# Quantum key distribution for *d*-level systems with generalized Bell states

Vahid Karimipour[1,*] and Alireza Bahraminasab[1,†]
[1]*Department of Physics, Sharif University of Technology, P.O. Box 11365-9161 Tehran, Iran*

Saber Bagherinezhad[2,‡]
[2]*Department of Computer Science, Sharif University of Technology, P.O. Box 11365-9161 Tehran, Iran*
(Received 18 November 2001; published 14 May 2002)

Using the generalized Bell states and controlled-NOT gates, we introduce an entanglement-based quantum key distribution (QKD) of *d*-level states (qudits). In case of eavesdropping, Eve's information gain is zero and a quantum error rate of $(d-1)/d$ is introduced in Bob's received qudits, so that for large *d*, comparison of only a tiny fraction of received qudits with the sent ones can detect the presence of Eve.

DOI: 10.1103/PhysRevA.65.052331 PACS number(s): 03.67.−a, 03.65.−w, 03.65.Ud

## I. INTRODUCTION

As far as classical computation and classical communication are concerned, binary units of memory and binary logic gates play an inevitable and natural role due to the inherent simplicity of Boolean algebra on the one hand and their compatibility with on and off states of electronic switches on the other hand. With such classical gates as NOT, AND, and OR, the simplest logical operations with which we are familiar in everyday life, and also any binary function, can be implemented. They are also quite simple to design electronically. However, in quantum computation and communication (see [1,2] and references therein), the main resources that have the potential of surpassing our conventional classical methods, are quantum parallelism (for massive computation), nonlocality and entanglement (for communication), and uncertainty relations (e.g., for quantum key distribution, among other things). For utilizing these resources, two-level quantum states are by no means inevitable. Only considerations of quantum hardware should decide between using two-level or multilevel states. At present a major difficulty in quantum computation is the limit on the number of qubits that can be coupled experimentally [3]. Although it may be easier to construct universal gates for qubits than for qudits, the use of *d*-dimensional systems or qudits has the advantage of the fact that compared to qubits, fewer systems should be coupled to obtain a given dimensionality of the Hilbert space. Apart from practical considerations, it will enhance and deepen our understanding of the subject if we try to reformulate quantum computation and communications in a dimension-free context. In view of this, various authors have tried to generalize some of the algorithms, protocols, or error correcting codes of two-level quantum computation to arbitrary-dimensional Hilbert spaces [4–13]. Consequently, one sees in the literature that the same basic tool (i.e., a generalized gate) has been defined independently in several works.

For example, the generalization of one of the basic gates of quantum computation, that is, the controlled-NOT gate, appears to have been given independently by a number of authors under different names [4–6,8,14,15]. The same is also true for the generalized Hadamard gate. Especially in Ref. [5] an experimental realization of the generalized XOR gate to *d*-levels has been proposed, where the number *n* of photons in an electromagnetic mode signifies the state $|n\rangle$, $n=0,\ldots,d-1$ and a Kerr interaction between these photons and their Fourier transform is used to induce the generalized XOR gate on the states.

In this paper we are concerned with a protocol of quantum key distribution (QKD) and its generalization to states of arbitrary dimension. Quantum cryptography (QC) that is based on very simple ideas and yet not far from real applications as the other highlights of quantum computations are (like factoring large integers) is one of the most promising areas of research in quantum computation and information.

Particularly interesting is that in QC one tries to turn the apparently negative or counterintuitive rules of quantum mechanics, which has resulted in epistemological debates in the past decades, into enormously useful devices for engineering applications. One such concept has been the uncertainty principle, or the fact that observation or measurement perturbs the observable. This rule has been utilized in a most beautiful application in the form of the Bennet-Brassard 1984 (BB84) protocol for QKD [16], where bits of a key prepared by two legitimate parties, in the form of spin or polarization of particles in random bases, are inevitably perturbed by a nonlegitimate third party. (For a review on QC including many theoretical and practical issues, see Ref. [17].)

Another nonclassical and counterintuitive concept, has been the concept of nonlocality and entanglement that has found even wider applications, to the extent that nowadays a major problem about nonlocality is not how to interpret it, but how to measure it like other useful resources as energy and momentum.

