Quantum cryptography: Security criteria reexamined

Dagomir Kaszlikowski,[1] Ajay Gopinathan,[1,2] Yeong Cherng Liang,[1] L. C. Kwek,[1,2] and Berthold-Georg Englert[1]
[1]*Department of Physics, National University of Singapore, Singapore 117 542, Singapore*
[2]*National Institute of Education, Nanyang Technological University, Singapore 637616, Singapore*
(Received 23 October 2003; revised manuscript received 26 May 2004; published 8 September 2004)

We find that the generally accepted security criteria are flawed for a whole class of protocols for quantum cryptography. This is so because a standard assumption of the security analysis, namely that the so-called square-root measurement is optimal for eavesdropping purposes, is not true in general. There are rather large parameter regimes in which the optimal measurement extracts substantially more information than the square-root measurement.

DOI: 10.1103/PhysRevA.70.032306 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

All practical implementations of protocols for quantum cryptography have to deal with the unavoidable noise in the transmission lines, and possibly the intervention of an eavesdropper, that degrade the correlations in the raw-key data of the communicating parties, namely Alice and Bob. They then face a double task: First, they must establish how much Eve, the evildoing eavesdropper, can possibly know about their data; and second, they must extract a secure noise-free key sequence from the insecure noisy raw data.

The second task of key generation is solved by exploiting the findings and methods of classical information theory, in particular the lesson of the seminal work by Csiszár and Körner [1]. They demonstrated that Alice and Bob can always generate a secure key, provided that the mutual information between them exceeds the mutual information between either one of them and Eve.

The first task of determining how much Eve knows thus amounts to figuring out the maximally attainable mutual information between her and either Alice or Bob. There are two different, but equivalent, lines of reasoning that one can choose to follow, depending on how one pictures the communication between Alice and Bob, and Eve's tampering with it.

One scenario is that of the 1984 protocol by Bennett and Brassard (BB84 [2]), in which Alice sends quantum-information carriers to Bob through an appropriate, authenticated quantum channel. Eve intercepts each carrier in transmission and keeps an imperfect copy, obtained by operating a quantum-cloning machine, before forwarding the carrier to Bob. The quest is then for the best cloning machine—best for *this* purpose—in conjunction with the best way of extracting information from the clones.

The other scenario is that of the 1991 protocol by Ekert (E91 [3]), in which a source distributes entangled pairs of carriers to Alice and Bob, who make statistically independent measurements on them, thereby effectively establishing a quantum channel between themselves. Eve is given full control of the source. She keeps a quantum record of what is sent in the form of auxiliary quantum systems, usually termed *ancillas*, that she entangles with the paired carriers. Here the quest is for the best ancilla states in conjunction with the best way of extracting information from the ancillas.

Because of the lack of superior alternatives, the standard analysis of protocols of BB84 type invokes unproven assumptions about optimal cloning machines; see, for example, Refs. [4,5] and the recent paper by Acín *et al.* [6]. Likewise, there is a common assumption in the analysis of E91-type protocols, namely that the so-called square-root measurement (SRM [7]) is optimal for Eve's processing of the ancillas; see the recent paper by Liang *et al.* [8], for example. The established equivalence of the BB84 and E91 scenarios [9], and the fully equivalent security criteria thus found, is strong circumstantial evidence that these assumptions—about Eve's best intercept strategy and her best way of processing the ancillas, respectively—are equivalent as well.

It is the objective of this article to demonstrate that the SRM is *not* optimal for a whole class of quantum cryptography protocols, the tomographic protocols of Refs. [8,10]; it may very well not be optimal for other protocols, too. The equivalence stated above then implies the well-founded conjecture that there are also better intercept strategies than those usually regarded as best. We offer some remarks about the connection of this work with intercept strategies in the Appendix.

