Security of continuous-variable quantum key distribution with coarse-grained detector

Zhengyu Li[1], Yichen Zhang[2], Christian Weedbrook[3], and Hong Guo[1]*
[1] *State Key Laboratory of Advanced Optical Communication Systems and Networks, School of Electronics Engineering and Computer Science, and Center for Quantum Information Technology, Peking University, Beijing 100871, China*
[2] *State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing 100876, China and*
[3] *CipherQ, 10 Dundas St E, Toronto, M5B 2G9, Canada*
(Dated: April 2016)

In practical continuous-variable quantum key distribution (CV-QKD) system, the homodyne or heterodyne detector is cascaded with an analog-to-digital converter (ADC) to sample the measurement results, with only a finite sampling range and resolution. The ADC's coarse-grained property can lead to the loss of detailed information with respect to the quadratures, which may potentially compromise the security if the outputs are directly used for parameter estimation. Here we propose a method to analyze the security of a CV-QKD system with coarse-grained detectors in finite-size conditions, which enhances the practical security of a CV-QKD system.

PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) can generate secure keys remotely through an insecure quantum channel, among which continuous-variable (CV) QKD [1, 2] is one of the two main branches. CV-QKD using coherent states [3] shares similar technologies with standard telecommunication systems, however they need to be modified to fulfill the requirements of quantum security. For instance, the homodyne or heterodyne detector should be quantum shot-noise-limited. Therefore, although the theoretical security of a CV-QKD protocol has been proven in many conditions [4–8], the practical security of a system relies on the property of the practical devices.

Among all devices, the receiver's detector plays a crucial role, since it provides the information of a rough "tomography" of the channel which has presumably been eavesdropped and hence determines the final secret key length. A practical detector consists of two stages, and each has its imperfections. The first is the homodyne or heterodyne detection, which has finite detection efficiency, electronics noise and the saturation problem of the amplifier. The second is the analog-to-digital (ADC) conversion, which has sampling noise, finite sampling range and finite resolution.

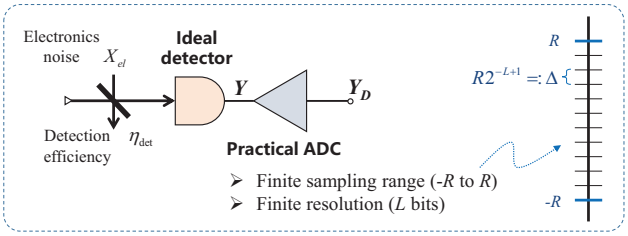

FIG. 1: The model of a practical homodyne or heterodyne detector, which consists of three main parts. The first is a beam splitter and thermal noise in order to model the finite detection efficiency and the electronic noise. The second is an ideal detector, and the third is a practical analog-to-digital converter (ADC) with finite sampling range and resolution.

Thus, we model the practical detector as shown in Fig. 1, which consists of three parts. First, the finite detection efficiency and the electronics noise are modeled as a beam splitter, whose transmittance equals the detection efficiency $\eta_{\det}$, coupling the signal with a thermal noise, whose variance is related to the electronics noise and the sampling noise. The second part is an ideal detector, which outputs the real quadrature measurement result, denoted as Y. The third part is a practical ADC, which only has a finite sampling range (say from $-R$ to R) and resolution (say L digitized bits).

Suppose the ADC's digitization map is as follows:

$$Y_D = \begin{cases} \frac{1}{2}\Delta - R, & -\infty \le Y < \Delta - R; \\ \left(i+\frac{1}{2}\right)\Delta - R, & i\Delta - R \le Y < (i+1)\Delta - R; \\ -\frac{1}{2}\Delta + R, & -\Delta + R \le Y < +\infty, \end{cases} \tag{1}$$

where $1 \le i < 2^L - 1$. Generally speaking, the extra loss and noise in the first part only influences the performance of the system, which is well studied in previous papers [9]. On the other hand, the coarse-grained property of the third part can affect the security analysis, which if ignored, the practical security of a system may be compromised. This is because in current security analyzes it requires the real quadrature measurement result Y, not the digitized output Y_D which only contains partial information of Y.

More specifically,

1. The finite sampling range makes Y_D lack of the information about Y when it is out of the range $[-R, R]$. Each $|Y_i| \ge R$ only gives the output $Y_D = R$ or $-R$, which makes the estimation of Bob's variance V_B smaller than the actual case, and this leads to the underestimation of the excess noise. This may open a security

*Corresponding author: hongguo@pku.edu.cn

loophole similar as the saturation attack [10].

2. The finite sampling resolution makes Y_D lack of the information about Y within each sampling interval. This also influence the estimation of the covariance matrix.

Here, we propose a method to analyze the security of CV-QKD with a practical ADC under finite-size conditions, which directly comes from the universal composable security analysis given in [8], i.e., a simple modification of the parameter estimation step. The relations between the total data length n, ADC sampling range R, and the digitized bits L are analyzed. A composition of (n, R, L) suitable for metropolitan area networks is found, which can be achieved with current technologies.

