Tomographic quantum cryptography

Yeong Cherng Liang,[1] Dagomir Kaszlikowski,[1] Berthold-Georg Englert,[1] Leong Chuan Kwek,[2,1] and C. H. Oh[1]

[1]*Department of Physics, National University of Singapore, 2 Science Drive 3, Singapore 117542, Singapore*

[2]*National Institute of Education, Nanyang Technological University, 1 Nanyang Walk, Singapore 639798, Singapore*

(Received 5 May 2003; published 29 August 2003)

We present a protocol for quantum cryptography in which the data obtained for mismatched bases are used in full for the purpose of quantum state tomography. Eavesdropping on the quantum channel is seriously impeded by requiring that the outcome of the tomography is consistent with unbiased noise in the channel. We study the incoherent eavesdropping attacks that are still permissible and establish under which conditions a secure cryptographic key can be generated. The whole analysis is carried out for channels that transmit quantum systems of any finite dimension.

DOI: 10.1103/PhysRevA.68.022324 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

The objective of quantum cryptography is the distribution of a secure cryptographic key between two parties, traditionally called Alice and Bob. The key consists of a truly random sequence of ‘‘letters.’’ The most important among the schemes proposed for this purpose—the 1984 protocol of Bennitt and Brassard (BB84) [1], and the 1991 protocol of Ekert's (E91) [2]—and all experimentally realized schemes (Refs. [3–7], in particular, but also others) use a binary alphabet, i.e., just two letters that are usually denoted by the numbers 0 and 1. A very readable account of the state of this art is the recent review paper by Gisin *et al.* [8].

Binary keys suffice, of course, for all practical purposes and they are relatively easily generated with the aid of binary quantum alternatives (qubits). In fact, the selected experiments cited above provide increasing evidence that it may be commercially viable to introduce feasible quantum cryptographic systems in the near future.

The utter simplicity of the kinematics of a qubit, the most elementary quantum degree of freedom, facilitates both the theoretical analysis and the experimental implementations. And yet, there is a natural curiosity about schemes for quantum cryptography that exploit richer degrees of freedom, especially ternary quantum alternatives (quutrits, for three-letter keys), and generally n-fold quantum alternatives (qunits, for n-letter keys with $n=2,3,4,\ldots$).

Almost all qunit schemes are generalizations of the familiar BB84 and E91 qubit protocols [9–12], and we deal with a particular generalization of E91 in the present paper. It is worth mentioning, however, that there is also at least one higher-dimensional scheme of quite a different kind, namely, the deterministic protocol of Beige *et al.* [13], in which four-dimensional systems (pairs of qubits, for instance) are used for the generation of a binary key.

The BB84 and E91 protocols are *in*deterministic because key letters are only obtained when Alice's and Bob's measurement bases match and, therefore, a substantial fraction of the data is not used at all (in BB84) or used just for security checks (in E91). In the protocol we analyze here, all measurement results for mismatched bases are exploited for complete quantum state tomography, by which Alice and Bob manage to impose very stringent conditions on the quantum channel and so limit eavesdropper Eve's possibilities substantially.

The paper is organized as follows. In Sec. II the stage is set by defining the tomographic protocol. Then we analyze, in Sec. III, what the eavesdropper can do and achieve, which prepares the subsequent determination of the security criterion in Sec. IV. We close with a summary of our results and a critical discussion of some crucial details.

II. THE TOMOGRAPHIC PROTOCOL

We consider a setup of the kind sketched in Fig. 1. A source emits entangled pairs of qunits to Alice and Bob, who receive one qunit each of every pair. The qunits distributed by the source in this manner constitute an effective quantum

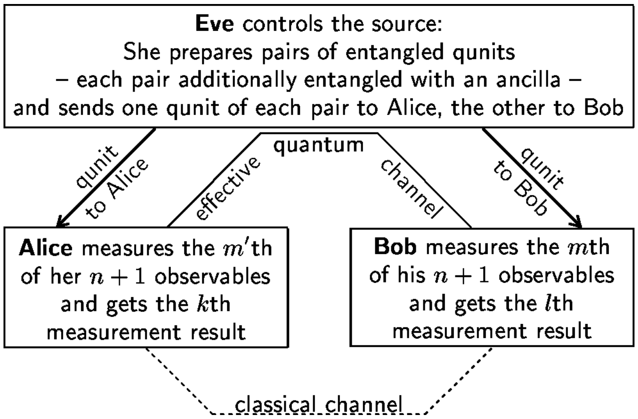
Eve controls the source:
She prepares pairs of entangled qunits
– each pair additionally entangled with an ancilla –
and sends one qunit of each pair to Alice, the other to Bob
qunit to Alice
effective
quantum
channel
qunit to Bob
Alice measures the m'th of her $n+1$ observables and gets the kth measurement result
Bob measures the mth of his $n+1$ observables and gets the lth measurement result
classical channel

FIG. 1. Schematic setup of the key distribution system. Alice and Bob are connected to each other by an effective quantum channel, which consists of a source that distributes entangled qunit pairs. For each qunit, Alice measures one of her tomographically complete observables, chosen at random when the qunit arrives. Bob does the same for each of his qunits. They exchange well-chosen information about their measurements through a classical channel, and conclude then whether or not the quantum channel has the right characteristics to allow for the generation of a secure cryptographic key from their raw data. In their security analysis, Alice and Bob assume that all imperfections of the quantum channel result from eavesdropper Eve's intervention and, to be on the safe side, they grant Eve full control of the source.

channel between Alice and Bob (A&B), although these two users are not themselves sending any quantum systems to each other. As a consequence of unavoidable imperfections, both in the functioning of the source and in the transmission line, this quantum channel will be noisy to some extent, so that A&B will not receive qunit pairs with the ideal properties they hope for.

Nevertheless, they will be able to generate a secure cryptographic key if the noise level is below a certain threshold. But to be on the safe side, they must determine this threshold level under the assumption that all imperfections result from their adversary Eve's intervention, who eavesdrops on the communication between A&B. In particular, one must grant Eve full control over the qunit-pair source, and she will try to know as much about the qunits detected by A&B as the laws of physics allow her to know.