The first entanglement-based protocol of QKD has been the work of Ekert [18], which later was shown to be equivalent to the original BB84 protocol [19], (see Ref. [17] for finer details). Two other QKD protocols that have used entanglement in an essential way has been reported in Refs. [20] and [21]. The first of these uses entanglement swapping via Bell measurements to safely transfer a key and has been generalized to *d*-level systems in Ref. [15]. The second is

*Email address: vahid@sina.sharif.edu
†Email address: baramina@physics.sharif.edu
‡Email address: bagherin@ce.sharif.edu

 

based on local gate operations on a reusable EPR pair, where Alice tries to hide the secure data by entangling each bit with the EPR pair, sending the bit to Bob who can disentangle the bit and read the data. The strategy of Eve is to somehow entangle herself with the whole state of the EPR and the bit by suitable operations and find access to the data, without being revealed by Alice and Bob.

The aim of this paper is to generalize this second protocol to higher-dimensional states and at the same time give a clear exposition of its basics.

For the sake of brevity, we will not go into the details of the two-level protocol. For this, the reader can either consult Ref. [21], or else go through the following sections and at each step set $d=2$.

The basic advantage of this protocol is that as we will show, not only Eve's presence will be detected by Alice and Bob, but also her information gain is zero, compared to the 50% information gain in the BB84 protocol. This is true in every dimension, but as we will show, Eve's presence introduces a higher quantum bit error rate, in higher-dimensional states, so that her presence can be detected more easily.

The structure of this paper is as follows. In Sec. II we first review some known and new facts about the generalized Bell states, and the generalizations of controlled-NOT (c-NOT), and the Hadamard gates to qudits. In Sec. III which has been divided into several subsections, we generalize the QKD scheme of Ref. [21] to *d*-level systems, and discuss the security of the protocol against some individual attacks. We show that the information gain of Eve is actually zero and show how the intervention of Eve introduces an error rate of $(d-1)/d$ into the data received by Bob, and greatly enhances the chance of her detection by the legitimate parties. In all this we are concerned only with theoretical considerations and do not consider practical issues, or any rigor in proving security. All these are important but should be considered in separate works. Finally in Sec. IV, which concludes the paper, we discuss a possible route for generalization of our results to the continuous variables. Some of the calculations that are not detailed in the main text, are collected in the Appendices.

## II. STATES AND GATES FOR *d*-LEVEL SYSTEMS

For qudits, a generalization of the familiar Bell states, has been introduced in Refs. [5,22–24]. These are a set of $d^2$ maximally entangled states that form an orthonormal basis for the space of two qudits. Their explicit forms are

$$|\Psi_{m,n}\rangle := \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} \zeta^{nj} |j, j+m\rangle, \tag{1}$$

where $\zeta = e^{2\pi i/d}$ and $m$ and $n$ run from 0 to $d-1$. These states have the properties $\langle \Psi_{m,n} | \Psi_{m',n'} \rangle = \delta_{n,n'} \delta_{m,m'}$ (orthonormality) and $\mathrm{tr}_2(|\Psi_{m,n}\rangle\langle\Psi_{m,n}|) = (1/d)\mathbb{1}$ (maximal entanglement). The following operators [4,22–24] are also useful, since they play the analogous role of Pauli operators for qudits:

$$U_{m,n} = \sum_{j=0}^{d-1} \zeta^{nj} |j+m\rangle\langle j|. \tag{2}$$

For example, given the entangled state $|\Psi_{0,0}\rangle$, only one of the parties, say Alice, can generate any Bell state $|\Psi_{m,n}\rangle$ by acting on $|\Psi_{0,0}\rangle$ with $U_{m,n}$, i.e.,

$$(\mathbb{1} \otimes U_{m,n}) |\Psi_{0,0}\rangle = |\Psi_{m,n}\rangle. \tag{3}$$

One should, however, note that contrary to the Pauli operators, the operators $U_{m,n}$ are not necessarily Hermitian.

One can also generalize the Hadamard gate that turns out to be quite useful in manipulating qudits for various applications [4,5,14],

$$H := \frac{1}{\sqrt{d}} \sum_{i,j=0}^{d-1} \zeta^{ij} |i\rangle\langle j|, \tag{4}$$

where $\zeta = e^{2\pi i/d}$. This operator is really not new and it is known as the quantum Fourier transform when $d=2^n$. In that case it acts on $n$ qubits. Here we are assuming it to be a basic gate on one single qudit, in the same way as the ordinary Hadamard gate is a basic gate on one qubit. This operator is symmetric and unitary ($HH^*=\mathbb{1}$), but not Hermitian.

