Squash operator and symmetry

Toyohiro Tsurumaru

Mitsubishi Electric Corporation, Information Technology R&D Center, 5-1-1 Ofuna, Kamakura-shi, Kanagawa, 247-8501 Japan

(Received 19 October 2009; published 27 January 2010)

This article begins with a simple proof of the existence of squash operators compatible with the Bennett-Brassard 1984 (BB84) protocol that suits single-mode as well as multimode threshold detectors. The proof shows that, when a given detector is symmetric under cyclic group C_4, and a certain observable associated with it has rank two as a matrix, then there always exists a corresponding squash operator. Next, we go on to investigate whether the above restriction of "rank two" can be eliminated; i.e., is cyclic symmetry alone sufficient to guarantee the existence of a squash operator? The motivation behind this question is that, if this were true, it would imply that one could realize a device-independent and unconditionally secure quantum key distribution protocol. However, the answer turns out to be negative, and moreover, one can instead prove a no-go theorem that any symmetry is, by itself, insufficient to guarantee the existence of a squash operator.

DOI: 10.1103/PhysRevA.81.012328 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD) is a technique for distributing information-theoretically secure secret keys between two parties connected by a quantum channel. The oldest, and now *de facto*, standard protocol for QKD is the well-known Bennett-Brassard 1984 (BB84) protocol [1]. Several different approaches have been advanced for proving its unconditional security [2–6], e.g., one based on virtual entanglement distillation protocol (EDP) [2,3] and another based on the complementarity of quantum theory [4].

The most widely used of these approaches is the one based on EDP, where an actual QKD protocol is converted to an equivalent and virtual EDP performed by Alice and Bob. The conversions must be made so that Alice's and Bob's quantum operations are seen by Eve to retain the same positive operator valued measures (POVM); i.e., Eve's information regarding the secret key bits is not changed by conversion. The original EDP-based proofs [2] assumed that the actual protocol had access to a perfect single-photon source and photon-number resolving detectors. However, this assumption is invalid for real-world QKD systems, which use attenuated lasers as light sources, and the receiver uses "threshold detectors," which can discriminate a nonzero photon state from the vacuum but cannot determine the exact photon number.

In fact, techniques are already known that can fill these gaps. As for light sources, by exploiting decoy states, lasers can be driven to effectively emit single-photon pulses [7]. One of the known solutions for detectors [8,9,11] is the powerful theoretical tool called "squash operator." Squash operator is a quantum operation that transforms an incoming n-photon state to a qubit state. By incorporating this operator into a conventional type of security proof where BOB has a photon-number discriminating detector, one automatically obtains a new proof that remains valid even if threshold detectors are used. A squash operator was first assumed in the security proof by Gottesman *et al.* [3], however, its existence was only conjectured; no proof was given. For threshold detectors, which are sensitive only to single-mode photon pulses, its existence was proved first by the present author and Tamaki [8], and also independently by Beaudry *et al.* [9]. Although this method was originally introduced in the context of EDP-based security proofs, it can also be applied to other proof approaches, e.g., the one based on the quantum de Finetti representation theorem [5] (for details, see Refs. [8,9]).

The aim of this article is to investigate how far we can generalize this result from the viewpoint of symmetry constraints imposed on the detector. In the first half of this article, we show that when a given set of POVM is symmetric under transformations of cyclic group C_4, and the observable M_z related with it has rank two, then there always exists a corresponding squash operator compatible with the BB84 protocol (Theorem 1). An immediate corollary of this theorem is that a squash operator exists, not only for single-mode threshold detectors, but also for multimode threshold detectors. Next, in the second half of the article, we tackle the question of whether the above restriction of "rank two" can be eliminated. The answer turns out to be negative. Furthermore, it can be shown that, more generally, no symmetry is sufficient by itself to guarantee the existence of a squash operator (Theorem 2).

