RAPID COMMUNICATIONS

PHYSICAL REVIEW A **84**, 020303(R) (2011)

Universal squash model for optical communications using linear optics and threshold detectors

Chi-Hang Fred Fung,[1] H. F. Chau,[1] and Hoi-Kwong Lo[2]

[1]*Department of Physics and Center of Computational and Theoretical Physics, University of Hong Kong, Pokfulam Road, Hong Kong*
[2]*Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

(Received 28 December 2010; published 17 August 2011)

Transmission of photons through open-air or optical fibers is an important primitive in quantum-information processing. Theoretical descriptions of this process often consider single photons as information carriers and thus fail to accurately describe experimental implementations where any number of photons may enter a detector. It has been a great challenge to bridge this big gap between theory and experiments. One powerful method for achieving this goal is by conceptually squashing the received multiphoton states to single-photon states. However, until now, only a few protocols admit a squash model; furthermore, a recently proven no-go theorem appears to rule out the existence of a universal squash model. Here we show that a necessary condition presumed by all existing squash models is in fact too stringent. By relaxing this condition, we find that, rather surprisingly, a universal squash model actually exists for many protocols, including quantum key distribution, quantum state tomography, Bell's inequality testing, and entanglement verification.

DOI: 10.1103/PhysRevA.84.020303 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Ex, 42.79.Sz

Quantum communication is an important branch of research in quantum-information processing. Many quantum communication schemes (such as the well-known quantum key distribution (QKD) protocol—the Bennett-Brassard-1984 protocol (BB84) [1]) are qubit-based. Analyses of qubit-based protocols assume that the source emits a single photon into the channel, which also emits a single photon to the receiver. However, in practice, experimental equipment falls short in guaranteeing such a pure single-photon environment; also we cannot assume that the eavesdropper in QKD is well behaved and always sends single-photon signals to the receiver. This gives rise to multiphoton problems at the source and the receiver. The *source problem* is due to the use of practical photon sources that occasionally emit more than one photon into the channel, whereas the *receiver problem* is due to the channel emitting a multiphoton signal into the receiver (because of channel noise, eavesdropping attacks, or multiphoton signals from the source). Current detectors are threshold detectors (such as standard InGaAs or silicon avalanche photodiodes) that are incapable of revealing the number of incoming photons; they only produce a click if the input signal contains one or more photons.

Due to the multiphoton problems at the source and the receiver, it is unclear whether all single-photon-based quantum communication schemes can run as expected from their original design and analyses. For QKD, the source problem was first solved by Gottesman *et al*. [2] and was further solved with great performance enhancement with decoy states [3] when a weak coherent source is used. Also, the source problem can be solved by using a single-photon source [4]. On the other hand, the receiver problem was solved only recently using squash models [5,6] [for the BB84 protocol] and other techniques [7,8] [for the BB84, Bennett-Brassard-Mermin 1992 (BBM92), and six-state protocols]. Unlike the decoy-state solutions to the source problem, the receiver solutions are protocol-specific, meaning that the receiver problem has to be solved separately for each qubit-based protocol.

Given that there are many qubit-based protocols in addition to the ones mentioned (such as the Scarani-Acin-Ribordy-Gisin 2004 protocol (SARG04) [9], N-state [10], and six-state SARG04 protocols [11]), it is not effective to study them one by one to check whether each admits a squash model or to tackle each with a specific technique. Here we extend the power of squash models and solve the receiver problem in a general way that is applicable to virtually all qubit-based protocols, including QKD protocols and qubit tomography.

The squash model approach [2] to the receiver problem is to construct a *virtual protocol* by arguing for the conceptual presence of a predetection quantum operation, called a *squash operation*, that maps the channel's multiphoton output state to a single-photon one. Therefore the channel output of the virtual protocol is a qubit, to which any analyses that assume a qubit input to the receiver (which we simply call qubit-based analyses in this paper) can be applied. Because we can regard that the virtual protocol could have been run, the inferred statistics of the virtual protocol can be used in an existing qubit-based analysis as if these statistics are of the real protocol considered in the analysis. Notice that a virtual protocol is not implemented in practice. It is simply a proof technique. Therefore when analyzing a real protocol, the key question is whether the real protocol admits a universal squash operation and thus a virtual qubit protocol. A squash model was shown to exist for the BB84 [5,6] and the BBM92 protocols [5] but was proved [6] *not* to exist for the six-state QKD scheme with active basis selection [12]. In summary, previous works show that a universal squash operation does not exist. This is a highly disappointing result because it appears to mean that for each protocol, one has to prove its security by a specific method.