After receiving a qunit from the source, Alice measures a nondegenerate observable that she selects at random from her set of $n+1$ tomographically complete observables [14,15]. She keeps a private record of the observables she measures and of the outcomes of her measurements. Likewise, Bob measures on each of his qunits an observable randomly chosen from his corresponding set, and keeps a record of his data as well. We adopt the notation of Ref. [20] and denote by $|m_k\rangle$ the kth eigenket of Alice's mth observable and by $|\overline{m_k}\rangle$ the kth eigenket of Bob's mth observable. The correspondence between the two sets of observables, or rather between the orthonormal measurement bases they provide, is then established by requiring that

$$\langle 0_j|m_k\rangle = \langle \overline{m_k}|\overline{0_j}\rangle \tag{1}$$

hold for $j,k=0,1,2,\ldots,n-1$ and $m=0,1,2,\ldots,n$. In short, the roles of bras and kets are interchanged.

Ideally, A&B wish to receive from the source the maximally entangled two-qunit state $|\psi\rangle$ that is specified by

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}|0_k\overline{0_k}\rangle\\ &= \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}|1_k\overline{1_k}\rangle\\ &= \cdots\\ &= \frac{1}{\sqrt{n}}\sum_{k=0}^{n-1}|n_k\overline{n_k}\rangle.\end{aligned} \tag{2}$$

As a consequence of Eq. (1), it has the same form regardless of the pair of observables that is used to define it.

When the transmission is over, A&B announce their choice of observables, their respective m values, for all qunits through a public channel. They can then divide the detected qunit pairs into two groups, one in which the measurement bases match [both m values are the same, which happens with a probability of $1/(n+1)$], and the other in which the bases do not match. In the absence of noise, the measurement results of the first group (the respective k values—referred to as *nit values*) are perfectly correlated and thus give rise to a cryptographic key in an alphabet with n letters.

In reality, however, A&B must take into account Eve's attempts at eavesdropping and the resulting disturbance of the quantum channel. As a consequence thereof, the statistical properties of the detected qunit pairs will not be correctly described by the pure two-qunit state of Eq. (2). Rather than the projector $|\psi\rangle\langle\psi|$, an appropriate statistical operator ρ applies to the qunit pairs emitted by a nonideal source.

Since A&B measure tomographically complete sets of observables on their respective qunits, they can determine the actual two-qunit state ρ from their measurement results. They exploit all data of the mismatched bases for this purpose, and some of the matched-bases data. Ideally, they wish for the projector $|\psi\rangle\langle\psi|$ but, realistically, they expect to find a ρ of the form

$$\rho=(\beta_0-\beta_1)|\psi\rangle\langle\psi|+\frac{\beta_1}{n}\quad\text{with}\quad\beta_0+(n-1)\beta_1=1, \tag{3}$$

which is what one gets when an imperfect transmission line admixes unbiased noise to $|\psi\rangle\langle\psi|$. The non-negative parameters β_0 and β_1 have the following physical significance: β_0 is the probability that Alice and Bob get the same nit value when the bases match, and β_1 is the probability that Bob gets a particular one of the $n-1$ values that are different from Alice's nit value.

Formally, ρ is a nonnegative operator of unit trace, and thus permissible as a statistical operator, whenever $0\leqslant\beta_1/\beta_0\leqslant n/(n-1)$. But only values in the range

$$0\leqslant\frac{\beta_1}{\beta_0}\leqslant 1 \tag{4}$$

correspond to an admixture of symmetric noise to $|\psi\rangle\langle\psi|$ and, therefore, this is the parameter range of interest. The limiting values mark the extreme situations of "no noise at all" ($\beta_0=1$, $\beta_1=0$) and "nothing but noise" ($\beta_0=\beta_1=1/n$).

Sources that emit two-qunit states of a kind different from Eq. (3) are not regarded as trustworthy by Alice and Bob. As the crucial, defining step of the *tomographic protocol*, they thus accept the raw key sequence only if their state tomography confirms that the source emits a two-qunit state of form (3). Otherwise, they reject the data wholly and use a different source.

III. EAVESDROPPING

A. Choosing the right ancilla states

By imposing this rather stringent requirement, A&B restrict Eve's possibilities markedly. Her strategy is to keep a quantum record of what she sends to A&B by entangling each qunit pair with an ancilla (an auxiliary system of her liking), and to perform a judiciously chosen measurement on the ancilla after carefully weighing the information exchanged by A&B through the public channel. Quite generally, Eve's option is to prepare an entangled pure state of the form

$$|\Psi\rangle=\sum_{k,l=0}^{n-1}|m_k\overline{m_l}\rangle|\tilde{E}_{kl}^{(m)}\rangle \quad (\text{any } m=0,1,\ldots,n), \tag{5}$$

where the $|\tilde{E}_{kl}^{(m)}\rangle$'s are the unnormalized kets of the ancilla states attached by Eve (with reference to the mth pair of A&B's observables). Since there is no advantage in generating a mixed state instead, it is sufficient to consider all such pure-state preparations.

Now, the two-qunit state received by A&B is obtained by tracing $|\Psi\rangle\langle\Psi|$ over the ancilla degree of freedom, and their insistence on getting ρ of Eq. (3) implies that Eve must choose her ancilla states such that they obey

$$\begin{aligned}\langle\tilde{E}_{kl}^{(m)}|\tilde{E}_{k'l'}^{(m)}\rangle&=\frac{\beta_0-\beta_1}{n}\delta_{kl}\delta_{k'l'}+\frac{\beta_1}{n}\delta_{kk'}\delta_{ll'}\\&=\begin{cases}\beta_0/n & \text{if} \quad k=l=k'=l',\\ \beta_1/n & \text{if} \quad k=k'\neq l=l',\\ (\beta_0-\beta_1)/n & \text{if} \quad k=l\neq k'=l',\\ 0 & \text{otherwise.}\end{cases}\end{aligned} \tag{6}$$

The right-hand side does not depend on the m value to which the ancilla states on the left refer and, therefore, the mapping $|\tilde{E}_{kl}^{(m)}\rangle\rightarrow|\tilde{E}_{kl}^{(m')}\rangle$ is unitary. Quite explicitly, two different sets of ancilla states are related to each other by

$$|\tilde{E}_{kl}^{(m)}\rangle=\sum_{k',l'}|\tilde{E}_{k'l'}^{(m')}\rangle\langle m_k|m'_{k'}\rangle\langle m'_{l'}|m_l\rangle, \tag{7}$$

which is an immediate consequence of Eqs. (5) and (1). As a check of consistency, one can exploit the completeness and orthonormality of the single-qunit states $|m_k\rangle$ to verify rather easily that Eq. (6) holds for any m value, if it holds for one of them. In summary, then, it does not matter which m value Eve chooses in Eq. (5).