II. DEFINITION OF SQUASH OPERATOR

In the BB84 protocol, ALICE and BOB use two different bases, r, for their measurements, interchangeably. They are usually denoted as the z and the x basis ($r = z, x$) because they are related to qubit measurements of the Pauli matrices σ_z, σ_x. Similarly, the notation of $r = +, \times$ bases is used to indicate the directions of photon polarization. In what follows, we stick to the notation of $r = z, x$ for the sake of simplicity.

We denote the Hilbert space of the receiver's incoming states as $\mathcal{H}_B$. In this space, there are two sets of POVM elements, $M_{(r,b)}$, corresponding to basis $r = z, x$ and the output bit $b = 0, 1$. We also define observables $M_r := M_{(r,0)} - M_{(r,1)}$ for later convenience. For example, if a receiver measures state $\rho_B \in \mathcal{H}_B$ using the x basis, he observes output bit $b = 0$ with probability $p_{(x,0)} = \mathrm{Tr}[\rho_B M_{(x,0)}]$. We also assume that the measurements are complete for each basis; that is,

$$M_{(r,0)} + M_{(r,1)} = \mathbb{I}_B \tag{1}$$

holds for $r = z, x$, where $\mathbb{I}_B$ is the identity operator of $\mathcal{H}_B$.

Squash operator F is a completely positive trace-preserving (CPTP) map with the following properties.[1] F maps states in $\mathcal{H}_B$ to those in qubit space $\mathcal{H}_C$, and, when F is followed by the z or the x measurement in $\mathcal{H}_C$, it reproduces M_r of the actual measurement device. That is, for an arbitrary mixed state $\rho_B \in \mathcal{H}_B$, it satisfies

$$\mathrm{Tr}\,[F(\rho_B)\sigma_r] = \mathrm{Tr}\,(\rho_B M_r) \quad \text{for} \quad r = z, x \tag{2}$$

with σ_r being the Pauli operators. In fact, in the article by Gottesman *et al.* [3], which gave the original definition of squash operator, it was assumed F might depend slightly on basis r, and Eq. (2) with F replaced by F_r was used as the definition. They then discussed the security of QKD when the basis dependence of F_r was small enough. In this article, however, we neglect this basis-dependent flaw for the sake of simplicity, and concentrate on cases where F is independent of r.

A convenient way of describing F is to use an operator sum representation with a set of Kraus operators F_c (see, e.g., Ref. [13].) In this notation, the trace-preserving condition of F takes the form $\sum_c F_c^\dagger F_c = \mathbb{I}_B$. Complete positiveness is guaranteed as long as F is expressed as $F(\rho_B) = \sum_c F_c \rho_B F_c^\dagger$. This notation has the additional merit that the Hermitian conjugate, $F^\dagger$, of F can be expressed in simple form as $F^\dagger(\rho_C) = \sum F_c^\dagger \rho_C F_c$ with ρ_C being an arbitrary state in $\mathcal{H}_C$. By using these relations, the definition of squash operator F for M_r given in Eq. (2) can be equivalently stated as the following two conditions for Kraus operator F_c,

$$M_r = \sum_c F_c^\dagger \sigma_r F_c, \tag{3}$$

$$\mathbb{I}_B = \sum_c F_c^\dagger F_c. \tag{4}$$

III. CYCLICALLY SYMMETRIC POVM FOR THE BB84 PROTOCOL

In the first half of this article, we show that F actually exists for multimode threshold detectors as well. Against this goal, we generalize the problem slightly by taking up finite group C_4, i.e., a cyclic group of order 4, and consider POVM elements $M_{(r,b)}$ that are symmetric under its transformations (for details of C_4 group, see, e.g., Ref. [10].) The C_4 symmetry of $M_{(r,b)}$ is stated rigorously as follows.

