Reduced randomness in quantum cryptography with sequences of qubits encoded in the same basis

L.-P. Lamoureux,[1] H. Bechmann-Pasquinucci,[2,3] N. J. Cerf,[1] N. Gisin,[4] and C. Macchiavello[2]
[1]*Quantum Information and Communication, Ecole Polytechnique, CP 165, Université Libre de Bruxelles, 1050 Brussels, Belgium*
[2]*Quantum Information Theory group (QUIT), Dipartimento di Fisica "A. Volta" and INFM - Unità di Pavia, Via Bassi 6, I-27100 Pavia, Italy*
[3]*UCCI.IT, via Olmo 26, I-23888 Rovagnate, Italy*
[4]*Group of Applied Physics, University of Geneva, 1211 Geneva 4, Switzerland*

(Received 6 July 2005; published 2 March 2006)

We consider the cloning of sequences of qubits prepared in the states used in the BB84 or six-state quantum cryptography protocol, and show that the single-qubit fidelity is unaffected even if entire sequences of qubits are prepared in the same basis. This result is only valid provided that the sequences are much shorter than the total key. It is of great importance for practical quantum cryptosystems because it reduces the need for high-speed random number generation without impairing on the security against finite-size cloning attacks.

DOI: 10.1103/PhysRevA.73.032304 PACS number(s): 03.67.Dd, 03.65.−w

I. INTRODUCTION

The security of quantum cryptography [1–3] is based on two main ingredients. The first refers to the impossibility of perfectly cloning some unknown quantum state selected from a nonorthogonal set [4]. As a result, the potential eavesdropper Eve cannot clone the quantum state transmitted by Alice and retransmit it undisturbed to the receiver Bob. The second ingredient, although often mentioned only implicitly in the literature, is also an absolute requirement: truly random numbers must be available on both Alice's and Bob's sides. Indeed, with pseudorandom number generators, the sequence of choices made by Alice and Bob could in principle be predicted by Eve if the seed is known to her. Clearly, quantum cryptography should use quantum randomness. But, in practice, this is a severe constraint because a complete protocol requires a huge amount of random numbers, from Alice's state choices to Bob's basis choices, as well as for the random choices and random permutations needed in error correction and privacy amplification. Making high-speed quantum random-number generators is a big technological challenge, so that most realizations of quantum cryptography today rely on an active [16] choice that uses a standard random-number generator. It is therefore of a great importance to investigate whether this requirement of high-rate random number generation can be relaxed, at least in part.

In this paper, we consider a variant of the BB84 [1] or six-state [5,6] protocols in which the basis chosen for encoding is kept unchanged over long sequences of qubits instead of being drawn at random for each qubit. Quite surprisingly, we show that, if the sequences are much shorter than the key, the security is unaffected by this modification of the protocol although the random number generation rate is significantly reduced. The BB84 and six-state protocols are among the cryptographic schemes for which the security has exhaustively been studied. In various cases the optimal eavesdropping strategy has been found explicitly [5–7], and was shown to coincide with approximate cloning [8]. For this reason, we restrict our analysis to cloning-based attacks in the following. Also, note that other methods for saving random numbers have been proposed, but rely on totally different modifications of quantum cryptographic protocols [9].

We consider the cloning of sequences of N qubits. In each sequence the qubits are prepared in the same basis, but the state is chosen at random among the basis states [17]. This is viewed as the optimal eavesdropping attack against a quantum cryptographic protocol in which we do not restrict Alice and Bob to make random choices of bases for every qubit, but allow them to use the same basis for the entire length-N sequence (N is assumed to be publicly known and much smaller than the size of the key). That is, for each sequence, Alice and Bob make new and independent random choices of bases. At first sight, one could imagine that this encoding would increase Eve's knowledge about the secret key, but we shall see that for the class of cloning transformations we have studied, this is not the case: Eve's optimal cloning attack provides her with no more Shannon information, for a given quantum bit error rate, than in the usual case where Alice and Bob make random basis choices for each qubit and Eve applies a cloning attack on each qubit. Under the assumption that this class of approximate cloning transformations corresponds to the optimal eavesdropping strategy, we have thus proven that the requirement for random number generation can be reduced without impairing on the security against finite-size attacks [10]. It should be noted that the security analysis in Ref. [8] differs fundamentally from the security analysis performed here. In this paper we are interested in the single-qubit fidelity for a cloned sequence of qubits (a d-dimensional system) whereas in Ref. [8] the authors are also interested in cloning d-dimensional systems (they consider secure QKD with such higher dimensional systems) but where the figure of merit is the fidelity of the total cloned d-dimensional system.

