Quantum key distribution between $N$ partners: Optimal eavesdropping and Bell’s inequalities

Valerio Scarani* and Nicolas Gisin

Group of Applied Physics, University of Geneva, 20 rue de l’Ecole-de-Médecine, CH-1211 Geneva, Switzerland

(Received 20 July 2001; published 12 December 2001)

Quantum secret-sharing protocols involving $N$ partners are key distribution protocols in which Alice encodes her key into $N-1$ qubits, in such a way that all the other partners must cooperate in order to retrieve the key. On these protocols, several eavesdropping scenarios are possible: some partners may want to reconstruct the key without the help of the other ones, and consequently collaborate with an Eve that eavesdrops on the other partners’ channels. For each of these scenarios, we give the optimal individual attack that Eve can perform. A link with Bell’s inequality is demonstrated analytically for half of the scenarios, and is conjectured on the basis of numerical estimates for the other scenarios: the authorized partners have a higher information on the key than the unauthorized ones if and only if they can violate a Bell’s inequality.

I. INTRODUCTION

In the rapidly growing field of quantum information, the first protocol that has almost reached the level of application is quantum cryptography [1], a beautiful solution to the important problem of secure key distribution. The authorized partners Alice and Bob can establish an absolutely secure communication provided that they share a common sequence of bits (the key), unknown to anybody else: this is the very principle of the so-called secret-key cryptographic schemes. In 1984, Bennett and Brassard [2] proposed a way of distributing the key in a physically secure way by using quantum physics: their protocol bears the acronym BB84, and was the first protocol of quantum cryptography—from now on, we shall use the more precise name of quantum key distribution (QKD). In the intuition of Bennett and Brassard, security is provided by the well-known feature of quantum mechanics: “measurement perturbs the system”; or, under a different viewpoint that is equivalent, by the no-cloning theorem. In 1991, Ekert [3] proposed a QKD protocol that uses entangled particles, and stated that the violation of Bell’s inequality might be the physical principle that ensures security. This view was challenged by Bennett, Brassard, and Mermin [4], who showed that Ekert’s protocol is actually equivalent to the BB84 protocol, that involves single particles. A link between security of QKD and Bell’s inequalities was nevertheless noticed in further studies [5–7].

The plan of this paper is as follows. In Sec. II, we consider two-partners QKD. Most of the material of this section is not new in itself, but the approach is; moreover, it is a useful introduction to the following sections. In Sec. III, we define the $N$-partners protocols that we consider. Several eavesdropping scenarios can be imagined on these protocols, and we give Eve’s optimal individual attack in each case. In Sec. IV, we introduce a family of $M$-qubit Bell’s inequalities (Mermin-Klyshko inequalities), and we discuss the link between the violation of these inequalities and the security of the $N$-partners protocol. Sec. V is devoted to two different questions linked with Bell’s inequalities, namely, the choice of the good inequality, and the violation of inequalities by overlapping sets of qubits. Sec. VI describes our conclusion.

II. QKD INVOLVING TWO PARTNERS

A. The BB84 protocol

The BB84 protocol of quantum key distribution between two partners, Alice and Bob, is characterized by the fact that two complementary bases are used to encode the bits. In the original version of the BB84 protocol [2], Alice prepares a qubit in a randomly chosen eigenstate of $\sigma_x$ or of $\sigma_y$, and sends it to Bob. Since we want to discuss Bell’s inequalities, we consider the following preparation method [4]: Alice has an Einstein-Podolsky-Rosen (EPR) source that produces a maximally entangled state, say $|\Phi^+\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle)$, where $|0\rangle$ and $|1\rangle$ are the eigenstates of $\sigma_z$. On her side, Alice measures randomly $\sigma_x$ or $\sigma_y$ on one qubit. The moment at which Alice performs her measurement is irrelevant; in particular, she can measure her qubit immediately after it leaves the source. This way, Alice’s measurement acts as a preparation of the second qubit, which goes to Bob through a quantum channel. Bob also measures either $\sigma_x$ or $\sigma_y$. If he measures the same observable as Alice, his result is perfectly correlated to hers, since $\langle \sigma_x \otimes \sigma_x \rangle_{\Phi^+} = -\langle \sigma_y \otimes \sigma_y \rangle_{\Phi^+} = 1$; if he measures the other observable, he has no information on Alice’s result, since $\langle \sigma_x \otimes \sigma_y \rangle_{\Phi^+} = \langle \sigma_y \otimes \sigma_x \rangle_{\Phi^+} = 0$. At the end of the transmission, for each qubit Alice and Bob reveal publicly the measurement that they performed (but of course not its result). They simply discard those cases where they have measured different observables, and they end up with two identical lists of random bits. Bob’s information on Alice’s bits is measured by the mutual information $I(A:B)$, defined as $H(A) + H(B) - H(A|B) = H(A) - H(A|B)$, where $H(p_i) = -\Sigma p_i \log_2 p_i$ is the Shannon entropy. Therefore, in the absence of eavesdropping, $H(A|B) = 0$ since knowing the list of B is equivalent to knowing the list of A; and since Alice is supposed to choose her measurement randomly, $H(A) = 1$; whence $I(A:B) = 1$, as it should.
B. Security and mutual information