Definition 1. A set of POVM elements $\{M_{(r,b)}\}$ of BB84 type is C_4 symmetric if there exists a unitary operator U satisfying $U^{4k} = \mathbb{I}_B$ with $k \in \mathbb{N}$, and it transforms them as follows

$$U M_{(z,b)} U^\dagger = M_{(x,b)}, \tag{5}$$

$$U^2 M_{(r,b)} U^{\dagger 2} = M_{(r,1-b)}. \tag{6}$$

Intuitively, operator U corresponds to rotating a detector spatially by 45°, when polarization encoding is used. It can be better seen if we newly define operators $L_0, \ldots, L_3$ as $L_{2b} = M_{(z,b)}$ and $L_{2b+1} = M_{(x,b)}$ for $b = 0, 1$. The relations (5) and (6) can thus be rewritten as $U L_c U^\dagger = L_{c+1}$, where modulo 4 is assumed in the summation of index c. Note here that with U being a 45° rotation, we have $U^8 = \mathbb{I}_B$ instead of $U^4 = \mathbb{I}_B$. This example demonstrates why we needed to consider cases of $k > 1$ in Definition 1.

Theorem 1. If a given set of POVM elements $\{M_{(r,b)}\}$ of BB84 type is C_4 symmetric, and the rank of the corresponding observable M_z (or equivalently, M_x) as a matrix is two, there always exists a corresponding squash operator compatible with the BB84 protocol.

Here, it should be noted that the restriction of "rank two" does not necessarily mean that the Hilbert space $\mathcal{H}_B$ is a qubit space, as illustrated by the following example.

An important example of C_4-symmetric POVMs is the threshold detector. In this paragraph, following Refs. [8,9], we concentrate on photon detection modules consisting of two photon threshold detectors, each of which corresponds to output bits $b = 0, 1$; we call such photon detection units simply "threshold detectors" with only a slight abuse of the terminology. We also assume that, when both detectors click coincidently (double-click events), the detection system outputs a random bit as its output, b. However, we differ from Refs. [8,9] in that we do not restrict ourselves to a single mode but assume that an incoming light pulse may have $m \geqslant 1$ modes of propagation; we label each using index i. We also denote the number of photons in mode i as n_i and let $N = (n_1, n_2, \ldots, n_m)$. Clearly, any threshold detector is block diagonalized with respect to the photon number configuration N, and there is no loss of generality in considering each of the blocks individually when analyzing security. For each such section, N, the observables M_r can be written as a matrix with rank two

$$M_r = |N; r, 0\rangle\langle N; r, 0| - |N; r, 1\rangle\langle N; r, 1| \tag{7}$$

for $r \in \{z, x\}$, where

$$|N; r, b\rangle := A_N (a_{1rb}^\dagger)^{n_1} (a_{2rb}^\dagger)^{n_2} \cdots (a_{mrb}^\dagger)^{n_m} |0\rangle. \tag{8}$$

Note here that M_r has rank two because double-click events are replaced by a random bit in our model, and thus all states besides $|N; r, 0\rangle$ and $|N; r, 1\rangle$ are canceled in the subtraction $M_r = M_{(r,0)} - M_{(r,1)}$ (a similar argument can be found in Ref. [11].) Coefficient A_N in Eq. (8) is the normalization constant for state $|N; r, b\rangle$, and $a_{irb}^\dagger$ are the creation operators for photons propagating in mode i, having bit value b of basis r. In accordance with the usual notations of Pauli matrices, creation operators $a_{irb}^\dagger$ for two bases $r = z, x$ are related as $a_{ixb}^\dagger = \frac{1}{\sqrt{2}}[a_{iz0}^\dagger + (-1)^b a_{iz1}^\dagger]$. The single-mode threshold detectors discussed in Refs. [8,9] correspond to the special case of $m = 1$. C_4 symmetry can be shown by using an explicit form of the transforming operator U_N,

$$U_N = \exp\left[\frac{i}{2}\sum_i (a_{iy0}^\dagger a_{iy0} - a_{iy1}^\dagger a_{iy1})\right].$$

The creation operator along the y axis appearing in the above equation is defined as $a_{iyb}^\dagger = (a_{iz0}^\dagger + i(-1)^b a_{iz1}^\dagger)/\sqrt{2}$.

From these facts, and also from Theorem 1, it immediately follows that a squash operator exists, not only for single-mode threshold detectors but also for multimode threshold detectors.

