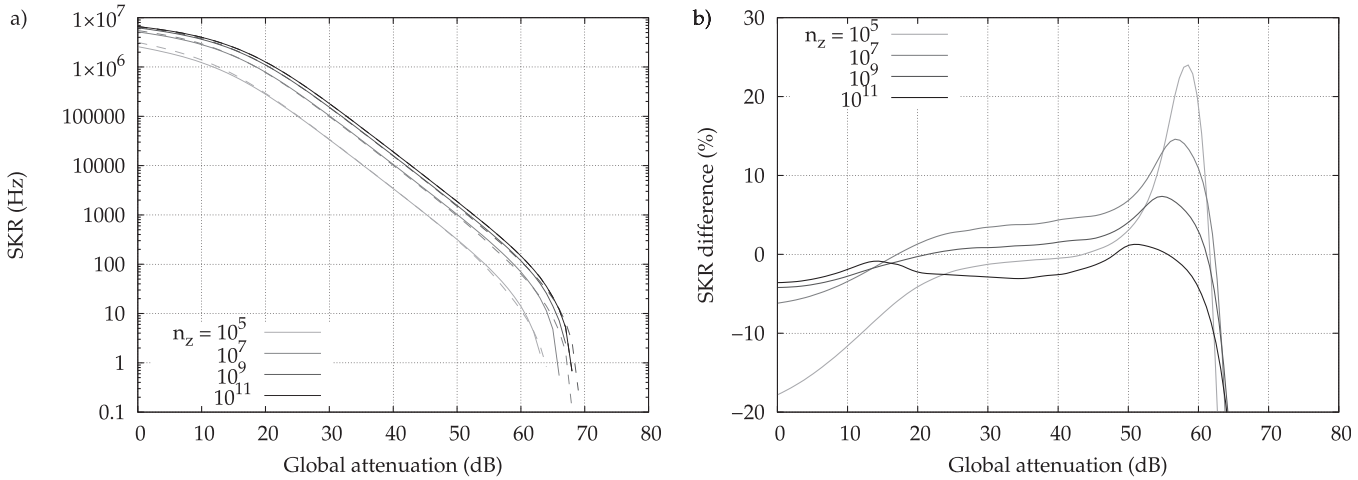

FIG. 1. (a) Comparison between different PA block sizes of the obtainable SKR considering a repetition rate of 1 GHz. For each block size, the two protocols are shown: continuous line for the 1-decoy method and dashed line for the 2-decoy method. (b) Analysis of the percentage difference between the two protocols for different PA block sizes. (SKR difference $= \frac{SKR_{1D}-SKR_{2D}}{SKR_{2D}}$).

In this case, different from the previous approach, the number of vacuum events must be upper bounded. In order to achieve this, we take into account that the probability of error from a vacuum event is 1/2. We cannot directly measure this quantity, but we can upper bound it by the total number of errors $m_{Z,k}$, for the intensity k. Considering the finite-key correction, we obtain the following relation (see supplementary material for the derivation):

$$s_{Z,0} \leq s^{u}_{Z,0} := 2\left(\tau_0 \frac{e^k}{p_k}\left(m_{Z,k} + \sqrt{\frac{m_Z}{2}\log\frac{1}{\varepsilon_2}}\right) + \sqrt{\frac{n_Z}{2}\log\frac{1}{\varepsilon_1}}\right). \tag{5}$$

This is a pessimistic estimate given that the number of errors is not only due to vacuum events, i.e., dark counts and afterpulsing of the detector and counts due to parasitic light, but also by imperfections in the preparation and measurement apparatus and quantum channel de-coherence that result in a non-vacuum state error.

In our simulation to maximize the SKR for a given global attenuation (η), we fix a number of parameters that depend on the characteristics of the devices and we optimize over a set of variables that can be easily tuned experimentally. For practicality, the efficiency of the detector and the internal losses of Bob's apparatus are included in the global attenuation η. The parameters considered are the probability of dark-count (p_{DC}), the detector dead-time (τ_{DT}), and the alignment imperfection of the devices (p_{Err}). For a given set of these parameters, we optimize the SKR over the different decoy state variables, i.e., μ_i and the associated probability p_{μ_i}, and the probability to choose the Z basis for Alice (p_{Z_a}) and Bob (p_{Z_b}).

