Optimal encryption of quantum bits

P. Oscar Boykin* and Vwani Roychowdhury†
Electrical Engineering Department, UCLA, Los Angeles, California 90095
(Received 19 September 2002; revised manuscript received 28 January 2003; published 22 April 2003)

We show that $2n$ random classical bits are both necessary and sufficient for encrypting any unknown state of n quantum bits in an informationally secure manner. We also characterize the complete set of optimal protocols in terms of a set of unitary operations that comprise an *orthonormal basis* in a canonical inner product space. Moreover, a connection is made between quantum encryption and quantum teleportation that allows for a different proof of optimality of teleportation.

DOI: 10.1103/PhysRevA.67.042317 PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

A natural generalization of the encryption process for classical information in the context of quantum data can be described as follows. Alice has a quantum state comprising n qubits that she intends either to send to Bob, or to store in a quantum memory for later use. Eve may intercept the state during transmission or may access the quantum memory. Alice wants to make sure that *even if* Eve receives the entire state, she learns nothing. Toward this end, Alice performs one of many possible operations on her quantum data, and keeps the identity of the chosen operation secret from Eve. Without loss of generality, we assume the set of all possible operations that Alice can choose from is known to everyone, including Eve. The index of the exact operation performed by Alice on her quantum data is the *key*, which is used later by Alice or by Bob (in which case, Alice and Bob must have shared the key at some point) to undo Alice's operation and retrieve the original data. Note that the set of operations that Alice can perform must be reversible and, hence, unitary [1]. Thus, a quantum encryption scheme consists of such a set of unitary operations, and a protocol for generating the key.

At this point, it is useful to provide a more formal description of the encryption framework and then introduce the concepts of security and optimality. For an n-qubit system, the most general scheme is to have a set of M operations $\{U_k\}$, $k=1,\ldots,M$, where each element U_k is a $2^n\times 2^n$ unitary matrix. The key k is chosen with some probability p_k, and the input quantum state is encrypted by applying the corresponding unitary operation U_k. In the decryption stage, $U_k^\dagger$ is applied to the quantum state to retrieve the original state. The input state ρ is called the message state, and the output state ρ_c is called the cipher state. Now, the protocol is informationally secure if for every input state ρ, the output state ρ_c is the totally mixed state:

$$\rho_c=\sum_k p_k U_k \rho U_k^\dagger=\frac{1}{2^n}I. \tag{1}$$

The reason that ρ_c must be the totally mixed state is twofold. First, for security, all inputs must be mapped to the same output density matrix (because ρ_c must be independent of the input). Second, since the encryption operations are unitary, the totally mixed state is clearly mapped to itself, and hence, $\rho_c=(1/2^n)I$. It is easy to verify now that the above scheme is informationally secure. Eve could prepare an n qubit, totally mixed state on her own. Since two processes that output the same density matrices are indistinguishable [2], anything that can be learned from ρ_c can also be learned from the totally mixed state that she prepares herself. Hence, the design criterion for quantum encryption is to find such a distribution of unitary operations $\{p_k,U_k\}$ that will map all inputs to the totally mixed state.

The issues we address in the rest of this paper include the following.

(1) Design of encryption algorithms: What is a natural choice of the encryption set $\{p_k,U_k\}$? In Sec. II, we provide a generalization of the classical one time pad, and describe a quantum one time pad that uses $2n$ random classical bits and applies bit-wise Pauli rotations to encrypt any n-qubit state.

(2) Optimality: To encrypt a quantum state comprising n qubits, how many classical bits would one need to store the key?

(3) Characterization of the set of optimal encryption protocols: Is there a succinct description of the set of all possible optimal (i.e., using the least number of bits for the key) encryption schemes that Alice can use? In Sec. III, we answer both these questions; and we show that $2n$ random classical bits are necessary, and that a set $\{p_k,U_k\}$, $k=1,\ldots,2^{2n}$ is an encryption set if and only if the set $\{U_k\}$ forms an orthonormal basis in a canonical inner product space.