To generalize the NOT and the controlled-NOT gates, we note that in the context of qudits, the NOT gate is, basically, a mod-2 adder. For qudits this operator gives way to a mod-$d$ adder, or a right-shift gate [4,5,8,14,15],

$$R|j\rangle = |j+1\rangle \bmod d, \tag{5}$$

$$R^{-1}|j\rangle \equiv L|j\rangle = |j-1\rangle \bmod d, \tag{6}$$

where $L$ has been used to denote a left shift. Note that $R^d = \mathbb{1}$, compared to $(\mathrm{NOT})^2 = \mathbb{1}$.

For every unitary operator $U$, the controlled gate $U_c$ that acts on the second qudit conditioned on the first qudit is naturally defined as follows:

$$U_c(|i\rangle \otimes |j\rangle) = |i\rangle \otimes U^i |j\rangle. \tag{7}$$

Note the difference with the qubit case. In the qubit case a controlled operator acts only if the value of the first bit is 1, here it acts $i$ times if the value of the first qudit is $i$. (Sometimes it is said that a controlled operator is like an *if statement* in classical computation [1]. If we take this statement literally, then a controlled operation for *d*-level states acts like a loop.) In particular, the controlled shift gates that play the role of controlled-NOT gate, act as follows:

$$R_c|i,j\rangle = |i,j+i\rangle, \quad L_c|i,j\rangle = |i,j-i\rangle. \tag{8}$$

Every function $f$ from $\{0,1,\ldots,d-1\}^n \to \{0,1,\ldots,d-1\}^m$ is made reversible by the definition $f_r(\mathbf{x},\mathbf{y}) = (\mathbf{x}, f(\mathbf{x})+\mathbf{y})$, where all additions are performed mod $d$. In quantum circuits such a function is implemented by a unitary operator $U_f|\mathbf{x},\mathbf{y}\rangle := |\mathbf{x}, f(\mathbf{x})+\mathbf{y}\rangle$, where $\mathbf{x} \in \{0,1,\ldots,d-1\}^n$ and $\mathbf{y} \in \{0,1,\ldots,d-1\}^m$. Note that here and in all that follows, addition of multidits is performed ditwise and mod $d$.

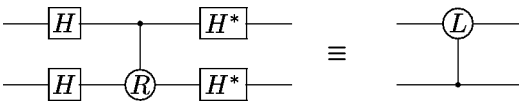


FIG. 1. Circuit identity for $d$-level gates.

Quite analogously to the $q$ bits, the Hadamard and the controlled shift gates can generate all the Bell states $\{|\Psi_{m,n}\rangle\}$ from the computational basis states $\{|m,n\rangle\}$ [5],

$$R_c(H\otimes\mathbb{1})|n,m\rangle=|\Psi_{m,n}\rangle. \tag{9}$$

Many other properties of these gates are simply carried over from the case of $q$ bits to the general case with appropriate modifications. For example, one can check the validity of the circuit identity in Fig. 1.

## III. AN ENTANGLEMENT-BASED PROTOCOL OF QKD FOR $d$-LEVEL STATES

In this section we generalize an entanglement-based protocol of quantum key distribution first put forward in Ref. [21] to $d$-level states and perform further analysis of the method.

### A. QKD in the absence of Eve

The starting point of this protocol is the sharing of a Bell state $|\Psi_{00}\rangle=(1/\sqrt{d})\Sigma_{j=0}^{d-1}|j,j\rangle_{a,b}$ by Alice and Bob. The qudit to be sent is denoted by $q$, which is encoded as a basis state $|q\rangle_k$. Throughout the paper we use the subscripts $a,b,k$, and $e$ for Alice, Bob, key, and Eve, respectively. The basic idea, neglecting considerations of Eve's attack for now, is that Alice performs a controlled-right shift on $|q\rangle_k$ and thus entangles this qudit to the previously shared Bell state, producing the state

$$|\Phi\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q+j\rangle_{a,b,k}. \tag{10}$$

She then sends the qudit to Bob. By this operation she is hiding the qudit $q$ in a completely mixed state, since $\rho_k := \mathrm{tr}_{a,b}|\Phi\rangle|\langle\Phi|=(1/d)\mathbb{1}_k$. At the destination, Bob performs a controlled-left shift on the qudit and disentangles it from the Bell state, hence revealing the value of $q$ with certainty.

Note that in contrast with the BB84 protocol, here the key is not determined *a posteriori* and randomly, hence a larger transfer rate is possible.

### B. An individual attack by Eve

A possible conceivable attack by Eve ($e$) is that she entangles her state to those of Alice, Bob, and the intercepted key so that after Bob's measurement of the qudit, she can obtain partial information about the qudit. The best way to describe and visualize the protocol is to refer to Fig. 2, where the qudits are drawn as lines and states at each stage are shown explicitly.