Despite the previous no-go theorem, here we show that, rather surprisingly, a universal squash operation actually exists and it can readily be applied to a wide range of protocols. This means that these real protocols automatically admit a virtual qubit protocol to which we can apply a qubit-based analysis. This leads to convenience in the security analyses of real protocols. In fact, our squash model together with decoy states allows qubit-based security proofs of the six-state QKD scheme with active basis selection to directly carry over to practical implementations. The success of our approach lies

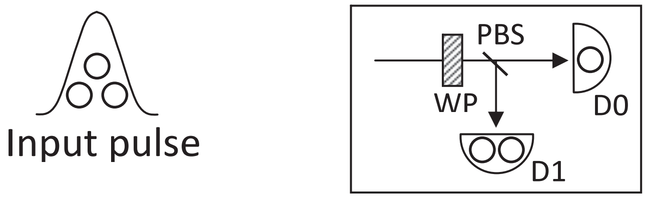

FIG. 1. Detection system used by Bob for one basis, where a set of waveplates (WP) selects the basis and a polarizing beamsplitter (PBS) splits the signal into two arms for detection by two threshold detectors (D0 and D1). Here the incoming signal consists of three photons and one is (two are) collapsed in detector D0 (D1).

in that we relax a stringent requirement to reproduce the exact statistics (as required by existing squash models) and we recognize that most protocols do not need exact statistics to function (bounds on statistics also suffice).

We discuss our result assuming the following settings [13]:

(1) Alice and Bob run a prepare-and-measure QKD protocol where Alice sends single-photon signals (each encoding a qubit in polarization) to Bob through a quantum channel controlled by Eve, who can control the number of photons entering Bob's detection system.[1]

(2) Bob's incoming photons are restricted to a single optical spatiotemporal mode.

(3) For simplicity, we assume that Bob uses active basis selection for his measurements so that his detection system projects the incoming signal onto the eigenstates of only one basis.[2]

(4) Bob's detection system consists of two threshold detectors plus possibly other linear optical elements (a representative structure is shown in Fig. 1). All photons in the same spatiotemporal mode entering each detection setup are measured and collapsed individually.

(5) The threshold detectors have perfect efficiencies and no dark counts. Thus all incoming photons are collapsed.

Our proof can be illustrated pictorially as shown in Fig. 2. Each situation i can be regarded as a positive operator-valued measure (POVM) $\mathcal{E}_i(U,n)$ acting on the channel's n-photon output state performed by Bob, where U is the unitary transform in the detection setup.[3] The essence is to link the real situation 3 (with threshold detectors and the possibility of double-click events) to the ideal situation 1 (consisting of a universal squash operation). Situation 1 serves as the virtual qubit protocol because the squash operation can be regarded as part of the channel. The key is to show that the statistics of the virtual protocol can be determined from the real protocol so that they can be used in a qubit-based analysis as if the virtual protocol is run. Situations 1 and 3 are connected by their respective POVM equivalences (situations 2 and 4), which are special cases of classical postprocessing for a detection setup with photon-number-resolving (PNR) detectors (situation 5). Since POVMs 2 and 4 are different degradations of POVM 5, the measurement statistics of POVMs 2 and 4 are related. This means that the statistics of the virtual qubit protocol with POVM 1 can be inferred from that of the real protocol with POVM 3. We discuss the elements of our proof as follows.

(A) State representation. We write an n-photon pure state in tensor product form and then impose bosonic symmetry by symmetrizing the state.[4] Similarly, an n-photon mixed state can be dealt with as a mixture of pure states. Let ρ denote the density matrix of an n-photon state. A squash operation is a quantum operation that takes an n-photon state as input and produces a single-photon state as output.