Proof of Theorem 1. Here we give only the proof for $k = 1$, since all other cases ($k \geqslant 2$) can be shown by exactly the same

[1] Squash operation is called a "squashing model" in Ref. [9].

argument. As can be seen from $U^2 M_z U^{\dagger 2} = -M_z$, for each normalized eigenstate $|v\rangle$ of M_z with an eigenvalue $0 < \lambda \leqslant 1$, there always exists another eigenstate $U^2|v\rangle$ having a different eigenvalue $-\lambda$, and thus is orthogonal

$$\langle v|U^2|v\rangle = 0. \tag{9}$$

From this, and since the rank of M_z is two, it follows that M_z takes the form

$$M_z = \lambda(|v\rangle\langle v| - U^2|v\rangle\langle v|U^{\dagger 2}). \tag{10}$$

By using a basis that diagonalizes U, we can always decompose $|v\rangle$ as

$$|v\rangle = \sum_{c=0}^{3} \mu_c |v_c\rangle , \tag{11}$$

with $U|v_c\rangle = i^c |v_c\rangle$. Then, from Eq. (9), we see that coefficients μ_i satisfy

$$|\mu_0|^2 + |\mu_2|^2 = |\mu_1|^2 + |\mu_3|^2 = \tfrac{1}{2}. \tag{12}$$

We now define a completely positive, but not necessarily trace-preserving map, F, with a set of Kraus operators $F_0, F_1, \ldots, F_3$ which take the form

$$F_c = \sqrt{2\lambda}(\mu_{c+1}|0_y\rangle\langle v_c| + \mu_c|1_y\rangle\langle v_{c+1}|) \tag{13}$$

if $\mu_c \mu_{c+1}^* \neq 0$, otherwise $F_c = 0$. In Eq. (13), modulo 4 is assumed for the summations of index c. From the linearity of $F^\dagger$, we obtain the following relation

$$\begin{aligned} F^\dagger(\sigma_z + i\sigma_x) &= \sum_{c=0}^{3} F_c^\dagger(\sigma_z + i\sigma_x)F_c \\ &= 2\sum_{c=0}^{3} F_c^\dagger|0_y\rangle\langle 1_y|F_c \\ &= 4\lambda \sum_{c=0}^{3} \mu_c \mu_{c+1}^* |v_c\rangle\langle v_{c+1}| \\ &= \lambda \sum_{c=0}^{3} i^c U^c |v\rangle\langle v| U^{\dagger c} = M_z + iM_x. \end{aligned} \tag{14}$$

Similarly, from Eqs. (12) and (13), we have $F^\dagger(\mathbb{I}_C) = \sum_{c=0}^{3} F_c^\dagger F_c \leqslant \mathbb{I}_B$. Furthermore, F can be modified such that it satisfies the trace-preserving condition (6) and also maintains relation $F^\dagger(\sigma_z + i\sigma_x) = M_z + iM_x$, obtained in Ref. (14). This can be done by introducing extra Kraus operators F_c, $c > 3$, having the form $F_c = |b_y\rangle\langle\psi_c|$ with $b = 0$ or 1.

That the CPTP map F thus obtained also satisfies (5) for $r = z$ can be shown as $F^\dagger(\sigma_z) = \frac{1}{2}F^\dagger((\sigma_z + i\sigma_x) + \text{H.c.}) = \frac{1}{2}(M_z + iM_x) + \text{H.c.} = M_z$, where H.c. denotes the Hermitian conjugate. The other relation for $r = x$ can be shown similarly. ■

IV. DOES SYMMETRY IMPLY THE EXISTENCE OF SQUASH OPERATORS?

A natural question that arises here is as follows: Can we eliminate the restriction of "rank two" appearing in Theorem 1? In other words, is cyclic symmetry C_4 alone sufficient to guarantee the existence of a squash operator or, more generally, is there any type of symmetry that is strong enough to ensure its existence? In the remaining half of this article, we shall investigate this possibility. This question is interesting because if this were actually the case, we would need no knowledge about microscopic structures of a detector in order to ensure the existence of its squash operator. In other words, we would succeed in proving the unconditional security of some of the existing protocols, such as the Bennett-Brassard-Mermin 1992 (BBM92) protocol [12], in a device-independent way [14,15].