II. THE PYRAMID OF ANCILLA STATES

We build on the work of Ref. [8], where the protocols are phrased as generalizations of the E91 scenario to N letter alphabets $(N=2,3,\ldots)$. The source controlled by Eve would emit pairs of qubits for $N=2$, pairs of qutrits for $N=3,\ldots$, and pairs of *qunits* in the general case. After everything is said and done, Eve knows that her ancilla is in the state described by ket $|E_k\rangle$ if Alice obtains value k for her qunit of the respective pair (with $k=0,1,\ldots,N-1$). Since there is a common (real) angle between every pair of ancilla states,

$$\langle E_k|E_l\rangle = \lambda + (1-\lambda)\delta_{kl} = \left\{\begin{matrix} 1 & \text{if } k=l \\ \lambda & \text{if } k\neq l \end{matrix}\right\} = r_0 - r_1 + Nr_1\delta_{kl}, \tag{1}$$

the N ancilla kets can be regarded as the edges of an N-dimensional pyramid [11]; see Fig. 1 for an illustration of the case of $N=3$. The average ancilla ket

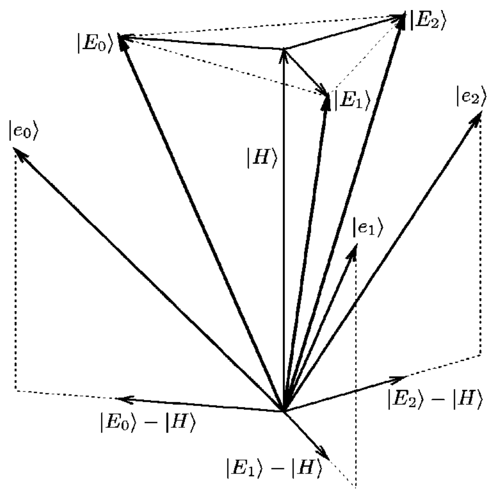

FIG. 1. Pyramid geometry for $N=3$. The ancilla kets $|E_k\rangle$, of unit length, are the edges of the ancilla pyramid. Its shape is determined by the parameter λ of Eq. (1), the cosine of the acute angle between any pair of edges. The height ket $|H\rangle$ of Eq. (2) points from the tip of the pyramid to the center of its base; its length is $\sqrt{r_0}$. The kets $|E_k\rangle-|H\rangle$, of length $\sqrt{1-r_0}$, point from the center of the pyramid base to its corners. The SRM kets $|e_k\rangle$ of Eq. (9), of unit length, define the SRM pyramid, which has right angles between its edge kets. The SRM pyramid is wider than, but not as high as, the ancilla pyramid.

$$|H\rangle = \frac{1}{N}\sum_{k=0}^{N-1} |E_k\rangle \tag{2}$$

points from the tip of the pyramid to the center of its $(N-1)$-dimensional base [12], so that the length of $|H\rangle$, $\sqrt{\langle H|H\rangle}=\sqrt{r_0}$, is the height of the pyramid. The pyramid volume is given by $(1/N!)(Nr_0)^{1/2}(Nr_1)^{(N-1)/2}$; it is largest for $\lambda=0$, $r_0=r_1=1/N$ when the pyramid is a corner of an N-dimensional cube.

Geometry restricts λ to the range $-1/(N-1)\leqslant\lambda\leqslant 1$, where both limits correspond to degenerate pyramids that have no N-dimensional volume. For $\lambda=1$, we have a single ancilla state and the pyramid is just a line, a pyramid of unit height and no base; and for $\lambda=-1/(N-1)$ we have linearly dependent ancilla kets that span an $(N-1)$-dimensional subspace, so that the pyramid has no height. In the context of quantum cryptography, however, only non-negative λ values are relevant, for which $r_0\geqslant r_1$. In other words, the pyramids of interest are acute, in the sense that the common angle between each pair of their edges is acute.

Alice gets each k value with probability $1/N$, so that

$$\rho = \frac{1}{N}\sum_{k=0}^{N-1} |E_k\rangle\langle E_k| \tag{3}$$

is the statistical operator for Eve's ancillas. The height ket $|H\rangle$ of Eq. (2) is the eigenket of ρ to the eigenvalue r_0 and all kets orthogonal to $|H\rangle$ are eigenkets to the $(N-1)$-fold degenerate eigenvalue $r_1=r_0-\lambda=(1-\lambda)/N$.

The N kets $|E_k\rangle-|H\rangle$, each of length $\sqrt{1-r_0}=\sqrt{(N-1)r_1}$, point from the center of the ancilla-pyramid base to its corners. They span the $(N-1)$-dimensional subspace to eigenvalue r_1.