It is expedient to introduce normalized ancilla states $|E_{kl}^{(m)}\rangle$ in accordance with

$$k=l: \quad |\tilde{E}_{kk}^{(m)}\rangle=|E_{kk}^{(m)}\rangle\sqrt{\beta_0/n}, \tag{8}$$

$$k\neq l: \quad |\tilde{E}_{kl}^{(m)}\rangle=|E_{kl}^{(m)}\rangle\sqrt{\beta_1/n}.$$

Then

$$\langle E_{kl}^{(m)}|E_{k'l'}^{(m)}\rangle=\begin{cases}1 & \text{if} \quad k=k' \text{ and } l=l',\\ 1-\beta_1/\beta_0 & \text{if} \quad k=l\neq k'=l',\\ 0 & \text{otherwise,}\end{cases} \tag{9}$$

and

$$|\Psi\rangle=\sqrt{\frac{\beta_0}{n}}\sum_{k=0}^{n-1}|m_k\overline{m_k}\rangle|E_{kk}^{(m)}\rangle+\sqrt{\frac{\beta_1}{n}}\sum_{k\neq l}|m_k\overline{m_l}\rangle|E_{kl}^{(m)}\rangle \quad (\text{any } m=0,\ldots,n). \tag{10}$$

As stated in Eq. (9), for each m value, the ancilla states $|E_{kl}^{(m)}\rangle$ with $k\neq l$ are orthogonal to each other and orthogonal to the ones with $k=l$. The latter are not orthogonal among themselves (except when $\beta_1=\beta_0$, the case of pure noise and of very little interest), but rather have the same inner products for all pairs,

$$k\neq l: \ \langle E_{kk}^{(m)}|E_{ll}^{(m)}\rangle=1-\frac{\beta_1}{\beta_0}. \tag{11}$$

The n ancilla states $|E_{kk}^{(m)}\rangle$ are thus linearly independent, except when $\beta_1=0$, which is the ideal situation of no noise at all, that is, no eavesdropping [27].

B. Ancilla subspaces

This exception aside, the $k=l$ ancilla states $|E_{kk}^{(m)}\rangle$ span an n-dimensional subspace that is orthogonal to the (n^2-n)-dimensional subspace spanned by the $k\neq l$ states. We refer to them as the *first* and the *second* subspace, respectively. The subspaces associated with different m values are related to each other by the unitary transformations of Eq. (7).

Eve takes advantage of the structure of these subspaces in the eavesdropping attack that we now proceed to describe. We shall deal solely with attacks, in which she performs measurements on the ancillas one by one, commonly termed *incoherent* attacks. By contrast, in a *coherent* attack, she would measure some joint observables of a few, or perhaps many, ancillas [28]. This limitation is mainly dictated by the technical difficulties that one faces when analyzing coherent attacks. We note, however, that some have argued—notably Cirac and Gisin [29], and Wang [30]—that coherent attacks are not more powerful than incoherent attacks, but their arguments refer rather explicitly to protocols of the BB84 type, with intercept-resend eavesdropping attacks, and are not immediately applicable to our tomographic qunit protocol.

Eve's incoherent eavesdropping procedure is as follows. The information exchanged by A&B over the classical channel identifies those qunit pairs that contribute to the raw key sequence, the ones for which Alice's m value is the same as Bob's. To find out, as much as she can, about the nit values that A&B have recorded for each of these matched qunit pairs, Eve performs a suitably chosen measurement on the respective ancillas, one at a time. The statistical operator for one of these ancillas is obtained by tracing $|\Psi\rangle\langle\Psi|$ over the qunit degrees of freedom, with the outcome

$$\rho_{\text{Eve}}^{(m)}=\frac{\beta_0}{n}\sum_{k=0}^{n-1}|E_{kk}^{(m)}\rangle\langle E_{kk}^{(m)}|+\frac{\beta_1}{n}\sum_{k\neq l}|E_{kl}^{(m)}\rangle\langle E_{kl}^{(m)}|, \tag{12}$$

where m identifies the matched pair of bases. The first summation corresponds to the situation, in which A&B get the same nit value and the ancilla ends up in the first subspace, which happens with probability β_0. And the situation of differing nit values, when the final ancilla state is in the second subspace, is accounted for by the second summation, which carries the complementary weight of $(n-1)\beta_1=1-\beta_0$.

Since the various $\rho_{\mathrm{Eve}}^{(m)}$'s $(m=0,1,\ldots,n)$ are unitarily equivalent, it is sufficiently general to consider just one m value. For notational simplicity, we leave it implicit from here on and suppress the m label. Then we have

$$\rho_{\mathrm{Eve}}=\beta_0\rho^{(=)}+(1-\beta_0)\rho^{(\neq)}, \tag{13}$$

with

$$\rho^{(=)}=\frac{1}{n}\sum_{k=0}^{n-1}|E_{kk}\rangle\langle E_{kk}| \tag{14}$$

and

$$\rho^{(\neq)}=\frac{1}{n(n-1)}\sum_{k\neq l}|E_{kl}\rangle\langle E_{kl}|. \tag{15}$$

The first of these conditional statistical operators, $\rho^{(=)}$, applies when A&B have the same nit value and the second, $\rho^{(\neq)}$, applies when they do not. Since $\rho^{(=)}$ and $\rho^{(\neq)}$ reside in the first and second subspaces, respectively, Eve can discriminate between the two situations unambiguously.

