Finite-key-size effect in commercial plug-and-play QKD system

Poompong Chaiwongkhot,[1,2,*] Shihan Sajeed,[1,3] Lars Lydersen,[4] and Vadim Makarov[1,2,3]

[1] *Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[2] *Department of Physics and Astronomy, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[3] *Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON, N2L 3G1 Canada*
[4] *Department of Electronics and Telecommunications, Norwegian University of Science and Technology, NO-7491 Trondheim, Norway*

(Dated: May 6, 2016)

This study is aimed to emphasize the significance of finite-key-size effects on a practical system. The goal is to demonstrate the ability of Eve to force the system to generate a secret key from a raw key size that is smaller than which was predicted in the system design. As a result, the asymptotic limit employed in the system might no longer hold. The subject of this study is a plug-and-play QKD system Clavis2 produced by ID Quantique 1. The security of this system implemented in the manufacturer's software is based on the security analysis in Ref. 2 which did not considered the finite-key-size effect.

Quantum channel of Alice and Bob consisted of a 2 m long optical fiber and a variable attenuator (OZ Optics DD-100-11-1550) simulating transmission loss of a longer line and also giving Eve the ability to control it. We ran multiple sessions of key distribution with quantum channel transmission loss of 2, 3 and 4 dB. After the system exchange the raw key for a set period, from 10–280 s in each session, then adjusted the channel loss to 40 dB which terminated the raw key exchange. After that, the system began the post-processing out of the raw key that had already been exchanged. At the same time, we reset the variable attenuator to the original loss value. The system returned to the synchronization step, and began a new session of key exchange.

We substituted the parameters from each session of the experiment into key rate equation under finite-key-size analysis [3–6] and plotted in Fig.1. Black $\times$ are experimental results with (a) 2 dB line loss and 3% error rate, (b) 3 dB line loss with 5% error rate, and (c) 4 dB line loss with 6% error rate. Blue (dark grey) line is the infinite key bound. Red (grey) line is finite-key size bound with $\epsilon = 10^{-10}$. Green (light grey) line is finite-key-size bound with $\epsilon = 10^{-1}$. Secure key bounds in each subfigure were calculated separately according to the error rate and line loss of each experiment. The result showed that the experimentally distilled key sizes satisfied the security criteria for the asymptotic assumption. However, the experimental results fall out of bound of finite-key size analysis with values of ϵ up to 10^{-1}.

In the middle of our study in 2014, ID Quantique released a new software patch for Clavis2. This patch accumulates the key if the key exchange session is terminated and lets the system perform post-processing only when the raw key size exceeds a threshold of around 2 Mbit.

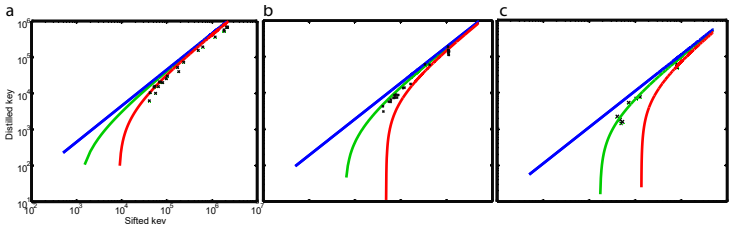

FIG. 1. Secret key rate versus sifted key rate.

We performed our experiment and recalculated our plot using the new parameters acquired from the system. The result showed that the distilled key is within the secure bound of $\epsilon = 10^{-10}$.

Our study only covers statistical evidence from the system against the theoretical bound. An explicit attack that exploits this effect is still open for future study. Our investigation highlights the significance of finite-key-size analysis and why this effect should be included in the implementations of QKD, especially in commercial systems.

We thank N. Lütkenhaus, R. Renner, and J. Skaar for discussions. We thank ID Quantique for cooperation, technical assistance, and providing us the QKD hardware. This work was supported by Industry Canada, NSERC, CFI and Ontario MRI. P.C. and S.S. acknowledge support from CryptoWorks21. P.C. acknowledges support by Thai DPST scholarship.

* poompong.ch@gmail.com

[1] Clavis2 specification sheet, `http://www.idquantique.com/images/stories/PDF/clavis2-quantum-key-distribution/clavis2-specs.pdf`, visited 25 May 2015.
[2] A. Niederberger, V. Scarani, and N. Gisin, Phys. Rev. A **71**, 042316 (2005).
[3] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comp. **4**, 325 (2004).
[4] R. Renner, N. Gisin, and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
[5] R. Y. Q. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).
[6] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nat. Commun. **3**, 634 (2012).