The concept of quantum encryption, as discussed in this paper, was first introduced in a Los Alamos archive paper [3]. As pointed out in Sec. IV of this paper, previous quantum communication protocols, such as teleportation [4] and superdense coding [5], are closely related to the concept of quantum encryption, and in that sense the basic idea of quantum encryption has been around for a while. In fact, we show in Sec. IV that the standard teleportation protocol based on bell-basis measurements is equivalent to the quantum one time pad procedure, derived in Sec. II. A few other results on quantum encryption have also been reported. Ambainis *et al.* [6] show that the bound on the size of the classical key also

*Electronic address: boykin@ee.ucla.edu
†Electronic address: vwani@ee.ucla.edu

applies in the case where the encryption process involves some ancillary qubits. Additionally, many of the connections between the quantum one-time pad, and teleportation and superdense coding (discussed in Sec. IV) have been further examined in Ref. [7]. Since any reversible encoding of quantum data has to involve unitary operations, it is natural that the unitary encoding and decoding sets, introduced here, would be an integral part of any cryptographic protocol, and indeed, [8,9] use them for their quantum authentication protocols.

II. A QUANTUM ONE-TIME PAD

For classical information, Shannon defined informationally secure cryptography [10], using the mutual information between two variables, $I(M;C)$, in the following way:

$$I(M;C)=H(C)-H(C|M)=0, \tag{2}$$

where M is the random variable for the message, C is the random variable for the cipher text (i.e., output of the encryption process), and $H(X)$ is the entropy of the random variable X given by $\Sigma_x p(X=x)\log_2(1/p(X=x))$. The above relationship implies $p(c|m)=p(c)$, i.e., the cipher-text c is independent of the message m. Since one must be able to recover the message from the cipher text given the key, one must also satisfy $I(M;C|K)=H(M)$. Hence, the secrecy condition combined with the recoverability condition implies that $H(K)\geqslant H(M)$ and $H(C)\geqslant H(M)$ for informationally secure cryptography. An example of informationally secure cryptography is the one-time pad [11]. The message m is compressed to its entropy, and then for each bit of the compressed message, a random key bit is generated. Thus the complete key k is a full-entropy random string of length $H(M)$. Then, the cipher text is $c=m\oplus k$; i.e., whenever a bit is 1 in the key, then a σ_x operation is applied to the corresponding message bit. Given c, one knows nothing of m; but given c and k, one has m exactly.

This same one-time pad approach may be applied in the quantum case. For each qubit, two random key bits are generated, instead of a single bit as in the classical one-time pad case. For secret-key quantum encryption, we assume that these bits are shared between Alice and Bob in advance. If the first bit is 0, then Alice does nothing, else she applies σ_z to the qubit. If the second bit is 0, she does nothing, else she applies σ_x. She continues this protocol for the rest of the bits.

We now show that this quantum one-time pad protocol is secure. First, note that the bit-wise protocol can be expressed in terms of our general quantum encryption setup by choosing $p_k=1/2^{2n}$ and $U_k=X^\alpha Z^\beta$ $(\alpha,\beta\in\{0,1\}^n)$, where $X^\alpha=\otimes_{i=1}^n\sigma_x^{\alpha(i)}$ and $Z^\beta=\otimes_{i=1}^n\sigma_z^{\beta(i)}$. Thus X^α corresponds to applying σ_x to the bits in positions given by the n-bit string α, and similarly for Z^β. Next, define the inner product of two matrices M_1 and M_2 as $\mathrm{Tr}(M_1M_2^\dagger)$. If the set of all $2^n\times 2^n$ matrices is seen as an inner product space (with respect to the preceding inner product), then one can easily verify that the set of 2^{2n} unitary matrices $\{X^\alpha Z^\beta\}$ forms an orthonormal basis. Expanding any message state ρ, in this $X^\alpha Z^\beta$ basis, gives:

$$\rho=\sum_{\alpha,\beta} a_{\alpha,\beta}X^\alpha Z^\beta, \tag{3}$$

where $a_{\alpha,\beta}=\mathrm{Tr}(\rho Z^\beta X^\alpha)/2^n$. Using this formalism, it is clear that the given choice of p_k and U_k satisfies Eq. (1), and hence, the underlying protocol is secure:

$$\begin{aligned}\sum_k p_k U_k\rho U_k^\dagger &= \frac{1}{2^{2n}}\sum_{\gamma,\delta} X^\gamma Z^\delta \rho Z^\delta X^\gamma \\ &= \frac{1}{2^{2n}}\sum_{\alpha,\beta} a_{\alpha,\beta}\sum_{\gamma,\delta} X^\gamma Z^\delta X^\alpha Z^\beta Z^\delta X^\gamma \\ &= \frac{1}{2^{2n}}\sum_{\alpha,\beta} a_{\alpha,\beta}\sum_{\gamma,\delta} (-1)^{\alpha\delta\oplus\gamma\beta} X^\alpha Z^\beta \\ &= \sum_{\alpha,\beta} a_{\alpha,\beta}\delta_{\alpha,0}\delta_{\beta,0}X^\alpha Z^\beta \\ &= a_{0,0}I=\frac{\mathrm{Tr}(\rho)}{2^n}I=\frac{1}{2^n}I.\end{aligned} \tag{4}$$

III. CHARACTERIZATION AND OPTIMALITY OF QUANTUM ONE-TIME PADS

So far, we have provided one quantum encryption protocol based on bit-wise Pauli rotations, which uses $2n$ random classical bits in order to encrypt n quantum bits. Now we explore other choices of $\{p_k,U_k\}$, and also investigate if the simple quantum one-time pad protocol is optimal. That is, can one encrypt n-bit quantum states using less than $2n$ random secret classical bits?

Since there are a continuum of valid density matrices (i.e., message states), the quantum security criterion (1) can be unwieldy to deal with. Hence, we first introduce a modified condition that is necessary and sufficient for security. An encryption set $\{p_k,U_k\}$ satisfies Eq. (1) if and only if it satisfies the following:

$$\sum_{k=1}^{M} p_k U_k X^\alpha Z^\beta U_k^\dagger=\delta_{\alpha,0}\delta_{\beta,0}I. \tag{5}$$

The equivalence of this to Eq. (1) is shown in the Appendix. Thus, the condition for security becomes discrete, and only 2^{2n} equations need to be satisfied by the set $\{p_k,U_k\}$ in order for the set to be a valid encryption set.

First, we show a sufficient condition for $\{p_k,U_k\}$ to act as a quantum encryption protocol. Particularly, we show that *any unitary orthonormal basis* for the $2^n\times 2^n$ matrices *uniformly applied encrypts n quantum bits*. We can always write the matrices U_k in terms of the $X^\alpha Z^\beta$ basis as

$$U_k = \sum_{\alpha,\beta} C^k_{\alpha,\beta} X^\alpha Z^\beta. \tag{6}$$

Since these U_k's form an orthonormal basis; the $2^{2n}\times 2^{2n}$ transformation matrix C, comprising of the transformation coefficients, is a unitary matrix. Hence, the rows and columns of C are orthonormal:

$$\sum_{k=1}^{M} C^k_{\alpha,\beta}(C^k_{\gamma,\delta})^* = \delta_{\alpha,\gamma}\delta_{\beta,\delta}$$

and

$$\sum_{\alpha,\beta} C^k_{\alpha,\beta}(C^l_{\alpha,\beta})^* = \delta_{k,l}. \tag{7}$$

By substituting U_k in Eq. (1), we obtain the following desired result:

$$\begin{aligned}\frac{1}{2^{2n}}\sum_k U_k \rho U_k^\dagger &= \frac{1}{2^{2n}}\sum_{\alpha,\beta}\sum_{\gamma,\delta}\left(\sum_k C^k_{\alpha,\beta}C^k_{\gamma,\delta}{}^*\right) X^\alpha Z^\beta \rho Z^\delta X^\gamma \\ &= \frac{1}{2^{2n}}\sum_{\alpha,\beta}\sum_{\gamma,\delta}\delta_{\alpha,\gamma}\delta_{\beta,\delta} X^\alpha Z^\beta \rho Z^\delta X^\gamma \\ &= \frac{1}{2^{2n}}\sum_{\alpha,\beta} X^\alpha Z^\beta \rho Z^\beta X^\alpha \\ &= \frac{1}{2^n} I.\end{aligned}$$

Since any unitary orthonormal basis will encrypt, then using $2n$ bits is the most one needs to use.

