Finite-key Security Analysis of Quantum Key Distribution with Information Leakage

Weilong Wang[1*] and Marcos Curty[1]
EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Vigo E-36310, Spain[1]

Introduction.—As one of the most promising quantum cryptographic applications, quantum key distribution (QKD) [1] has attracted great attention in recent years. This is so because in theory it can offer information-theoretic secure communications [2, 3]. Unfortunately, however, real-life implementations of QKD do not typically fulfill the assumptions made in the security proofs and thus their security cannot be guaranteed. Indeed, one key assumption in current security proofs of QKD is that Alice's and Bob's devices are perfectly isolated from Eve and they do not leak unwanted information to the channel. This assumption, however, is very difficult (if not impossible) to guarantee in practice. For instance, Eve can actively perform a so-called Trojan-Horse attack (THA) [4–6] to obtain additional side-channel information. In this attack, Eve sends bright light pulses to the users' devices and afterwards she measures the back-reflected light to extract information of their inner settings. Besides, information about the internal working of the devices can also be leaked out in a passive way like, for instance, via the power consumption of the apparatuses or via electromagnetic radiation.

Recently, the authors of Ref. [6] proposed a method to analyse the security of QKD against a particular THA specifically targeted against the phase modulators (PM) of the transmitter. More recently, the authors of Ref. [7] introduced a general formalism to prove the security of decoy-state QKD [8–10] using both phase and intensity modulators (IM) in their transmitters, which can leak their setting information to the channel in an arbitrary manner. In so doing, Ref. [7] was able to quantify the secure key rate of decoy-state QKD in the presence of leaky transmitters by considering three examples of THA. Also, they quantified the amount of isolation that is needed to achieve a certain performance. This work constitutes an important step to guarantee the security of quantum communication systems in the presence of information leakage.

Nonetheless, the results introduced in [6, 7] consider the asymptotic-key regime, i.e., they assume that Alice and Bob interchange an infinite number of signals. In real-life implementations, however, Alice can only send Bob a finite number of light pulses, which means that the users finally distill finite-length keys. This scenario has been extensively studied by several works [11–15], which analyse the finite-key security of QKD by taking the statistical fluctuations into account. However, none of these results considers the problem of information leakage. Here, we fill this gap and present a finite-key security analysis of QKD in a realistic situation where the users' devices can leak some information to Eve.

More precisely, we provide a finite-key security analysis of the standard decoy-state QKD system with three-intensity settings and a biased basis choice [16, 17] in the presence of information leakage. Note, however, that our results can be straightforwardly adapted to analyze as well any other decoy-state QKD system. Importantly, now due to the presence of information leakage, the detection events corresponding to optical pulses with the same photon number might depend on the actual intensity settings selected by Alice. As a result, one cannot use the typical counterfactual scenario which is usually employed in security proofs of decoy-state QKD, where one assumes that the intensity setting for each signal is selected *a posteriori*, that is, after Bob has already detected all the signals. To solve this problem, and also to be able to estimate the relevant quantities for the security analysis taking statistical fluctuations into account, we use Azuma's inequality [18] together with a relation between the n-photon yields associated to different intensity settings. Importantly, our analysis shows that the effect of information leakage is magnified in the finite-key regime. For instance, we can show that for a typical THA [7], when the intensity of the leaked light is as small as 10^{-12} photons/pulse, the maximum covered distance is limited to about 25km when the total number of pulses sent is 10^9. This result strongly contrasts with that in the asymptotic-key regime, where the covered distance is about 140km when the intensity of the leaked light is 10^{-12} photons/pulse [7]. Thus, our work provides an essential reference for experimentalists to implement practical QKD with information leakage.

Security analysis.—Here, we briefly sketch the main ingredients of our security analysis, which generalizes the previous works in [6, 7] to the finite-key regime. In the standard decoy-state BB84 QKD protocol, each given time, Alice selects one intensity setting from the set $\{\gamma^{\mathrm{s}}, \gamma^{\mathrm{v}}, \gamma^{\mathrm{w}}\}$ with the corresponding probabilities p_{s}, p_{v}, and $p_{\mathrm{w}} = 1 - p_{\mathrm{s}} - p_{\mathrm{v}}$, respectively. Also, Alice and Bob choose the basis $\{\mathrm{Z},\ \mathrm{X}\}$ with probabilities p_{Z} and $p_{\mathrm{X}} = 1 - p_{\mathrm{Z}}$, respectively.

