Realizing probabilistic identification and cloning of quantum states via universal quantum logic gates

Chuan-Wei Zhang, Zi-Yang Wang, Chuan-Feng Li,* and Guang-Can Guo†
Laboratory of Quantum Communication and Quantum Computation and Department of Physics, University of Science and Technology of China, Hefei 230026, People's Republic of China
(Received 18 June 1999; revised manuscript received 7 September 1999; published 16 May 2000)

Probabilistic quantum cloning and identifying machines can be constructed via unitary-reduction processes [Duan and Guo, Phys. Rev. Lett. **80**, 4999 (1998)]. Given the cloning (identifying) probabilities, we derive an explicit representation of the unitary evolution and corresponding Hamiltonian to realize probabilistic cloning (identification). The logic networks are obtained by decomposing the unitary representation into universal quantum logic operations. The robustness of the networks is also discussed. Our method is suitable for a *k*-partite system, such as quantum computer, and may be generalized to general state-dependent cloning and identification.

PACS number(s): 03.67.−a, 03.65.Bz, 89.70.+c

I. INTRODUCTION

Quantum no-cloning theorem [1], which asserts that unknown pure states cannot be reproduced exactly by any physical means, is one of the most astonishing features of quantum mechanics. Wootters and Zurek [1] have shown that the cloning machine violates the quantum superposition principle. Yuen and D'Ariano [2,3] showed that a violation of unitarity makes the cloning of two nonorthogonal states impossible. Barnum *et al.* [4] have extended such results to the case of mixed states and shown that two noncommuting mixed states cannot be broadcast. Furthermore, Koashi and Imoto [5] generalized the standard no-cloning theorem to the entangled states. The similar problem exists in the situation of identifying an arbitrary unknown state [6]. Since perfect quantum cloning and identification are impossible, the inaccurate cloning and identification of quantum states have attracted much attention with the development of quantum information theory [7].

The inaccurate cloning and identification may be divided into two main categories: deterministic and probabilistic. The deterministic quantum cloning machine generates approximate copies and further we get two subcategories: universal and state-dependent. Universal quantum cloning machines, first addressed by Bužek and Hillery [8], act on any unknown quantum state and produce approximate copies equally well. The Bužek-Hillery cloning machine has been optimized and generalized in Refs. [9–13]. Massar and Popescu [14] and Derka *et al.* [15] have also considered the problem of universal states estimation, given M independent realizations. The deterministic state-dependent cloning machine, proposed originally by Hillery and Bužek [16], is designed to generate approximate clones of states belonging to a finite set. Optimal results for two-state cloning have been obtained by Bruß *et al.* [10] and Chelfes and Barnett [17]. Deterministic exact cloning violates the no-cloning theorem, thus faithful cloning must be probabilistic. The probabilistic cloning machine was first considered by Duan and Guo [18,19] using a general unitary-reduction operation with a postselection of the measurement results. They showed that a set of nonorthogonal but linear-independent pure states can be faithfully cloned with optimal success probability. Recently, Chelfes and Barnett [17] presented the idea of hybrid cloning, which interpolates between deterministic and probabilistic cloning of a two-state system. In addition, we [20] have provided general identifying strategies for state-dependent system.

Clearly, it is important to obtain a physical means to carry out this cloning and identification. Quantum networks for universal cloning have been proposed by Bužek *et al.* [21]. Chelfes and Barnett [17] have constructed the cloning machine in a two-state system.

In this paper we provide a method to realize probabilistic identification and cloning for an n-state system. The method is also applicable to general cloning and identification of state-dependent systems. As any unitary evolution can be accomplished via universal quantum logic gates [22,23], the key to realizing probabilistic identification and cloning is to obtain the unitary representation or the Hamiltonian of the evolution in the machines. We derive the explicit unitary representation and the Hamiltonian which are determined by the probabilities of cloning or identification. Furthermore, we obtain the logic networks of probabilistic cloning and identification by decomposing the unitary representation into universal quantum logic operations. The robustness of the networks is also discussed.