The paper is organized as follows. In Sec. II, we describe a general formalism for quantum cloning [11,12], and adapt it to the case of interest here. In Secs. III and IV, we apply this formalism to two-qubit cloning attacks in the BB84 and six-state protocols, respectively, and show that using the same bases does not affect the cloning fidelity. Section V contains a generalization of these results in dimensions being any power of 2. Finally, in Sec. IV, we summarize our results.

II. GENERAL QUANTUM CLONING FORMALISM

We refer to a general class of cloning transformations as defined in Refs. [11,12]. Considering an arbitrary state $|\psi\rangle$ in a 2^N-dimensional Hilbert space, we wish to produce two (approximate) clones. The class of cloning transformations we will analyze is built following the "Cerf ansatz": if the input state is $|\psi\rangle$, then the resulting joint state of the two output clones (noted E and B) and the cloning machine (noted C) is

$$|\psi\rangle \rightarrow \sum_{\bar{m},\bar{n}=0}^{2^N-1} a_{\bar{m},\bar{n}} U_{\bar{m},\bar{n}} |\psi\rangle_E |B_{\bar{m},\bar{n}}\rangle_{B,C}$$

$$= \sum_{\bar{m},\bar{n}=0}^{2^N-1} b_{\bar{m},\bar{n}} U_{\bar{m},\bar{n}} |\psi\rangle_B |B_{\bar{m},\bar{n}}\rangle_{E,C}, \qquad (1)$$

where the couple $\{\bar{m},\bar{n}\} \Leftrightarrow \{m_1 \cdots m_N, n_1 \cdots n_N\}$ and $m_i, n_i \in \{0,1\}$. Here, E, B, and C are 2^N-dimensional systems and $U_{\bar{m},\bar{n}}$ is defined as

$$U_{\bar{m},\bar{n}} = \bigotimes_{i=1}^{N} X^{m_i} Z^{n_i}, \qquad (2)$$

where $X^{m_i} Z^{n_i}$ represents the identity and the three Pauli matrices

$$X^0 Z^0 = I,$$

$$X^1 Z^0 = \sigma_x,$$

$$X^0 Z^1 = \sigma_z,$$

$$X^1 Z^1 = -i\sigma_y.$$

Here, $|B_{\bar{m},\bar{n}}\rangle$ is defined as

$$|B_{\bar{m},\bar{n}}\rangle = \sum_{\bar{k}=0}^{2^N-1} (-1)^{(\bar{k}\cdot\bar{n})} |\bar{k}\rangle |\bar{k}+\bar{m}\rangle, \qquad (3)$$

where $\bar{k}\cdot\bar{n}$ represents the bitwise scalar product, i.e., $\bar{k}\cdot\bar{n} = \Sigma_i k_i n_i$. Thus $U_{\bar{m},\bar{n}}$ is the tensor product of N Pauli matrices each acting on a two-dimensional subsystem. An *error* operator U_{m_i,n_i} is associated to each subsystem. Such an operator shifts the state by m_i units (modulo 2) in the computational basis, and multiplies it by a phase so as to shift its Fourier transform by n_i units (modulo 2). Equation (3) defines the d^2 generalized Bell states for a pair of 2^N-dimensional systems with $|B_{\bar{m},\bar{n}}\rangle = U_{\bar{m},\bar{n}} \otimes I |B_{\bar{0},\bar{0}}\rangle$.

Tracing over systems B and C (or E and C) yields the final states of clone E (or clone B): if the input state is $|\psi\rangle$, the clones E and B are in a mixture of the states $|\psi_{\bar{m},\bar{n}}\rangle = U_{\bar{m},\bar{n}} |\psi\rangle$ with respective weights $p_{\bar{m},\bar{n}}$ and $q_{\bar{m},\bar{n}}$:

$$\rho_E = \sum_{\bar{m},\bar{n}=0}^{2^N-1} p_{\bar{m},\bar{n}} |\psi_{\bar{m},\bar{n}}\rangle\langle\psi_{\bar{m},\bar{n}}|,$$

$$\rho_B = \sum_{\bar{m},\bar{n}=0}^{2^N-1} q_{\bar{m},\bar{n}} |\psi_{\bar{m},\bar{n}}\rangle\langle\psi_{\bar{m},\bar{n}}|. \qquad (4)$$

In addition, the weight functions of the two clones ($p_{\bar{m},\bar{n}}$ and $q_{\bar{m},\bar{n}}$) are related by

$$p_{\bar{m},\bar{n}} = |a_{\bar{m},\bar{n}}|^2, \quad q_{\bar{m},\bar{n}} = |b_{\bar{m},\bar{n}}|^2, \qquad (5)$$

where $a_{\bar{m},\bar{n}}$ and $b_{\bar{m},\bar{n}}$ are two (complex) amplitude functions that are dual under N two-dimensional Fourier transforms:

$$b_{\bar{m},\bar{n}} = \frac{1}{2^N} \sum_{\bar{x},\bar{y}=0}^{2^N-1} (-1)^{\bar{n}\cdot\bar{x}-\bar{m}\cdot\bar{y}} a_{\bar{x},\bar{y}}. \qquad (6)$$