The security of a key-distribution protocol based on quantum mechanics comes from the no-cloning theorem. Suppose that Eve tries to eavesdrop on the quantum channel linking Alice and Bob: she cannot get information on the state that is sent on the channel without introducing perturbations, that should reveal her presence to the authorized partners. If A and B observe the presence of the spy, in most cases they can still perform some operations that ultimately lead them to share a secret key. More precisely [8] A and B can run a one-way protocol known as privacy amplification if and only if

\[ I(A:B) > \min[I(A:E), I(B:E)]. \]  

(1)

This is the condition that we ask for security. In fact, it has been shown that this condition is not strictly necessary: even if it does not hold, there exist a protocol allowing the extraction of a secret key [9]. But this protocol, called advantage distillation, is a two-way protocol, much less efficient than one-way privacy amplification.

The natural problem is now: for a given error rate that is introduced on Bob’s information, that is, for a given value of \( I(A:B) \), find the attack of Eve that optimizes her information on Alice’s key, \( I(A:E) \). The answer is not known in all generality; but it is, if we restrict the analysis to individual attacks [6]. This means that Eve acts separately on each qubit that is sent on the quantum channel, i.e., she does not perform coherent measurements of subsequent qubits. To date, it is not known whether a more general attack would be more efficient, only bounds are known [10]—as for the experimental state of the art, even the implementation of individual attacks would be a great challenge.

It has been shown [11] that Eve can perform the optimal individual attack having a single qubit as resource, by implementing the following unitary transformation affecting her and Bob’s qubits (by convention, we supposed that Eve prepares her qubit in the state \([0]\)):

\[
U_BE[00] = [00],
\]

\[
U_BE[10] = \cos \phi [10] + \sin \phi [01],
\]

(2)

where \([00]\), etc., are shorthand for \([0]_B \otimes [0]_E\), etc.; \(\phi \in [0, \pi/2]\) characterizes the strength of Eve’s attack. Note that the roles of B and E are symmetric under the exchange of \(\phi\) with \(\pi/2 - \phi\). Due to eavesdropping, the three-qubit state of A, B and E reads

\[
|\Psi_{21}(\phi)\rangle = \frac{1}{\sqrt{2}} (|000\rangle + \cos \phi |110\rangle + \sin \phi |101\rangle)
\]

(3)

(the labeling means that we consider a two-partners protocol in which 1 partner is spied by Eve). By tracing out one of the qubits, we obtain the density matrices \(\rho_{AB}\), \(\rho_{AE}\), and \(\rho_{BE}\) that describe the statistics of each pair. Let then \(M, N \in \{A, B, E\}, M \neq N\), be two of the three partners. We want to calculate \(I(M:N)\). In general, we must consider two statistics: the statistics \(p_x\) obtained when \(M\) and \(N\) measure \(\sigma_x\), and the statistics \(p_y\) obtained when \(M\) and \(N\) measure \(\sigma_y\);

\[ I(M:N) = 1 - \frac{1}{2}[H_x(M|N) + H_y(M|N)]. \]

Here, after calculation one finds that both statistics are the same, whatever the pair. Moreover, \(p(M = 0, N = 0) = p(M = 1, N = 1)\) and \(p(M = 0, N = 1) = p(M = 1, N = 0)\). Writing \(D_{MN} = p(M = 0, N = 1) + p(M = 1, N = 0)\) the probability that the bit of \(M\) is different from the bit of \(N\), we find finally

\[ I(M:N) = 1 - H([D_{MN}, 1 - D_{MN}]), \]

(4)

with

\[ D_{AB} = \frac{1 - \cos \phi}{2}, \quad D_{AE} = \frac{1 - \sin \phi}{2}, \quad D_{BE} = \frac{1 - \sin 2\phi}{2}. \]

(5)

In Fig. 1, we plotted \(I(A:B)\) vs \(\min[I(A:E), I(B:E)]\); we see that the condition for security (1) is fulfilled if and only if \(\phi \approx \pi/4\).