The plan of the paper is the following. In Sec. II we derive the unitary representation matrix and Hamiltonian for quantum identification provided with one copy and generalize this method to $M \rightarrow N$ quantum cloning and identification with M initial copies. For the special case of a quantum computer, we should be concerned with the system which includes k partites, each of them being an arbitrary two-state quantum system (qubit). The identification and cloning in such k-partite quantum systems have more prospective applications, which include normal qubits and multipartite entangled states. In Sec. III, we provide the networks of probabilistic cloning and identification of k-partite systems and discuss their stability properties.

*Electronic address: cfli@ustc.edu.cn
†Electronic address: gcguo@ustc.edu.cn

II. UNITARY EVOLUTIONS AND HAMILTONIANS FOR IDENTIFICATION AND CLONE

Any operation in quantum mechanics can be represented by a unitary evolution together with a measurement. Considering the states secretly chosen from the set $S=\{|\psi_i\rangle, i=1,2,\ldots,n\}$ which span an n-dimensional Hilbert space, Duan and Guo [19] have shown that these states can be probabilistically cloned by a general unitary-reduction operation if and only if $|\psi_1\rangle$, $|\psi_2\rangle,\ldots,|\psi_n\rangle$ are linear-independent. By introducing a probe P in an n_P-dimensional Hilbert space, where $n_P \geqslant n+1$, the unitary evolution $\hat{U}$ in the $M\rightarrow N$ probabilistic cloning machine can be written as follows:

$$\hat{U}|\psi_i\rangle^{\otimes M}|\varphi_1\rangle^{\otimes(N-M)}|P_0\rangle=\sqrt{\gamma_i}|\psi_i\rangle^{\otimes N}|P_i\rangle + \sum_j C_{ij}|\alpha_j\rangle|\varphi_1\rangle^{\otimes(N-M)}|P_0\rangle, \tag{2.1}$$

where $|P_0\rangle$ and $|P_i\rangle$ are normalized states of the probe system (not generally orthogonal, but each of $|P_i\rangle$ is orthogonal to $|P_0\rangle$), and $|\psi_i\rangle^{\otimes M}=|\psi_i\rangle_1|\psi_i\rangle_2\cdots|\psi_i\rangle_M$ ($|\psi_i\rangle_k$ is the kth copy of state $|\psi_i\rangle$). The n-dimensional Hilbert spaces spanned by state sets $\{|\psi_i\rangle\}$, $\{|\psi_i\rangle^{\otimes M}\}$, or $\{|\psi_i\rangle^{\otimes N}|P_i\rangle\}$ are denoted by $\mathcal{H}$, $\mathcal{H}^M$, and $\mathcal{H}^N$, respectively, and $\{|\varphi_i\rangle\}$, $\{|\alpha_i\rangle\}$, and $\{|\beta_i\rangle\}$ are the orthogonal bases of each space. The probe P is measured after the evolution. With probability γ_i, the cloning attempt succeeds and the output state is $|\psi_i\rangle^{\otimes N}$ if and only if the measurement result of the probe is $|P_i\rangle$. The $n\times n$ inter-inner products of Eq. (2.1) yield the matrix equation

$$X^{(M)}=\sqrt{\Gamma}X_P^{(N)}\sqrt{\Gamma}+CC^\dagger, \tag{2.2}$$

where the $n\times n$ matrices are $C=[C_{ij}]$, $X^{(M)}=[\langle\psi_i|\psi_j\rangle^M]$, and $X_P^{(N)}=[\langle\psi_i|\psi_j\rangle^N\langle P_i|P_j\rangle]$. The diagonal efficiency matrix Γ is defined as $\Gamma=\mathrm{diag}(\gamma_1,\gamma_2,\ldots,\gamma_n)$. Since $CC^\dagger \geqslant 0$ ($CC^\dagger$ is positive semidefinite), Eq. (2.2) yields

$$X^{(M)}-\sqrt{\Gamma}X_P^{(N)}\sqrt{\Gamma}\geqslant 0. \tag{2.3}$$

This inequality determines the optimal cloning efficiencies. For example, when $n=2$, we get [17]

$$\frac{\gamma_1+\gamma_2}{2}\leqslant\max_{\{|P_i\rangle\}}\frac{1-|\langle\psi_1|\psi_2\rangle|^M}{1-|\langle\psi_1|\psi_2\rangle|^N|\langle P_1|P_2\rangle|}=\frac{1-|\langle\psi_1|\psi_2\rangle|^M}{1-|\langle\psi_1|\psi_2\rangle|^N}. \tag{2.4}$$

