Finite-key analysis for subcarrier wave quantum key distribution

Anton Kozubov,* Andrei Gaidash, and George Miroshnichenko
Department of Photonics and Optical Information Technology,
ITMO University,199034 Kadetskaya Line 3b, Saint Petersburg, Russia

Arthur Gleim
Department of Photonics and Optical Information Technology,
ITMO University,199034 Kadetskaya Line 3b, Saint Petersburg, Russia and
Kazan National Research Technical University,
Karl Marx str. 10, Kazan, 420111, Russia

(Dated: August 9, 2018)

We show the finite-key analysis for subcarrier wave quantum key distribution systems using a fully quantum asymptotic equipartition property technique. This approach is implemented for the real subcarrier wave quantum key distribution system for the first time.

INTRODUCTION

Growing interest to quantum key distribution (QKD) systems [1, 2] in the last decades has led to emergence of a large number of experimental works dedicated to developing reliable QKD setups suitable for everyday operation in existing telecommunication networks. Among them stand subcarrier wave (SCW) QKD systems, the most valuable feature of which is exceptionally efficient use of quantum channel bandwidth and capability of signal multiplexing by adding independent sets of quantum subcarriers around the same carrier wave. It makes SCW QKD systems perfect candidates as a backbone of multiuser quantum networks.

Nevertheless security proofs for different QKD systems still requires special consideration. There are various approaches to consider security against general attacks. In this work we introduce first implementation of finite-key analysis to the real SCW QKD system.

FINITE-KEY ANALYSIS FOR SUBCARRIER WAVE QUANTUM KEY DISTRIBUTION

Despite the significant experimental effort in the development of SCW QKD systems[3–6, 8], their security analysis still requires special consideration. Security proof against collective attacks was introduced in [9]. However finite-key analysis for SCW QKD protocols was missed until now. In information theory, the "randomness" of one half of a joint system conditioned on having access to the other half can be quantified with the *ε-smooth min-entropy*, $H^{\varepsilon}_{\min}(\mathbf{A}|\mathbf{E})$. However, the smooth entropies of a large system are often difficult to calculate. Some approaches, such as the fully quantum asymptotic equipartition property (AEP)[10], overcome this difficulty by assuming that the protocol rounds are independent and identically distributed (IID). Roughly speaking, it means that for a large number of such rounds, the operationally relevant total uncertainty can be well approximated by the sum over all IID rounds.

After the quantum states are sent and measured, Alice and Bob each have n-bit strings $\mathbf{A}, \mathbf{B}$, with Eve's side-information being denoted by $\mathbf{E}$. The fully quantum AEP tells us that for any $\varepsilon > 0$, we have

$$H^{\varepsilon}_{min}(\mathbf{A}|\mathbf{E}) \geq n\left(H(\mathbf{A}|\mathbf{E}) - \frac{\delta(\varepsilon)}{\sqrt{n}}\right), \quad (1)$$

$$H^{\varepsilon}_{max}(\mathbf{A}|\mathbf{B}) \leq n\left(H(\mathbf{A}|\mathbf{B}) + \frac{\delta(\varepsilon)}{\sqrt{n}}\right), \quad (2)$$

where

$$\delta(\varepsilon) = 4\log\eta\sqrt{\log\frac{2}{\varepsilon^2}}, \quad (3)$$

where η is entropy convergence parameter and we maximize it as $\eta = 2+\sqrt{2}$. Also we use Theorems 1 and 2 from [11] as follows:

$$H^{\varepsilon+\varepsilon}_{min}(\mathbf{A}|\mathbf{E}) \geq H^{\varepsilon}_{min}(\mathbf{A}|\mathbf{E}) - 2\log_2\frac{1}{\varepsilon'}, \quad (4)$$

$$H^{\varepsilon+\varepsilon'}_{max}(\mathbf{A}|\mathbf{B}) \leq H^{\varepsilon}_{max}(\mathbf{A}|\mathbf{B}) + \log_2\frac{1}{\varepsilon'}. \quad (5)$$