C. Violation of a Bell’s inequality

Having the three density matrices \(\rho_{AB}\), \(\rho_{AE}\), and \(\rho_{BE}\) derived from the three-qubit state (3), we can also investigate whether one or more pairs violate a Bell’s inequality for a given value of \(\phi\). Given a set of four unit vectors \(q = \{\hat{a}_1, \hat{a}_1', \hat{a}_2, \hat{a}_2'\}\), we build the two-qubit Bell operator

\[ B_2(q) = (\sigma_{a_1} + \sigma_{a_1'}) \otimes \sigma_{a_2} + (\sigma_{a_1} - \sigma_{a_1'}) \otimes \sigma_{a_2'}. \]

(6)

with \(\sigma_{a} = \hat{a} \cdot \sigma\). The Clauser-Horne-Shimony-Holt (CHSH) inequality [12] reads \(S_2 = \max_\rho |\text{Tr}[\rho B_2(q)]| \leq 2\), while the maximal value allowed by quantum mechanics (QM) is \(S_2 = 2\sqrt{2}\) [13]. The calculation of \(S_2\) using the Horodecki criterion [14] can be carried out explicitly for the three pairs, and we find

\[ S_{AB} = 2\sqrt{2} \cos \phi, \quad S_{AE} = 2\sqrt{2} \sin \phi, \quad S_{BE} = \sqrt{2} \sin 2\phi. \]

(7)
Therefore, the pair $A-B$ violate the inequality if and only if the pair $A-E$ does not violate it, and the curves cross at $\phi = \pi/4$, exactly were the security condition ceases to be fulfilled (Fig. 1). As for the pair $B-E$, it never violates the inequality. The fact that the curves $S_{AB}$ and $S_{AE}$ cross at $\phi = \pi/4$ is an immediate consequence of the symmetry of the attack (2); but what is interesting is that they cross precisely for $S_{AB}=S_{AE}=2$. In other words: simply using the symmetry, we could have guessed that $I(A:B) > I(A:E)$ if and only if $S_{AB}>S_{AE}$; but here we found that Eve’s optimal attack is such that $A$ and $B$ can establish a secret key using one-way privacy amplification iff $S_{AB}>2$, i.e., iff they violate the CHSH inequality. This coincidence was already stressed in Refs. [5,6].

It has recently been shown that the analysis of the BB84 protocol holds unchanged even if we suppose that Eve controls the source [15]. Also, in the case of the six-state protocol for QKD [16], the violation of CHSH is still a sufficient, but no longer a necessary condition. In conclusion, an overview of the two-partners QKD protocols with qubits shows that the violation of the CHSH inequality is a sufficient condition for security. In Sec. IV, we generalize this statement to protocols in which the key is distributed among more than two partners. The next section is devoted to the definition of these protocols.

III. QKD INVOLVING $N$ PARTNERS: DEFINITION, AND EAVESDROPPING

A. The $N$-partners secret-sharing protocol

The QKD protocol can be generalized to more than two partners in several ways. For instance, one may think of a protocol in which Alice sends information to Bob and Charlie so that she can choose $a posteriori$ with whom a secret key will be established. Here we consider another family of protocols, based on the following idea: Alice sends information to her $N-1$ partners $B_1, \ldots, B_{N-1}$ in such a way that all of them must cooperate in order to retrieve the secret key, and any smaller subset of Bobs has no information on the key. More formally, this means that the bipartite mutual information $I(A:B_1, \ldots, B_k)$ must be 0 for $k<N-1$, and 1 for $k=N-1$. Such protocols exist, and are called secret-sharing protocols [17].

Now, take $k+1$ of the partners and divide the partners into three nonempty groups $A$, $B$, and $C$. In general, it holds $I(\{A\}:\{B\}) = I(\{A\}:\{C\}) + H(\{B\}) - H(\{B, A\})$. But in the protocols that we are considering, if we know only $A$, we have no information on $B$, since we lack the information of $C$; thus $H(\{B\}) = H(\{B\})$. Similarly, $H(\{B\}) = H(\{B\})$. Consequently for secret-sharing protocols we have $I(\{A\}:\{B\}) = I(\{A\}:\{C\}) = I(A:B_1, \ldots, B_k)$.

The quantum version of a secret sharing protocol involving $N$ partners (NQSS) goes as follows: Alice’s source produces the $N$-qubit Greenberger-Horne-Zeilinger (GHZ) state $|\text{GHZ}_N\rangle = (1/\sqrt{2})(|00\rangle + |11\rangle) \otimes |0\rangle^N$, with $|00\rangle = |0\rangle \otimes \cdots \otimes |0\rangle$, and $|11\rangle = |1\rangle \otimes \cdots \otimes |1\rangle$. Alice measures $\sigma_x$ or $\sigma_y$ on one of the qubits, and sends the other qubits to her partners $B_1, \ldots, B_{N-1}$.

