

Security Proof for QKD Systems with Threshold Detectors

Toyohiro Tsurumaru (1), Kiyoshi Tamaki (2, 3)

1: Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501, Japan, Tsurumaru.Toyohiro@da.MitsubishiElectric.co.jp

2: NTT Basic Research Laboratories, NTT Corporation, 3-1 Morinosato Wakamiya, Atsugi-shi, Kanagawa, 243-0198, Japan

3: CREST, JST Agency, 4-1-8 Honcho, Kawaguchi, Saitama, 332-0012, Japan

Abstract

We rigorously prove the intuition that in security proofs for BB84 one may regard an incoming signal to Bob as a qubit state. From this result, it follows that all security proofs for BB84 based on a virtual qubit entanglement distillation protocol, which was originally proposed by Lo and Chau [3], and Shor and Preskill [4], are all valid even if Bob's actual apparatus cannot distill a qubit state explicitly. Using the same technique, we also prove the security of the BBM92 protocol where Alice and Bob both use threshold detectors.

Introduction

Quantum key distribution (QKD) is a way to share secret keys between separated parties (Alice and Bob) with negligibly small leakage of its information to an unauthorized third party, Eve. The first QKD protocol, BB84, was introduced by Bennett and Brassard in 1984 [1], and its unconditional security was first proven by Mayers [2] in a bit complicated manner. After the first proof, researchers have tried to prove its security in a simple manner. Some proofs are based on entanglement distillation protocol (EDP) idea [3-6], and others rely on uncertainty principle [2, 7] or information-theoretic approach [8].

In EDP-based security proofs, we usually assume implicitly that Bob has a detector which can discriminate between vacuum, single-photon, and multi-photon states in order to distill a qubit state, while this is not the case for the security proof based on uncertainty principle [7], i.e., the conventional on-off detectors (threshold detectors) can be used in this case. On the other hand, EDP-based security proof can apply to many protocols, including BB84 with two-way classical communications [5], with decoy states [9], B92 [10], and so on [11], however the security proof based on uncertainty principle cannot directly apply to these protocols. Thus, it is important to consider from experimental or theoretical viewpoints how to accommodate the use of threshold detectors in EDP-based security proof, or to consider how to apply the uncertainty principle idea to the other protocols.

Main Results

In this presentation, we first prove unconditional security of BB84 with threshold detectors based on the argument of virtual EDP, which is valid regardless of one-way or two-way classical communications [12]. In order to show its security, instead of assuming photon-number discriminating detectors, we introduce an explicit squash operator in the virtual protocol, which transforms Bob's incoming multi-photon state to

a qubit state. Then we suppose that they run a virtual EDP on the obtained qubit pairs in order to extract secret keys. If one-way classical communications are used in this setup, the secret key rate R from the single photon part is $R=1-H_2(\epsilon_{\text{bit}})-H_2(\epsilon_{\text{ph}})$, where ϵ_{bit} and ϵ_{ph} are the phase and the bit error rates in the virtual protocol. As a consequence of introducing an explicit squash operator, all the formulas for key generation rate given in the preceding literatures of EDP-based security proofs are valid with threshold detectors, even when multi-photon emission is taken into account [6] or with decoy states [9]. Our formulation also applies to the case of two-way classical communications [5], hence the bit error rate threshold of 20% or higher is true with threshold detectors as well.

By using the same technique, we also prove the security of the Bennett-Brassard-Mermin 1992 (BBM92) protocol [13], where Alice and Bob both use threshold detectors [12]. In BBM92 protocol, a third party supplies entangled states to Alice and Bob, and they measure it with the same set of bases as in BB84. If both the receivers have photon-number discriminating detectors and can reject incoming multi-photon states, this protocol is theoretically equivalent to BB84. When threshold detectors are used, however, the security of this protocol is not straightforward, and we will give the security proof for this scheme in this presentation.

Recently, similar results regarding construction of squash operators were obtained independently by Beaudry, Moroder, and Lütkenhaus [15]. A security proof of BBM92 with threshold detectors was also given independently by Koashi et al. [16], although the techniques used there were different from ours.