The strategy that Eve follows should be described separately for the first qudit and the rest of the qudits. For the first

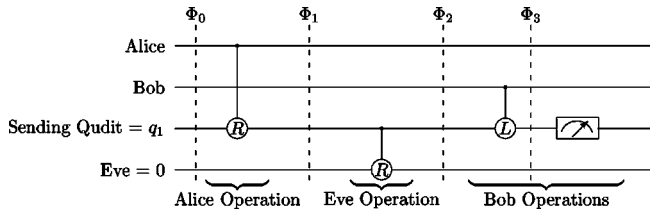


FIG. 2. Eve attacks for the first qudit.

qudit, she performs no measurement and proceeds so that her qudit gets entangled with the Bell state of Alice and Bob at the end of the process. For this she uses a controlled-right shift on her qudit conditioned on the value of the first qudit being sent (see Fig. 2). The states at various stages are as follows, where in each ket the qudits refer, respectively, from left to right to Alice ($a$), Bob ($b$), the key ($k$), and Eve ($e$):

$$|\Phi_0\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_1,0\rangle_{a,b,k,e}, \tag{11}$$

$$|\Phi_1\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_1+j,0\rangle_{a,b,k,e}, \tag{12}$$

$$|\Phi_2\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_1+j,q_1+j\rangle_{a,b,k,e}. \tag{13}$$

Note that choice of $|0\rangle$ for Eve's original state is quite arbitrary. Her strategy works with any other choice. In the last stage when Bob performs his left-shift gate, he produces the state

$$|\Phi_3\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_1,q_1+j\rangle_{a,b,k,e}, \tag{14}$$

and thus disentangles the key and correctly measures the value of its first dit $q_1$. However, his shared Bell state with Alice has now been left entangled with the state of Eve, which is used again by Alice and Bob (unaware of the entanglement with Eve) for the next round (i.e., for sending the dit $q_2$ of the key). Thus for the next round the state that Alice and Bob will start with is

$$|\Psi_0\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_2,q_1+j\rangle_{a,b,k,e}. \tag{15}$$

Note that we are assuming that Alice and Bob do not have access to a reservoir of Bell states, the later being supposedly expensive. Thus they are using one Bell state for sending the whole key or at least a considerable fraction of it.

It is important to note that Eve modifies her strategy for the next dits, by first performing a left shift, measuring her qudit, and then performing a right shift on her qudit. The rest of the process is like that for the first qudit (see Fig. 3). The various states in different stages shown in the figure are as follows:

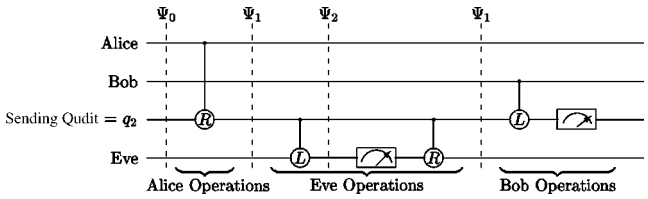


FIG. 3. Eve attacks for next qudits.

$$|\Psi_0\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_2,j+q_1\rangle_{a,b,k,e}, \tag{16}$$

$$|\Psi_1\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_2+j,j+q_1\rangle_{a,b,k,e}, \tag{17}$$

$$|\Psi_2\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,q_2+j,q_1-q_2\rangle_{a,b,k,e}. \tag{18}$$

At this stage Eve who has disentangled her qudit from the rest of the state measures her own qudit to be $q_1-q_2$. She then performs the controlled-right shift on her qudit to restore the original state $|\Psi_1\rangle$. At the destination Bob again proceeds as before, performs his left shift and measures the value of $q_2$, leaving the state of Alice, Eve, and his own state, in an entangled state ready for use in the next round.

In this way Eve intercepts the qudits

$$q_1-q_2,q_1-q_3,q_1-q_4,\ldots$$

from which she can infer all the sequence by checking $d$ possible values for $q_1$.

Note that for each qudit, Eve is effectively doing an intercept-recent strategy, however, she does not intercept the value of the qudit (say $q_2$) sent by Alice, but she measures a value $q_2-q_1$, where $q_1$ is the value of the first sent qudit that has been intercepted in an earlier stage.

### C. Protection against Eve's intervention

To protect this protocol against this kind of attack, Alice and Bob proceed as follows. Before sending *each* of the qudits, Alice and Bob act on their shared Bell state by the Hadamard gates $H$ and $H^*$, respectively. The key point is that a Bell state $|\psi_{0,0}\rangle$ disentangled from the outside world is unchanged under this operation, while a state entangled with outside is not:

$$(H\otimes H^*)|\Psi_{0,0}\rangle=|\Psi_{0,0}\rangle. \tag{19}$$

In the absence of the intervention of Eve, this extra operation has no effect on the protocol.