### TABLE I. Preparation of the state of $BC$ by measurements of $A$.

<table>
<thead>
<tr>
<th>Measure of $A$</th>
<th>Result</th>
<th>State of $BC$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\sigma_x$</td>
<td>$+ = 0$</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>$- = 1$</td>
<td>$</td>
</tr>
<tr>
<td>$\sigma_y$</td>
<td>$+ = 0$</td>
<td>$</td>
</tr>
<tr>
<td></td>
<td>$- = 1$</td>
<td>$</td>
</tr>
</tbody>
</table>

Each Bob also measures either $\sigma_x$ or $\sigma_y$. At the end of the transmission, all partners communicate publicly their measurements. Each time that an even number of partners have measured $\sigma_y$, the results exhibit the desired correlation. In fact, consider a measurement where all partners measured $\sigma_x$: each partner has one bit $s_5, s_6, \ldots, s_{B_{N-1}}$, where $s_5 = \pm 1$. Since $\langle \sigma_x \otimes \cdots \otimes \sigma_x \rangle_{\text{GHZ}} = 1$, these $N$ bits must satisfy $s_5 s_6 \cdots s_{B_{N-1}} = 1$. Consequently, if all the Bobs cooperate, they know Alice’s bit $s_A = s_B \cdots s_{B_{N-1}}$; and if one or more of the Bobs refuses to cooperate, then the other Bobs have strictly no information on what Alice has sent.

Before studying Eve’s optimal individual attacks on NQSS, we introduce the useful notations

$$
|0^N\rangle_z = |0\rangle_z \otimes \cdots \otimes |0\rangle_z, \quad |1^N\rangle_z = |1\rangle_z \otimes \cdots \otimes |1\rangle_z, $$

$$
|0^N\rangle_x = \frac{1}{\sqrt{2}}(|0^N\rangle_z + |1^N\rangle_z), \quad |1^N\rangle_x = \frac{1}{\sqrt{2}}(|0^N\rangle_z - |1^N\rangle_z), $$

$$
|0^N\rangle_y = \frac{1}{\sqrt{2}}(|0^N\rangle_z + i|1^N\rangle_z), \quad |1^N\rangle_y = \frac{1}{\sqrt{2}}(|0^N\rangle_z - i|1^N\rangle_z).
$$

These notations may seem misleading, since $|0^N\rangle_x, |1^N\rangle_x, |0^N\rangle_y, \text{ and } |1^N\rangle_y$ are not product states like $|0^N\rangle_z$ and $|1^N\rangle_z$, but GHZ states. It will become evident in the following why such notations are indeed suited to our analysis.

B. Optimal eavesdropping for 3QSS

For clarity, we discuss in all detail Eve’s attacks in the case $N=3$, that is, on the quantum secret sharing protocol proposed in Ref. [17] and demonstrated experimentally in Ref. [18]. Alice’s authorized partners are called Bob and Charlie. Two scenarios for eavesdropping can be imagined.

**Scenario 1.** An external Eve tries to eavesdrop on both channels $A-B$ and $A-C$, in order to gain as much information as possible on Alice’s message. For the analysis of this scenario, it is convenient to suppose that Alice measures immediately $\sigma_x$ or $\sigma_y$, on her qubit. This way, she prepares the two-qubit state that is sent to Bob and Charlie, according to Table I. If we forget the difference in the physical realization of the flying bit and stick to the information content of what is being transmitted, this eavesdropping scenario is identical to the eavesdropping on the BB84 protocol. Therefore, we know an individual attack that maximizes $I(A:E)$ for a given $I(A:B)$: it is given by Eq. (2), replacing $|0\rangle$ with $|0^2\rangle$ on Bob’s side. Note that this attack is “coherent,” in the sense that Eve attacks coherently the two qubits flying to $B$ and $C$; but is nevertheless an “individual” attack, since each pair of qubits is attacked separately form the other pairs.
includes the study of scenario 1.

Scenario 2. Bob does not want to cooperate with Charlie in order to retrieve Alice’s message. Consequently, he collaborates with an Eve that tries to eavesdrop on the line A-C. In this scenario, two triples come into play: A-B-C and A-B-E, and the meaningful information measures are \(I(A:BC)\) and \(I(A:BE)\). Just as in the analysis of scenario 1, it is useful to recast the protocol in the following form: by measuring \(\sigma_x\) or \(\sigma_y\), A and B prepare the state of the qubit that is sent to C. The preparation is given in Table II. The bits flying on the channel A-C are exactly in the same physical state as in a BB84 protocol. The conclusion here is not as straightforward as for scenario 1, however, because the individual attack (2) optimizes for \(I(AB:E)\) with respect to \(I(AB:C)\). But \(I(AB:C) = I(A:BC)\) and \(I(AB:E) = I(A:BE)\) hold even in the presence of the eavesdropper: in fact, B and C are not correlated with A and E is not correlated with A and B; therefore, \(H(B|A) = H(B|C) = H(B|E) = H(B)\). Thus Eve’s optimal individual attack is given directly by Eq. (2)—of course, here Eve is eavesdropping on Charlie, so one would write \(U_{CE}\) instead of \(U_{BE}\).