III. WHICH EDGE OF THE PYRAMID?

A. The pretty good square-root measurement

Eve extracts information out of ρ with the aid of a generalized measurement, a positive-operator-valued measure (POVM), specified by a decomposition of the identity in the N-dimensional ancilla space into M non-negative operators,

$$1 = \sum_{m=0}^{M-1} P_m, \quad P_m \geqslant 0. \tag{4}$$

The mutual information between Alice and Eve,

$$I = \sum_{n=0}^{N-1}\sum_{m=0}^{M-1} p_{nm}\log_N \frac{p_{nm}}{p_{n\cdot}p_{\cdot m}}, \tag{5}$$

is then computable from the joint probabilities

$$p_{nm} = \frac{1}{N}\langle E_n|P_m|E_n\rangle \tag{6}$$

and their marginals

$$p_{n\cdot} = \sum_{m=0}^{M-1} p_{nm} = \frac{1}{N}, \quad p_{\cdot m} = \sum_{n=0}^{N-1} p_{nm}. \tag{7}$$

For convenient normalization, the logarithm in Eq. (5) is taken to base N, so that $I\leqslant 1$ with the maximum achieved for uniform perfect correlations, that is, for $M=N$ and $p_{nm}=\delta_{nm}/N$.

The POVM for the SRM is specified by setting $M=N$ and

$$P_m = (N\rho)^{-1/2}|E_m\rangle\langle E_m|(N\rho)^{-1/2} \equiv |e_m\rangle\langle e_m| \tag{8}$$

with

$$|e_m\rangle = (|E_m\rangle - |H\rangle)\frac{1}{\sqrt{Nr_1}} + |H\rangle\frac{1}{\sqrt{Nr_0}}. \tag{9}$$

The resulting joint probabilities are

$$p_{nm} = \frac{1}{N}|\langle E_n|e_m\rangle|^2 = \frac{1}{N}[\eta_1 + (\eta_0 - \eta_1)\delta_{nm}], \tag{10}$$

where

$$\sqrt{\eta_0} - \sqrt{\eta_1} = \sqrt{Nr_1} \quad \text{and} \quad \eta_0 + (N-1)\eta_1 = 1. \tag{11}$$

We note that the SRM thus associated with the ancilla pyramid happens to be a standard von Neumann measurement, not a POVM proper, because the projectors in Eq. (8) are pairwise orthogonal, $\mathrm{tr}\{P_mP_{m'}\}=\delta_{mm'}$. The mutual information acquired by performing the SRM,

$$I^{(\mathrm{SRM})} = \eta_0\log_N(N\eta_0) + (N-1)\eta_1\log_N(N\eta_1), \tag{12}$$

is shown in Fig. 2 for $N=2,3,5,10,20,100$.

B. Better than pretty good

Whereas the SRM is known to be "pretty good" as a rule [13], it is also known that it does not always optimize the

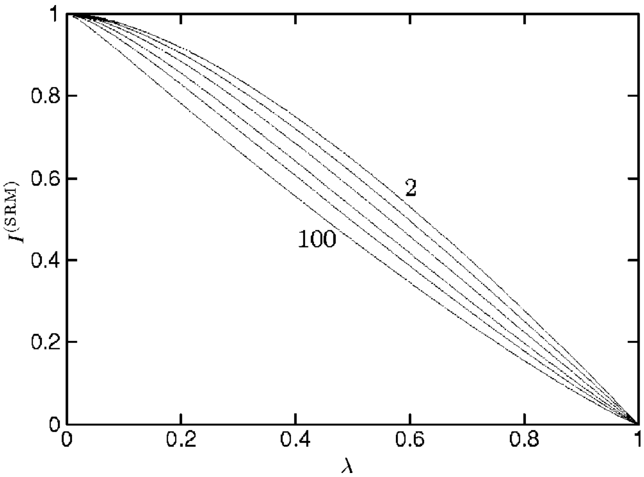

FIG. 2. Mutual information between Alice and Eve if Eve performs the square-root measurement. The curves refer to $N=2,3,5,10,20$, and 100, and the plot covers the range $0 \leqslant \lambda \leqslant 1$ that is relevant for quantum cryptography.