(B) Universal squash operation. We define our *universal squash operation* as the mapping from ρ to ρ_{qubit}, where $\rho_{\text{qubit}} = \text{Tr}(\rho)$ over any $n-1$ photons is the reduced density matrix of one photon. It does not matter which $n-1$ photons we trace over, and the same ρ_{qubit} will result due to the bosonic symmetry. We denote this mapping as $\Lambda_{n\to 1}(\rho) = \rho_{\text{qubit}}$. Note that $\Lambda_{n\to 1}$ is a valid quantum operation.

(C) Equivalence of POVMs 1 and 2.

Theorem 1. POVMs 1 and 2 are equivalent, i.e., $\mathcal{E}_1(U,n) = \mathcal{E}_2(U,n)$.

This theorem is a direct consequence that the bit value outputs of situations 1 and 2 have the same statistics for any n-photon input state and any unitary transform U. This result is nontrivial and its proof is discussed in Supplementary Materials.[5] Since the squash operation in situation 1 can be regarded as part of the channel, it is valid to apply the result of any single-qubit-based analysis to situation 1 and, by theorem 1, to situation 2.

(D) Equivalence of POVMs 3 and 4. It is easy to see that the real situation with threshold detectors (situation 3) is equivalent to another special classical postprocessing method for a detection system with PNR detectors (situation 4). Thus, $\mathcal{E}_3(U,n) = \mathcal{E}_4(U,n)$.

(E) Relationship between POVMs 2 and 4. Both situations 2 and 4 are special cases of classical postprocessing of the same detection setup with PNR detectors (situation 5). Thus all measurements could really be performed in that same setup and no counterfactual arguments are made. Since POVMs 2 and 4 are different degradations of POVM 5, the statistics of POVM 4 can be used to infer the statistics of POVM 2.

For qubit-based QKD protocols, the statistic of interest is the error rate e_b between Alice and Bob for basis b. We emphasize that this error rate refers to the qubit error rate in situation 1, where a squash operation exists. Thus there

[1] Thus, we assume that the source problem is solved by using a single-photon source.

[2] We have also analyzed the case for passive basis selection [13].

[3] Quantum non-demolition (QND) measurements are implicitly assumed in the virtual protocols, without loss of generality, to be used by Bob to determine the input photon number throughout the proof, and are not implemented in practice.

[4] We note that our formalism and result are fully consistent with the standard Hong-Ou-Mandel effect [C. K. Hong, Z. Y. Ou, and L. Mandel, Phys. Rev. Lett. **59**, 2044 (1987)] in quantum optics because we have imposed bosonic symmetry in our wave function.

[5] Hayashi [7] also considered before using the same probabilities to select the bit values in Situation 2 and discussed the resultant bit-value statistics for the rectilinear basis being equivalent to an operation identical to our $\Lambda_{n\to 1}$. Even though this idea is common among our works, it is used in different contexts and followed by different analyses [13].

