Multi-partite squash operation and its application to device-independent quantum key distribution

Toyohiro Tsurumaru[1] and Tsubasa Ichikawa[2]

[1]*Mitsubishi Electric Corporation, Information Technology R&D Center,*
5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501, Japan
[2]*Department of Physics, Gakushuin University,*
Mejiro, Toshima-ku, Tokyo, 171-8588, Japan

The squash operation, or the squashing model, is a useful mathematical tool for proving the security of quantum key distribution systems using practical (i.e., non-ideal) detectors. At the present, however, this method can only be applied to a limited class of detectors, such as the threshold detector of the Bennett-Brassard 1984 type. In this presentation, we generalize this method to include multi-partite measurements, and show how it can be applied to a wider class of detectors. We demonstrate the effectiveness of this generalization by applying it to the security proof of the Ekert 1991 protocol using any memoryless detectors. The result is that the Ekert 1991 protocol achieves the device-independent security, and simultaneously the same high key generation rate as in the implementation using ideal qubit detectors. For proving this result we use two physical assumptions, namely, that quantum mechanics is valid, and that Alice's and Bob's detectors are memoryless.

Quantum key distribution (QKD) [1] is a technique for distributing information-theoretically secure secret keys between two parties connected by a quantum channel. Beginning from the Bennett-Brassard 1984 (BB84) [1], and the Ekert 1991 protocols [2], there is now a variety of protocols proposed, e.g., [3–6]. Several different approaches have been advanced for proving the security of QKD systems using the ideal qubit detectors [7–9].

The squash operation, or the squashing model, is a useful mathematical tool for proving the security of QKD systems using practical (i.e., non-ideal) detectors [10, 11]. Once its existence is proved for a given practical detector, one can incorporate it into a conventional type of security proof where receivers have ideal qubit detectors, and automatically obtains a new proof that remains valid even if the practical detectors are used. The squash operation literally *squashes* an incoming state a qubit, and also has a property that, when followed by qubit measurements, it acts exactly the same way as the practical detector. In security proofs, there is no loss of generality in supposing that the squash operation is conducted by the attacker, and as the result of that, the security of a protocol using practical detectors is reduced to that using ideal qubit detectors.

A type of squash operation was first assumed in the security proof by Gottesman et al. [12], however, its existence was only conjectured, no proof was given. The first proof was given by one of the present authors and Tamaki [10], for the case of the threshold detector of the BB84 type measurement. This result was also verified independently by Beaudry, Moroder, and Lütkenhaus [11]. There were also attempts toward constructing squash operations for a wider class of practical detectors. For example, Ref. [11] gave an explicit condition for the existence of a squash operation, and used it to show positive and negative results on the six-state protocol. In Ref. [13], one of the present authors discussed whether symmetries of a given detector can imply the existence of the squash operation corresponding to it, and also showed that the above result on the BB84 type measurement is valid even for multi-mode cases. However, for other types of detectors, e.g., homodyne measurements, the squash operation is not known to exist.

In this presentation (and its arXiv version [14]), we demonstrate that the situation changes drastically by considering a generalized case where multi-partite measurements are involved. That is, while all previous studies on the squash operation were concerned only with detectors used by a single player, we here consider a generalization including global measurements performed jointly by two players or more, such as the Clauser-Horne-Shimony-Holt (CHSH) measurement [15], used, e.g., in the E91 protocol. This approach allows us to relax mathematical conditions required for the existence of the squash operation, such that they can be fulfilled for a wider class of detectors. Perhaps this is most easily illustrated by considering the CHSH measurement as an example. If one regards the CHSH measurement as a mixture of local x, z-basis measurements performed by Alice and Bob, there are two basis for each player, which together yield four conditions that the squash operation has to satisfy. On the contrary, if one regards the same measurement as one global measurement, there is no basis choice, and thus only one condition required for the existence of the squash operation.

As an evidence of the effectiveness of this generalization, we apply it to the E91 protocol using any detectors, and show that it achieves the same high key generation rate as in the same protocol implemented with ideal qubit detectors [14]. In other words, we show that the E91 protocol achieves the device-independent security, and simultaneously the high key generation rate R as in the ideal device-dependent implementation: $R = 1 - (1 + f_{\rm ec})h(p)$, with p being quantum error rate (QBER), $h(p)$ the binary entropy, and $f_{\rm ec}$ the efficiency of error correction. Hence when the optimal error correcting code with $f_{\rm ec}=1$ is available, one can generate the secret key with QBER up to 11%. This key rate is higher than in any of the existing literature on device-independent QKD [16–20], and in fact the highest known for any QKD protocols with one-way post-processing, including device-dependent ones. For obtaining this result, we use two physical assumptions. Namely, we assume that quantum mechanics is valid, and that Alice's and Bob's detectors are memoryless, i.e., different detectors operate on different Hilbert spaces. In comparison with the existing literature, our assumptions are weaker than that of Ref. [16], where collective attacks are assumed, but stronger than in Refs. [18–20], where detectors are not necessarily memoryless, and also stronger than in Ref. [17], which does not assume quantum mechanics.