In fact the shared Bell state is unchanged under more general operators of the form $U\otimes U^*$, where $U$ is any unitary operator. We will investigate this possibility in Appendix B.

It is clear from Fig. 2, that for the first qudit nothing changes. However, for the second qudit and other qudits, essential changes occur in the intermediate states in the process. As we will see, in this way Alice and Bob can prevent Eve from getting any useful information. The entangled state of Alice, Bob, and Eve which remained from the first round is

$$|\chi\rangle=\frac{1}{\sqrt{d}}\sum_{j=0}^{d-1}|j,j,j+q_1\rangle_{a,b,e}. \tag{20}$$

When Alice and Bob perform their Hadamard gates on their qudits, this state changes to

$$|\tilde{\chi}\rangle=\frac{1}{\sqrt{d}}\sum_{i,j,k=0}^{d-1}H_{i,j}H^*_{k,j}|i,k,j+q_1\rangle_{a,b,e}. \tag{21}$$

Thus the second round of the protocol after Alice inserts the second dit of the key, starts with the state

$$|\widehat{\Psi_0}\rangle=\frac{1}{\sqrt{d}}\sum_{i,j,k=0}^{d-1}H_{i,j}H^*_{k,j}|i,k,q_2,j+q_1\rangle_{a,b,k,e}. \tag{22}$$

The state $|\widehat{\Psi_1}\rangle$ that results after Alice's controlled $R$ operation will be

$$|\widehat{\Psi_1}\rangle=\frac{1}{\sqrt{d}}\sum_{i,j,k=0}^{d-1}H_{i,j}H^*_{k,j}|i,k,i+q_2,j+q_1\rangle_{a,b,k,e}. \tag{23}$$

The qudit is now sent to Bob. We will show in Appendix A, that this new state has no information for Eve. In fact we will show that, the density matrix of her system and the qudit will be

$$\rho_{k,e}=\frac{1}{d^2}\mathbb{1}_k\otimes\mathbb{1}_e. \tag{24}$$

Therefore, under any unitary operation on her qudit and the sent qudit whether it be the controlled $L$ gate used for the first round or a more complex cleverly chosen operator, she will not be able to get useful information from the intercepted data. More generally, it is hardly possible for Eve that by a quantum operation derived from suitable interactions with her ancillas, can derive any useful information from this density matrix.

### D. The information gain of Eve

The above situation is analogous to the case of BB84 protocol, where with respect to any basis chosen by Eve, the density matrix of the qubits intercepted by Eve are identity matrices. However, there is one major difference in that in the BB84 protocol and its variations and generalizations to higher-dimensional states, the protocol ends up with a public announcement of the bases of Alice and Bob, from which Eve finds that she has intercepted a fraction of the qubits or qudits correctly. Therefore, Eve finds partial information about the key and only her revealing by Alice and Bob saves those protocols. Here we will show that the information gain of Eve is actually zero and she obtains no information at all about the key. The mean information gain per bit of Eve $I$, is the difference between two relative entropies and is inter-

preted as the percentage of bits that are saved when Eve wants to write the data of Alice from her own intercepted data [17]. We have

$$I = H_{a\ priori} - H_{a\ posterieri}. \tag{25}$$

Assuming that Alice sends the qudits uniformly, we have $H_{a\ priori} = \log_2 d$. We also have

$$H_{a\ posterieri} = -\sum_r p(r)p(i|r)\log_2 p(i|r), \tag{26}$$

where $p(r)$ is the probability that Eve receives a dit value of $r$ and $p(i|r)$ is the *a posterieri* probability that Alice has sent a dit value of $i$ given that Eve has received a dit value of $r$. The later can be easily calculated from Bayes's formula

$$p(i|r) = \frac{p(i)p(r|i)}{\sum p(i)p(r|i)}. \tag{27}$$

Since Alice is assumed to send the dits uniformly, we have $p(i) = 1/d$ and since the density matrix of Eve is unity, $p(r|i) = 1/d$, thus we find: $p(i|r) = 1/d$. Inserting all this in Eq. (26) we find that $H_{a\ posterieri} = \log_2 d = H_{a\ priori}$ and hence zero information gain for Eve. This is a very interesting property of this protocol compared with the BB84 protocol and its variations or generalizations to higher-dimensional systems where the information gain of Eve is nonzero. In fact in the BB84 protocol the 50% information gain is due to those occasions where the basis of Eve happens to be the same as the publicly announced baseis of Alice and Bob. Here there is no public announcement of any kind and so all the dits that Eve measures are really worthless at the end of the protocol.