The fidelity of a clone, say E, is given by

$$F_E = \langle\psi|\rho_E|\psi\rangle = \sum_{\bar{m},\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 |\langle\psi|U_{\bar{m},\bar{n}}|\psi\rangle|^2 \qquad (7)$$

and similarly for the B clone (replace the $|a_{\bar{m},\bar{n}}|^2$ term by $|b_{\bar{m},\bar{n}}|^2$).

III. BB84 PROTOCOL WITH TWO-QUBIT CORRELATED BASES

In this section we compare the amount of information that can be gained by Eve when performing a cloning attack on individual qubits (two-dimensional) and on pairs of qubits (four-dimensional) which may have been chosen from correlated bases. We study here how this affects the BB84 protocol and in the next section we move on to the six-state protocol.

In the BB84 protocol, Alice chooses from states belonging to two mutually unbiased bases. Two bases A and B for a d-dimensional system are said to be MU [13] if a state prepared in any element of A (such as $|A,\alpha\rangle$) has a uniform probability distribution of being found in any element of B, namely

$$|\langle A,\alpha|B,\beta\rangle| = \frac{1}{\sqrt{d}}. \qquad (8)$$

Conventionally, Alice and Bob choose the first basis as the so-called computational basis (eigenstates of σ_z) $\{|0\rangle,|1\rangle\}$ and the second as the dual basis (eigenstates of σ_x) $\{1/\sqrt{2}(|0\rangle \pm |1\rangle)\}$.

A. BB84–single qubit attack–no basis correlation

If Eve chooses to clone the qubits individually, she must use a cloning strategy which is optimal for this set of states. When using the cloning formalism described in Sec. I, one can easily verify that the expression of the fidelity for all states of a given basis is the same. The reader familiar with this calculation can easily skip to the next subsection without any loss of generality. Here and throughout the paper, we consider fidelities as expressed by Eq. (7). Particularly for Eve's clone one finds that the fidelity for the computational basis is $F_E=|a_{0,0}|^2+|a_{0,1}|^2$ and the dual basis is $F_E=|a_{0,0}|^2+|a_{1,0}|^2$. A cloning machine that acts equally well for this set of states implies $|a_{0,0}|^2+|a_{0,1}|^2=|a_{0,0}|^2+|a_{1,0}|^2$. Since there is *a priori* no reason why the optimal values of these elements be different from each other, we make the hypothesis that they should all be equal and real. Furthermore, we extend our hypothesis to the remaining element, $|a_{1,1}|^2$ such that the form of the amplitude matrix reduces to

$$a_{\bar{m},\bar{n}}=\begin{pmatrix} v & x \\ x & y \end{pmatrix}. \tag{9}$$

Eve's fidelity is now expressed as $F_E=v^2+x^2$ and normalization requires $v^2+2x^2+y^2=1$. Bob's clone can be characterized by a similar amplitude matrix by making the same hypotheses:

$$b_{\bar{m},\bar{n}}=\begin{pmatrix} v' & x' \\ x' & y' \end{pmatrix}, \tag{10}$$

where the different matrix elements are related to the $a_{m,n}$ coefficients by Eq. (6). Thus Bob's fidelity is $F_B=v'^2+x'^2$ in both bases and the corresponding mutual information between Alice and Bob (if the latter measures his clone in the good basis) is given by

$$I_{AB}=1+F_B\log_2 F_B+(1-F_B)\log_2(1-F_B). \tag{11}$$

Maximizing Eve's fidelity F_E for a given value of Bob's fidelity F_B under the normalization constraint yields

$$v=\frac{1}{2}+\sqrt{F_B(1-F_B)},$$

$$x=F_B-\frac{1}{2},$$

$$y=\frac{1}{2}-\sqrt{F_B(1-F_B)}$$

such that the corresponding optimal fidelity for Eve is

$$F_E=\frac{F_B}{2}+\frac{1-F_B}{2}+\sqrt{F_B(1-F_B)}. \tag{12}$$

Under the assumption that Alice and Bob exchange many sequences which are short in comparison to the size of the total key, Alice and Bob can rely on the randomness of the sequence basis distribution to guarantee the security of their exchange. Csiszár and Körner's theorem [14] provides a lower bound on the rate R at which Alice and Bob can generate secret key bits using privacy amplification:

$$R\geqslant\max(I_{AB}-I_{AE},I_{AB}-I_{BE}), \tag{13}$$

where I_{AE} and I_{BE} represent the mutual information between Alice and Eve, and Bob and Eve, respectively. It is therefore a sufficient condition that $I_{AB}>I_{AE}$ in order to establish a secret key with nonzero rate for one way communication channels. It has been shown in Ref. [8] that Bob and Eve's information curves intersect exactly where the fidelities coincide because, in this particular case, the mutual information shared between Alice and Eve is also expressed by Eq. (11). This yields the optimal symmetric fidelity of phase covariant cloning [15],

$$F_E=F_B=\frac{1}{2}+\frac{1}{\sqrt{8}}\simeq 0.8536. \tag{14}$$

Note that this result is independent of the fact that Alice may have chosen to encode sequences of consecutive qubits in the same basis since Eve is intercepting them individually.

B. BB84–two qubit attack–no correlation

Suppose now that Eve intercepts the qubits in sequences of two and clones them. We make the same assumption as before, namely that Alice has randomly chosen the basis she has encoded her qubit with. We would like to know if Eve can gain more information per qubit using this cloning approach as opposed to cloning them individually. Our first task is to determine the set of states that she will have to clone. If Alice chooses among the computational and dual bases, the possible sequences Eve might encounter are products of eigenstates of $\sigma_z^{\otimes 2}$: $|00\rangle$, $|01\rangle$, $|10\rangle$, $|11\rangle$, products of eigenstates of $\sigma_x^{\otimes 2}$:

$$\frac{1}{2}(|00\rangle+|01\rangle+|10\rangle+|11\rangle),$$

$$\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle-|11\rangle),$$

$$\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle-|11\rangle),$$

$$\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle),$$

and products between eigenstates of these two bases ($\sigma_z\otimes\sigma_x$ and $\sigma_x\otimes\sigma_z$):

$$\frac{1}{\sqrt{2}}(|00\rangle\pm|01\rangle),\quad \frac{1}{\sqrt{2}}(|10\rangle\pm|11\rangle),$$

$$\frac{1}{\sqrt{2}}(|00\rangle\pm|10\rangle),\quad \frac{1}{\sqrt{2}}(|01\rangle\pm|11\rangle).$$

Because we are now dealing with a *four*-dimensional Hilbert space ($N=2$) with tensor product structure, the $U_{\bar{m},\bar{n}}$ operators take the following form:

$$U_{m_1m_2;n_1n_2}=\begin{pmatrix} I & Z \\ X & Y \end{pmatrix}\otimes\begin{pmatrix} I & Z \\ X & Y \end{pmatrix}.$$

Each of these matrix elements consists in a tensor product of two Pauli operators each acting on an associated qubit. Eve is interested in the information she can gain from a single qubit when she clones them in sequences of two. In other words, Eve is interested in the optimal *four*-dimensional cloning map where the figure of merit is not the single-clone *four*-dimensional fidelity but rather the single-clone, single-qubit *two*-dimensional fidelity averaged over the two qubits. To obtain this fidelity, we must trace over the second qubit subsystem and compute the fidelity of the first qubit, repeat this operation for the second qubit by tracing out the first qubit subsystem and finally average over the two fidelities. For example, the reduced density matrix of the first qubit for Eve's clone is expressed as

$$\rho_E^1 = \mathrm{Tr}_2\biggl(\sum_{\bar{m},\bar{n}} |a_{\bar{m},\bar{n}}|^2 X^{m_1}Z^{n_1}|\phi_1\rangle\langle\phi_1|Z^{n_1}X^{m_1}\otimes X^{m_2}Z^{n_2}|\phi_2\rangle \times\langle\phi_2|Z^{n_2}X^{m_2}\biggr)$$

$$=\sum_{\bar{m},\bar{n}} |a_{\bar{m},\bar{n}}|^2 X^{m_1}Z^{n_1}|\phi_1\rangle\langle\phi_1|Z^{n_1}X^{m_1},$$

where $|\phi_i\rangle$ is a two-dimensional system. For sequences of qubits both drawn from eigenstates of σ_z the fidelity is

$$F_{E,zz}^1 = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 |\langle\phi_1|X^{m_1}Z^{n_1}|\phi_1\rangle|^2 = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{m_1,0} \tag{15}$$

for the first qubit and

$$F_{E,zz}^2 = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 |\langle\phi_2|X^{m_2}Z^{n_2}|\phi_2\rangle|^2 = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{m_2,0} \tag{16}$$

for the second qubit. For clusters of qubits both drawn from eigenstates of σ_x the fidelity is

$$F_{E,xx}^1 = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{n_1,0} \tag{17}$$

for the first qubit and

$$F_{E,xx}^2 = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{n_2,0} \tag{18}$$