To analyse the security against information leakage coming from the IM, our starting point is a relation between the expected number of events and the probability of each event in the asymptotic case [7]. In particular, let us denote the expected number of detection events by:

$$N_{\mathrm{click},\Omega,n,\gamma^j} \equiv \sum_{i=1}^{N_\Omega} P^i\left(\mathrm{click}, n, \gamma^j \,|\Omega\right), \qquad (1)$$

* wwang@com.uvigo.es

where N_Ω is the actual number of events where both Alice and Bob select the Ω basis with $\Omega \in \{\mathrm{Z},\ \mathrm{X}\}$ and $P^i\left(\mathrm{click}, n, \gamma^j \,|\Omega\right)$ denotes the conditional probability that in the ith trial Alice sends Bob an n-photon pulse with intensity setting γ^j and Bob's detector clicks given that both Alice and Bob selected the Ω basis, with $j \in \{\mathrm{s}, \mathrm{v}, \mathrm{w}\}$. Then it can be shown that the following inequality is satisfied:

$$\begin{aligned} &|N_{\mathrm{click},\Omega,n,\gamma^j} - [q_{nkl}\tfrac{p_j p_n^j}{p_k p_n^k} N_{\mathrm{click},\Omega,n,\gamma^k} \\ &+ (1-q_{nkl})\tfrac{p_j p_n^j}{p_l p_n^l} N_{\mathrm{click},\Omega,n,\gamma^l}]| \leq p_j p_n^j N_\Omega D_{\Omega,n,j,k,l}, \end{aligned} \tag{2}$$

where $p_n^j = \left(\gamma^j\right)^n e^{-\gamma^j}/n!$ is the probability that the optical pulse sent by Alice contains n photons when she selects the intensity setting γ^j, $q_{nkl} := p_k p_n^k/(p_k p_n^k + p_l p_n^l)$ with $j,k,l \in \{\mathrm{s},\mathrm{v},\mathrm{w}\}$ and

$$D_{\Omega,n,j,k,l} = \frac{1}{N_\Omega}\sum_{i=1}^{N_\Omega} D^i_{\Omega,n,j,k,l}, \tag{3}$$

where $D^i_{\Omega,n,j,k,l} := \mathrm{Tr}\left|\rho^{\gamma^j,i}_{\Omega,n}, \sigma^{\gamma^{kl},i}_{\Omega,n}\right|/2$ is defined as the trace distance between certain states $\rho^{\gamma^j,i}_{\Omega,n}$ and $\sigma^{\gamma^{kl},i}_{\Omega,n}$. Here the state $\rho^{\gamma^j,i}_{\Omega,n}$ denotes the joint state of Alice's ith n-photon pulse with intensity γ^j and Eve's system, and $\sigma^{\gamma^{kl},i}_{\Omega,n} := q_{nkl}\rho^{\gamma^k,i}_{\Omega,n} + (1-q_{nkl})\,\rho^{\gamma^l,i}_{\Omega,n}$. Basically, the parameter $D_{\Omega,n,j,k,l}$ quantifies how well can Eve distinguish the joint state of Alice's output n-photon signals together with the back-reflected light (coming from the THA) for different intensity settings.

Next, we relate the expected numbers of detected events with the actual numbers of detected events, which we shall denote by $\left|\Omega^j_n\right|$, plus the corresponding deviation terms due to statistical fluctuations. We obtain

$$N_{\mathrm{click},\Omega,n,\gamma^j} \equiv \sum_{i=1}^{N_\Omega} P^i\left(\mathrm{click}, n, \gamma^j\,|\Omega\right) = \left|\Omega^j_n\right| + \delta_{\Omega^j_n}, \tag{4}$$

where $\delta_{\Omega^j_n}$ denotes the deviation term due to statistical fluctuations. This quantity lies in an interval $[-\Delta_{\Omega^j_n}, \widehat{\Delta}_{\Omega^j_n}]$ except with error probability $\varepsilon_{\Omega^j_n} + \widehat{\varepsilon}_{\Omega^j_n}$, where the bounds $\Delta_{\Omega^j_n}$ and $\widehat{\Delta}_{\Omega^j_n}$ satisfy $\Delta_{\Omega^j_n} = g_A(N_\Omega, \varepsilon_{\Omega^j_n})$ and $\widehat{\Delta}_{\Omega^j_n} = g_A(N_\Omega, \widehat{\varepsilon}_{\Omega^j_n})$, with $g_A(x,y) = \sqrt{2x\ln(1/y)}$ [18]. In so doing, we obtain a set of linear equations that relate the detection events corresponding to different intensity settings taking statistical fluctuations into consideration. From this set of linear equations we can estimate some parameters needed to calculate the secure key rate like, for instance, $|\Omega^{\mathrm{s}}_1|$.