C. Optimal eavesdropping for NQSS

Let us turn now to the protocol NQSS, for arbitrary \(N\). In the general eavesdropping scenario (Fig. 2), Alice’s partners \(B_1, \ldots, B_{N-n-1}\) are dishonest, and would like to retrieve the key without collaborating with the \(n\) honest partners \(B_{N-n}, \ldots, B_{N-1}\). Thus Eve attacks the \(n\) qubits flying to the honest partners. We shall call \((A,B_1, \ldots, B_{N-n-1})\) the authorized partners, and \((A,B_1, \ldots, B_{N-n-1}, E)\) the unauthorized partners.

To find the optimal individual attack in any eavesdropping scenario, we can apply the same argument that was used in the case of 3QSS. One the one side, as discussed, even under eavesdropping, it holds that \(I(AB_1 \cdot B_{2-n-1}:B_{N-n} \cdot \cdot \cdot B_{N-1}) = I(A:B_1 \cdot B_{2-n} \cdot \cdot \cdot B_{N-1})\). On the other side, conditioned to the measurements of \(\sigma_x\) and \(\sigma_y\), any honest partner can only receive one of the four states \(|0\rangle_x\), \(|1\rangle_x\), \(|0\rangle_y\), \(|1\rangle_y\). In fact, take as an example the case where all the \(N-n\) partners measure \(\sigma_x\). The \(N\)-qubit GHZ state \(|GHZ_N\rangle\) can be rewritten as (we neglect normalization)

\[
|0^N\rangle_x + |1^N\rangle_x = (|0\rangle_x + |1\rangle_x)^{\otimes(N-n)}|0^n\rangle_x \\
+ (|0\rangle_x - |1\rangle_x)^{\otimes(N-n)}|1^n\rangle_x \\
= \text{(even number of $1's$)} \otimes |0^n\rangle_x \\
+ \text{(odd number of $1's$)} \otimes |1^n\rangle_x.
\]

Then, conditioned on the result of the measurement of \(\sigma_x\) on the first \(N-n\) qubits, either \(|0^n\rangle_x\) or \(|1^n\rangle_x\) is sent to the remaining \(n\) partners. The case where some of the \(N-n\) partners measure \(\sigma_y\) is analogous; the states that are prepared are \(|0^n\rangle_y\) or \(|1^n\rangle_y\) if an even number of partners measure \(\sigma_y\), \(|0^n\rangle_y\) or \(|1^n\rangle_y\) otherwise.

In conclusion, we have shown that, for all possible eavesdropping scenarios on NQSS protocols, Eve can perform the optimal individual attack having a single qubit as resource. The interaction that describes the optimal individual attack on \(n\) channels is

\[
|0^n\rangle_x \otimes |0\rangle_x \rightarrow |0^n\rangle_x \otimes |0\rangle_x \\
|1^n\rangle_x \otimes |0\rangle_x \rightarrow \cos \phi |1^n\rangle_x \otimes |0\rangle_x + \sin \phi |0^n\rangle_x \otimes |1\rangle_x,
\]

where \(\phi \in [0, \pi/2]\) measures the strength of the interaction. Of course, this interaction is presumably more complicated when she eavesdrops on several channels (like in scenario 1 for 3QSS), since she must have her qubit interacting coherently with all flying qubits. For the attack (8), the mutual information for the authorized and for the unauthorized partners, \(I_a\) and \(I_u\), respectively, can be calculated explicitly; it is not astonishing that the result is

\[
\begin{array}{|c|c|}
\hline
\text{Measurements of } A \text{ and } B & \text{Result} & \text{State of } C \\
\hline
\sigma_x \otimes \sigma_x & + + & |0\rangle_x \\
- + & |1\rangle_x \\
- - & |0\rangle_x \\
\hline
\sigma_x \otimes \sigma_y & + + & |0\rangle_y \\
- + & |1\rangle_y \\
- - & |0\rangle_y \\
\hline
\end{array}
\]
\[ I_a = I(A: B_1, \ldots, B_{N-1}) = I_{N-2}(A: B) = 1 - H(\{D_{AB}, 1 - D_{AB}\}), \quad (9) \]
\[ I_a = I(A: B_1, \ldots, B_{N-n-1}, E) = I_{N-2}(A: E) = 1 - H(\{D_{AE}, 1 - D_{AE}\}). \quad (10) \]

with \( D_{AB} \) and \( D_{AE} \) given by Eq. (5). So again by symmetry \( I_a > I_b \) if and only if \( \phi < \pi/4 \). To our knowledge, privacy amplification has not been studied in secret-sharing protocols; in particular, it is not clear if there is still a huge difference in efficiency between “one-way” and “two-way” protocols. It seems, however, obvious that the set of partners having the highest mutual information can run some protocol to extract a secret key.