In the limit as $N\rightarrow\infty$, the $M\rightarrow N$ probabilistic clone has a close connection with the problem of identification of a set of states. That is, Eq. (2.1) is applicable to describe the probabilistic identification evolution, since $\{|\psi_i\rangle^{\otimes\infty}, i=1,2,\ldots,n\}$ are the orthogonal bases of n -dimension Hilbert space. Inequality (2.3) turns into $X^{(M)}-\Gamma\geqslant 0$, and inequality (2.4) results in $(\gamma_1+\gamma_2)/2\leqslant 1-|\langle\psi_1|\psi_2\rangle|^M$, which is the maximum identification probability when $n=2$, with M initial copies. In fact, there is a trade-off between identification and cloning. When the probe states $|P_i\rangle$ are orthogonal to each other, we can identify and clone the input states simultaneously. When $|P_i\rangle$ are the same for all the to-be-cloned states, we obtain no information about the input states and the probabilities of successful clone approach the maximum. For a normal situation interpolating between the cloning and identification, where states $|P_i\rangle\neq|P_j\rangle$ exist, we can identify them with no-zero probability and get some information about the input, which means the cloning probabilities must decrease.

Now that the existence of probabilistic cloning and identifying machines has been demonstrated, the next step is to determine the representations of the unitary evolution $\hat{U}$ for the cloning and identifying machines with the given probability matrix Γ.

To simplify the deduction, we start with probabilistic identification of one initial copy. A unitary evolution $\hat{U}$ is utilized to identify $|\psi_i\rangle$,

$$\hat{U}|\psi_i\rangle|P_0\rangle=\sqrt{\gamma_i}|\varphi_i\rangle|P_1\rangle+\sum_j C_{ij}|\varphi_j\rangle|P_0\rangle, \tag{2.5}$$

where $|P_0\rangle$ and $|P_1\rangle$ are the orthogonal bases of the probe system. If a postselective measurement of probe P results in $|P_0\rangle$, the identification fails. Otherwise we make a further measurement of the to-be-identified system and if $|\varphi_k\rangle$ is detected, the input state should be identified as $|\psi_k\rangle$. The inter-inner products of Eq. (2.5) yield the matrix equation

$$X=\Gamma+CC^\dagger. \tag{2.6}$$

Denoting matrix $A=[\langle\varphi_i|\psi_j\rangle]_{n\times n}$, we get

$$X=A^\dagger A. \tag{2.7}$$

Obviously A is reversible. Since $|\psi_i\rangle|P_0\rangle=\sum_{m=1}^n|\varphi_m\rangle|P_0\rangle\langle\varphi_m|\psi_i\rangle$, Eq. (2.5) can be rewritten as

$$\begin{aligned}\hat{U}(|\varphi_1\rangle|P_0\rangle,\ldots,|\varphi_n\rangle|P_0\rangle)&=(|\varphi_1\rangle|P_1\rangle,\ldots,|\varphi_n\rangle|P_1\rangle)\sqrt{\Gamma}A^{-1}\\&\quad+(|\varphi_1\rangle|P_0\rangle,\ldots,|\varphi_n\rangle|P_0\rangle)C^\dagger A^{-1}.\end{aligned}$$