for the second qubit. To be complete, we must also compute the fidelity for clusters expressed as tensor products drawn from eigenstates of $\sigma_z\otimes\sigma_x$ and $\sigma_x\otimes\sigma_z$. The former yields $F_{E,zx}^1=F_{E,zz}^1$ for the first qubit and $F_{E,zx}^2=F_{E,xx}^2$ for the second qubit. The latter yields a fidelity of $F_{E,xz}^1=F_{E,xx}^1$ for the first qubit and $F_{E,xz}^2=F_{E,zz}^2$ for the second qubit. The expressions for these fidelities F_E^i can easily be interpreted as follows. Every single-qubit fidelity consists in a sum of eight terms for which the first four express the fidelity of the *four*-dimensional system in question (in other words the contribution from the $a_{\bar{m},\bar{n}}$ coefficients where no errors occur on either qubits) while the remaining four terms correspond to the $a_{\bar{m},\bar{n}}$ coefficients for which the *i*th qubit is not affected by an error but the remaining one is. Generally, the fidelity of the *i*th qubit is expressed as

$$F_E^i = F_{4E} + D_E^i, \tag{19}$$

where F_{4E} is the fidelity of the *four*-dimensional system and D_E^i is the disturbance of the *i*th qubit and is expressed as

$$D_E^i = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{m_i,1}\delta_{m_{\neg i},0} \tag{20}$$

for qubits drawn from the computational basis and

$$D_E^i = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{n_i,1}\delta_{n_{\neg i},0} \tag{21}$$

for qubits drawn from the dual basis. Here, the qubit of the pair which is not the *i*th qubit is given the index $\neg i$. The average qubit fidelity of Eve's clone is therefore

$$F_E = F_{4E} + \frac{1}{2}(D_E^1 + D_E^2). \tag{22}$$

A similar analysis can be made for Bob's clone from which we obtain a single-qubit fidelity

$$F_B = F_{4B} + \frac{1}{2}(D_B^1 + D_B^2) \tag{23}$$

which is function of the $b_{\bar{m},\bar{n}}$ coefficients. We are again interested in the mutual information shared between Alice and Bob and Alice and Eve. To do this, let us first compute Eve's optimal fidelity F_E for a fixed value of Bob's fidelity F_B under the normalization constraint

$$\sum_{\bar{m}=0,\bar{n}=0}^{3} |a_{\bar{m},\bar{n}}|^2 = 1 \tag{24}$$

and the constraint that the single-qubit fidelity be the same for all 16 considered input states. The optimization yields the following $a_{\bar{m},\bar{n}}$ matrix:

$$a_{\bar{m},\bar{n}} = \begin{pmatrix} v_1 & x_1 \\ x_1 & y_1 \end{pmatrix} \otimes \begin{pmatrix} v_2 & x_2 \\ x_2 & y_2 \end{pmatrix}, \tag{25}$$

where

$$v_1 = v_2 = \frac{1}{2} + \sqrt{F_B(1-F_B)},$$

$$x_1 = x_2 = F_B - \frac{1}{2},$$

$$y_1 = y_2 = \frac{1}{2} - \sqrt{F_B(1-F_B)}$$

such that

$$F_E = \frac{F_B}{2} + \frac{1-F_B}{2} + \sqrt{F_B(1-F_B)}. \tag{26}$$

From the previous subsection we know that Bob and Eve's information curves intersect exactly where the fidelities coincide. This implies that Alice and Bob can share secret bits via privacy amplification as long as $F_B > F_E$, that is

$$F_B > \frac{1}{2} + \frac{1}{\sqrt{8}}.$$

This optimal symmetric fidelity turns out to be the same as the optimal fidelity obtained when the cloner is designed for *two*-dimensional systems meaning that the optimal *four*-dimensional cloning map for single-qubit single-clone fidelity boils down to the tensor product of the *two*-dimensional optimal cloners.

C. BB84–two qubit attack–correlated bases

Now consider the situation where Alice is limited by her random number generator and must therefore send two consecutive states drawn from the same basis in order to keep a decent cadence [10]. Of course if Eve intercepts every qubit individually, the fidelity she obtains after cloning is just the same as before, namely $F = \frac{1}{2} + 1/\sqrt{8}$. If she intercepts them in sequences of two qubits she will necessarily find that they are correlated: either she expects to find two qubits drawn from the computational basis σ_z (equivalently, a four-dimensional state drawn from the eigenstates of $\sigma_z \otimes \sigma_z$) or two qubits drawn from the dual basis σ_x (equivalently, a four-dimensional state drawn from the eigenstates of $\sigma_x \otimes \sigma_x$). Compared to the previous situation where no correlation was present, the set of input states Eve has to consider has now decreased. Intuitively we should expect that the optimal single-qubit cloner would give rise to a higher fidelity. We shall see that this is not the case.