We next show that one must use at least $2n$ bits, and in the process derive a succinct characterization of all optimal quantum encryption protocols. As a first step, we prove the following result: Given any quantum encryption set $\{p_k, U_k\}$, $k=1,\ldots,M$ [i.e., $\Sigma_k p_k = 1$, U_k is unitary, and Eqs. (1) and (5) are satisfied], let $\tilde{U}_k = \sqrt{p_k}U_k = \Sigma_{\alpha,\beta}\tilde{C}^k_{\alpha,\beta}X^\alpha Z^\beta$ and let $\tilde{C}$ be the $M\times 2^{2n}$ transformation matrix, comprising of the transformation coefficients $\tilde{C}^k_{\alpha,\beta}$. Then $M \geqslant 2^{2n}$, and

$$\tilde{C}^\dagger\tilde{C} = \frac{1}{2^{2n}} I_{2^{2n}\times 2^{2n}}.$$

In order to provide a proof for the above claim, we introduce the following shorthand notation:

$$\Psi_{\alpha,\beta,\gamma,\delta} = \sum_{k=1}^{M} \tilde{C}^k_{\alpha,\beta}(\tilde{C}^k_{\gamma,\delta})^*,$$

which is the standard inner product of the (α,β)th and the (γ,δ)th columns of $\tilde{C}$ or $(\tilde{C}^\dagger\tilde{C})_{(\alpha,\beta),(\gamma,\delta)}$. Note $\{p_k, U_k\}$ satisfies Eqs. (1) and (5). Hence, for every $\ell, m \in \{0,1\}^n$,

$$\begin{aligned}\delta_{\ell,0}\delta_{m,0} I &= \sum_{k=1}^{M} p_k U_k X^\ell Z^m U_k^\dagger \\ &= \sum_{k=1}^{M} \tilde{U}_k X^\ell Z^m \tilde{U}_k^\dagger \\ &= \sum_{k=1}^{M}\sum_{\alpha,\beta}\sum_{\gamma,\delta} \tilde{C}^k_{\alpha,\beta}(\tilde{C}^k_{\gamma,\delta})^* X^\alpha Z^\beta X^\ell Z^m Z^\delta X^\gamma \\ &= \sum_{\alpha,\beta}\sum_{\gamma,\delta} (-1)^{\beta\ell+\gamma(\beta+\delta+m)}\Psi_{\alpha,\beta,\gamma,\delta} \\ &\quad \times X^{\alpha+\gamma+\ell} Z^{\beta+\delta+m} \\ &= \sum_{p,q} (-1)^{(p+\ell)q} A_{l,m,p,q} X^p Z^q,\end{aligned}$$

where we have defined

$$A_{l,m,p,q} \equiv \sum_{\alpha,\beta,\gamma,\delta} \delta_{\gamma,\alpha+p+\ell}\delta_{\delta,\beta+q+m}(-1)^{\beta\ell+\alpha q}\Psi_{\alpha,\beta,\gamma,\delta}.$$

Using the linear independence of the X^pZ^q, only the identity component is nonzero: $A_{l,m,p,q} = \delta_{\ell,0}\delta_{m,0}\delta_{p,0}\delta_{q,0}$. Hence, security implies

$$\begin{aligned}&\delta_{\ell,0}\delta_{m,0}\delta_{p,0}\delta_{q,0} \\ &\quad = \sum_{\alpha,\beta,\gamma,\delta} (-1)^{\beta\ell+\alpha q}\delta_{\gamma,\alpha+p+\ell}\delta_{\delta,\beta+q+m}\Psi_{\alpha,\beta,\gamma,\delta}.\end{aligned} \tag{8}$$