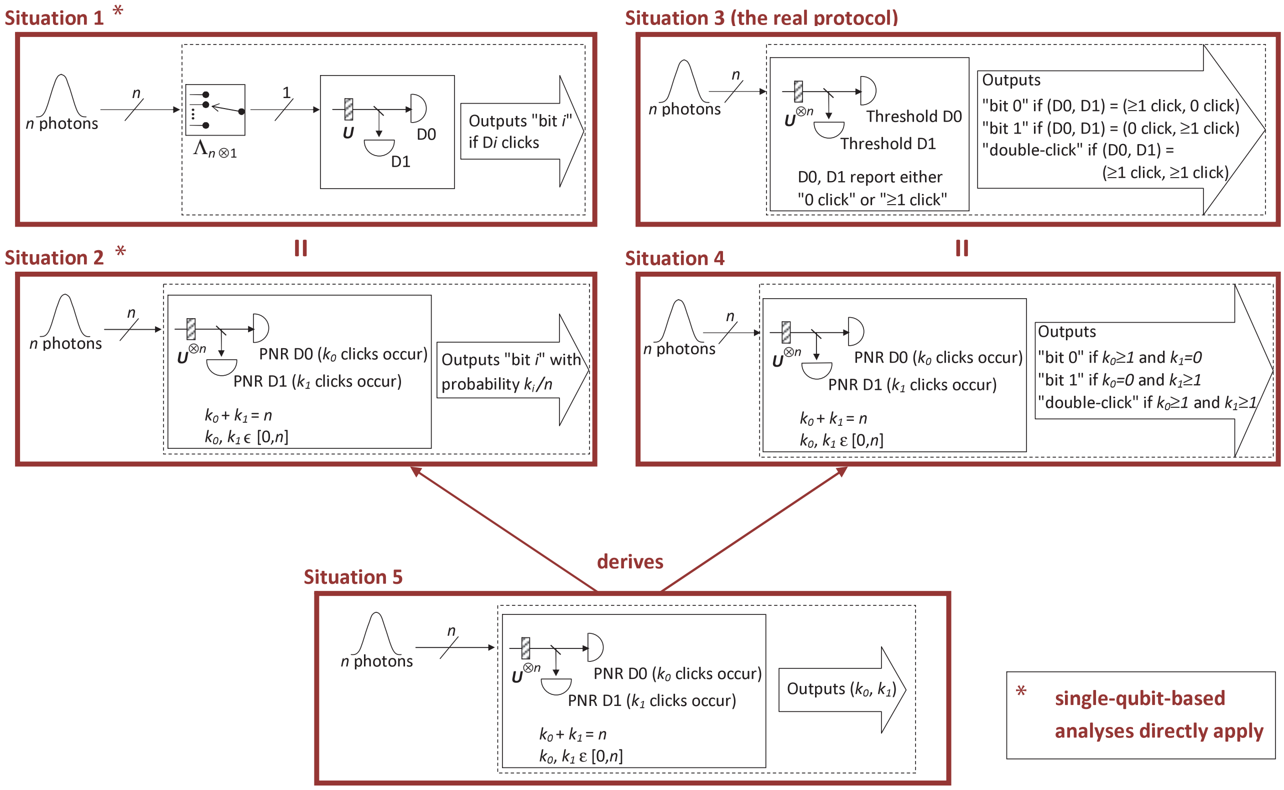
Situation 1 *
n photons
n
$\Lambda_{n\otimes 1}$
1
U
D0
D1
Outputs "bit i" if Di clicks
Situation 3 (the real protocol)
n photons
n
$U^{\otimes n}$
Threshold D0
Threshold D1
D0, D1 report either "0 click" or "≥1 click"
Outputs
"bit 0" if (D0, D1) = (≥1 click, 0 click)
"bit 1" if (D0, D1) = (0 click, ≥1 click)
"double-click" if (D0, D1) = (≥1 click, ≥1 click)
Situation 2 *
II
n photons
n
$U^{\otimes n}$
PNR D0 (k_0 clicks occur)
PNR D1 (k_1 clicks occur)
$k_0 + k_1 = n$
$k_0, k_1 \in [0,n]$
Outputs "bit i" with probability k_i/n
Situation 4
II
n photons
n
$U^{\otimes n}$
PNR D0 (k_0 clicks occur)
PNR D1 (k_1 clicks occur)
$k_0 + k_1 = n$
$k_0, k_1 \in [0,n]$
Outputs
"bit 0" if $k_0 \geq 1$ and $k_1 = 0$
"bit 1" if $k_0 = 0$ and $k_1 \geq 1$
"double-click" if $k_0 \geq 1$ and $k_1 \geq 1$
derives
Situation 5
n photons
n
$U^{\otimes n}$
PNR D0 (k_0 clicks occur)
PNR D1 (k_1 clicks occur)
$k_0 + k_1 = n$
$k_0, k_1 \in [0,n]$
Outputs (k_0, k_1)
* single-qubit-based analyses directly apply

FIG. 2. (Color online) Relationship map for the five situations used to prove our universal squash model. The POVM corresponding to each situation is shown in a dashed box. The goal is to link the real situation (situation 3) with the ideal situation (situation 1) consisting of the universal squash operation.