The cloner is again characterized by the "Cerf ansatz" (1) such that the single-qubit fidelity for this set of input states is defined exactly like Eqs. (15) and (16) for eigenstates of σ_z and like Eqs. (17) and (18) for eigenstates of σ_x. These are the four expressions of the fidelity for which the $a_{\bar{m},\bar{n}}$ (and consequently the $b_{\bar{m},\bar{n}}$) coefficients must be optimized for. The constraints we must consider here are the normalization constraint and the constraint that these four expressions be equal. Of course, these fidelities are again characterized by Eq. (22). Interestingly, the constrained optimization yields $a_{\bar{m},\bar{n}}$ coefficients which have exactly the same form as Eq. (25) and therefore the same expressions for Eve's fidelity as a function of Bob's. Once again, the lower bound on the mutual information Alice and Bob must share in order to generate a secret key is given by

$$F > \frac{1}{2} + \frac{1}{\sqrt{8}}.$$

We conclude that even if Alice chooses to encode two consecutive states in the same basis, Eve's optimal cloning strategy does not permit her to gain more information than complete random choices. In Sec. V we will generalize this idea for sequences of N qubits, but first let us examine how these cloning strategies apply to the six-state protocol.

IV. SIX-STATE PROTOCOL WITH TWO-QUBIT CORRELATED BASES

The six-state protocol is very similar to the BB84 protocol, the only difference being that Alice now has the choice to pick up states from a third basis MU to the other two. Again, let us choose the first two bases as the computational basis and the dual basis and let the third basis be the eigenstates of σ_y: $\{(1/\sqrt{2})(|0\rangle \pm i|1\rangle)\}$.

A. Six-state protocol–single qubit attack–no correlation

The cloner that must be used for the six-state protocol is an asymmetric *two*-dimensional universal cloner [8] characterized by the same amplitude matrix as Eq. (9) except that we make the change $y = x$:

$$a_{\bar{m},\bar{n}} = \begin{pmatrix} v & x \\ x & x \end{pmatrix}.$$

Eve's fidelity is expressed as $F_E = v^2 + x^2$ and normalization requires $v^2 + 3x^2 = 1$. Maximizing her fidelity for a fixed value of Bob's fidelity yields the optimal cloner:

$$v = \sqrt{\frac{3F_B - 1}{2}},$$

$$x = \sqrt{\frac{1 - F_B}{2}}.$$

Bob's clone is characterized by a similar amplitude matrix:

$$b_{\bar{m},\bar{n}} = \begin{pmatrix} v' & x' \\ x' & x' \end{pmatrix}, \tag{27}$$

where as before, v' and x' are given by Eq. (6) while the mutual information he shares with Alice by Eq. (11). It has been shown in Ref. [8] that the mutual information shared between Alice and Eve for the six-state protocol is given by

$$I_{AE} = 1 + (F_B + F_E - 1)\log_2\left(\frac{F_B + F_E - 1}{F_B}\right) + (1 - F_E)\log_2\left(\frac{1 - F_E}{F_B}\right) \tag{28}$$

such that for a given F_B, I_{AE} is lower than for the BB84 protocol which is consistent with the stronger requirement we put on that cloner. This implies that the fidelity F_B for which $I_{AE} = I_{AB}$ is slightly lower, and equal to $F_B \simeq 0.8436$.

B. Six-state–two qubit attack–no basis correlation

If Eve chooses to clone the incoming states in sequences of two, the set of four-dimensional states she has to clone consists of tensor products of states belonging to the three maximally unbiased bases above. The single-qubit fidelity is computed as above, with the exception that there are extra constraints, namely that the fidelity should also clone equally well eigenstates of σ_y:

$$F_{E,yy}^{1} = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{m_1,n_1}$$

for the first qubit and

$$F_{E,yy}^{2} = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{m_2,n_2}$$

for the second qubit. The other constraints come from tensor products of $\sigma_y \otimes \sigma_z$, $\sigma_y \otimes \sigma_x$ and vice versa. The expression for the fidelity of the *i*th qubit can be expressed as

$$F_E^i = F_{4E} + D_E^i, \tag{29}$$

where, for eigenstates of σ_y,

$$D_E^i = \sum_{\bar{m}=0,\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 \delta_{m_i,n_i+1} \delta_{m_{\neg i},n_{\neg i}}. \tag{30}$$