Assumptions for Security Proofs

The assumptions that we make for theoretical description of BB84 are as follows. First, it is assumed that Alice's signals are block diagonalized with respect to photon number, and thus one can

treat events having different photon numbers as distinct classical events. Moreover, we assume that Alice's mixed states in the z basis and the one in the x basis are the same, i.e., there is no basis information flow from Alice's source.

We also suppose that when Alice emits a multi-photon state, all information regarding that bit is freely leaked to Eve due to the photon-number splitting attack [14]. It is proven, however, that we can still generate a secret key as long as Alice's signals contain a sufficiently high ratio of single-photon states [5]. This ratio can be well-monitored by the decoy state method [9], resulting in longer distances of communications. Thus, only single-photon emission part is important, to which we restrict our attention in this presentation.

Another assumption we make is that all imperfections of Alice's and Bob's devices, i.e., non-unit quantum efficiency of Bob's detectors, dark counts, miss-alignment, etc., are under Eve's control. This is the so-called untrusted device scenario, and with this hypothesis we are in a situation where Alice's and Bob's devices are all perfect. In addition, we suppose that Bob's phase modulator acts on multi-photon states as linear operations on tensor product states. In other words, they transform each photon contained in a signal independently, whether they are in a superposition or not (for more details, see [12]). Finally, when Bob's two detectors click simultaneously (coincidence count), he assigns a random bit to the corresponding event. These assumptions are also made in our security proof of BBM92 except that Alice, as well as Bob, plays the role of a receiver. That is, imperfections of apparatuses are attributed to Eve's attack, and Alice's and Bob's phase modulators transform their incoming multi-photon states as tensor products. If a coincident-detection event occurs on either Alice's or Bob's side, he or she manually replaces it by a random bit. We emphasize in the case of BBM92 that we do not put any assumption on incoming signals.

Acknowledgments

The authors would like to thank T. Moroder, M. Curty, H.-K. Lo and, especially, M. Koashi for enlightening discussions. This work was supported by the project "Research and Development on Quantum Cryptography of the National Institute of Information and Communications Technology," as part of Ministry of Internal Affairs and Communications of Japan's

program "R&D on Quantum Communication Technology."

References

1. C. H. Bennett and G. Brassard, in Proceeding of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), pp.175-179.
2. D. Mayers, JACM **48**, 351 (2001).
3. H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999).
4. P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
5. D. Gottesman and H.-K. Lo, IEEE Trans. Inform. Theory **49**, 457 (2003); H. F. Chau, Phys. Rev. A **66**, 060302(R) (2002); K. S. Ranade and G. Alber, J. Phys. A: Math. Gen. **39**, 1701 (2006).
6. D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **5**, 325 (2004).
7. M. Koashi, arXiv:quant-ph/0609180v1.
8. B. Kraus, N. Gisin and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005); R. Renner, N. Gisin and B. Kraus, Phys. Rev. A **72**, 012332 (2005).
9. W. -Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005); X. -B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).
10. K. Tamaki, M. Koashi, and N. Imoto, Phys. Rev. Lett. **90**, 167904 (2003); K. Tamaki and N. Lütkenhaus, Phys. Rev. A **69**, 032316 (2004); M. Koashi, Phys. Rev. Lett. **93**, 120501 (2004); K. Tamaki, N. Lütkenhaus, M. Koashi, and J. Batuwantudawe, arXiv:quant-ph/0607082v1.
11. K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006); C.-H. F. Fung, K. Tamaki, H.-K. Lo, Phys. Rev. A **73**, 012337 (2006).
12. T. Tsurumar, and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).
13. C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992); X. Ma, C.-H. F. Fung, H.-K. Lo, Phys. Rev. A **76**, 012307 (2007).
14. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, Phys. Rev. Lett. **85**, 1330 (2000); N. Lütkenhaus, Phys. Rev. A **61**, 052304 (2000).
15. N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).
16. M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, arXiv:0804.0891v1.