On the orthogonal bases $\{|\varphi_i\rangle|P_j\rangle, i=1,2,\ldots,n, j=0,1\}$ in Hilbert space $\mathcal{H}^{AP}=\mathcal{H}\otimes\mathcal{H}^P$, $\hat{U}$ can be represented as

$$U=\begin{pmatrix}C^\dagger A^{-1} & M\\ \sqrt{\Gamma}A^{-1} & N\end{pmatrix}, \tag{2.8}$$

where M,N are $n\times n$ matrices. In Appendix A, we derive the expressions of the four submatrices in Eq. (2.8) and get

$$U=\tilde{V}S\tilde{V}^\dagger, \tag{2.9}$$

where $\tilde{V}=\mathrm{diag}(V,V)$,

$$S=\begin{pmatrix}F & -E\\ E & F\end{pmatrix}$$

with $E=\mathrm{diag}(\sqrt{m_1},\ldots,\sqrt{m_n})$, and $F=\mathrm{diag}(\sqrt{1-m_1},\ldots,\sqrt{1-m_n})$. V and m_i are determined by

$$I_n - C^\dagger X^{-1} C = V\,\mathrm{diag}(m_1,\ldots,m_n)V^\dagger. \tag{2.10}$$

Since the coefficient matrix C can be deduced from Eq. (2.6), the parameters V and $m_i, i=1,\ldots,n$ are determined by the probabilities $\gamma_i, i=1,\ldots,n$. Hence, the representation U is obtained from the given probabilities. The expressions of E and F require $0\leqslant m_i\leqslant 1$, $i=1,2,\ldots,n$. In Appendix A we show a more strict limitation $0<m_i\leqslant 1$.

Equation (2.9) is fundamental in obtaining the Hamiltonian and realizing a quantum probabilistic identifying machine. Based on this representation, we use the following method to derive the corresponding Hamiltonian. We adopt the approach in the quantum computation literature of assuming that a constant Hamiltonian H acts during a short time interval Δt. Here we only consider evolution from t to $t+\Delta t$. The time interval is then related to the strength of couplings in H, which are of the order $\hbar/\triangle t$. Under this condition we deduce H with

$$U = e^{-iH\Delta t/\hbar}. \tag{2.11}$$

The unitary representation U in Eq. (2.9) can be diagnolized by interchanging the columns and rows of the matrix (refer to Appendix B) as

$$U = O\,\mathrm{diag}(e^{i\theta_1}, e^{-i\theta_1},\ldots,e^{i\theta_n},e^{-i\theta_n})O^\dagger, \tag{2.12}$$

where O is a unitary matrix and θ_j, $j=1,\ldots,n$ are determined by

$$e^{i\theta_j} = \sqrt{1-m_j} + i\sqrt{m_j}\quad\left(0<\theta_j\leqslant\frac{\pi}{2}\right). \tag{2.13}$$

Comparing Eq. (2.12) with Eq. (2.11), the eigenvalues $E_{\pm k}$ of the Hamiltonians should be

$$E_{\pm k} = \mp\frac{\theta_k\hbar}{\Delta t} + \frac{2\pi N_{\pm k}\hbar}{\Delta t}, \tag{2.14}$$

where $N_{\pm k}$ are arbitrary integers. H can be represented as

$$H = O\,\mathrm{diag}(E_1,E_{-1},\ldots,E_n,E_{-n})O^\dagger. \tag{2.15}$$

Now we have successfully derived the diagonalized representation and Hamiltonian of the evolution described by Eq. (2.5), which are essential to realizing the identification via universal quantum logic gates. We will extend the result to M-initial-copy identification and $M\to N$ cloning in a similar way. In the situation of probabilistic identification with M initial copies, we generalize Eq. (2.5) to

$$\hat{U}|\psi_i\rangle^{\otimes M}|P_0\rangle = \sqrt{\gamma_i}|\tilde{\varphi}_i\rangle|P_1\rangle + \sum_j C_{ij}|\alpha_j\rangle|P_0\rangle, \tag{2.16}$$

where $\{|\tilde{\varphi}_i\rangle, i=1,2,\ldots,n\}$ is a set of orthogonal states in n^M-dimensional Hilbert space $\mathcal{H}^{\otimes M}$. With the method mentioned above, we can prove that U has the same representation as that in Eq. (2.9) on different orthogonal bases $\{\{|\alpha_i\rangle|P_0\rangle\}, \{|\tilde{\varphi}_j\rangle|P_1\rangle\}, i,j=1,2,\ldots,n\}$, where the definitions of V, m_i, E, and F are also the same as that of Eq. (2.9). However, they are different in fact because the determining condition Eq. (2.10) turns into

$$I_n - C^\dagger (X^{(M)})^{-1} C = V\,\mathrm{diag}(m_1,\ldots,m_n)V^\dagger. \tag{2.17}$$