The average qubit fidelity is again

$$F_E = F_{4E} + \frac{1}{2}(D_E^1 + D_E^2). \tag{31}$$

As before a similar analysis can be made for Bob's clone from which we obtain a single-qubit fidelity,

$$F_B = F_{4B} + \frac{1}{2}(D_B^1 + D_B^2). \tag{32}$$

We are again interested in the mutual information shared between Alice and Bob, and Alice and Eve. We compute Eve's optimal fidelity F_E for a fixed value of Bob's fidelity F_B under the normalization constraint Eq. (24) and the constraint that the single-qubit fidelity be the same for all input states. The optimization yields the following $a_{\bar{m},\bar{n}}$ matrix:

$$a_{\bar{m},\bar{n}} = \begin{pmatrix} v_1 & x_1 \\ x_1 & x_1 \end{pmatrix} \otimes \begin{pmatrix} v_2 & x_2 \\ x_2 & x_2 \end{pmatrix}, \tag{33}$$

where

$$v_1 = v_2 = \sqrt{\frac{3F_B - 1}{2}},$$

$$x_1 = x_2 = \sqrt{\frac{1 - F_B}{2}}$$

such that

$$F_E = 1 - \frac{F_B}{2} + \frac{1}{4}\sqrt{6F_B - 2}\sqrt{2 - 2F_B}. \tag{34}$$

In the previous subsection, we have seen how to express I_{AB} and I_{AE}. Again in this case the lower bound on Bob's fidelity needed for $I_{AB} > I_{AE}$ is given by $F_B > 0.8436$ which is the same fidelity for individual attacks. Thus, so far, we arrive to the same conclusions as for the BB84 protocol.

C. Six-state–two qubit attack–correlated bases

If Alice is again limited by her random number generator and must encode two consecutive qubits in the same basis, Eve can clone the incoming states by sequences of two expecting to find four-dimensional states expressed as eigenstates of $\sigma_z \otimes \sigma_z$, $\sigma_x \otimes \sigma_x$, or $\sigma_y \otimes \sigma_y$. By making a similar reasoning as in the previous subsection we arrive to the same conclusions as before, namely that the information Eve can gain when cloning a *four*-dimensional system boils down to the optimal single qubit information.

V. CLONING OF *N*-QUBIT SEQUENCES

We now proceed to generalize the cloning strategies considered in the previous sections. We suppose that Alice encodes her qubits using the same basis for sequences of *N* qubits. We also suppose that *N* is much smaller than the total size of the raw key she will be exchanging with Bob. We also suppose that Eve is aware of when a new sequence begins and ends.

Generally, for a sequence of *N* qubits, the reduced density matrix of the *i*th qubit for a given clone (say *E*) is written as

$$\begin{aligned} \rho_E^i &= \mathrm{Tr}_{j \neq i} \sum_{\bar{m},\bar{n}} |a_{\bar{m},\bar{n}}|^2 \bigotimes_{j=1}^{N} X^{m_j} Z^{n_j} |\phi_j\rangle\langle\phi_j| Z^{n_j} X^{m_j} \\ &= \sum_{\bar{m},\bar{n}} |a_{\bar{m},\bar{n}}|^2 X^{m_i} Z^{n_i} |\phi_i\rangle\langle\phi_i| Z^{n_i} X^{m_i}, \end{aligned} \tag{35}$$

such that fidelity of the *j*th qubit is written as

$$F_E^j = F_{E2^N} + D_E^j \tag{36}$$

and similarly for qubits of Bob's clone. The average qubit fidelity is therefore expressed as

$$F_E = F_{E2^N} + \frac{1}{N}\sum_{i=1}^{N} D_E^i. \tag{37}$$

If we assume that the optimal $a_{\bar{m},\bar{n}}$ amplitude matrices are expressed as

$$a_{\bar{m},\bar{n}} = \begin{pmatrix} v & x \\ x & y \end{pmatrix}^{\otimes N} \tag{38}$$

for the BB84 protocol and

$$a_{\bar{m},\bar{n}} = \begin{pmatrix} v & x \\ x & x \end{pmatrix}^{\otimes N} \tag{39}$$

for the six-state protocol, we can check that they indeed satisfy a constrained optimization. Since the information curves are both monotonically increasing functions of the fidelities, we use the Lagrange multiplier method to optimize Eve's fidelity for a fixed value of Bob's.

The constraint that the fidelity for different qubits in the sequence be the same is already satisfied by the hypothesized $a_{\bar{m},\bar{n}}$ matrix. The function is

$$\begin{aligned}\mathcal{L} &= F_E + \lambda_1 F_B + \lambda_2\left(\sum_{\bar{m},\bar{n}=0}^{2^N-1} |a_{\bar{m},\bar{n}}|^2 - 1\right)\\ &= \frac{1}{N}\sum_{\bar{m}=0}^{N}\left(N - \sum_{i=1}^{N} m_i\right)\prod_{i=1}^{N}(v^2+x^2)^{m_i\oplus 1}(x^2+y^2)^{m_i}\\ &\quad + \lambda_1\Bigg[\frac{1}{N}\sum_{\bar{m}=0}^{N}\left(N-\sum_{i=1}^{N} m_i\right)\prod_{i=1}^{N}\left(\frac{1}{2}+vx+xy\right)^{m_i\oplus 1}\\ &\quad \times\left(\frac{1}{2}-vx-xy\right)^{m_i}\Bigg] + \lambda_2[(v^2+2x^2+y^2)^N - 1],\end{aligned} \tag{40}$$

where the modular sum is in base 2. The equivalent expression of Eq. (40) for the six-state protocol is very similar except that one should exchange y^2 for x^2.