Indeed, C_4 symmetry is already realized in most conventional BB84 systems (c.f. the paragraph below Definition 1). For example, when polarization encoding is used, bases z, x can be switched by rotating the detector by 45°. In addition, the receiver may interchange the assignment of two detectors to output bit $b = 0, 1$ randomly, by rotating them by 90° and flipping b. This may be done in order to cancel the mismatch between two detectors in terms of quantum bit error rate. These two types of rotation generate a C_4 group.

Moreover, for some QKD protocols, no knowledge about microscopic structures of any components *besides detectors* is needed to prove security. For example, consider the BBM92 protocol, where an untrusted third party prepares an entangled state. It is clear that if symmetry could actually imply the existence of squash operators, we would be able to prove the security of a QKD system without knowing anything of the microscopic structure of the devices, only the macroscopic operations by ALICE and BOB. Note here that, although there are already remarkable results on the device-independent security of QKD [14,15], whether there exists an efficient protocol that can achieve unconditional security is still an open problem.

However, as we shall show below, that is not actually the case. The fact is that we can prove a no-go theorem that denies such relations between a squash operator and symmetry. In order to discuss this point rigorously, we define general symmetries of POVM below and then present a theorem.

Definition 2. A set of POVM elements $\{M_{(r,b)}\}$ of BB84 type is symmetric under finite group G if they transform under G as

$$V(g)M_{(r,b)}V^\dagger(g) = M_{g(r,b)} \quad \text{for} \quad g \in G,$$

with $V(g)$ being a unitary representation of group G. Here, map $g : (r, b) \mapsto (r', b')$ determines how each POVM element $M_{(r,b)}$ is transformed into another element by $g \in G$.

Theorem 2. No symmetry is sufficient by itself to guarantee the existence of a squash operator. That is, one cannot prove a theorem that states that "For an arbitrary G-symmetric set of POVM, there always exists a squash operator compatible with the BB84 protocol."

We present below a proof of this theorem. The basic strategy here is to show that if the type of theorems as quoted in Theorem 2 holds, it can be used to show the improbable proposition that any arbitrary operator, whether symmetric or asymmetric, possesses a squash operator.

Proof of Theorem 2. For an arbitrary set of operators $M_{(r,b)}$ of BB84 type, which may not be symmetric, one can always define other G-symmetric operators $\tilde{M}_{(r,b)}$ as

$$\tilde{M}_{(r,b)} := \sum_{g\in G} M_{g^{-1}(r,b)} \otimes |g\rangle\langle g|$$

in $\mathcal{H}_B \otimes \mathcal{H}_D$. Here, $\mathcal{H}_D$ is an ancilla space that is spanned by orthonormal basis $\{|g\rangle\}_{g\in G}$, that is, a set of orthonormal states

$|g\rangle$ labeled by all elements $g \in G$. $\tilde{M}$ is G symmetric under unitary transformation $\tilde{V}$ as defined by $\tilde{V}(g) := \mathrm{id}_B \otimes R_D(g)$ with R_D being the regular representation of G defined by $R_D(g)|h\rangle_D = |gh\rangle_D$ (see, e.g., Ref. [10]). Hence if one could prove the type of theorems quoted in Theorem 2, it would readily follow that there is a squash operator for $\tilde{M}_{(r,b)}$.