IV. VIOLATIONS OF BELL’S INEQUALITIES

A. Multiqubit Bell’s inequalities

In the case \( N=2 \), we saw that \( I_a > I_b \) if and only if the authorized partners violate the CHSH inequality, that is if \( S_a > 2 > S_u \). We extend this result to all NQSS protocols. The number of inequivalent Bell grows rapidly with \( M \), the number of qubits. We restrict to the family of inequalities obtained when only two measurement are performed on each qubit, which are the natural generalization of the CHSH inequality. Even with this restriction, the number of possible inequalities grows as \( 2^M \); but recently, the inequalities in this family have been completely classified by Werner and Wolf [19]. In particular, they have shown that, the \( M \)-particle GHZ state being given, the maximal violation is obtained precisely using the \( M \)-qubit Mermin-Klyshko (MK) inequality [20,21]. These are the inequalities that we consider in this section.

Let \( \vec{a} \) be a set of \( 2^M \) unit vectors. The Bell operator that enters the MK inequality for \( M \) qubits is defined recursively as

\[ B'_m(a) = B_m = (\sigma_{a_{m}} + \sigma_{a_{m}}') \otimes B_{M-1} \]
\[ + \frac{1}{2}(\sigma_{a_{m}} - \sigma_{a_{m}}') \otimes B'_{M-1}, \quad (11) \]

where \( B'_m \) is obtained from \( B_m \) by exchanging all the \( \vec{a}_k \) and \( \vec{a}_k' \). The maximal value for product states is \( B_M = 2^2 \); quantum correlations allow \( B_M > 2 \), up to \( B_M = 2^{(M+1)/2} \), obtained for \( M \)-qubit GHZ states. It is important to stress another property of MK inequalities [21,22]. Let \( \rho \) be a \( M \)-qubit state, and suppose that you can find a decomposition \( \rho = \sum \rho_i \rho_i \) such that in all \( \rho_i \), at most \( m < M \) qubits are entangled (not necessarily the same ones in each \( \rho_i \)); then \( \langle B'_m \rangle_\rho \leq 2^{(m+1)/2} \). In other words, if \( 2^{m/2} \langle B'_m \rangle_\rho \leq 2^{(m+1)/2} \), the inequality for product states is violated, but this violation is weak, in the sense that it can be achieved with \( m \)-qubit entanglement. Now, for NQSS to work, \( \rho \) must be “close” to \( \{|GHZ\_M\} \), that is, must exhibit “strong” \( M \)-qubit entanglement. Thus in all that follows we shall say that a \( M \)-qubit state \( \rho \) violates the MK inequality if the violation is higher than the one that could be achieved with \( M-1 \) qubits, that is, if \( \langle B'_m \rangle_\rho \geq 2^{M/2} \).

B. Violation of MK inequalities in NQSS

We consider the state that is generated in an eavesdropping scenario on NQSS. As usual, Alice is the sender. Some of the receivers would like to retrieve Alice’s message without the other \( n \) partners to know it; they ask then Eve to spy on those lines. We call Bobs \( B_1, \ldots, B_{N-n-1} \) the partners that collaborate with Eve, and Charles \( C_1, \ldots, C_n \) those that are spied. In the quantum protocol, each partner has a qubit, so we consider a system of \( N+1 \) qubits. We write the Hilbert space as \( H_{AB} \otimes H_C \otimes H_E \). We have demonstrated in the previous section that under Eve’s optimal attack the state shared by the \( N + 1 \) partners becomes (we drop the subscript \( z \))

\[ |\Psi_{N,n} \rangle = \frac{1}{\sqrt{2}}(|0^{N-n})|0^n)|0 \rangle + \cos \phi |1^{N-n})|1^n)|0 \rangle \]
\[ + \sin \phi |1^{N-n})|0^n)|1 \rangle). \quad (12) \]

Let \( \rho_{ABC} = \rho_a \) and \( \rho_{ABE} = \rho_e \) be the density matrices of the authorized and of the unauthorized partners that are derived from \( |\Psi_{N,n} \rangle \). We have \( S_n = \max \text{Tr}[B_n(a) \rho_a] \) and \( S_u = \max \text{Tr}[B_{N-n+1}(a) \rho_e] \). In the absence of a criterion like Horodecki’s [14], it is difficult to perform the optimization that gives \( S_n \), even for the particular state that we consider. We found an explicit result when \( N \) and \( n \) have different parity, and relied on numerical optimization for the other cases. These results are given in Appendix A. Within these warnings, we can safely state that the following holds: in the NQSS protocol, whatever the number \( n \) of honest partners that are eavesdropped by Eve:

\[ I_a > I_b \] if and only if \( S_u > 2^{N/2}; \quad (13) \]

and in this case \( S_u < 2^{(N-n+1)/2} \). This is the exact analog of the result obtained for \( N = 2 \); in case of optimal attack by Eve, the authorized partners have a higher information than the unauthorized ones if and only if they violate the MK inequalities.