The above equation will be used to introduce a linear algebra formulation of the problem. Let

$$\mathbf{M}_{(\ell,m,p,q),(\alpha,\beta,\gamma,\delta)} = (-1)^{\beta\ell+\alpha q}\delta_{\gamma,\alpha+p+\ell}\delta_{\delta,\beta+q+m}.$$

Equation (8) can now be written as a set of 2^{4n} linear equations: $\mathbf{M}\boldsymbol{\Psi} = [1,0,\ldots,0]^T$, where $\boldsymbol{\Psi}$ is the $2^{4n}\times 1$ vector consisting of all the possible inner products of pairs of columns of $\tilde{C}$ and $\mathbf{M}$ is a $2^{4n}\times 2^{4n}$ matrix with elements from the set $1,0,-1$. Next, we observe that a matrix $\mathbf{A}$ is orthogonal if and only if $\Sigma_j A_{i,j}A_{i',j} = A_i^2\delta_{i,i'}$, where A_i is the norm of the ith row (which must be greater than zero). One can easily verify that $\mathbf{M}$ is an orthogonal matrix. In showing that $\mathbf{M}$ is orthogonal, one finds the inverse of $\mathbf{M}$. The orthonormality of $\mathbf{M}$ means that $\mathbf{M}\mathbf{M}^T = 2^{2n}I$, and hence, $\mathbf{M}^{-1} = \mathbf{M}^T/2^{2n}$. Therefore, $\boldsymbol{\Psi} = \mathbf{M}^T[1,0,\ldots,0]^T/2^{2n}$, which means $\boldsymbol{\Psi}$ is the first row of $\mathbf{M}$ renormalized:

$$\Psi_{\alpha,\beta,\gamma,\delta} = \frac{\mathbf{M}_{(0,0,0,0)(\alpha,\beta,\gamma,\delta)}}{2^{2n}} = \frac{1}{2^{2n}}\delta_{\alpha,\gamma}\delta_{\beta,\delta}.$$

Since $(\tilde{C}^\dagger\tilde{C})_{(\alpha,\beta),(\gamma,\delta)} = \Psi_{\alpha,\beta,\gamma,\delta}$, we have

$$\tilde{C}^\dagger \tilde{C} = \frac{1}{2^{2n}} I_{2^{2n}\times 2^{2n}}. \tag{9}$$

Since $I_{2^{2n}\times 2^{2n}}$ is a full rank matrix, then $\tilde{C}$ must have at least as many rows as columns. Since $\tilde{C}$ has 2^{2n} columns, it implies that $M \geqslant 2^{2n}$.

We are now ready to prove that *one must use at least* $2n$ *random classical bits* for any quantum encryption, and that a set $\{p_k, U_k\}$ involving only $2n$ secret classical bits *is a quantum encryption set if and only if the unitary matrix elements form an orthonormal basis, and they are all equally likely*. That is, we make the following claim: Any given quantum encryption set $\{p_k, U_k\}$, $k=1,\ldots,M$, satisfies

$$H(p_1,\ldots,p_M) = \sum_{i=1}^{M} p_i \log_2 \frac{1}{p_i} \geqslant 2n. \tag{10}$$

Moreover, if $M=2^{2n}$, then $p_k = 1/2^{2n}$ and U_k's form an orthonormal basis.