Our security proof of the E91 protocol proceeds as follows. In the first step, we convert the E91 protocol using arbitrary detectors into a simplified version where uncharacterized qubit detectors are used. For this purpose we borrow the technique used in Ref. [16], and the result is that, without loss of security, we may restrict ourselves to a protocol where Alice and Bob use qubit detectors, parameterized by complex numbers α,β. In the next step, we eliminate the α,β-dependence by applying a bipartite squash operation $F_{\alpha,\beta}$, which is designed such that the CHSH measurement, jointly performed by Alice and Bob, is transformed to the phase error measurement of the BB84 type, also jointly performed by the two players. $F_{\alpha,\beta}$ is also designed so that it leaves Alice's sifted-key measurement unchanged. As a consequence, the original E91 protocol is transformed to the BB84 protocol, which can readily be shown secure by referring to the existing literature, e.g., [7, 21–23]. Further details can be found in our full paper [14].

The crucial observation here is that the minimum entropy of Alice's sifted key depends only on the results of Alice's sifted-key measurement, and of the CHSH measurements on sample pulses. No other measurements affect the sifted key as they are performed locally and remotely from it. Hence for proving the security of the E91 protocol, it suffices to find a squash operation that properly transforms the CHSH and Alice's sifted-key measurement. While the previous formulation based on the one-partite squash operation demands four conditions, corresponding to Alice's and Bob's choices of x,z basis, which cannot be fulfilled in general, the bipartite generalization demands only two. This is why this new setting realizes the security proofs that were not possible previously.

All the details of our results are given in our arXiv version [14], which is constructed as follows. In Section II of [14], we review basic concepts regarding quantum key distribution, including typical setting of QKD protocols, the corresponding security criteria, and the previous method of security proof using the squash operation. In Section III, we give definition of the squash operation in multi-partite cases, and then sketch roughly how it can be used to prove of device-independent security of the E91 protocol. Section IV is devoted to the exact mathematical statements corresponding to the device-independent security of the E91 protocol. That is, we elaborate on the version of the E91 protocol under consideration, and then claim its device-independent security as a theorem. In Section V we give the proof of the theorem.

Acknowledgment This work was partially supported by the National Institute of Information and Communications Technology (NICT), Japan.

[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 (1984).

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).

[4] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[5] T. Hirano, H. Yamanaka, M. Ashikaga, T. Konishi, and R. Namiki, Phys. Rev. A **68**, 042331 (2003).

[6] T. Sasaki, Y. Yamamoto, and M. Koashi, Nature **509**, 475 (2014).

[7] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[8] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).

[9] M. Koashi, arXiv:0704.3661 [quant-ph] (2007).

[10] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).

[11] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).

[12] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quant. Inf. Comput. **5**, 325 (2004).

[13] T. Tsurumaru, Phys. Rev. A **81**, 012328 (2010).

[14] T. Tsurumaru and T. Ichikawa, arXiv:1502.04802v2 [quant-ph] (2015).

[15] J. F. Clauser, M. A. Horne, A. Shimony, and R. A. Holt, Phys. Rev. Lett. **23**, 880 (1969).

[16] S. Pironio, A. Acín, N. Brunner, N. Gisin, S. Massar, and V. Scarani, New J. Phys. **11**, 045021 (2009).

[17] E. Hänggi, R. Renner, and S. Wolf, Lecture Notes in Computer Science **6110**, 216 (2010).

[18] J. Barrett, R. Colbeck, and A. Kent, Phys. Rev. A **86**, 062326 (2012).

[19] B. W. Reichardt, F. Unger, and U. Vazirani, Nature **496**, 456 (2013).

[20] U. Vazirani and T. Vidick, Phys. Rev. Lett. **113**, 140501 (2014).

[21] R. Renner, Ph.D. thesis, Diss. ETH No. 16242 (2005).

[22] M. Hayashi and T. Tsurumaru, New J. Phys. **14**, 093014 (2012).

[23] M. Tomamichel, C. C. W. Lim, N. Gisin, and R. Renner, Nature Communications **3**, 634 (2012).