V. MORE ON BELL’S INEQUALITIES

A. Other Bell’s inequalities

We have just described a sharp link between security of NQSS and the violation of the MK inequalities. MK inequalities have been chosen for this study (see above) because they give the maximal violation for the GHZ state, which is the state produced by Alice. This argument is reasonable but certainly not compelling. It is natural to ask what becomes of the link between Bell and security of NQSS if we choose other inequalities. To be more precise, the general program would be: take the state \( |\Psi_{N,n} \rangle \) given by Eq. (12) with \( \phi = \pi/4 \) (because by symmetry \( I_a = I_b \) at this point), and optimize the Bell parameter \( S_a \) for all inequalities. The fulfillment of this program in its full generality is beyond reach to date. As a first exploration beyond the realm of MK inequalities, we consider the case of 3QSS and calculate the Bell’s parameters \( S_a \) using the inequalities (A2)–(A4) of Ref. [19], which are inequivalent to Mermin’s. The operators
that define these inequalities are (for conciseness, we write $a_k$ instead of $\sigma_{a_k}$, and omit tensor products):

$$B_1 = (a_i a_j + a_i a_j' + a_i' a_j - a_i' a_j') a_k,$$

$$B_{II} = a_i a_j (a_k + a_k') + a_i' a_j' (a_k - a_k'),$$

$$B_{III} = \frac{1}{2} (a_1 + a_1')(a_2 + a_2')(a_3 + a_3') - 2a_1 a_2 a_3,$$

with $(i,j,k)$ a permutation of $(1,2,3)$. As above, we have adopted the scaling such that the violation of the inequality reads $S > 2$. The following results are numerical; $S_\alpha$ is the same for both $|\Psi_{32}\rangle$ (external Eve) and $|\Psi_{31}\rangle$ (Bob collaborating with Eve).

The operator $B_1$ is the CHSH operator (6) on $i$ and $j$, and a trivial operator on $k$. The structure of the operator $B_{II}$ is also the one of CHSH, but here $i$ and $j$ are taken together. For both operators, the maximal expectation value allowed by QM is $2\sqrt{2}$, which is achieved by states of the form $|\text{EPR}\rangle|0\rangle$ as well as, for different settings, by GHZ states. It is not astonishing that using either of these inequalities, we find $S_\alpha = 1$ for $\phi = \pi/4$: this is the threshold of violation, but these inequalities are less sensitive because they have no threshold distinguishing two- from three-particles entanglement.

The operator $B_{III}$ is different, and shows a more complex behavior in our problem. The maximal value achievable by QM is $2\sqrt{2}$, reached for GHZ states. States of the form $|\text{EPR}\rangle|0\rangle$ achieve $2\sqrt{2}$. For our states, we find $S_\alpha = 2.357$ for $\phi = \pi/4$: this does not correspond to any threshold, but is below the threshold for two-particles entanglement.

In summary: for our problem, the inequalities (A2)–(A4) of Ref. [19] are less sensitive than Mermin’s. In fact, in all cases it holds that if $S_\alpha$ is bigger than the threshold between two- and three-particle entanglement (if such threshold exists), then security is ensured. Mermin’s inequality showed that the condition is also sufficient.

B. Violation of MK inequalities by overlapping sets of qubits

The main feature of the link between optimal eavesdropping and the violation of MK inequalities is that the authorized partners violate the inequality if and only if the unauthorized partners don’t. Of course, it is trivial to loosen this link: nonoptimal attacks can easily be found in which neither set of partners violate an inequality. Thus, so far we have met only states of qubits characterized by the following property: if a set $M$ of $M$ qubits violate a MK inequality, then all other sets of qubits having an overlap with $M$ do not violate a MK inequalities. A natural question is: is this property true for all possible states of qubits? If the answer were positive, then for any given state the violation of MK inequalities would define a unique partition of the set of qubits, into subsets of “strongly entangled” qubits. This would provide an unexpected link between the violation of MK inequalities and the structure of the Hilbert space.

However, the answer to this question turns out to be negative in the general case. The simplest counterexample is provided by states of four qubits $A$, $B$, $C$, and $D$, in which two triples $(A,B,C)$ and $(B,C,D)$ violate the Mermin’s inequality. For example, for $\alpha \approx 0.955$, the state $|\xi(a)\rangle = \cos \alpha |0011\rangle + |1100\rangle + i|0101\rangle + i|1010\rangle/2 + \sin \alpha |i010\rangle + |1111\rangle)/\sqrt{2}$ gives $S_{ABC} = S_{BCD} = 3$, obviously higher than $2\sqrt{2}$, which is the bound for a three-qubit violation. We have found numerically several more examples in which a violation of MK inequalities by two overlapping sets is allowed; these results are listed in Appendix B. Interestingly, there are also some cases in which a double violation is not possible; thus there is indeed a link between the violation of MK inequalities and the structure of the Hilbert space, although this link may be difficult to unravel. In particular, we do not know whether this link is due to a property of quantum nonlocality, or if it is a consequence of the special form of the MK inequalities.