We now provide a proof for Eq. (10) and the above claim. We have already shown that

$$\tilde{C}^\dagger \tilde{C} = \frac{1}{2^{2n}} I_{2^{2n}\times 2^{2n}}.$$

Using a singular value decomposition [12] of $\tilde{C}$, we have the following relationships:

$$\tilde{C} = W \Lambda V^\dagger,$$

$$\tilde{C}^\dagger \tilde{C} = V(\Lambda^\dagger \Lambda) V^\dagger,$$

$$\tilde{C}\tilde{C}^\dagger = W(\Lambda \Lambda^\dagger) W^\dagger,$$

where W and V are $M\times M$ and $2^{2n}\times 2^{2n}$ unitary matrices, respectively, and Λ is an $M\times 2^{2n}$ diagonal rectangular matrix: $\Lambda(i,j) = \lambda_i \delta_{i,j}$. Note that $\Lambda^\dagger\Lambda$ and $\Lambda\Lambda^\dagger$ are real diagonal matrices and have the same nonzero elements; hence, $\tilde{C}^\dagger\tilde{C}$ and $\tilde{C}\tilde{C}^\dagger$ have the *same* nonzero eigenvalues. Since $\tilde{C}^\dagger\tilde{C}$ has 2^{2n} repeated eigenvalues $(=1/2^{2n})$ and $M \geqslant 2^{2n}$, $\tilde{C}\tilde{C}^\dagger$ has 2^{2n} repeated eigenvalues $(=1/2^{2n})$ and the rest of its $M-2^{2n}$ eigenvalues are 0. Also note that the diagonal entries of $\tilde{C}\tilde{C}^\dagger$ are the probabilities p_k's and, hence,

$$p_k = \frac{\mathrm{Tr}(\tilde{U}_k \tilde{U}_k{}^\dagger)}{2^n} = (\tilde{C}\tilde{C}^\dagger)_{k,k} = \frac{1}{2^{2n}} \sum_{i=1}^{2^{2n}} |W_{i,k}|^2 \leqslant \frac{1}{2^{2n}}.$$

The above uses the facts that, since W is unitary, $\Sigma_{i=1}^{M} |W_{i,k}|^2 = 1$ and that $M \geqslant 2^{2n}$. Hence,

$$H(p_1,\ldots,p_M) = \sum_{i=1}^{M} p_i \log_2 \frac{1}{p_i} \geqslant 2n \sum_{i=1}^{M} p_i = 2n.$$

If we use exactly $2n$ unitary matrices to form $\{U_k\}$ and $2n$ classical bits for the key, we have $M=2^{2n}$ and $\tilde{C}\tilde{C}^\dagger = \tilde{C}^\dagger\tilde{C} = (1/2^{2n}) I_{2^{2n}\times 2^{2n}}$. Hence

$$\frac{\mathrm{Tr}(\tilde{U}_k \tilde{U}_j{}^\dagger)}{2^n} = \delta_{k,j} \frac{1}{2^{2n}},$$

which gives $p_k = 1/2^{2n}$, and the set $\{U_k\}$ necessarily forms an orthonormal basis. So we have our main results: *one must use at least* $2n$ *classical bits, and* $\{p_k, U_k\}$ *is an optimal encryption set, if and only if all the* p_k*'s are equal and the set* $\{U_k\}$ *forms an orthonormal basis.*

IV. DISCUSSIONS

We have presented a quantum one-time pad protocol that uses $2n$ secret classical bits and bit-wise Pauli rotations to secure n quantum bits. We have also shown that $2n$ random classical bits are necessary. Furthermore, we have generalized the notion of the quantum one-time pad protocol, and shown that any orthonormal set of 2^{2n} unitary matrices can be used to securely encrypt n-qubit quantum states. More interestingly, perhaps, we have shown that all optimal quantum encryption protocols (i.e., using $2n$ random classical bits for key generation) must use a uniform distribution of 2^{2n} orthonormal unitary operations.