Suppose she thus establishes that different nit values are the case. Under this circumstance, she performs a measurement that distinguishes between the $k\neq l$ ancilla states, which is surely possible because they are mutually orthogonal. She finds the ancilla in the state with ket $|E_{kl}\rangle$, say, and then knows with certainty that Alice's nit value is k and Bob's is l (with $k\neq l$, of course).

By contrast, if Eve establishes that the nit values of A&B are the same, she cannot find out with certainty what is this common value because the $k=l$ ancilla states are not orthogonal to each other, except when the $\beta_1=\beta_0$ limit is reached in Eq. (4) and the right-hand side vanishes in Eq. (11).

For $\beta_1<\beta_0$, Eve's attempts in discerning the nonorthogonal $|E_{kk}\rangle$ ancilla states in the first subspace are prone to error. Recalling Eq. (11), we note that the inner product for each pair of them is the same positive number, just like it is for the vectors pointing from the tip of a pyramid to the corners at its base. It is known that the error-minimizing measurement for such "pyramid states" is the so-called *square-root measurement* (see, e.g., Refs. [31,32] and the pertinent references therein, in particular Refs. [33,34]). Although demonstrating this optimality requires a careful argument, it is easy to grasp the basic idea of a square-root measurement.

C. Square-root measurement

For the following, up to and including Eq. (27), we restrict the discussion to the first subspace. Then, the n kets

$$|e_{kk}\rangle=\frac{1}{\sqrt{n\rho^{(=)}}}|E_{kk}\rangle \tag{16}$$

decompose the identity by construction,

$$\sum_k |e_{kk}\rangle\langle e_{kk}|=1, \tag{17}$$

and thus define a generalized measurement—the square-root measurement. Now note the eigenvalue equations

$$(\rho^{(=)}-r_0)\sum_j |E_{jj}\rangle=0, \tag{18a}$$

$$(\rho^{(=)}-r_1)\left(|E_{kk}\rangle-\frac{1}{n}\sum_j |E_{jj}\rangle\right)=0, \tag{18b}$$

with

$$r_0=1-\frac{n-1}{n}\frac{\beta_1}{\beta_0},\quad r_1=\frac{\beta_1}{n\beta_0}, \tag{19}$$

so that

$$r_0+(n-1)r_1=1,\quad r_0-r_1=1-\frac{\beta_1}{\beta_0}. \tag{20}$$

The eigenvalue r_0 is nondegenerate, whereas r_1 is $(n-1)$-fold, and not n-fold, because the n kets in Eq. (18b) have a vanishing sum. We make use of these eigenvalues in writing

$$\frac{1}{\sqrt{\rho^{(=)}}}=\frac{r_0+\sqrt{r_0r_1}+r_1-\rho^{(=)}}{\sqrt{r_0r_1}(\sqrt{r_0}+\sqrt{r_1})} \tag{21}$$

and then exploit Eq. (18) to establish

$$|e_{kk}\rangle=\frac{1}{\sqrt{nr_1}}\Big(|E_{kk}\rangle-\frac{1-\sqrt{r_1/r_0}}{n}\sum_j |E_{jj}\rangle. \tag{22}$$

The parameters η_0 and η_1 that appear in the probability amplitudes

$$\langle e_{kk}|E_{ll}\rangle=\sqrt{\eta_0}\delta_{kl}+\sqrt{\eta_1}(1-\delta_{kl}) \tag{23}$$

are crucial, inasmuch as they quantify Eve's knowledge about the common nit value of A&B: Upon finding $|e_{kk}\rangle$, she knows that the actual nit value is k with probability η_0, and that it is either one of the $n-1$ other values with probability η_1. In conjunction with Eq. (20), the required normalization

$$\eta_0+(n-1)\eta_1=1 \tag{24}$$

follows immediately from the explicit expressions

$$\sqrt{\eta_0}=\frac{\sqrt{r_0}+(n-1)\sqrt{r_1}}{\sqrt{n}},\quad \sqrt{\eta_1}=\frac{\sqrt{r_0}-\sqrt{r_1}}{\sqrt{n}}. \tag{25}$$

The implied identity

$$\sqrt{\eta_0} - \sqrt{\eta_1} = \sqrt{\frac{\beta_1}{\beta_0}} \tag{26}$$

is worth noting.

We close the discussion of the square-root measurement in the first subspace with the observation that Eve's reference states $|e_{kk}\rangle$ are orthonormal,

$$\langle e_{kk}|e_{ll}\rangle = \delta_{kl}\,. \tag{27}$$

As a consequence, the generalized measurement defined by decomposition (17) is in fact a standard von Neumann measurement.

Now returning to the general discussion of the full statistical operator (13), we summarize Eve's strategy as follows. She performs a measurement that distinguishes the n^2 states [35]

$$|e_{kl}\rangle = \begin{cases} \text{as given in Eq. (22)} & \text{for } k=l, \\ |E_{kl}\rangle & \text{for } k\neq l, \end{cases} \tag{28}$$

which are orthonormal. With probability $(n-1)\beta_1 = 1-\beta_0$ she finds a state with $k\neq l$, and then infers that Alice's nit value is k, and Bob's is l. And when Eve finds a $k=l$ state, which happens with probability β_0, she knows that A&B have the same nit value and can guess it right with probability η_0, but will guess a particular one of the $n-1$ wrong values with probability η_1.