As to $M\to N$ probabilistic cloning, the unitary evolution equation is Eq. (2.1). Under the same condition of Eq. (2.17) but different orthogonal bases $\{\{|\alpha_i\rangle|\varphi_1\rangle^{\otimes(N-M)}|P_0\rangle\}, \{|\beta_i\rangle\}, i=1,2,\ldots,n\}$, U may still be represented as that in Eq. (2.9).

We notice that in different situations for probabilistic identification and cloning, the unitary representation and Hamiltonian are of the same form. However, since the determining conditions are different, the values of V, m_i, θ_i, and $E_{\pm k}$ are different as well. The unitary representations and Hamiltonians of different identifications and clones are based on different bases. All these show that these $\hat{U}$ or $\hat{H}$ are actually different.

In this section, we choose appropriate orthogonal bases and represent the $2n^N$-dimensional unitary evolution as Eq. (2.9) in a $2n$-dimensional subspace. In the subspace orthogonal to such $2n$-dimensional subspace, $U=I$.

III. NETWORKS OF PROBABILISTIC CLONING AND IDENTIFICATION IN A *k*-PARTITE SYSTEM

So far we have derived the explicit representation of the unitary evolutions for quantum probabilistic cloning and identification. The next problem is how to realize these cloning and identifying transformations by physical means. The fundamental unit of quantum information transmission is the quantum bit (qubit), i.e., a two-state quantum system, which is capable of existing in a superposition of Boolean states and of being entangled with one another. Just as classical bit strings can represent the discrete states of arbitrary finite dimensionality, a string of k qubits can be used to represent quantum states in any 2^k-dimensional Hilbert space. Obviously there exist 2^k linear-independent states in such a k-partite system. In this section we apply the method provided in Sec. II to this special system and realize probabilistic cloning and identification of an arbitrary state secretly chosen from a linear-independent state set via universal logic gates. This solution may be essential to the realization of a quantum computer.

A. Some basic ideas and notations

Quantum logic gates have the same number of input and output qubits and a k-qubit gate carries out a unitary operation of the group $U(2^k)$, i.e., a generalized rotation in a 2^k-dimensional Hilbert space. The formalism we use for quantum computation, which is called a quantum gate array, was introduced by Deutsch [22], who showed that a simple generalization of the Toffoli gate is sufficient as a universal gate for quantum computation. We introduce this gate as follows.

For any 2×2 unitary matrix

$$U=\begin{pmatrix} u_{00} & u_{01} \\ u_{10} & u_{11} \end{pmatrix}$$

and $m\in\{0,1,2,\ldots\}$, the matrix corresponding to the $(m+1)$-bit operation is $\Lambda_m(U)=\mathrm{diag}(I_{2^m},U)$, where the bases are lexicographically ordered, i.e., $|000\rangle,|001\rangle,\ldots,|111\rangle$. For a general U, $\Lambda_m(U)$ can be regarded as a generalization of the Toffoli gate, which, on the $m+1$ input bits, applies U to the $(m+1)$th bit if and only if the other m bits are all on state $|1\rangle$. Barenco *et al.* [23] have further demonstrated that arbitrary $\Lambda_m(U)$ can be executed by the combination of a set of one-bit quantum gates $[U(2)]$ and two-bit Controlled-NOT (C-NOT) gate [that maps Boolean values (x,y) to $(x,x\oplus y)$].

We first introduce a lemma which shows how to decompose a general unitary matrix to the product of the matrices $\Lambda_m(U)$.