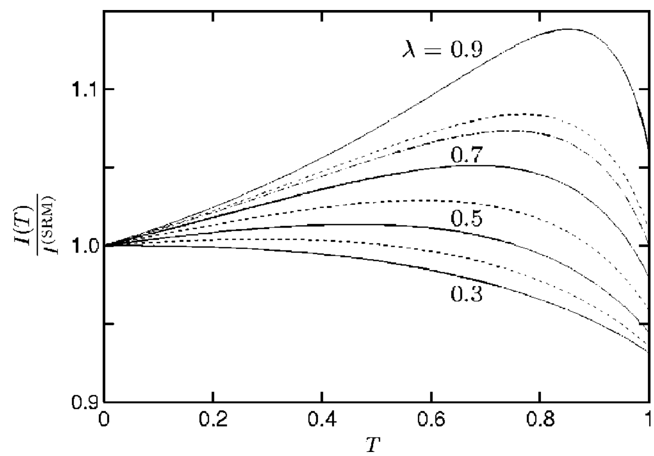

FIG. 3. Mutual information for the POVM of Eq. (13) relative to that of the SRM. For $N=10$, the plot shows the ratio of $I(T)/I^{(\mathrm{SRM})}$ as a function of T for $\lambda=0.9,0.7,0.5,0.3$ (solid lines) and for $\lambda=0.8,0.6,0.4$ (dashed lines). The left end ($T=0$) refers to the SRM, the right end ($T=1$) to the MUD. For $\lambda=0.772\,76$ (dash-dotted line), both give the same mutual information.

mutual information. In particular, Shor has pointed out that there are superior POVMs for $N=3$ and some $\lambda<0$, and has conjectured that there is also a $\lambda>0$ range in which other POVMs could be better [14]. Shor's explicit example for $\lambda<0$ is interesting in its own right but does not seem to have any bearing on the security analysis of quantum-cryptography protocols. By contrast, the $\lambda>0$ examples reported below are of immediate relevance, as they invalidate, at least partly, established security criteria.

Consider the one-parametric family of POVMs defined by $M=N+1$ and $P_m=|\overline{e_m}\rangle\langle\overline{e_m}|$ with

$$|\overline{e_m}\rangle = (|E_m\rangle - |H\rangle)\frac{1}{\sqrt{Nr_1}} + |H\rangle\frac{t}{\sqrt{Nr_0}}, \quad \text{for } m < N,$$

$$|\overline{e_N}\rangle = |H\rangle\sqrt{\frac{1-t^2}{r_0}}, \tag{13}$$

where $0 \leqslant t \leqslant 1$. The SRM kets of Eq. (9) obtain for $t=1$.

For $t<1$, the measurement pyramid, which has the kets $|\overline{e_0}\rangle, \ldots, |\overline{e_{N-1}}\rangle$ for its edges, has the same base area as the SRM pyramid, but is of smaller height and therefore obtuse. Since the angle between any such given $|\overline{e_m}\rangle$ and the ancilla kets $|E_n\rangle$ with $n\neq m$ increases as t decreases from $t=1$, the sector of $m<N$ will have increased mutual information. But this comes at a price: When Eve finds $|\overline{e_N}\rangle \propto |H\rangle$, she has no clue about Alice's value; the sector $m=N$ is inconclusive and provides no contribution at all to the mutual information. Accordingly, the optimal choice of t is such that the increase of mutual information in the $m<N$ sector is balanced against the increase in the probability of the inconclusive result; this probability equals $(1-t^2)r_0$.

For $t=\sqrt{r_1/r_0}$, the POVM specified by Eq. (13) is the "measurement for unambiguous discrimination" (MUD [7]), for which $\langle E_n|\overline{e_m}\rangle=0$ if $n\neq m<N$, so that there are perfect correlations, and thus full mutual information, in the $m<N$ sector. The cost for this perfection is, however, so high that the MUD never maximizes the mutual information, although it can outperform the SRM. The optimal choice for t is always in the range $\sqrt{r_1/r_0}<t\leqslant 1$. This observation is illustrated in Fig. 3 for $N=10$ and various values of λ, including $\lambda=0.772\,76$, for which the MUD and the SRM give the same mutual information. The plot shows only the t range of interest, conveniently reparametrized in terms of T, a scaled version of t, introduced in accordance with

$$t = 1 - T + T\sqrt{r_1/r_0}. \tag{14}$$

Thus, $T=0$ refers to the SRM, and $T=1$ to the MUD.