The analysis in the asymptotic case was already carried out in previous works. Now, considering the finite-key scenario, the most important parameter is the number of detections in the Z basis. This defines the privacy amplification (PA) block size n_Z which is included in our analysis by Hoeffding's correction. In addition, we set the secrecy and correctness parameters (ϵ_{sec} and ϵ_{cor}) to the values 10^{-9} and 10^{-15}, respectively, similarly to what is commonly used in the literature.[14,16–18] In Fig. 1(a), we plot the SKR for the two different approaches and for four PA block sizes. We consider a system working at a repetition rate of 1 GHz, which, as an order of magnitude, represents the source's state of the art in QKD technologies.[17,18] For the detection apparatus, we refer to recent superconducting nanowire single-photon detectors (SNSPD)[19] which have a dead-time $\tau_{DT} = 100$ ns, dark-count rate (DCR) of 10 Hz which correspond to $p_{DC} = 10^{-8}$ and an efficiency (η_{det} around 50%). In the supplementary material, we show also the analysis taking into account an InGaAs detector.[20] The dead-time is responsible for the saturation of the SKR at short distances, whereas the DCR at long distances is the cause of the fast drop of the SKR. Indeed in this regime, the amount of valid detections becomes comparable to the random detector's dark counts, which raises the Quantum Bit Error Rate (QBER). We choose a typical value p_{Err} of 1%.

In this paragraph, we will analyse the effect of different PA block sizes to our security analysis. As we see from Fig. 1(a), by increasing the block size we increase slightly the SKR as well as the maximum transmission distance. But, in this way, the time needed to collect the data increases proportionally to the PA block size. For this reason, in real application it is preferable to use a small PA block size. By doing this, it becomes apparent from our simulation [Fig. 1(b)] that deploying 1-decoy is advantageous in most configurations. For attenuations going from 10 dB up to 60 dB, it is apparent that, unless a really big ($>10^{11}$) or really small ($<10^5$) PA block size is applied, the simpler approach gives a higher SKR. For block sizes smaller than 10^5, we see that for an attenuation between 40 dB and 60 dB [Fig. 1(b)], the advantage of the 1-decoy protocol is still present. Moreover, for small attenuation, there is no practical reason to use small PA block sizes; in fact, even for $n_z = 10^7$ at 40 dB, the acquisition time does not exceed few minutes as presented in Fig. 2.

Intuitively, in an infinite-key scenario, sending the vacuum state to better estimate, the s_0 contribution has a little positive effect on the final SKR. Indeed, in this configuration, even a small probability to send this intensity results in a good estimation on the vacuum events. In the case of a finite-key scenario, instead, this probability starts to be

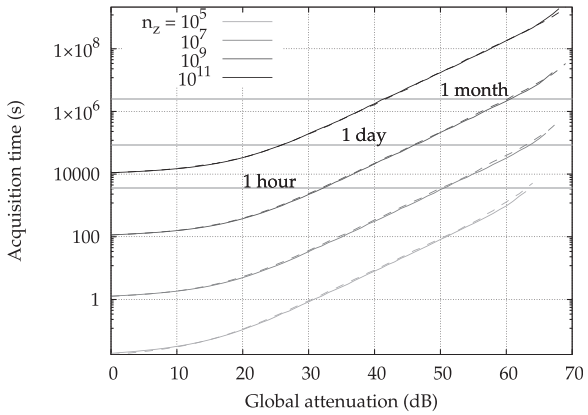

FIG. 2. Analysis of the time required to the QKD protocol when different block sizes are chosen. For each block size, the two protocols are considered, continuous line for the 1-decoy and dashed line for the 2-decoy. For the simulations, a repetition rate of 1 GHz was considered.

TABLE I. Comparison of SKR obtainable and time required for 1-decoy and 2-decoys using two different PA block sizes.

Distance	26 dB	46 dB	56 dB	64 dB
	100 km	200 km	250 km	290 km
$n_Z = 10^7$				
SKR	243 kHz	2627 Hz	227 Hz	11.3 Hz
	236 kHz	2503 Hz	197 Hz	14.1 Hz
Time	14 s	20 min	3.4 h	26 h
	16 s	23 min	3.9 h	31 h
$n_Z = 10^9$				
SKR	357 kHz	3970 Hz	356 Hz	25.5 Hz
	355 kHz	3881 Hz	333 Hz	30.7 Hz
Time	17 min	23 h	10 d	67 d
	18 min	24 h	11 d	75 d

significant for reasonable block sizes. Sending a considerable amount of vacuum states diminishes the total number of detections and consequently the SKR of the protocol. Quantitatively, when the block size chosen is $n_Z = 10^7$, the probability to send a vacuum state (p_{μ_3}) is always greater than 10% (see supplementary material); in order for this probability to go under 2%, the block size should be already greater than 10^{11}.