Lemma 1. Any unitary matrix $U=[u_{ij}]_{n\times n}$ can be decomposed into

$$U=\left(\prod_{t=1}^{n-1}\prod_{l=t+1}^{n}A_{tl}\right)\left(\prod_{k=1}^{n}B_k\right), \tag{3.1}$$

where $A_{tl}=[a_{ij}^{(tl)}]_{n\times n}=P_{t,n-1}P_{l,n}\hat{A}(\hat{u}_{tl})P_{l,n}^{\dagger}P_{t,n-1}^{\dagger}$, $B_k=P_{k,n}\hat{B}(\exp(i\alpha_k))P_{k,n}$, $\hat{A}(\hat{u}_{tl})=\mathrm{diag}(1,1,\ldots,1,\hat{u}_{tl})$, $\hat{u}_{tl}$ is a 2×2 unitary matrix, $\hat{B}(\exp(i\alpha_k))=\mathrm{diag}(1,1,\ldots,1,\exp(i\alpha_k))$, P_{ij} left-multiplying a matrix interchanges the ith and jth row of the matrix, and similarly $P_{ij}^{\dagger}$ right-multiplying a matrix interchanges columns. On the lexicographically ordered orthogonal bases, the representations of operators P_{ij} and $P_{ij}^{\dagger}$ are identical. When $n=2^{m+1}$, obviously $\hat{A}(\hat{u}_{tl})=\Lambda_m(\hat{u}_{tl})$, and $\hat{B}(\exp(i\alpha_k))=\Lambda_m(\mathrm{diag}(1,\exp(i\alpha_k)))$.

The meaning of this decomposition in mathematics is that some unitary matrices, namely $A_{tl}^{\dagger}$, left-multiply U to transfer it to a upper triangular matrix. Since U is unitary, it should be diagonal and can be decomposed into the product of matrices B_k. Thus unitary matrix U is decomposed into the form of Eq. (3.1).

We show how to transfer the operation P_{ij} to operation $\Lambda_m(\sigma_x)$ via C-NOT operations. In fact $P_{ij}=|\{x_k^i\}\rangle\langle\{x_k^j\}|+|\{x_k^j\}\rangle\langle\{x_k^i\}|+\Sigma_{l\neq i,j}|\{x_k^l\}\rangle\langle\{x_k^l\}|$, where $|\{x_k^t\}\rangle=|x_1^t,x_2^t,\ldots,x_{m+1}^t\rangle$ with $x_k^t\in\{0,1\}$, $k=1,2,\ldots,m+1$. These C-NOT operations transfer the subspace spanned by $|\{x_k^i\}\rangle$ and $|\{x_k^j\}\rangle$ to the subspace spanned by $|11\cdots11\rangle$ and $|11\cdots10\rangle$. For $i\neq j$, there must exist k satisfying $x_k^i\neq x_k^j$. Denote the minimum value of k by k_0 and assume $x_{k_0}^i=1$, $x_{k_0}^j=0$. For an integer s, $k_0<s\leq n$, if $x_s^i\neq x_s^j$, we execute C-NOT operation (the k_0th bit controls the sth bit). Then for $1\leq h\leq n$, $x_h^i=x_h^j=0$, we execute σ_x^h on the hth bit. At last we interchange the input sequence of the k_0th bit and the $(m+1)$th bit.

With the lemma above, a unitary evolution can be expressed as the product of some controlled unitary operations.

The representations of the input states are another important problem. As to two linear-independent states $|\psi_1\rangle,|\psi_2\rangle$ of one qubit system, we set them symmetric,

$$|\psi_{1,2}(\theta)\rangle=|\psi_{\pm}(\theta)\rangle=\cos\theta|0\rangle_A\pm\sin\theta|1\rangle_A, \tag{3.2}$$

where $0\leq\theta\leq\pi/4$ and A represents the system for identification and cloning. [This simplification is reasonable because arbitrary states $|\psi_1\rangle,|\psi_2\rangle$ can be transformed to Eq. (3.2) via unitary rotation.]