D. Probabilities

In more formal terms, the joint probability that, for matched bases, Alice gets nit value k, Bob gets l, and Eve detects $|e_{k'l'}\rangle$ is given by

$$\begin{aligned} p_{kl;k'l'} &= |\langle \tilde{E}_{kl}|e_{k'l'}\rangle|^2 \\ &= \frac{\beta_0}{n}\delta_{kl}\delta_{k'l'}[(\eta_0-\eta_1)\delta_{kk'}+\eta_1] \\ &\quad + \frac{\beta_1}{n}(1-\delta_{kl})\delta_{kk'}\delta_{ll'}\,. \end{aligned} \tag{29}$$

All reduced and conditional probabilities are derived from this expression by partial summation and normalization. For later reference we note the joint probabilities for Alice and Bob,

$$p_{kl}^{(\text{A\&B})} = \sum_{k',l'} p_{kl;k'l'} = \frac{1}{n}[(\beta_0-\beta_1)\delta_{kl}+\beta_1], \tag{30}$$

and for Alice and Eve,

$$\begin{aligned} p_{k;k'l'}^{(\text{A\&E})} &= \sum_{l} p_{kl;k'l'} \\ &= \frac{\beta_0}{n}\delta_{k'l'}[(\eta_0-\eta_1)\delta_{kk'}+\eta_1] + \frac{\beta_1}{n}\delta_{kk'}(1-\delta_{k'l'}), \end{aligned} \tag{31}$$

as well as the individual probabilities for Alice and Bob,

$$p_k^{(\text{A})} = \sum_{l,k',l'} p_{kl;k'l'} = \frac{1}{n}, \quad p_l^{(\text{B})} = \sum_{k,k',l'} p_{kl;k'l'} = \frac{1}{n}, \tag{32}$$

and for Eve,

$$p_{k'l'}^{(\text{E})} = \sum_{k,l} p_{kl;k'l'} = \frac{1}{n}[(\beta_0-\beta_1)\delta_{k'l'}+\beta_1]. \tag{33}$$

To get a first rough understanding of the significance of A&B's probabilities β_0,β_1 and Eve's conditional probabilities η_0,η_1, consider this scenario. A qunit pair has been received by A&B and detected with matched bases. Both Bob and Eve are asked to bet on Alice's nit value. Bob's best strategy is to guess that Alice's value agrees with his own, and he guesses right with probability β_0, but he is never sure about Alice's nit value. Eve, by contrast, knows Alice's nit value with certainty when detecting the ancilla in one of the $k\neq l$ states of Eq. (28), and guesses right with probability η_0 otherwise. Her total betting odds are thus $1-\beta_0+\beta_0\eta_0$. The comparison with Bob's establishes that, if such bets are performed frequently,

$$\text{Bob wins more often if } \beta_0 > (n+3)\beta_1\,, \tag{34}$$

$$\text{Eve wins more often if } \beta_0 < (n+3)\beta_1\,,$$

$$\text{and they come out even if } \beta_0 = (n+3)\beta_1\,.$$

These betting odds are, however, really only a rough measure of Bob's and Eve's knowledge about Alice's nit value, because Eve's information is qualitatively different from Bob's. As discussed in the following section, the ratio β_1/β_0 must be substantially below the $1/(n+3)$ threshold of Eq. (34) if A&B want to be able to generate a secure key from the raw key sequence that these bets are about.

IV. SECURITY CRITERION

A. Csiszár-Körner threshold

A more systematic quantitative measure of what Bob and Eve know about Alice's nit values is the mutual information between the respective parties. With the probabilities of Eqs. (30) and (32), we get

$$\begin{aligned} I(\text{A\&B}) &= \sum_{k,l} p_{kl}^{(\text{A\&B})} \log_n \frac{p_{kl}^{(\text{A\&B})}}{p_k^{(\text{A})} p_l^{(\text{B})}} \\ &= 1+\beta_0\log_n\beta_0+(1-\beta_0)\log_n\beta_1 \end{aligned} \tag{35}$$

for the mutual information between Alice and Bob, where, fitting to the n-letter alphabet, the logarithm is taken to base n. Likewise, the mutual information between Alice (or Bob) and Eve is given by

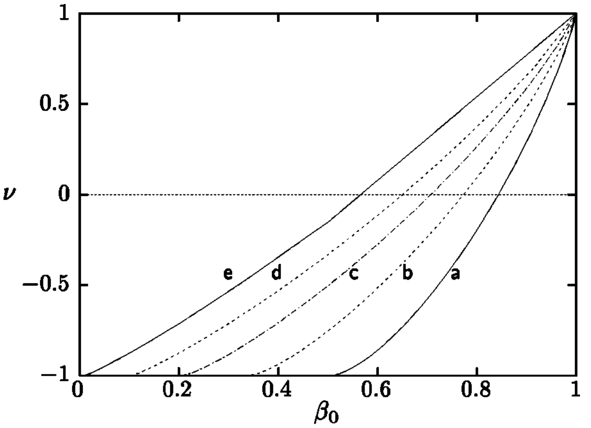

FIG. 2. The difference ν, defined in Eq. (37), of the mutual information between Alice and Bob and between Eve and either one of them, as a function of β_0, for various values of n. Curves a–e are for $n=2$, 3, 5, 10, and 100, respectively. A secure key can be generated from the raw key sequence if ν is positive. The threshold value of β_0, the point of intersection with the $\nu=0$ line, decreases with increasing n and approaches $\beta_0=\frac{1}{2}$ for $n\rightarrow\infty$.

$$I(\mathrm{A\&E})=\sum_{k,k',l'} p^{(\mathrm{A\&E})}_{k;k'l'}\log_n\frac{p^{(\mathrm{A\&E})}_{k;k'l'}}{p^{(\mathrm{A})}_{k}p^{(\mathrm{E})}_{k'l'}}$$

$$=1+\beta_0[\eta_0\log_n\eta_0+(1-\eta_0)\log_n\eta_1]. \quad (36)$$

Their difference

$$\nu\equiv I(\mathrm{A\&B})-I(\mathrm{A\&E})$$

$$=\beta_0\log_n\beta_0+(1-\beta_0)\log_n\beta_1$$

$$-\beta_0[\eta_0\log_n\eta_0+(1-\eta_0)\log_n\eta_1] \quad (37)$$

is shown in Fig. 2 for $n=2$, 3, 5, 10, and 100 over the β_0 range of Eq. (4). There, it is a monotonically increasing function of β_0 that grows from $\nu=-1$ for $\beta_0=1/n$ to $\nu=1$ for $\beta_0=1$. The values of β_0, where the sign of ν changes, are listed in Table I for some n, along with the corresponding values of $n\beta_1/\beta_0$ and the ratio η_1/η_0 of Eve's conditional probabilities.