The mutual information for the POVMs specified by Eqs. (13) is given by

$$I(T) = \overline{\eta_0}\log_N\frac{N\overline{\eta_0}}{\overline{\eta_0}+(N-1)\overline{\eta_1}} + (N-1)\overline{\eta_1}\log_N\frac{N\overline{\eta_1}}{\overline{\eta_0}+(N-1)\overline{\eta_1}}, \tag{15}$$

where

$$\overline{\eta_0} = (\sqrt{\eta_0} - T\sqrt{\eta_1})^2, \quad \overline{\eta_1} = (1-T)^2\eta_1 \tag{16}$$

are the T-dependent versions of η_0, η_1. For ancilla pyramids with a large volume, $0<\lambda<(3-4/N)/(N-1)\equiv\Lambda$, the maximum of $I(T)$ is obtained for $T=0$, which is to say that the SRM is optimal in this range of small λ values. By contrast, for ancilla pyramids with a rather small volume, $\Lambda<\lambda<1$, the maximum of $I(T)$ is reached for $T=1-(\sqrt{\eta_0/\eta_1}-1)/(N-2)$, that is, when the arguments of the two logarithms in Eq. (15) equal $N-1$ and $1/(N-1)$, respectively. Then, the measurement pyramid is obtuse.

In summary, we have

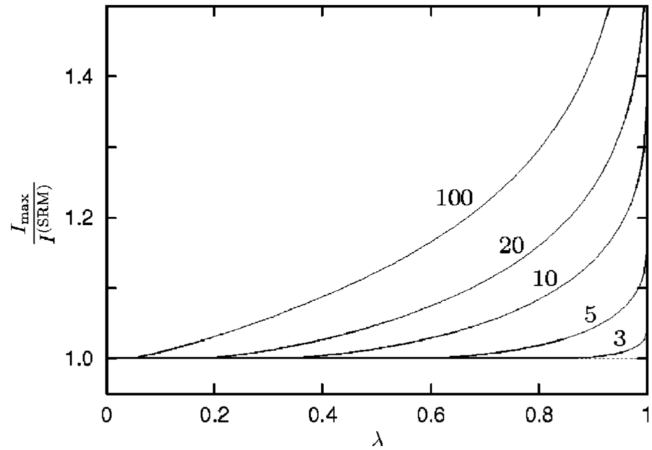

FIG. 4. Ratio of the maximal mutual information I_{max} and the SRM value $I^{(SRM)}$, for $N=3,5,10,20,100$, as a function of λ.

$$I_{max} \equiv \max_T I(T) = \begin{cases} I^{(SRM)} \text{ of Eq. (12)} & \text{if } 0 \leq \lambda \leq \Lambda = \dfrac{3N-4}{N(N-1)}, \\ (1-\lambda)\dfrac{N-1}{N-2}\log_N(N-1) & \text{if } \Lambda \leq \lambda \leq 1. \end{cases} \tag{17}$$

This is our central result.

For λ values that exceed the threshold value of Λ substantially, the optimal POVM from the family (13) gives significantly more mutual information than the SRM. This can be seen by plotting the ratio $I_{max}/I^{(SRM)}$ as a function of λ; see Fig. 4. The $\lambda \to 1$ limit,

$$\frac{I_{max}}{I^{(SRM)}} \to \frac{N/2}{N-2}\ln(N-1) \quad \text{as } \lambda \to 1, \tag{18}$$

shows that the optimal POVM provides much more information than the SRM if N is large, and then the range $0 \leq \lambda < \Lambda \simeq 3/N$ is small in addition.

IV. SUMMARY AND DISCUSSION

In summary, there are POVMs that outperform the SRM for $\lambda > \Lambda$, and we know the optimal POVM of the sort defined by Eq. (13) quite explicitly. We are, in fact, quite sure that it is the global optimum because an extensive numerical search failed to find any better POVM.

A first search covered a large class of POVMs that respect the geometry of the ancilla pyramid: We took parameter t to be complex; we rotated around the symmetry axis specified by ket $|H\rangle$; and we considered weighted sums of several such POVMs, with different t parameters and different rotations. For all of the many N and λ values, for which the numerical investigation was performed, the optimal POVM was always of the kind described above.

A second search, not restricted by geometrical or other constraints, confirmed these findings. It used the numerical method of Ref. [15], which is a fix-point iteration that converges monotonically toward the optimal POVM.