In the case of a two-partite system, the orthogonal bases are $\{|\phi_i\rangle_{1,2}\}=\{|00\rangle_{1,2},|01\rangle_{1,2},|10\rangle_{1,2},|11\rangle_{1,2}\}$ and the input states are $\{|\psi_i\rangle_{1,2},\ i=1,2,3,4\}$, each of which may be expressed as $|\psi_i\rangle_{1,2}=\Sigma_{j=1}^{4}t_{ij}|\phi_j\rangle_{1,2}$ with $\Sigma_{j=1}^{4}|t_{ij}|^2=1$. However, they cannot be converted to symmetric forms as those in Eq. (3.2). Define $T=[t_{ij}]_{4\times4}$; the determinant of T should be nonzero since $|\psi_i\rangle_{1,2}$ are linear-independent.

Lemma 2. For any four states $\{|\psi_i\rangle_{1,2},\ i=1,2,3,4\}$ in Hilbert space $\mathcal{H}^{\otimes2}$ (two-partite system), there exists a unitary operator U_0,

$$U_0(|\psi_1\rangle_{1,2},|\psi_2\rangle_{1,2},|\psi_3\rangle_{1,2},|\psi_4\rangle_{1,2})=(|\phi_1\rangle_{1,2},|\phi_2\rangle_{1,2},|\phi_3\rangle_{1,2},|\phi_4\rangle_{1,2})\tilde{T}, \tag{3.3}$$

where

$$\tilde{T}=\begin{pmatrix} 1 & e^{i\mu_2^{(1)}}\cos\theta_2^{(1)} & e^{i\mu_3^{(1)}}\cos\theta_3^{(1)}\cos\theta_3^{(2)} & e^{i\mu_4^{(1)}}\cos\theta_4^{(1)}\cos\theta_4^{(2)}\cos\theta_4^{(3)} \\ 0 & \sin\theta_2^{(1)} & e^{i\mu_3^{(2)}}\cos\theta_3^{(1)}\sin\theta_3^{(2)} & e^{i\mu_4^{(2)}}\cos\theta_4^{(1)}\cos\theta_4^{(2)}\sin\theta_4^{(3)} \\ 0 & 0 & \sin\theta_3^{(1)} & e^{i\mu_4^{(3)}}\cos\theta_4^{(1)}\sin\theta_4^{(2)} \\ 0 & 0 & 0 & \sin\theta_4^{(1)} \end{pmatrix}$$

with $0\leq\theta_i^{(1)}<\pi$, $0\leq\theta_i^{(j)}<2\pi$, $0\leq\mu_i^{(j)}<2\pi$.

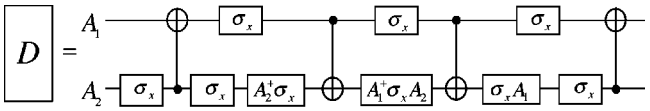

FIG. 1. The networks of of D gate [17]. ● and ⊕ denote the controller and target bit of a C-NOT operation, respectively.

If $\{|\psi_i\rangle_{1,2}\}$ are linear-independent, then $\theta_i^{(1)}>0$. The unitarity of U_0 yields

$$T^\dagger T=\tilde{T}^\dagger\tilde{T}. \tag{3.4}$$

Lemma 2 can be generalized to a k-partite system. According to this lemma, we may concentrate on probabilistic cloning and identification of states $|\tilde{\psi}_i\rangle_{1,2}=U_0|\psi_i\rangle_{1,2}$, $i=1,2,3,4$.

All unitary representations have physical meaning only when the orthogonal bases have been set. To represent the bases $\{|\alpha_i\rangle\}$ and $\{|\beta_i\rangle\}$, we adopt the distinguishability transfer gate (D-gate) operation introduced in Ref. [17] and generalize it to a k-partite system. This operation compresses all the information of the M input copies into one qubit and acts as follows:

$$D(\theta_1,\theta_2)|\psi_\pm(\theta_1)\rangle|\psi_\pm(\theta_2)\rangle=|\psi_\pm(\theta_3)\rangle|0\rangle. \tag{3.5}$$