First, we note that in the universal composable security analysis of CV-QKD using Gaussian modulated squeezed states and homodyne detector [7], the above sampling problems are automatically solved, because what the uncertainty principle used is the correlation between Alice and Bob's final data. The digitization from Y to Y_D only decreases the performance, and will not influence the security. Thus, we only focus on the case of CV-QKD using gaussian modulated coherent states and heterodyne detector [11].

In the universal composable security analysis [8], the secret key length l under collective attack is

$$\begin{aligned} l \leq & 2n\left[2\hat{H}_{MLE}\left(U\right)-f\left(\Sigma_a^{\max},\Sigma_b^{\max},\Sigma_c^{\min}\right)\right] \\ & -\mathrm{leak}_{EC}-\Delta_{\mathrm{AEP}}-\Delta_{\mathrm{ent}}-2\log\left(1/2\bar{\epsilon}\right), \end{aligned} \tag{2}$$

where Δ_{AEP} and Δ_{ent} are related to the data length n and the security parameters ϵ, ϵ_{sm}. $\hat{H}_{MLE}\left(U\right)$ is the empiric entropy of U. f is the Holevo information between Bob and Eve according to a covariance matrix characterized by the pre-set parameters $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$.

The key step of universal composable security analysis is the parameter estimation test, in which Alice first estimates the parameters as following:

$$\begin{aligned} \gamma_a &:= \frac{1}{2n}\left[1+2\sqrt{\frac{\log\left(36/\epsilon_{PE}\right)}{n}}\right]\|X\|^2-1, \\ \gamma_b &:= \frac{1}{2n}\left[1+2\sqrt{\frac{\log\left(36/\epsilon_{PE}\right)}{n}}\right]\|Y\|^2-1, \\ \gamma_c &:= \frac{1}{2n}\langle X,Y\rangle-5\sqrt{\frac{\log\left(8/\epsilon_{PE}\right)}{n^3}}\left(\|X\|^2+\|Y\|^2\right), \end{aligned} \tag{3}$$

where X is Alice's ideal data. Then she compares these three values with the pre-set parameters: $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$. If the condition $\left[\gamma_a \leq \Sigma_a^{\max}\right] \wedge \left[\gamma_b \leq \Sigma_b^{\max}\right] \wedge \left[\gamma_c \geq \Sigma_c^{\min}\right]$ is fulfilled, then the secret key length will be the same as Eq. (2). Otherwise, the protocol aborts (PE test fails).

In the above parameter estimation step, $\gamma_a, \gamma_b, \gamma_c$ should be calculated from the real quadrature measurement result Y[12]. Since we only have the digitized data Y_D, thus we propose to use the following modification methods of the data Y_D to give an upper bound of γ_b and a lower bound of γ_c.

1) To calculate the upper bound of γ_b, each Y_D should be modified to reach the upper bound of $\|Y\|^2$ even if it is infinity:

$$Y_D' = \begin{cases} -\infty, & Y_D = \frac{1}{2}\Delta - R; \\ Y_D - \frac{1}{2}\Delta, & \frac{1}{2}\Delta - R < Y_D < 0; \\ Y_D + \frac{1}{2}\Delta, & -\frac{1}{2}\Delta + R > Y_D > 0; \\ +\infty, & Y_D = -\frac{1}{2}\Delta + R \end{cases} \tag{4}$$

2) To calculate the lower bound of γ_c, if $X < 0$, then Y_D should be modified as

$$Y_D'' = \begin{cases} Y_D + \frac{1}{2}\Delta, & -\frac{1}{2}\Delta + R > Y_D; \\ +\infty, & Y_D = -\frac{1}{2}\Delta + R. \end{cases} \tag{5}$$

If $X > 0$, then Y_D should be modified as

$$Y_D'' = \begin{cases} Y_D - \frac{1}{2}\Delta, & \frac{1}{2}\Delta - R < Y_D; \\ -\infty, & Y_D = \frac{1}{2}\Delta - R. \end{cases} \tag{6}$$

Then use the upper and lower bounds to do the PE test. After the above modification, to ensure a high probability of passing the PE test, the pre-set parameters $\Sigma_a^{\max}, \Sigma_b^{\max}, \Sigma_c^{\min}$ should choose a worse case, which will decrease the secret key length. In this way, the calculated secret key length is secure under the practical ADC condition.

One could note that, if there is one (or more than one) Y_D is the highest output $R - \frac{1}{2}\Delta$ or the lowest output $-R + \frac{1}{2}\Delta$, then the PE test will fail. Therefore, the sampling range R should be large enough to make the probability of having at least one extreme output $P_{\infty|n,R}$ enough small, to ensure a high probability of passing the PE test. This means the data length n is no longer the larger the better. If one needs to increase n to suppress the finite-size effect, then R should also be enlarged.