### E. Detection of Eve

At this stage we want to show how Alice and Bob can infer the presence of Eve from comparison of their data. Although by no unitary operation on her system and the key, she can gain information from the key, she may want to use a clever operation to reduce as much as possible the quantum bit error rate (QBER) introduced into the data received by Bob, and hence her chance of being detected. The QBER depends on her choice of the operation. Suppose that she performs the same sequence of (controlled $R$ + measurement + controlled $L$) operations that she was doing in her successful attacks. It is straightforward to see that with the preservation of Hadamard gates, the new state that reaches Bob, provided that the qudits $q_1$ and $q_2$ have been sent and Eve has measured a qudit value of $q$ in the second round, is

$$|\Phi_3\rangle = \sum_{i,k=0}^{d-1} H_{i,i+q_2-q_1+q} H^*_{k,i+q_2-q_1+q} \times |i,k,i+q_2,q\rangle_{a,b,k,e}. \tag{28}$$

After Bob performs his controlled-$L$ operation, the final state ready for measurement will be

$$|\Phi_4\rangle = \sum_{i,k=0}^{d-1} H_{i,i+q_2-q_1+q} H^*_{k,i+q_2-q_1+q} \times |i,k,i+q_2-k,i+q+q_2\rangle. \tag{29}$$

It is again a simple computation to find the density matrix corresponding to the key space from this state, which turns out to be

$$\rho_k := \mathrm{tr}_{a,b,e} |\Phi_4\rangle\langle\Phi_4| = \frac{1}{d}\mathbb{1}_k. \tag{30}$$

This means that Bob measures all the values of the key qudit with equal probability and his chance of getting the correct qudit is $1/d$. Hence the QBER introduced into the data by Eve's intervention is $(d-1)/d$.

## IV. DISCUSSIONS

We have studied a protocol of quantum key distribution for $d$-level systems based on shared entanglement of a reusable Bell state and have shown that in this protocol, the information gain of Eve is zero and the QBER introduced by her interception into the data received by Bob is $(d-1)/d$. The situation is similar to the generalizations of the BB84 protocol to higher-dimensional states [11–13], in which the larger the number of states, the larger is the QBER, which in turn may be larger than any noise already present in the channel. This later fact seems to be an advantage in terms of the security of the key distribution scheme [25]. These results are based only on the analysis of a direct individual attack by Eve. It may be interesting to study further types of attacks and to establish theoretical bounds to the information gain and the QBER in this protocol or go through a general analysis along the lines that have been followed for the BB84 protocol in Refs. [25–27] and to see if this protocol has an unconditional security or not.

Another route for extending our results is to consider the continuous variables. There has been a lot of interest toward quantum computation and quantum communication with continuous variables in the past couple of years (see [28,29] and references therein), where instead of bits, information may be stored in infinite-dimensional states such as position or momentum of a particle or amplitude of an electromagnetic field. Part of this interest derives from the fact that it has been shown that a combination of optical devices such as phase shifters and beam splitters may be sufficient to act as a set of universal gates. Therefore many algorithms and protocols have been restudied for continuous variables [29]. Now that we have a QKD protocol for $d$-level states for any $d$, a natural question arises whether it is possible to go to a proper continuous limit and define the above process for continuous variables. We can simply replace the discrete states $|j\rangle$ with continuous variables $|x\rangle, -\infty < x < \infty$ and $\zeta = e^{2\pi i/d}$ with $\zeta = e^{2\pi i}$ in all the formulas for states and operators to adapt the protocol to the continuous variables. In all stages we need to also change summations to integrations,

$$\frac{1}{\sqrt{d}}\sum_{0}^{d-1}\rightarrow\frac{1}{\sqrt{2\pi}}\int_{-\infty}^{+\infty}dx. \tag{31}$$

Following these we will find the generalized Bell states in the continuous case

$$|\Psi_{\alpha,\beta}\rangle=\frac{1}{\sqrt{2\pi}}\int e^{i\beta x}|x,x+\alpha\rangle dx, \tag{32}$$

where $\alpha$ and $\beta$ are continuous labels ranging from $-\infty$ to $+\infty$ and $|x\rangle$ is a continuous state such as position and all the integrals now and hereafter are over the real line. These states are normalized in the sense that

$$\langle\Psi_{\alpha,\beta}|\Psi_{\alpha',\beta'}\rangle=\delta(\alpha-\alpha')\,\delta(\beta-\beta') \tag{33}$$

and are maximally entangled in the sense that

$$\mathrm{tr}_2(|\Psi_{\alpha,\beta}\rangle\langle\Psi_{\alpha,\beta}|)=\frac{1}{2\pi}\int_{-\infty}^{+\infty}|x\rangle\langle x|dx.$$