TABLE I. Threshold values of some parameters. For the various n values of the first column, table reports values of β_0, $n\beta_1/\beta_0$, and η_1/η_0 for which the CK threshold is reached ($\nu=0$), or for which the CK yield is 50% ($\nu=\frac{1}{2}$). The limiting values for $n\rightarrow\infty$ are shown in the last row.

	$\nu=0$			$\nu=0.5$		
n	β_0	$n\beta_1/\beta_0$	η_1/η_0	β_0	$n\beta_1/\beta_0$	η_1/η_0
2	0.8436	0.3707	0.2659	0.9357	0.1373	0.4661
3	0.7733	0.4398	0.2741	0.9050	0.1574	0.4649
4	0.7334	0.4846	0.2790	0.8870	0.1698	0.4641
5	0.7077	0.5163	0.2821	0.8750	0.1785	0.4635
10	0.6503	0.5975	0.2880	0.8468	0.2010	0.4604
30	0.6016	0.6851	0.2887	0.8203	0.2266	0.4532
50	0.5881	0.7146	0.2872	0.8123	0.2358	0.4496
100	0.5747	0.7475	0.2843	0.8040	0.2462	0.4448
∞	0.5	1	0.25	0.75	0.3333	0.4019

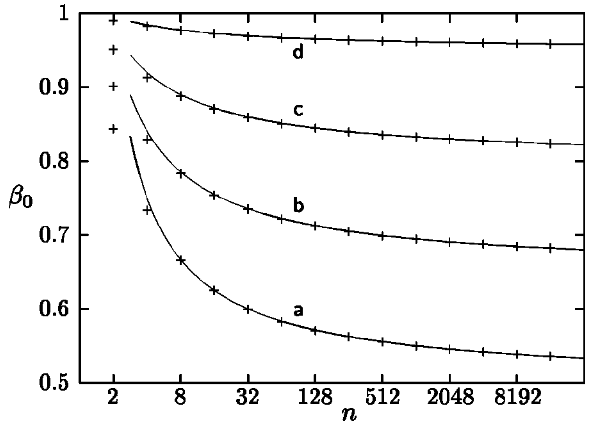

FIG. 3. Threshold values of β_0 for CK yields of 0%, 30%, 60%, and 90%. As a function of n, with the abscissa linear in $\log n$, the crosses display the exact values of β_0 for which $\nu=0$ (set a), $\nu=0.3$ (set b), $\nu=0.6$ (set c), or $\nu=0.9$ (set d), respectively. The solid lines show the corresponding values of the analytical approximation (38), which is assuredly good for large n values, but performs remarkably well even for small ones.

Now, according to the Csiszár-Körner (CK) Theorem [36], a secure cryptographic key can be generated from the raw key sequence, by means of a suitably chosen error correcting code and classical (one-way) communication between Alice and Bob, if the mutual information between Alice and Bob exceeds that between Eve and either of them. In the present context, this is to say that the tomographic protocol is secure (under the incoherent eavesdropping attacks considered) if $\nu>0$. Moreover, ν is then the yield of the key generation, in the sense that a secure key of length νL can be obtained from a raw key sequence of length L. This invites to call $\max\{0,\nu\}$ the *CK yield*. It is positive when β_0 is larger than the threshold values of Table I and vanishes at and below the threshold.

Any actual implementation of the tomographic protocol for quantum key distribution needs a reasonable efficiency. The $\nu=0$ threshold is then of less interest than, say, the $\nu=\frac{1}{2}$ threshold at which the CK yield reaches 50%. The respective values of β_0, $n\beta_1/\beta_0$, and η_1/η_0 are also listed in Table I.

For sufficiently large n, the threshold values of β_0 are well approximated by

$$\beta_0\approx\frac{1+\nu+\log_n\dfrac{2}{1-\nu}}{2+\log_n\dfrac{1+\nu}{1-\nu}}, \quad (38)$$

which becomes the strikingly simple $\beta_0\approx\frac{1}{2}(1+\log_n 2)$ for $\nu=0$. By comparing with the entries given in the second and fifth columns of Table I, we observe that the error is 1% or less for $\nu=0$ and $n>4$, or $\nu=\frac{1}{2}$ and $n>3$. For $\nu=0$, 0.3, 0.6, and 0.9, we illustrate (38) in Fig. 3.

B. Channel capacities

It is interesting to view the CK security criterion also from another perspective of information theory. Rather than mutual information, the relevant notion is then that of channel capacity.

The generation of the raw key can be regarded as the outcome of a communication between Alice and Bob through the effective quantum channel of Fig. 1. By choosing her observables and measuring them, Alice effectively prepares the qunits sent to Bob in the states resulting from the formal procedure of state reduction. For instance, after Alice has measured her mth observable and found $|m_k\rangle$ for her qunit, her reduced statistical operator for Bob's qunit is

$$\rho_k^{(\mathrm{B},m)}=(\beta_0-\beta_1)|\overline{m_k}\rangle\langle\overline{m_k}|+\beta_1, \tag{39}$$

with each k value occurring—or, now, *being sent*—with probability $1/n$. Upon measuring his mth observable, Bob gets the nit value k with probability β_0 and each of the $n-1$ other ones with probability β_1, quite consistent, of course, with the joint probabilities (30).

These projective measurements carried out by Bob can be interpreted as his attempt to extract the information encoded by Alice in the states $\rho_k^{(\mathrm{B},m)}$, so that, for every m, a certain quantum channel is thus defined between Alice and Bob. Since, for a given m, Bob gets all right nit values with the same probability β_0/n, and all wrong values with the same probability β_1/n, we are in fact dealing with a so-called *weakly symmetric channel* [37]. For a channel of this kind, transmission at full capacity is achieved for totally random input, as is the case here.