In situation 1 (a virtual protocol), an n-photon state enters a detection system comprising the squash operation $\Lambda_{n\to 1}$, a set of waveplates (acting as unitary transform U), a polarizing beamsplitter, and two detectors. The universal squash operation $\Lambda_{n\to 1}$ maps n photons to one. We do not specify whether the detectors are photon-number-resolving (PNR) or threshold detectors, since after the squash operation, only one photon remains. The output of the detection system is a bit value corresponding to the detector that has a click. This is a single-qubit situation since we can regard the squash operation as part of the channel.

In situation 2 (a virtual protocol), an n-photon state enters a detection system comprising a set of waveplates (acting as unitary transform $U^{\otimes n}$), a polarizing beamsplitter, and two PNR detectors, followed by a classical postprocessor. The classical postprocessor serves as the classical analog of the squash operation $\Lambda_{n\to 1}$ and outputs a bit value according to probabilities given by the detectors' clicks. More concretely, suppose that detectors D0 and D1 register k_0 and k_1 photons, respectively. Then the classical postprocessor in situation 2 outputs event "bit i" ($i = 0,1$) with probability $k_i/(k_0 + k_1)$.

We show that POVMs 1 and 2 are equivalent (see theorem 1 and Supplementary Materials for proof).

Situation 3 (the real protocol) is similar to situation 2 with the PNR detectors replaced by threshold detectors. Situation 3 outputs event "bit i" if only detector D$i$clicks ($i = 0,1$) and event "double clicks" if both detectors click. Situation 4 is also similar to situation 2 with a difference in the postprocessing part. Here, the postprocessing only announces one of three events corresponding to a single click for "0," a single click for "1," and a double click. It is easy to see that situations 3 and 4 produce the same output statistics for the same input state. In this paper, we consider only those protocols for which situations 3 and 4 are equivalent.

Situation 5 is the mother protocol that derives situations 2 and 4. Note that the detection parts of situations 2, 4, and 5 are all the same; only their classical processing parts are different. In fact, the classical processing parts of situations 2 and 4 can be generated by that of situation 5, which outputs the full information on the numbers of detection clicks.

is a qubit to talk about and e_b is well defined. Note that this is also consistent with the decoy-state solution to the source problem. There the single-photon part of the source is separately considered from the remaining multiphoton parts. A single-photon signal coming from the source may arrive at Bob as a multiphoton signal (due to Eve's manipulation) which is squashed into a single-photon signal with our result. Thus, the single-qubit error rate is also well defined in this case.

We bound this single-qubit error rate as follows. Note that a single click in situation 4 immediately tells us that a definite bit value would have been obtained in situation 2, and we directly use this bit value for the evaluation of the error rate. On the other hand, a double click in situation 4 tells us nothing about the bit value it corresponds to in situation 2. To overcome this, we recognize that we do not need to know the definite bit value since all we care about are bounds on the error rate. Our key idea is to bound the range of possible error rates by using the most pessimistic and optimistic values for double-click events. Specifically, a double-click event counts as an error bit (correct bit) for the calculation of the upper (lower) bound on the error rate. Suppose that the number of test bits for basis b is N_b, where $N_b = N_b^{\mathrm{s,c}} + N_b^{\mathrm{s,e}} + N_b^{\mathrm{d}}$. Here, $N_b^{\mathrm{s,c}}$, $N_b^{\mathrm{s,e}}$, and N_b^{d} are the correct single-click events, erroneous single-click events, and double-click events, respectively. Then the error rate of the test bits is bounded by

$$e_b^{\rm L} = \frac{N_b^{\rm s,e}}{N_b} \leqslant e_b \leqslant \frac{N_b^{\rm s,e} + N_b^{\rm d}}{N_b} = e_b^{\rm U}. \qquad (1)$$

Corollary 1. (Single-qubit description) We regard the original quantum channel followed by the squash operation $\Lambda_{n\to 1}$ in situation 1 as the *effective single-qubit quantum channel*. Thus we can ascribe a single-qubit description to the actual received signals and the associated channel error statistics are bounded by Eq. (1).