As for the information leakage coming from the PM, Eve can also try to perform a THA to learn partial information about Alice's basis choice each given time. As a consequence, we need to reexamine the estimation of the phase error rate. This is solved by using the concept of 'quantum coin' [19] and by applying the Bloch sphere bound [20]. This way, we can derive expressions that relate the phase error rate with the expected number of error events in the asymptotic case [7]. Finally, by using Azuma's inequality [18], we can relate the actual number of error events (plus the corresponding deviation terms) with the expected number of error events, and thus we can derive an expression for the phase error rate in the finite-key regime. This last process also requires to solve a set of linear equations.

Simulation results—To evaluate our results, we consider a particular type of THA, where Eve sends high-intensity coherent pulses to Alice. Then by measuring the back-reflected light, which we assume, for simplicity, is still a coherent state, Eve can extract side-channel information of Alice's inner settings. To illustrate the effect of information leakage on the secure key rate in the finite-key regime, we consider the worst-case scenario where the intensity of the back-reflected light is upper bounded by a quantity, I_{max}, but Eve can freely choose the phases of the different output coherent states to maximize her knowledge of Alice's inner settings. To solve the sets of linear equations involved in the calculation, we use the linear programming package 'linprog' from Matlab. In this way, we calculate all the quantities that are needed to determine the secure key rates. The results are shown in Figs. 1 and 2.

Fig. 1 shows the effect of the finite data block sizes on the secure key rate for a fixed value of the intensity of the leaked light, $I_{max} = 10^{-12}$. We can see that compared to the asymptotic case (where we also assume that $I_{max} = 10^{-12}$), the fact that Alice sends a finite number of pulses indeed has a great impact on the secure key rates. This indicates that in the presence of information leakage, it is necessary to use much larger data block sizes for obtaining a similar performance to that where there is no information leakage. From Fig. 2, we can see that when I_{max} is no larger than 10^{-11}, the secure key rates in the presence of a THA differ just a little bit and are close to those of a perfectly isolated system given that the data block size is large enough. When I_{max} increases, the difference between the secure key rates becomes bigger. Particularly, when I_{max} reaches 10^{-7}, the users cannot obtain secure keys over 45km even if the number of pulses sent is as large as 10^{12}.

Conclusions—We have analysed the security of QKD with information leakage in the finite-key regime. To illustrate our results, we have simulated the secure key rate of a standard three-intensity decoy-state QKD protocol with a biased basis choice against particular examples of THA. Our results show that both the information leakage and the finite-key effect have a great impact on the secure key rates. One could readily use our analysis to quantify the amount of isolation that is needed to achieve a certain performance as a function of the data block size interchanged. In addition, let us mention that we have applied a similar analysis to measurement-device-independent QKD (MDI-QKD) [21] by considering information leakage from both Alice's and Bob's de-

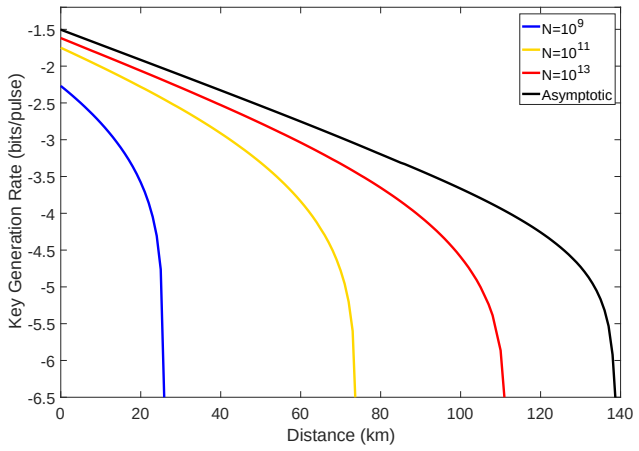

FIG. 1. Secure key rate in logarithmic scale as a function of the distance in the presence of a THA. Each colour corresponds to a different value of the total number of pulses sent by Alice, N, with a fixed value of the intensity of the leaked light, $I_{max} = 10^{-12}$. The black line represents the asymptotic case where Alice sends an infinite number of pulses.