The 2-decoy protocol turns to be useful only for either really short or really long distances. In the first case, due to the saturation of the detectors, sending vacuum states is less detrimental. However, the attenuation at Bob's side (including the detector efficiency) could be high enough already at zero distance that the detectors are no longer in the saturation regime. In the second case, even if the key exchange is possible, the results are not interesting from a practical point of view, since the SKR obtained is on the order of magnitude of 10 Hz, whereas the acquisition time starts to exceed one day. In order to give a better understanding of our thesis, we show a comparison of acquisition time and SKR for two block sizes ($n_Z = 10^7$ and $n_Z = 10^9$) at different distances in Table I. We can see that the 1-decoy protocol almost always outperforms the 2-decoy one. The only exception within the chosen attenuations appears at 64 dB; in this case, however, the accumulation time for a PA block starts to be impractical.

Also other practical considerations suggest to always take the 1-decoy approach over the 2-decoy one. Having to implement only two intensity levels instead of three can give a net increase, both in terms of performances and cost efficiency of the whole system. At the same time, implementing one more intensity could result in an increase in the error probability in the preparation p_{Err} that would decrease the SKR.

To conclude, we presented in our work the extension of the 1-decoy protocol security to the finite-key scenario using the formalism introduced in the work of Lim *et al.*[14] By comparing the results of the finite-key effects on both 1-decoy and 2-decoy protocols, we show that for practical block sizes, the strategy of deploying the former protocol is advantageous. Indeed, despite the fact that we cannot measure the vacuum events directly, we achieve a higher SKR within a shorter acquisition time. We would like to stress that even if the difference between the two protocols is small, in practice they could result in a huge experimental and economical advantage.

See supplementary material for the complete analysis for the 1-decoy protocol.

We would like to acknowledge Charles Ci Wen Lim for the useful discussions about the security proof. We thank the Swiss NCCR QSIT and the EUs H2020 Program under the Marie Skłodowska-Curie Project QCALL (No. GA 675662) for financial support.

[1]C. H. Bennett and G. Brassard, in *International Conference on Computers, Systems & Signal Processing*, Bangalore, India, 9–12 December 1984 (1984), pp. 175–179.
[2]N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[3]V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[4]B. Huttner, N. Imoto, N. Gisin, and T. Mor, Phys. Rev. A **51**, 1863 (1995).
[5]G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000).
[6]V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).
[7]K. Inoue, E. Waks, and Y. Yamamoto, Phys. Rev. Lett. **89**, 037902 (2002).
[8]D. Stucki, N. Brunner, N. Gisin, V. Scarani, and H. Zbinden, Appl. Phys. Lett. **87**, 194108 (2005).
[9]W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).
[10]H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); e-print arXiv:0411004 [quant-ph].
[11]X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
[12]X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Phys. Rev. A **72**, 012326 (2005).
[13]M. Hayashi and R. Nakayama, New J. Phys. **16**, 063009 (2014).
[14]C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Phys. Rev. A **89**, 022307 (2014).
[15]W. Hoeffding, J. Am. Stat. Assoc. **58**, 13 (1963).
[16]B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden, Nat. Photonics **9**, 163 (2015).
[17]M. Lucamarini, K. Patel, J. Dynes, B. Fröhlich, A. Sharpe, A. Dixon, Z. Yuan, R. Penty, and A. Shields, Opt. Express **21**, 24550 (2013).
[18]B. Fröhlich, M. Lucamarini, J. F. Dynes, L. C. Comandar, W. W.-S. Tam, A. Plews, A. W. Sharpe, Z. Yuan, and A. J. Shields, Optica **4**, 163 (2017).
[19]M. Caloz, B. Korzh, N. Timoney, M. Weiss, S. Gariglio, R. J. Warburton, C. Schönenberger, J. Renema, H. Zbinden, and F. Bussieres, Appl. Phys. Lett. **110**, 083106 (2017).
[20]B. Korzh, N. Walenta, T. Lunghi, N. Gisin, and H. Zbinden, Appl. Phys. Lett. **104**, 081108 (2014).