This allows us to apply any single-qubit-based security analysis to qubit-based QKD protocols whose qubit assumption is violated in practical implementation due to the reception of multiphotons. For entanglement-based QKD protocols (in which an entanglement source sends two signals, one to Bob and one to Alice), corollary 1 may be applied to each of the two parties.

Postselection of key bits in QKD. In QKD, test bits are used for parameter estimation and key bits are for producing the final secret key. Since the double-click key bits have ambiguous bit values, we propose to discard them. The bounds given in Eq. (1), established by the test bits, also serve as the bounds for the key bits before discarding. After discarding, the bounds for the remaining key bits can be computed by considering the worst-case statistics of the discarded bits. Specifically, the error rate of basis b for the key measured in basis b^* after discarding is

$$\frac{e_b^{\rm L} N_{b^*}^{\rm key} - N_{b^*}^{\rm key,d}}{N_{b^*}^{\rm key,s}} \leqslant e_b^{\rm key} \leqslant \frac{e_b^{\rm U} N_{b^*}^{\rm key}}{N_{b^*}^{\rm key,s}}, \quad \text{for} \quad b \neq b^*, \qquad (2)$$

where $N_{b^*}^{\rm key,s}$ ($N_{b^*}^{\rm key,d}$) is the number of single-click (double-click) events among all the $N_{b^*}^{\rm key} = N_{b^*}^{\rm key,s} + N_{b^*}^{\rm key,d}$ key bits, and $e_b^{\rm U,L}$ are given in Eq. (1). In practice, the double-click rate is very small and thus our bounds in Eqs. (1) and (2) are rather tight. Consequently, the key generation rate we get is very close to the theoretical limit when the double-click rate is zero. This means that we have restored the advantage of the six-state QKD protocol over the standard BB84 protocol in terms of the key generation rate. Also, in comparison, the key generation rate of our method is almost as good as that of protocol-specific methods such as Refs. [5,6] in general [13].

Conclusions. The use of threshold detectors has been a major obstacle in bridging the practical experiments on quantum protocols and their theoretical qubit-based analyses. In this Rapid Communication we provide a universal solution that allows the translation of existing analyses that assume single-photon inputs to ones that can handle multiple-photon inputs detected with threshold detectors. We emphasize that, in addition to QKD, our work also applies to quantum state tomography, Bell's inequality testing, and entanglement verification [13]. Furthermore, our universal squash model enables not only reduction to qubits but also to high-dimensional states [13].

Acknowledgments. We thank N. Lütkenhaus and K. Tamaki for enlightening discussion. This work was supported by HKSAR RGC Grants Nos. HKU 701007P and 700709P, the CRC program, CIFAR, NSERC, and QuantumWorks.

[1] C. H. Bennett and G. Brassard, in *Proc. of IEEE Int. Conference on Computers, Systems, and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

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

[3] 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).

[4] S. Fasel, O. Alibart, S. Tanzilli, P. Baldi, A. Beveratos, N. Gisin, and H. Zbinden, New J. Phys. **6**, 163 (2004).

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

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

[7] M. Hayashi, Phys. Rev. A **76**, 012329 (2007).

[8] M. Koashi, Y. Adachi, T. Yamamoto, and N. Imoto, e-print arXiv:0804.0891 [quant-ph]; G. Kato and K. Tamaki, e-print arXiv:1008.4663 [quant-ph].

[9] V. Scarani, A. Acín, G. Ribordy, and N. Gisin, Phys. Rev. Lett. **92**, 057901 (2004).

[10] M. Koashi, e-print arXiv:quant-ph/0507154; D. Shirokoff, C.-H. F. Fung, and H.-K. Lo, Phys. Rev. A **75**, 032341 (2007).

[11] K. Tamaki and H.-K. Lo, Phys. Rev. A **73**, 010302(R) (2006).

[12] C. H. Bennett, G. Brassard, S. Breidbart, and S. Wiesner, IBM Tech. Disclosure Bull. **26**, 4363 (1984); D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[13] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.84.020303 for detailed explanation of our proof of the universal squash model and its application.