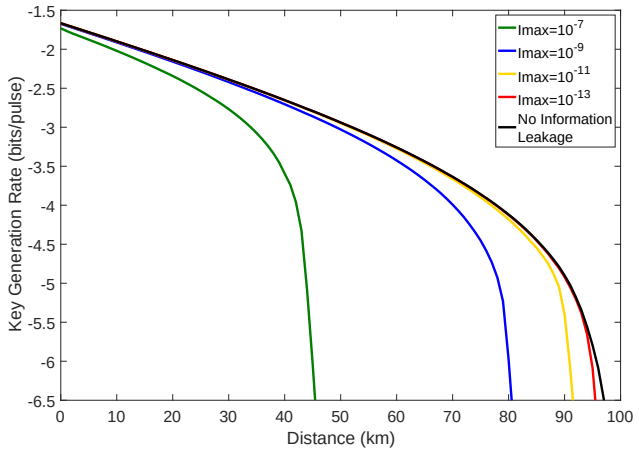

FIG. 2. Secure key rate in logarithmic scale as a function of the distance in the presence of a THA. Each colour corresponds to a different value of the intensity of the leaked light, I_{max}, with a fixed value of the total number of pulses sent by Alice, $N = 10^{12}$. The black line represents the ideal case of no information leakage.

vices. There, we can show the presence of information leakage has even a higher impact than that in the standard decoy-state QKD scheme. Indeed, for each data block size, it turns out that the maximum intensity of the leaked light should be at most about $I^2_{\max}$ to achieve a similar performance to that of the standard decoy-state QKD.

Acknowledgments—This work was supported by the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through grant TEC2014-54898-R and the European Commission under project "QCALL" (H2020-MSCA-ITN-2015, project 675662). W.W. gratefully acknowledges support from the National Natural Science Foundation of China under Grant No. 61472446.

[1] C. H. Bennett and G. Brassard, in *International Conference on Computer System and Signal Processing, IEEE* (1984) pp. 175–179.
[2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Reviews of Modern Physics **81**, 1301 (2009).
[3] H.-K. Lo, M. Curty, and K. Tamaki, Nature Photonics **8**, 595 (2014).
[4] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Physical Review A **73**, 022320 (2006).
[5] N. Jain, B. Stiller, I. Khan, V. Makarov, C. Marquardt, and G. Leuchs, Selected Topics in Quantum Electronics, IEEE Journal of **21**, 168 (2015).
[6] M. Lucamarini, I. Choi, M. B. Ward, J. F. Dynes, Z. Yuan, and A. J. Shields, Physical Review X **5**, 031030 (2015).
[7] K. Tamaki, M. Curty, and M. Lucamarini, New Journal of Physics **18**, 065008 (2016).
[8] W.-Y. Hwang, Physical Review Letters **91**, 057901 (2003).
[9] H.-K. Lo, X. Ma, and K. Chen, Physical Review Letters **94**, 230504 (2005).
[10] X.-B. Wang, Physical Review Letters **94**, 230503 (2005).
[11] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).
[12] M. Hayashi and T. Tsurumaru, New Journal of Physics **14**, 093014 (2012).
[13] M. Curty, F. Xu, W. Cui, C. C. W. Lim, K. Tamaki, and H.-K. Lo, Nature Communications **5** (2014).
[14] C. C. W. Lim, M. Curty, N. Walenta, F. Xu, and H. Zbinden, Physical Review A **89**, 022307 (2014).
[15] A. Mizutani, M. Curty, C. C. W. Lim, N. Imoto, and K. Tamaki, New Journal of Physics **17**, 093011 (2015).
[16] H.-K. Lo, H. F. Chau, and M. Ardehali, Journal of Cryptology **18**, 133 (2005).
[17] Z. Wei, W. Wang, Z. Zhang, M. Gao, Z. Ma, and X. Ma, Scientific Reports **3**, 2453 (2013).
[18] K. Azuma, Tohoku Mathematical Journal, Second Series **19**, 357 (1967).
[19] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, in *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on* (IEEE, 2004) p. 136.
[20] K. Tamaki, M. Koashi, and N. Imoto, Physical Review Letters **90**, 167904 (2003).
[21] H.-K. Lo, M. Curty, and B. Qi, Physical Review Letters **108**, 130503 (2012).