We have checked, using a symbolic calculator, that the hypothesized amplitude matrices satisfy the constrained optimization and yield the optimal fidelities [Eqs. (26) and (34)] for $N=2$ and $N=3$.

VI. CONCLUSION

We have considered the cloning of sequences of N qubits, where all the qubits in each sequence are prepared in the same basis while each state is chosen at random. This situation is very different from the usual scenario of cloning multiple copies, where all the copies are prepared in the same state. Our investigation was motivated by the situation in quantum cryptography where the legitimate users are required to make truly random choices for each single qubit. From a practical point of view, this requirement on high-rate random-number generation is a severe constraint. Indeed, high-rate quantum random number generators on the market today produce much lower rates than the anticipated high-rate (e.g., 100 Mb/s) quantum key distribution of the future.

However, under the assumption that the class of cloning transformations we considered here provides the optimal eavesdropping strategy, we have shown that this requirement can be relaxed, so that Alice can prepare long sequences of qubits in the same basis without compromising the security. Surprisingly, Eve cannot exploit her knowledge that the used basis is fixed for the entire sequence, regardless of its length provided it is much shorter than the total key size. The constraint on the sequence size is necessary because even though we assume Alice and Bob to exchange qubits encoded by a single photon source (i.e., Eve cannot exploit photon number splitting attacks), Eve could still make a naive attack where she randomly guesses the value of the basis for each sequence. For example in the extreme case where the sequence is the same size as the key, i.e., when the variance of the information gain is high, Eve would, with probability $\frac{1}{2}$, completely guess the secret key. Conversely, when $N=1$ (i.e., the standard BB84 or six-state protocol) the variance will be lower and implies that the optimal eavesdropping strategy is achieved through cloning. In order to avoid this security threat, Alice and Bob should choose N in such a way that the variance of the information gain implies that the optimal strategy Eve should use remains the single-qubit cloning strategies utilized in the original BB84 and six-state protocols. We leave as an open question as to which bounds can be achieved. Nevertheless, even with reasonably low values of the sequence size, such as $N=10$, the saving of the random bits is already significant (in this case, 45%). This result is quite important for practical applications of quantum cryptography as it implies that higher secret-key rates may be obtained using the same random number generator but with this new modified protocol.

ACKNOWLEDGMENTS

The authors acknowledge financial support from the Action de Recherche Concertée de la Communauté Française de Belgique, from the IUAP program of the Belgian Federal Government under Grant No. V-18, and from the European Union through projects RESQ (Grant No. IST-2001-37559) and SECOQC (Grant No. IST-2003-506813).

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India*, 1984, pp. 175–179.

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

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

[4] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).

[5] D. Bruß, Phys. Rev. Lett. **81**, 3018 (1998).

[6] H. Bechmann-Pasquinucci and N. Gisin, Phys. Rev. A **59**, 4238 (1999).

[7] C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres, Phys. Rev. A **56**, 1163 (1997).

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

[9] H.-K. Lo, H. F. Chau, and M. Ardehali, J. Cryptology **18**, 2 (2005).

[10] N. Gisin, quant-ph/0303052.

[11] N. J. Cerf, *Proceedings of the 1st NASA International Conference QCQC'98, Palm Springs*, February 1998; also in Acta Phys. Slov. **48**, 115 (1998).

[12] N. J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000); J. Mod. Opt. **47**, 187 (2000).

[13] J. Lawrence, C. Brukner, and A. Zeilinger, Phys. Rev. A **65**, 032320 (2002).

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

[15] D. Bruß, M. Cinchetti, G. M. D'Ariano, and C. Macchiavello, Phys. Rev. A **62**, 012302 (2000).

[16] Note that if the choice is passive, based on quantum effects (e.g., the photon being detected at one or the other output port of a beam splitter at Bob's station), then it is still not com-

pletely equivalent to using a quantum random-number generator. Indeed, in the latter case, the photon involved in the random-number generation is generated locally, and has not been transmitted over the line and potentially tapped by Eve.

[17] Note that this situation is different from the usual scenario of $N \rightarrow M$ cloning transformations, where N identical replicas of a quantum state are considered at the input, and are used to produce M clones.