All m values are equivalent, and the capacity of each channel, $C(\mathrm{A\&B})=1+\beta_0\log_n\beta_0+(1-\beta_0)\log_n\beta_1$, is just equal to the mutual information $I(\mathrm{A\&B})$ of Eq. (35) [38]. A similar reasoning applies to the effective ancilla channel between Alice and Eve that is associated with Eve's square-root measurement. The capacity $C(\mathrm{A\&E})$ of this channel is also equal to the corresponding mutual information $I(\mathrm{A\&E})$ of Eq. (36).

It follows that the CK threshold criterion for the tomographic protocol has a simple intuitive meaning: secure one-way communication is possible if the capacity of the channel between Alice and Bob is higher than the capacity of the channel between Alice and Eve.

V. SUMMARY AND DISCUSSION

The protocol for quantum key distribution that is described and analyzed in this paper differs from other protocols by the element of complete quantum state tomography. For this purpose, Alice and Bob exploit the measurement results they obtain for unmatched bases, rather than just discarding these data as one does in the BB84 protocol and its various generalizations. The check for a violation of Bell's inequality in the E91 protocol amounts to a partial state tomography and, in this sense, our tomographic protocol might be viewed as a refinement and generalization of the E91 protocol.

In the tomographic protocol, Alice and Bob insist on the source emitting entangled two-qunit states of a particular form—only states from a one-parametric family are in fact regarded as acceptable—and thereby they limit Eve's choice of eavesdropping attacks stringently. Up to unitary equivalence, there is then only one preparation by Eve of the qunit pairs, entangled with her ancilla states, that gives her best knowledge of the raw key sequence obtained by Alice and Bob. But even with this optimized eavesdropping attack, Eve does not acquire enough information to prevent Alice and Bob from generating a secure key, provided that the two-qunit state is in the parameter range where the Csiszár-Körner theorem applies. Alice and Bob find out whether this is the case when they determine the parameters of the two-qunit state by state tomography.

But the story does not end here. If the source emits states outside the parameter regime where an immediate key generation is possible, Alice and Bob might still be able to achieve their objective although it seems that Eve knows too much. They just need to first "distill" a better raw key, for which purpose they can choose between the quantum procedure of *entanglement distillation* [39,40] and the classical procedure of *advantage distillation* [41]. Recent work establishes [42] that both procedures are applicable if $\beta_0>2\beta_1$ and only then, which is, therefore, the true threshold condition for the tomographic protocol.

The square-root measurement, on which the present analysis of Eve's incoherent attack is based (and also the analysis in Ref. [42]), maximizes Eve's odds of guessing Alice's nit values right but, as noted by Shor [43], it does not always maximize her information about them. In other words, it may happen that a (slightly) larger value of the mutual information between Alice and Eve obtains for another measurement. The only case on record for which this is known to occur is, however, a very flat $n=3$ pyramid of states, outside the physical parameter range of Eq. (4). Other cases are likely to exist, possibly also for larger n values and rather tall pyramids. If so, the CK threshold values would be changed (slightly), but presently there is no indication that the $\beta_0>2\beta_1$ condition for successful distillation is affected. These matters are not settled as yet, systematic investigations are being performed, and results will be reported in due course.

In protocols of the BB84 type, Alice prepares qunits and sends them to Bob, with Eve eavesdropping on the quantum channel. As discussed in Sec. IV B, one method of preparation could be to detect one qunit of an entangled pair, thereby reducing the state of the other, which is on its way to Bob. In the setup of Fig. 1 this would amount to having, so to say, the source inside Alice's laboratory. It follows that our analysis has a bearing also on schemes of the BB84 type. Reversing the argument, no matter how Alice prepares the qunit sent to Bob, she can treat her record of it as if it were the result of a measurement on another qunit, be it real or virtual. Alice and Bob can then treat their joint records as if the data referred to entangled qunit pairs, and apply the tomographic protocol. In effect, this limits Eve's choice of eavesdropping attacks on the quantum channel in an analogous way and, as a consequence, our results are also applicable to tomographic protocols of this other kind.

In the security analysis of protocols of BB84 type, Eve is assumed to intercept the qunits in transmission, to use some cloning device for copying the qunit state with the fidelity permitted by quantum limitations, and to perform eventually a suitable measurement on the quantum copy. It is in this context of single-qunit protocols that relations equivalent to Eq. (25) were first derived for qutrits ($n=3$) by Bruß and Macchiavello [9,44], and conjectured to hold for arbitrary n [9,45]. Also, the $\beta_0 > 2\beta_1$ threshold condition for both distillation procedures applies to BB84-type qunit protocols [45,46]. And for the question about the optimality of Eve's square-root measurement in the tomographic protocol, there is an analogous question about the optimal cloning device in single-qunit protocols. In view of these close interrelations, a definite answer to one of them will surely teach us a lesson about the other question too.

ACKNOWLEDGMENTS

We gratefully acknowledge valuable discussions with D. Bruß, K. Chang, M. Christandl, T. Durt, A. Ekert, A. Gopinathan, D. Gosal, and C. Macchiavello. This work was supported by A*Star Grant No. 012-104-0040.

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

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

[3] T. Jennewein, C. Simon, G. Weihs, H. Weinfurter, and A. Zeilinger, Phys. Rev. Lett. **84**, 4729 (2000).

[4] D.S. Naik, C.G. Peterson, A.G. White, A.J. Berglund, and P.G. Kwiat, Phys. Rev. Lett. **84**, 4733 (2000).

[5] W. Tittel, J. Brendel, H. Zbinden, and N. Gisin, Phys. Rev. Lett. **84**, 4737 (2000).

[6] C. Kurtsiefer, P. Zarda, M. Halder, H. Weinfurter, P.M. Gorman, P.R. Tapster, and J.G. Rarity, Nature (London) **419**, 450 (2002).

[7] E. Waks, K. Inoue, C. Santori, D. Fattal, J. Vuckovic, G.S. Solomon, and Y. Yamamoto, Nature (London) **420**, 762 (2002).