TABLE I. Threshold values for the disturbance below which the Csiszár-Körner theorem ensures that a secure key can be extracted from the noisy raw data. The second column gives the critical disturbance, that is, $(N-2)^2/[(N-2)^2+N]$, above which the SRM is optimal, as implied by Eq. (17). The third column repeats the values of Refs. [5,8], where Eve extracts information with the aid of the SRM. The true threshold values of the fourth column are obtained for the optimal POVM.

	Critical	Csiszár-Körner thresholds	
N	value	SRM	true
2	0.0%	15.6373%	15.6373%
3	25.0%	22.6714%	22.6707%
4	50.0%	26.6561%	26.5989%
5	64.3%	29.2303%	29.1038%
10	86.5%	34.9713%	34.7051%
30	96.3%	39.8403%	39.6259%
50	97.9%	41.1886%	41.0284%
100	99.0%	42.5282%	42.4295%
∞	100.0%	50.0000%	50.0000%

We note further that the large relative difference shown in Fig. 4 occurs where both I_{max} and $I^{(SRM)}$ are small, and so the absolute difference is rather small (see the figure in Ref. [16]). Therefore, the SRM threshold values given in Table I of Ref. [8] are quite good approximations for the true threshold values, as shown by the numerical values in Table I.

The "disturbance" values listed in this table are the quantities denoted by D_{d+1}^{ind} in Ref. [5] and by $1-\beta_0$ in Ref. [8], respectively. There is no difference for $N=2$, of course, but for all $N>2$ the true threshold is noticeably lower than the SRM threshold. In addition to this shift of the threshold, there is also a reduced efficiency inside the Csiszár-Körner regime (below the threshold) and this must be taken into account when extracting the secure key sequence from the noisy raw data. Fortunately, however, almost all of the practical quantum cryptography scheme presently implemented use qubits ($N=2$), and then the SRM *is* optimal. Also, the optimal POVMs have no bearing on the threshold for classical advantage distillation [6,10], because the SRM remains optimal in the relevant limit, even for coherent eavesdropping attacks [17].

In the spirit of Shor's investigation of obtuse pyramids, the eavesdropping procedure presented here can be viewed as a quantum communication channel, in which Alice transmits nonorthogonal and equally distributed signal states to Eve. The amount of information about the sequence of states sent by Alice, maximized over all possible POVMs, is then the *accessible information* of this quantum channel. Therefore, the maximal mutual information (17) between Alice and Eve gives us also this accessible information for $0 \leq \lambda$, which supplements, for $N=3$, Shor's $\lambda < 0$ result.

ACKNOWLEDGMENTS

We wish to thank Antonio Acín, Thomas Durt, and Jaroslav Řeháček for valuable discussions. We gratefully acknowledge the financial support from A*Star Grant No. 012-104-0040 and from NUS Grant No. WBS: R-144-000-089-112.

APPENDIX: INTERCEPT ATTACKS

Here are a few remarks about the connection with intercept attacks on qunits sent through an authenticated quantum channel. We make use of the notational conventions of Ref. [8] without explaining them anew, and refer to Eq. (12), say, of Ref. [8] by ([8]-12).

The geometry of the unnormalized ancilla states $|\widetilde{E}_{kl}^{(m)}\rangle$ is completely determined, for a given m value, by the inner products of Eq. ([8]-6), and Eq. ([8]-7) states the transformation law between ancilla states to different m values. It follows from this equation that the k index of $|\widetilde{E}_{kl}^{(m)}\rangle$ is analogous to that in $|\overline{m_k}\rangle$, and the l index to that in $|m_l\rangle$. Therefore, it is expedient to regard the $|\widetilde{E}_{kl}^{(m)}\rangle$'s as the kets of two-qunit states that are superpositions of basis kets of the $|\overline{m_k}m_l\rangle$ kind. They then acquire the strikingly simple explicit form

$$|\widetilde{E}_{kl}^{(m)}\rangle = |\overline{\psi}\rangle\delta_{kl}\frac{a}{\sqrt{N}} + |\overline{m_k}m_l\rangle\frac{b}{N}, \tag{A1}$$

where

$$\overline{\psi} = \frac{1}{\sqrt{N}}\sum_k |\overline{m_k}m_k\rangle \quad (\text{any} \quad m \quad \text{value}) \tag{A2}$$

is the maximally entangled state that is conjugate to $|\psi\rangle$ of Eq. ([8]-2). This ansatz for $|\widetilde{E}_{kl}^{(m)}\rangle$ is consistent with Eq. ([8]-6) if the complex amplitudes a,b obey

$$\left|a + \frac{1}{N}b\right|^2 = \beta_0 - \frac{N-1}{N}\beta_1, \quad |b|^2 = N\beta_1, \tag{A3}$$

but no other restrictions apply, so that $a=\sqrt{\beta_0-\beta_1}$, $b=i\sqrt{N\beta_1}$ is a permissible choice.