When passes the parameter estimation test, the deviation of γ_b, γ_c caused by the modification of Y_D is of

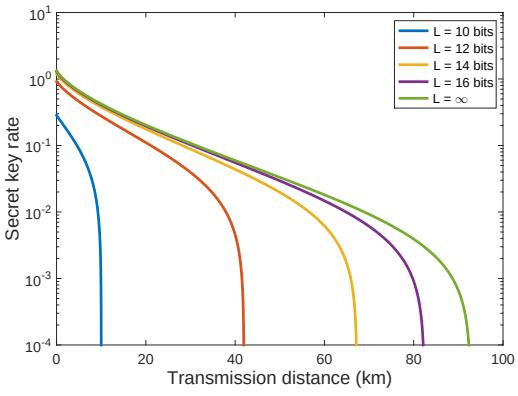

FIG. 2: Secret key rate of different digitized bits L when the data length is fixed as $n = 10^{12}$. $L = 10$ to 16 correspond to the solid lines from left to right.

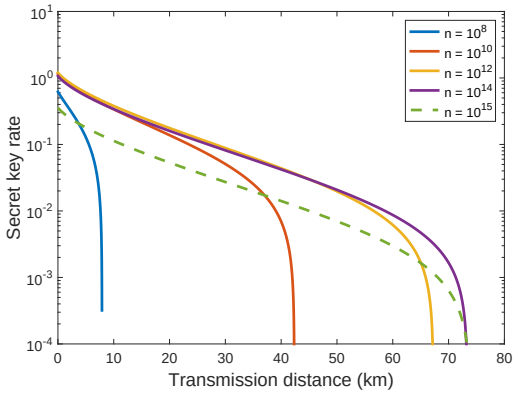

FIG. 3: Secret key rate of different data length n when the digitized bits is fixed as $L = 14$. $n = 10^8$ to 10^{14} correspond to the solid lines from left to right respectively. 10^{15} corresponds to the dashed line.

the first order of Δ. Thus, when R increases, the digitized bits L should also be enlarged, to make the Δ small enough. However, the L and n is constrained by current technologies, one needs to find a trade-off between these three parameters.

To explore the possibility of a realizable composition of (n, R, L), we do the simulation under following conditions: Alice's variance $V_A = 5$, channel excess noise $\varepsilon = 0.01$, reconciliation efficiency $\beta = 0.95$, channel loss $a = 0.2$dB/km, and we choose $R = 8\sqrt{V_B}$ for each transmission distance.

Fig. 2 shows the secret key rate l/n, when the data length is fixed as $n = 10^{12}$, while the digitized bits L is changed from 10 to 16 (corresponding to the solid lines from left to right respectively). As analyzed above, when L increases, the performance of the protocol gets enhanced.

Fig. 3 shows the secret key rate, when the digitized bits is fixed as $L = 14$, while the data length n changes from 10^8 to 10^{15}. $n = 10^8$ to 10^{14} corresponding to the solid lines from left to right respectively. 10^{15} corresponds to the dashed line. One could find that when the data length is not too large, as n increases, the performance of the protocol increases. However, since the R is fixed, when n is large enough to decrease the probability of passing the PE test, although the transmission distance does not decrease, the secret key rate decreases.

From the above simulation, we can find a realizable composition of $(n, R, L) = (10^{10}, 8\sqrt{V_B}, 14)$, which makes the secret key rate greater than 10^{-3} at 40km, a typical distance between two stations of classical fiber communication. For a 1GHz system, it takes around 10s to gathering enough data for post-processing. And a 14-bits commercial ADC with 1GS/s sampling rate is also achievable.

In summary, the coarse-grained property of a heterodyne detector, due to the finite sampling range and resolution of a practical ADC, may open a security loophole of CV-QKD protocol using Gaussian modulated coherent states. We propose a simple modification method of Bob's data to solve this loophole under the universal composable framework, which enhances the practical security of a CV-QKD system.

The author would like to thank Yanbao Zhang and Patrick J. Coles for interesting discussion. This work is supported by the National Science Fund for Distinguished Young Scholars of China (Grant No. 61225003), the State Key Project of National Natural Science Foundation of China (Grant No. 61531003).

[1] S. L. Braunstein and P. van Loock, Rev. Mod. Phys. **77**, 513 (2005).
[2] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[3] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[4] R. Garcia-Patron and N. J. Cerf, Physical review letters **97**, 190503 (2006).
[5] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[6] R. Renner and J. I. Cirac, Physical review letters **102**, 110504 (2009).
[7] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, Phys. Rev. Lett. **109**, 100502 (2012).
[8] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[9] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B: At. Mol. Opt. Phys. **42**, 114014 (2009).
[10] H. Qin, R. Kumar, and R. Alléaume, in *SPIE Security+ Defence. International Society for Optics and Photonics,*"Saturation attack on continuous-variable quantum key distribution system" (2013).
[11] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[12] For simplicity, we assume Alice's data is ideal. The non-ideal case shares a similar modification method as Bob's.