We next show, how quantum encryption sets are related to two fundamental quantum information tasks: teleportation [4] and superdense coding [5]. A general teleportation scheme can be described as follows: Alice and Bob share a pure state ρ_{AB}, comprising $2n$ qubits such that the traced out n-bit states of Alice and Bob satisfy: $\rho_A = \rho_B = (1/2^n) I$. Next, Alice receives an unknown n-bit quantum state ρ, and performs a joint measurement (i.e., on ρ and ρ_A), which produces one of a fixed set of outcomes m_k, $k=1,\ldots,M$, each with probability p_k. The particular outcome m_k is classically communicated to Bob using $H(p_1,\ldots,p_M)$ bits. Bob performs a corresponding unitary operation U_k on his state to retrieve ρ. Hence, after Alice's measurement (and before Bob learns the outcome), Bob's state can be expressed as $\rho_B = (1/2^n) I = \Sigma_{k=1}^{M} p_k U_k \rho U_k^\dagger$, which is exactly the encrypted state of the message ρ defined in Eq. (1). Hence, *every teleportation scheme corresponds to an encryption set* $\{p_k, U_k\}$. Since we prove that all quantum encryption sets require $2n$ classical bits, then all teleportation schemes must also require $2n$ classical bits. Note that our proof only relies on the properties of the underlying vector spaces. In the original teleportation paper [4], a proof that two classical bits are required to teleport is given. The proof is based on a construction that gives superluminal communication if teleportation can be done with less than two bits. This proof, however, does not imply that all quantum encryption sets require $2n$ bits. To do so, one would require to prove that all quantum encryption sets correspond to a teleportation protocol. On the other hand, as we showed above, all teleportation protocols correspond to a quantum encryption set; hence, *our result provides a different proof of optimality of teleportation.*

Superdense coding also has a connection to quantum encryption. Consider the case where Alice asks Bob to encrypt something, and then Alice wishes to learn the key that Bob used for encryption. In the case of the classical one-time pad

[11] $c=m\oplus k$, and so, given a message and its accompanying cipher text, one learns the key: $k=m\oplus c$. Quantumly, each quantum bit has two classical key bits to learn. Due to Holevo's theorem [13], it may seem that this implies that there is no way to learn the classical key exactly. This intuition is not correct. Alice can learn Bob's key in the following way. Alice prepares n singlets and gives half of each singlet to Bob. Bob encrypts them using the simple quantum one-time pad, and returns them to Alice. Alice can learn the key exactly by measuring each former singlet in the bell basis. The outcome would tell Alice exactly which transformation Bob applied. This protocol corresponds exactly to the superdense coding scheme [5].

We conclude our discussions by pointing out potential applications of the quantum encryption scheme described here. For example, classical one-time pads are almost never used: Instead of keeping an n-bit message secret, one must keep an n-bit key secret. In most cases, there will be no advantage. With the quantum one-time pad, the situation is different. Instead of keeping n quantum bits secure, one must keep $2n$ classical bits secure. Classical bits have different properties than quantum bits, so there may be situations where this will be of great value. Moreover, encrypting quantum data using classical random bits may allow for straightforward generalizations of many classical protocols to quantum data. For instance, rather than using random classical data of size $2n$, one could use secret key ciphers [14] or stream ciphers [14] to keep a small finite classical key, for instance 256 bits, to generate pseudorandom bits to encrypt quantum data. The ability to secure quantum bits with classical keys may expand the scope of previous work [15], which allows users with only classical resources to use quantum protocols via a quantum center that stores quantum data.

ACKNOWLEDGMENTS

We would like to thank Tal Mor for helpful discussions. This work was supported in part by the Defense Advanced Research Projects Agency (DARPA) under Project No. MDA 972-99-1-0017, in part by the U.S. Army Research Office/ DARPA under Contract No. DAAD 19-00-1-0172, and in part by the NSF under Contract No. EIA-0113440.

APPENDIX

We provide a proof of the following claim (see Sec. III): an encryption set $\{p_k, U_k\}$ satisfies Eq. (1) if and only if it satisfies the following:

$$\sum_{k=1}^{M} p(k) U_k X^\alpha Z^\beta U_k^\dagger = \delta_{\alpha,0}\delta_{\beta,0} I. \tag{A1}$$