The entangled pure state $|\Psi\rangle$ of Eq. ([8]-5) that is prepared by Eve is then of the compact form

$$|\Psi\rangle = |\psi_{12}\overline{\psi_{34}}\rangle a + |\psi_{13}\overline{\psi_{24}}\rangle b, \tag{A4}$$

where qunit 1 is sent to Alice, qunit 2 is sent to Bob, and qunits 3 and 4 make up Eve's ancilla. We note that this is the generic form of $|\Psi\rangle$ because *all* alternatives are obtained from this $|\Psi\rangle$ by unitary transformations on the ancilla.

Now, the "asymmetric universal quantum cloning machines" [18], generalizations of the symmetric ones introduced by Bužek and Hillery [19], that are employed in Refs. [4,5] for the analysis of intercept attacks on the qunit in transmission from Alice to Bob, are characterized by a four-qunit state of the form (A4). The resulting states of the clone-anticlone pair are thus fully analogous to the ancilla states $|\widetilde{E}_{kl}^{(m)}\rangle$ in Eq. (A1). Of those, the ones with $k\neq l$ are orthogonal among themselves and orthogonal to those with $k=l$, and the latter form the pyramid of ancilla states described in Sec. II. Accordingly, Eve can extract more information if she applies the optimal POVM of Sec. III B to the clone-anticlone pair, rather than submitting them to the usual SRM.

[1] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978).

[2] C. H. Bennett and G. Brassard, in *IEEE Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.

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

[4] M. Bourennane, A. Karlsson, G. Björk, N. Gisin, and N. J. Cerf, J. Phys. A **35**, 10 065 (2002).

[5] N. J. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, Phys. Rev. Lett. **88**, 127902 (2002).

[6] A. Acín, N. Gisin, and V. Scarani, Quantum Inf. Comput. **3**, 563 (2003).

[7] See, e.g., the review article by A. Chefles, Contemp. Phys. **41**, 401 (2000), and the pertinent references therein.

[8] Y. C. Liang, D. Kaszlikowski, B.-G. Englert, L. C. Kwek, and C. H. Oh, Phys. Rev. A **68**, 022324 (2003).

[9] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).

[10] D. Bruß, M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, Phys. Rev. Lett. **91**, 097901 (2003).

[11] Put $N\to n$, $|E_k\rangle\to|E_{kk}\rangle$, and $\lambda\to 1-\beta_1/\beta_0$ to convert to the notational conventions of Ref. [8] . Other symbols, in particular r_0, r_1 and η_0, η_1, have the same significance.

[12] Geometrically speaking, the base of the N-dimensional pyramid is itself an $(N-1)$-dimensional pyramid with edges of length $\sqrt{2Nr_1}$ and an angle of 60° between them.

[13] P. Hausladen and W. K. Wootters, J. Mod. Opt. **41**, 2385 (1994).

[14] P. W. Shor, IBM J. Res. Dev. **48**, 115 (2004).

[15] J. Řeháček, B.-G. Englert, and D. Kaszlikowski, e-print quant-ph/0408134.

[16] D. Kaszlikowski, A. Gopinathan, Y. C. Liang, L. C. Kwek, and B.-G. Englert, e-print quant-ph/0307086.

[17] D. Kaszlikowski, J. Y. Lim, L. C. Kwek, and B.-G. Englert, e-print quant-ph/0312172.

[18] N. J. Cerf, Acta Phys. Slov. **48**, 115 (1998); J. Mod. Opt. **47**, 187 (2000); Phys. Rev. Lett. **84**, 4497 (2000).

[19] V. Bužek and M. Hillery, Phys. Rev. Lett. **81**, 5003 (1998).