On the contrary, however, once such a $\tilde{F}$ is obtained, one can also construct squash operator F for the original operators $M_{(r,b)}$. In order to see this, note that we have for an arbitrary $\rho_B \in \mathcal{H}_B$

$$\begin{aligned}\mathrm{Tr}\,[M_r \rho_B] &= \mathrm{Tr}[\tilde{M}_r\,(\rho_B \otimes |e\rangle\langle e|)] \\ &= \mathrm{Tr}[\sigma_r \tilde{F}(\rho_B \otimes |e\rangle\langle e|)].\end{aligned}$$

with e being the identity element of G. Thus, applying $\tilde{F}$ on $\rho_B \otimes |e\rangle\langle e|$ serves as a correct squash operator for ρ_B. This result shows that any POVM $M_{(r,b)}$ of BB84 type, whether symmetric or not, possesses a squash operator. However, this leads to a contradiction because there exists the counterexample of POVM M_0 defined by

$$M_{0z} = M_{0x} = \sigma_z,$$

which has no squash operator.

The fact that M_0 possesses no squash operator can be shown, e.g, by the same argument as Beaudry, Moroder, and Lütkenhaus used for the six-state protocol [9], but it can alternatively be shown by the following simple argument. Consider the situation where Alice and Bob perform the BBM92 protocol using M_0 as their detectors, and, as the entanglement source, Eve provides states $|\psi_b\rangle := |b_z\rangle_A \otimes |b_z\rangle_B$ with a bit $b \in \{0, 1\}$ of her choice. In this setup, clearly, all sifted key bits b are known to Eve, and thus Alice and Bob will never succeed in sharing secret keys. Hence, the existence of squash operator F for M_0 would lead to a contradiction, since F could be used to prove the unconditional security of this system, with the quantum bit error rate measured by Alice and Bob being exactly zero. ■

V. SUMMARY

In this article, we first showed that, if a given detector is C_4 symmetric, and the observable M_z associated with it has rank two, then there always exists a corresponding squash operator compatible with the BB84 protocol (Theorem 1). By using this result, we then proved that squash operators exist not only for single-mode threshold detectors but also for multimode threshold detectors.

Next, we took up the question of whether this result can be generalized to symmetric detectors with arbitrary ranks, as an attempt toward the realization of device-independent and unconditionally secure QKD protocols. However, it turned out that the truth is quite opposite. That is, we have succeed in proving that, no matter what symmetry one imposes on the detectors, the symmetry is never sufficient, by itself, to guarantee the existence of a corresponding squash operator (Theorem 2).

Finally, we would like to stress that our result is not intended to rule out the possibility of device-independent and unconditionally secure QKD protocols based on other approaches. Indeed, such a protocol has already been given by Barrett *et al.* [14], although it is rather inefficient and supports only the zero-error case. Moreover, even with our approach using detector symmetry, there are still possibilities that they may be realized by extending the framework, for example, by considering a small basis-dependent flaw of squash operator F [c.f. the argument below eq. (2)], or by generalizing the definition of detector symmetry given in Definition 2. These topics remain as future work.

ACKNOWLEDGMENTS

The author thanks M. Koashi and K. Tamaki for their valuable comments. This work was 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.
[2] H.-K. Lo and H. F. Chau, Science **283**, 2050 (1999); P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[3] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).
[4] M. Koashi, New J. Phys. **11**, 045018 (2009).
[5] B. Kraus, N. Gisin, and R. Renner, Phys. Rev. Lett. **95**, 080501 (2005).
[6] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).
[7] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003); H.-K. Lo, X. Ma, and K. Chen, *ibid.* **94**, 230504 (2005); X.-B. Wang, *ibid.* **94**, 230503 (2005).
[8] T. Tsurumaru and K. Tamaki, Phys. Rev. A **78**, 032302 (2008).
[9] N. J. Beaudry, T. Moroder, and N. Lütkenhaus, Phys. Rev. Lett. **101**, 093601 (2008).
[10] J.-P. Serre, *Linear Representations of Finite Groups* (Springer Verlag, New York, 1977).
[11] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, e-print arXiv:0804.0891.
[12] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[13] M. A. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information* (Cambridge University Press, Cambridge, 2000).
[14] J. Barrett, L. Hardy, and A. Kent, Phys. Rev. Lett. **95**, 010503 (2005).
[15] A. Acin *et al.*, Phys. Rev. Lett. **98**, 230501 (2007); S. Pironio *et al.*, New J. Phys. **11**, 045021 (2009).