[8] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[9] D. Bruß and C. Macchiavello, Phys. Rev. Lett. **88**, 127901 (2002).

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

[11] D. Kaszlikowski, D.K.L. Oi, M. Christandl, K. Chang, A. Ekert, L.C. Kwek, and C.H. Oh, Phys. Rev. A **67**, 012310 (2003).

[12] T. Durt, N.J. Cerf, N. Gisin, and M. Żukowski, e-print quant-ph/0207057.

[13] A. Beige, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, J. Phys. A **35**, L407 (2002).

[14] The statistical operator of a single qunit has $n^2-1=(n+1)(n-1)$ independent real parameters. Repeated measurements of one nondegenerate qunit observable establish the values of $n-1$ parameters and, therefore, any tomographically complete set of single-qunit observables contains at least a total number of $n+1$ independent observables. Alice and Bob could each use more than this minimum number of observables, but for the sake of simplicity in notation we assume that they do not. Note that a qunit pair would require only n^2+1 two-qunit observables for complete state tomography, rather than the $(n+1)^2$ pairs of single-qunit observables that Alice and Bob are using.

[15] Wootters and Fields [16] showed that sets of pairwise complementary observables [17] are ideal for tomographic purposes and, extending earlier work by Ivanović [18], they constructed such sets for the case that n is a prime or a power of a prime. These distinguished sets of tomographically complete observables are central to the generalizations [19–21] of the 1987 spin-retrodiction puzzle of Vaidman, Aharonov, and Albert [22], of which a quantum-optical version was realized recently [23].

[16] W.K. Wootters and B.D. Fields, Ann. Phys. (N.Y.) **191**, 363 (1989).

[17] Any single pair of complementary observables is *algebraically complete*, and for any quantum degree of freedom one can find such pairs, with characteristic properties. See Ref. [24] for a textbook discussion of these insights of Weyl [25] and Schwinger [26].

[18] I.D. Ivanović, J. Phys. A **14**, 3241 (1981).

[19] Y. Aharonov and B.-G. Englert, Z. Naturforsch. **56a**, 16 (2001).

[20] B.-G. Englert and Y. Aharonov, Phys. Lett. A **284**, 1 (2001).

[21] P.K. Aravind, Z. Naturforsch. **58a**, 85 (2003).

[22] L. Vaidman, Y. Aharonov, and D.Z. Albert, Phys. Rev. Lett. **58**, 1385 (1987).

[23] O. Schulz, R. Steinhübl, M. Weber, B.-G. Englert, C. Kurtsiefer, and H. Weinfurter, Phys. Rev. Lett. **90**, 177901 (2003).

[24] J. Schwinger, *Quantum Mechanics. Symbolism of Atomic Measurements* (Springer, Heidelberg, 2001).

[25] H. Weyl, Z. Phys. **46**, 1 (1927); *Gruppentheorie und Quantenmechanik* (Hirzel, Leipzig, 1928); English translation by H. P. Robertson, *Theory of Groups and Quantum Mechanics* (Dutton, New York, 1932).

[26] J. Schwinger, Proc. Natl. Acad. Sci. U.S.A. **46**, 570 (1960); in *Exact Sciences and Their Philosophical Foundations*, edited by W. Deppert, K. Hübner, A. Oberschelp, and V. Weidemann (Verlag Peter Lang, Frankfurt am Main, 1985).

[27] Another exception occurs for $\beta_1/\beta_0=n/(n-1)$, but this ratio is outside range (4) of physical interest.

[28] More generally, one could consider coherent attacks in which Eve prepares entangled multiqunit-pair states rather than the single-qunit-pair state of Eq. (3). Alice and Bob would then notice correlations between different qunit pairs. We take for granted that they protect themselves by also looking for such correlations at the time when they exchange information for the primary purpose of state tomography.

[29] J.I. Cirac and N. Gisin, Phys. Lett. A **229**, 1 (1997).

[30] Wang Xiang-bin, e-print quant-ph/0110089.

[31] A. Chefles, Contemp. Phys. **41**, 401 (2000).

[32] S.M. Barnett, Phys. Rev. A **64**, 030303 (2001).

[33] C. W. Helstrom, *Quantum Detection and Estimation Theory* (Academic Press, New York, 1976).

[34] A.S. Holevo, Theor. Probab. Appl. **23**, 411 (1978).

[35] Remember that the m label is suppressed. There is a set of n^2 states of kind (28) for each value of m.

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

[37] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley-Interscience, New York, 1991).

[38] More precisely, we have $n+1$ *sub*channels, one for each m value, and together they constitute the total channel. Its capacity is $C_{\mathrm{tot}}(\mathrm{A\&B})=I(\mathrm{A\&B})+\log_n(n+1)$, where the last term accounts for the fact that each subchannel appears with the same probability. However, this additional term is of no consequence, because no information is encoded in the switching between the subchannels. Or, put formally, the extra term is added both to $C_{\mathrm{tot}}(\mathrm{A\&B})$ and to $C_{\mathrm{tot}}(\mathrm{A\&E})$, and has no effect on their difference.

[39] Entanglement distillation was originally proposed for qubits under the name of *quantum privacy amplification* by D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera, Phys. Rev. Lett. **77**, 2818 (1996).

[40] M. Horodecki and P. Horodecki, Phys. Rev. A **59**, 4206 (1999).

[41] U.M. Maurer, IEEE Trans. Inf. Theory **39**, 733 (1993).

[42] D. Bruß, M. Christandl, A. Ekert, B.-G. Englert, D. Kaszlikowski, and C. Macchiavello, e-print quant-ph/0303184.

[43] P.W. Shor, e-print quant-ph/0206058.

[44] Put $n \rightarrow d$, $\beta_0 \rightarrow 1-D$, and $\eta_0 \rightarrow f_d(D)$ to convert our notational conventions to those of Ref. [9].

[45] A. Acín, N. Gisin, and V. Scarani, e-print quant-ph/0303009.

[46] N. Gisin and S. Wolf, Phys. Rev. Lett. **83**, 4200 (1999).