In the meantime, the link between violation of MK inequalities and security is strengthened by these remarks. In fact, even though there exist states in the Hilbert space that would allow double violations of MK inequalities, these states can never be produced in any eavesdropping scenario. Consider the case of four qubits. Two triples $(A,B,C)$ and $(A,B,E)$ appear in the description of 3QSS with scenario 2 for eavesdropping, in which Bob collaborates with Eve who attacks the qubit flying to Charlie. Since Alice has prepared a GHZ state, the most general state that can be produced in such a situation is $(|AB\rangle \otimes U_{CE}(\text{GHZ})_{ABC}|0\rangle)$. We verified by a numerical optimization that no state of this form can violate the Mermin’s inequality for more than one triple [obviously, the state $|\xi(a)\rangle$ cannot be written in this form].

VI. CONCLUSION

We discussed link between the security of some quantum key distribution protocols and the violation of some Bell inequalities. Precisely: in a secret-sharing protocol, the authorized partners have a higher mutual information than the unauthorized ones if and only if they violate a Mermin-Klyshko inequality. This link has been demonstrated for half of the possible eavesdropping scenarios, and is conjectured to be always valid. Whether a similar result holds for other protocols, or for other inequalities, is an open question worth investigating.

All the protocols described in this paper can be implemented using qubits. It is a current field of investigation whether higher security can be achieved using higher-dimensional quantum systems [24]. Moreover, Bell’s inequalities that seem optimal for higher-dimensional bipartite systems have recently been proposed [25]. The link between security and violation of a Bell’s inequality is likely to provide powerful insight for these topics of research.

ACKNOWLEDGMENTS

We acknowledge partial financial support from the Swiss FNRS and the Swiss OFES within the European project EQUIP (IST-1999-11053).

APPENDIX A

We want to calculate $S_\alpha = \max_\alpha \text{Tr}[B_N(a)\rho_\alpha]$ and $S_\alpha = \max_\alpha \text{Tr}[B_{N+n+1}(a)\rho_\alpha]$, where $\rho_\alpha = \rho_{ABC}$ and $\rho_\alpha = \rho_{ABE}$.
rigorously demonstrated for a first the calculation of S a 2 (eral numerical estimates strongly suggest that S a 5 N1N050 for the qubits in the two subsets obtained from |Ψ⟩⟨Ψ| by partial traces. We ask if it is possible to find a state |Ψ⟩ ∈ H K such that

S N = maxχ Tr[ρ N B χ (χ)] > 2 m 2

and

S M = max δ Tr[ρ M B m (δ)] > 2 m 2.

where χ and δ are sets of, respectively, 2n and 2m unit vectors. To tackle this question, we define the observable

V k m = B χ (χ) ⊗ 1 k m + 2 n m / 2 1 k m ⊗ B m (δ).

The computer program maximizes the highest eigenvalue of V k m over all possible choices of χ and δ. If the highest eigenvalue does not exceed 2 × 2 m 2 , then it is impossible to find a state that allows both S N > 2 m 2 and S M > 2 m 2. The results of the numerical calculations that we performed are listed here (for clarity, we print in boldface the common qubits).

(i) max(SAB + S AC) = 4: double violation impossible (Theorem 1 in Ref. [23]).
(ii) max(S ABC + S ADE) = 4√2: impossible.
(iii) max(S ABC + S ABD) = 6.0945 > 4√2: possible; see main text for a state that gives a double violation.
(iv) max(S ABC + 2√2 S AD) = 4√2: impossible.
(v) max(S ABC + 2 S AB) = 6.9282 > 4√2: possible, e.g., for the state |ψ⟩ = (|000⟩ + cos α|111⟩ + sin α|110⟩), α ∈ [π/2].
(vi) max(S ABCD + S ADEF) = 8: impossible.
(vii) max(S ABCD + S ABEF) = 8.6128 > 8: possible.
(viii) max(S ABCD + S ABCF) = 8: impossible.
(ix) max(S ABCD + 2 S AE) = 8: impossible.
(x) max(S ABCD + 2 S AR) = 9.7566 > 8: impossible.
(xi) max(S ABCD + 2√2 S AEF) = 8: impossible.
(xii) max(S ABCD + 2 S ABE) = 6√2 > 8: possible.
(xiii) max(S ABCD + 2√2 S ABC) = 9.6566 > 8: possible.
(xiv) max(S ABCDE + S ABCFG) = 12.088 > 8√2: possible.
(xv) max(S ABCDE + S ABCF) = 8√2: impossible.
(xvi) max(S ABCDE + S ABCD) = 8√2: impossible.
(xvii) max(S ABCDE + 2 S ABE) = 12.18 > 8√2: possible.

In these examples, double violations appear to be possible when one set is completely contained into the other one, i.e., M ⊂ N, or when Card(M ∩ N) = 2. Of course, it is difficult to guess general rules from these observations, since we have explored only the cases n, m = 2, 3, 4 and some cases with  n, m = 5.
[26] We verified the case $N=3$, $n=1$, and some cases for $N=4$ and $N=5$. 

012311-8