Applying this technique to our system we obtain the final expression for the length of the extracted key:

$$K = (n-k)(1 - H(\mathbf{A}|\mathbf{E}) - \frac{\delta(\varepsilon_S)}{\sqrt{n-k}}) - \quad (6)$$
$$- \mathit{code}_{EC} - \sqrt{n}\delta(\varepsilon_S) - 2\log_2\frac{1}{\varepsilon_{PA}} - \log_2\frac{1}{\varepsilon_{EC}},$$

where k is the amount of bits used for estimating the number of errors are discarded completely, and $H(\mathbf{A}|\mathbf{E})$ is the conditional von Neumann entropy and code_{EC} is the number of bits

[*] avkozubov@corp.ifmo.ru

sent when the error correction protocol is implemented (LPDC code).

RESULTS

In this work finite-key analysis based on fully quantum asymptotic equipartition property technique the real SCW QKD system was shown for the first time.

The obtained results are important for constructing real secure long-distance QKD links and multiuser quantum networks by exploiting advantages of the SCW QKD: ultra-high QKD bandwidth capacity and compatibility with the existing optical communication infrastructure.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lütkenhaus, and M. Peev, “The security of practical quantum key distribution,” Rev. Mod. Phys, **81**, 1301 (2009).

[2] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, “Practical challenges in quantum key distribution,” NPJ Quantum. Inf. **2**, 16025 (2016).

[3] J.-M. Merolla, Y. Mazurenko, J.-P. Goedgebuer, and W. T. Rhodes, “Single-photon interference in sidebands of phase-modulated light for quantum cryptography,” Phys. Rev. Lett. **82**, 1656 (1999).

[4] J.-M. Merolla, L. Duraffourg, J.-P. Goedgebuer, A. Soujaeff, F. Patois, and W. T. Rhodes, “Integrated quantum key distribution system using single sideband detection,” Eur. Phys. J. D **18**, 141–146 (2002).

[5] J. Mora, W. Amaya, A. Ruiz-Alba, A. Martinez, D. Calvo, V. Garcia Munoz, and J. Capmany, “Simultaneous transmission of 20x2 WDM/SCM-QKD and 4 bidirectional classical channels over a PON,” Opt. Express **20**, pp. 16358–16365 (2012).

[6] O. Guerreau, F. J. Malassenet, S. W. McLaughlin, and J.-M. Merolla, “Quantum key distribution without a single-photon source using a strong reference,” IEEE Photonics Technol. Lett. **17**, 1755–1757 (2005).

[7] M. Koashi, “Unconditional security of coherent-state quantum key distribution with a strong phase-reference pulse,” Phys. Rev. Lett. **93**, 120501 (2004).

[8] A. V. Gleim, V. I. Egorov, Yu. V. Nazarov, S. V. Smirnov, V. V. Chistyakov, O. I. Bannik, A. A. Anisimov, S. M. Kynev, A. E. Ivanova, R. J. Collins, S. A. Kozlov, and G. S. Buller,“Secure polarization-independent subcarrier quantum key distribution in optical fiber channel using BB84 protocol with a strong reference,” Opt. Express **24**, pp. 2619–2633 (2016).

[9] G. P. Miroshnichenko, A. V. Kozubov, A. A. Gaidash, A. V. Gleim, D. B. Horoshko “Security of subcarrier wave quantum key distribution against the collective beam-splitting attack,”Opt. Express **26**, 9.

[10] M. Tomamichel, R. Colbeck, and R. Renner. A fully quantum asymptotic equipartition property. IEEE Trans. Inform. Theory, 55:5840–5847, 2009. arXiv:0811.1221.

[11] Renner, Renato, and Stefan Wolf. "Simple and tight bounds for information reconciliation and privacy amplification." International Conference on the Theory and Application of Cryptology and Information Security. Springer, Berlin, Heidelberg, 2005.