To show that the above condition is sufficient, express ρ in the $X^\alpha Z^\beta$ basis, as was done in Eq. (4), and apply Eq. (5)

$$\begin{aligned}\sum_{k=1}^{M} p(k) U_k \rho U_k^\dagger &= \sum_{k=1}^{M} p(k) U_k \left(\sum_{\alpha,\beta} a_{\alpha,\beta} X^\alpha Z^\beta \right) U_k^\dagger \\ &= \sum_{\alpha,\beta} a_{\alpha,\beta} \sum_{k=1}^{M} p(k) U_k X^\alpha Z^\beta U_k^\dagger \\ &= \sum_{\alpha,\beta} a_{\alpha,\beta} \delta_{\alpha,0}\delta_{\beta,0} I \\ &= a_{0,0} I = \frac{\mathrm{Tr}(\rho)}{2^n} I = \frac{1}{2^n} I.\end{aligned}$$

To show that the modified condition, Eq. (5), is necessary, is somewhat more involved. First, let us introduce some new notations

$$\rho_i = \frac{I+\sigma_i}{2} \quad \text{and} \quad \rho_{mix} = \frac{I}{2}.$$

The proof may be obtained by induction. Suppose all X^α with $|\alpha| \leqslant k$ are mapped to zero by the encryption process. Now consider the following product state of $n-k-1$ mixed states, with exactly $k+1$ pure states ρ_x:

$$\rho = \rho_{mix} \otimes \rho_{mix} \otimes, \ldots, \otimes \rho_{mix} \otimes \rho_x \otimes \rho_x \otimes, \ldots, \otimes \rho_x .$$

By expanding, the above becomes

$$\rho = \frac{I}{2^n} + \frac{1}{2^n} \sum_{\alpha=1}^{2^k-1} X^\alpha + \frac{1}{2^n} X^{2^{k+1}-1}.$$

In the above, we use decimal numbers where before we defined X^α with α in binary; hence $X^3 = X^{00,\ldots,011}$. When ρ is encrypted, we know that $I/2^n$ is mapped to itself. By assumption, X^α with $|\alpha| \leqslant k$ is mapped to zero; hence, the sum in the expansion of ρ disappears. Since ρ must be mapped to $I/2^n$, then the last term in the above, which is X^α with $|\alpha| = k+1$, must be mapped to zero. By permuting the initial input states, all X^α with $|\alpha| = k+1$ must be mapped to zero. The case where $k=1$, is our base case. By induction, all X^α are mapped to zero.

If x is replaced by z in the above, then all Z^β are also mapped to zero. If x is replaced by y and using the fact that all X^α and Z^β are mapped to zero, one sees that all $X^\alpha Z^\beta$ are mapped to zero, which proves our claim.

[1] See J. Preskill, URL http://www.theory.caltech.edu/ people/ preskill/ph229/
[2] A. Peres, *Quantum Theory: Concepts and Methods* (Kluwer Academik, Dordrecht, 1993).
[3] P.O. Boykin and V. Roychowdhury, e-print quant-ph/0003059.
[4] C.H. Bennett, G. Brassard, C. Crépeau, R. Jozsa, A. Peres, and W.K. Wootters, Phys. Rev. Lett. **70**, 1895 (1993).
[5] C.H. Bennett and S.J. Wiesner, Phys. Rev. Lett. **69**, 2881 (1993).
[6] See, A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf, URL

citeseer.nj.nec.com/ambainis00private.html
[7] D. Leung, Quantum Inf. Comput. **2**, 14 (2002).
[8] H. Barnum, C. Crepeau, D. Gottesman, A. Smith, and A. Tapp, e-print quant-ph/0205128.
[9] E. Perez, M. Curty, D.J. Santos, and P. Garcia-Fernandez, e-print quant-ph/0209061.
[10] C.E. Shannon, Bell Syst. Tech. J. **28**, 656 (1949).
[11] G.S. Vernam, J. Am. Inst. Electr. Eng. **55**, 109 (1926).
[12] G. Golub and C. V. Loan, *Matrix Computations* (Johns Hopkins University Press, Baltimore, 1989).
[13] A.S. Holevo, Probl. Inf. Transm. **9**, 177 (1973).
[14] B. Schneier, *Applied Cryptography Second Edition* (Wiley, New York, 1996).
[15] E. Biham, B. Huttner, and T. Mor, Phys. Rev. A **54**, 2651 (1996).