The generalization of the Hadamard operator is nothing but the Fourier transform operator that has already been used in Ref. [29] to generalize the Grover algorithm [30] to continuous domain,

$$H|x\rangle=\frac{1}{\sqrt{2\pi}}\int e^{ixy}|y\rangle dy. \tag{34}$$

The controlled-right shift operator now takes the form

$$R_c|x,y\rangle=|x,x+y\rangle, \tag{35}$$

which as an operator takes the particularly simple form

$$R_c=e^{-iX\otimes P}. \tag{36}$$

This operator has also appeared in Ref. [5]. To define the form of the protocol for the continuous variables, it is enough to modify all the states in various stages of the protocol as stated above. It may then be practically more feasible to really implement this protocol by optical means.

## APPENDIX A

In this appendix we show that Eve cannot counteract the action of the Hadamard gates by replacing her controlled-shift gate by any other unitary operator or even by any quantum operation. Therefore, any measurement of her system or the intercepted qudit will reveal nothing to her.

When Eve intercepts the sent qudit, she will have access to the last two parts of the following state:

$$|\Psi_2\rangle=\frac{1}{\sqrt{d}}\sum_{i,j,k=0}^{d-1}H_{i,j}H_{k,j}^{*}|i,k,i+q_2,j+q_1\rangle_{a,b,k,e}. \tag{A1}$$

One can now find the density matrix of Eve and the sent qudit from $\rho_{k,e}=\mathrm{tr}_{a,b}(|\Psi_2\rangle\langle\Psi_2|)$. Using the primed dummy indices such as $i',j'\cdots$ for the bra state $\langle\Psi_2|$, we have

$$\rho_{k,e}=\frac{1}{d}\sum H_{ij}H_{kj}^{*}H_{i'j'}^{*}H_{k'j'}\delta_{ii'}\delta_{kk'}\times|i+q_2,j+q_1\rangle\langle i'+q_2,j'+q_1|. \tag{A2}$$

Summing over $i',k'$ we find

$$\rho_{k,e}=\frac{1}{d}\sum H_{ij}H_{kj}^{*}H_{ij'}^{*}H_{kj'}\times|i+q_2,j+q_1\rangle\langle i+q_2,j'+q_1|. \tag{A3}$$

Summing over $k$ and using the symmetry and unitarity of $H$ ($\Sigma H_{kj}^{*}H_{kj'}=\delta_{jj'}$) and then summing over $j'$, we obtain

$$\rho_{k,e}=\frac{1}{d}\sum H_{ij}H_{ij}^{*}|i+q_2,j+q_1\rangle\langle i+q_2,j+q_1|. \tag{A4}$$

Now we use the definition of $H_{ij}:=(1/\sqrt{d})\zeta^{ij}$, to set $H_{ij}H_{ij}^{*}=1/d$. The last step is done by a relabeling of the indices $i+q_2$ and $j+q_1$ to end with

$$\rho_{k,e}=\frac{1}{d^2}\sum_{l,m}|l,m\rangle\langle l,m|=\frac{1}{d^2}\mathbb{1}_k\otimes\mathbb{1}_e. \tag{A5}$$

## APPENDIX B

In this appendix we investigate the consequences of replacing the Hadamard gates with an arbitrary unitary gate $U$. As stated in the text, the Bell state $|\Psi_{0,0}\rangle$ is invariant under the action of $U\otimes U^{*}$ for any unitary operator. Suppose that Alice or Bob use an operator $U$ instead of $H$, either deliberately or by unwanted errors in their gates. To find the information gain of Eve, we need to calculate as in Appendix A, the density matrix $\rho_{k,e}=\mathrm{tr}_{a,b}(|\Xi_2\rangle\langle\Xi_2|)$, where $|\Xi_2\rangle$ is

$$|\Xi_2\rangle=\frac{1}{\sqrt{d}}\sum_{i,j,k=0}^{d-1}U_{i,j}U_{k,j}^{*}|i,k,i+q_2,j+q_1\rangle_{a,b,q,e}. \tag{B1}$$

The calculations are similar to Appendix A, and the final result is

$$\rho_{k,e}=\frac{1}{d}\sum_{i,j=0}^{d-1}|U_{i,j}|^2|i+q_2,j+q_1\rangle_{k,e}\langle i+q_2,j+q_1|. \tag{B2}$$

Thus if the operator $U$ shares only the property with the Hadamard gate that $|U_{i,j}|^2=1/d$, then again we will have $\rho_{k,e}=1/d^2\mathbb{1}_k\otimes\mathbb{1}_e$ and the information gain of Eve reduces to zero. In this sense the protocol is somehow robust against a large number of errors in the Hadamard gates.

Second, we can repeat the calculation that leads to the final density matrix of the key dits in the hands of Bob, Eq. (30), to determine the new QBER. This time we have

$$|\Xi_4\rangle = \sum_{i,k=0}^{d-1} U_{i,i+q_2-q_1+q} U^*_{k,i+q_2-q_1+q} \times |i,k,i+q_2-k,i+q+q_2\rangle. \quad \text{(B3)}$$

It is again a simple computation to find the density matrix corresponding to the key space from this state:

$$\rho_k := \mathrm{tr}_{a,b,e} |\Xi_4\rangle\langle\Xi_4| = \frac{1}{d} \sum_{i,k} |U_{i,i+q_2-q_1+q}|^2 |U_{k,i+q_2-q_1+q}|^2 \times |i+q_2-k\rangle_k\langle i+q_2-k|.$$

Again, if for $|U_{i,j}|^2 = 1/d$, we will obtain a completely mixed matrix $(1/d)\mathbb{1}_k$, and the same QBER as with the Hadamard gates.


[1] M. A. Nielson and I. L. Chuang, *Quantum Computation and Information* (Cambridge University Press, Cambridge, UK, 2000).
[2] J. Preskill, *Quantum Information and Computation*, available from www.caltech.edu
[3] A. Steane, Rep. Prog. Phys. **64**, 117 (1998).
[4] D. Gottesman, e-print quant-ph/9802007.
[5] G. Alber, D. Delgado, N. Gisin, and I. Jex, e-print quant-ph/0008022.
[6] G. Alber, D. Delgado, N. Gisin, and I. Jex, e-print quant-ph/0102035.
[7] G. Alber, D. Delgado, and I. Jex, e-print quant-ph/0006040.
[8] S.D. Bartlett, H. de Guise, and B.C. Sanders, e-print quant-ph/0109066.
[9] E. Knill, e-print quant-ph/9608048.
[10] H.F. Chau, e-print quant-ph/9610023.
[11] H. Bechmann-Pasquinucci and W. Tittel, Phys. Rev. A **61**, 062308 (2000).
[12] H. Bechmann-Pasquinucci and A. Peres, Phys. Rev. Lett. **85**, 3313 (2000).
[13] N. Cerf, M. Bourennane, A. Karlsson, and N. Gisin, e-print quant-ph/0107130.
[14] N.D. Mermin, e-print quant-ph/0105117.
[15] V. Karimipour, S. Bagherinezhad, and A. Bahraminasab, Phys. Rev. A. (to be published), quant-ph/0112050.
[16] C. H. Bennet and G. Brassard, in *IEEE International Conference on Computers, Systems, and Signal Processing, Banglore, India, 1984* (IEEE, New York, 1984), p. 175.
[17] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, e-print quant-ph/0101098.
[18] A.K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[19] C.H. Bennet, G. Brassard, and A.K. Ekert, Sci. Am. (Int. Ed) **267**, 26 (1992).
[20] A. Cabello, Phys. Rev. A **61**, 052312 (2000).
[21] Y.S. Zhang, C.F. Li, and G.C. Guo, Phys. Rev. A **64**, 024302 (2001).
[22] N.J. Cerf, Phys. Rev. Lett. **84**, 4497 (2000).
[23] N.J. Cerf, J. Mod. Opt. **47**, 187 (2000).
[24] N.J. Cerf, Acta Phys. Slov. **48**, 115 (1998).
[25] D. Gottesman and H.-K. Lo, e-print quant-ph/0105121.
[26] H.-K. Lo, e-print quant-ph/0102138.
[27] H.-K. Lo, H.F. Chau, and M. Ardehali, e-print quant-ph/0011056.
[28] S.L. Braunstein, Phys. Rev. Lett. **80**, 4084 (1998).
[29] A.K. Pati, S.L. Braunstein, and S. Loyd, e-print quant-ph/0002082.
[30] L.K. Grover, Phys. Rev. Lett. **79**, 325 (1997).