The unitarity of operation $D(\theta_1,\theta_2)$ requires

$$\cos 2\theta_3=\cos 2\theta_1\cos 2\theta_2. \tag{3.6}$$

This condition, together with $0\leqslant\theta_j\leqslant\pi/4$, suffices to determine θ_3 uniquely. Since $D(\theta_1,\theta_2)$ is Hermitian [17], it can also transfer state $|\psi_\pm(\theta_3)\rangle|0\rangle$ back to $|\psi_\pm(\theta_1)\rangle|\psi_\pm(\theta_2)\rangle$. This accomplishes the process of information decompression. Both the compression and decompression will be useful in implementing the cloning and identification.

The D-gate operation can be used as an element in a network for $M\to N$ cloning. Define $D_K=D_1(\theta_1,\theta_{K-1})D_2(\theta_1,\theta_{K-2})\cdots D_{K-1}(\theta_1,\theta_1)$, where the operation $D_j(\theta_1,\theta_{K-j})$ compresses the information of partites j, $j+1$ to partite j, and angles θ_j are uniquely determined by $\cos 2\theta_{j+1}=\cos 2\theta_1\cos 2\theta_j$ $(0\leqslant\theta_j\leqslant\pi/4)$. D_K acts as

$$D_K|\psi_\pm(\theta_1)\rangle^{\otimes K}=|\psi_\pm(\theta_K)\rangle_1|0\rangle^{\otimes(K-1)}. \tag{3.7}$$

The operations D_K, by pairwise interactions, compress all the information to partite 1. $D(\theta_1,\theta_2)$ may be decomposed into universal operations [17], i.e., local unitary (LU) operations on a single qubit and C-NOT operations. Here we directly use the results obtained by Chelfes and Barnett [17] and illustrate the D gate in Fig. 1.

Operation D_K that is suitable for a one-partite system can be generalized to a k-partite system. In the previous part of this subsection we have discussed the special representations of input states in a k-partite system and we will adopt them below. Consider a two-partite system. Define $\tilde{\theta}=\{\theta_i^{(j)},\ \mu_i^{(j)},\ 2\leqslant i\leqslant 4,\ 1\leqslant j\leqslant i-1\}$ to represent the parameters in matrix $\tilde{T}$ in lemma 2. We generalize the D-gate to two-partite system, which acts as

$$D(\tilde{\theta},\tilde{\xi})|\tilde{\psi}_i(\tilde{\theta})\rangle_A|\tilde{\psi}_i(\tilde{\xi})\rangle_B=|\tilde{\psi}_i(\tilde{\eta})\rangle_A|00\rangle_B, \tag{3.8}$$

where $\tilde{\xi}$ and $\tilde{\eta}$ have a definition similar to $\tilde{\theta}$. The unitarity of operation $D(\tilde{\theta},\tilde{\xi})$ yields

$$X(\tilde{\theta},\tilde{\xi})=\tilde{T}^\dagger(\tilde{\eta})\tilde{T}(\tilde{\eta}), \tag{3.9}$$

where $X(\tilde{\theta},\tilde{\xi})=[{}_A\langle\tilde{\psi}_i(\tilde{\theta})|\tilde{\psi}_j(\tilde{\theta})\rangle_{AB}\langle\tilde{\psi}_i(\tilde{\xi})|\tilde{\psi}_j(\tilde{\xi})\rangle_B]_{4\times 4}$. The upper triangular representation of $\tilde{T}(\tilde{\eta})$ determines $\tilde{\eta}$ uniquely through Eq. (3.9).

To obtain an explicit expression for the operation $D(\tilde{\theta},\tilde{\xi})$, we must specify how it transforms states in the subspace orthogonal to that spanned by $|\tilde{\psi}_i(\tilde{\theta})\rangle_A|\tilde{\psi}_i(\tilde{\xi})\rangle_B$. Equation (3.8) may be rewritten as

$$D^{-1}(\tilde{\theta},\tilde{\xi})\{\phi_i\rangle_A|00\rangle_B,\ i=1,2,3,4\}=\{|\phi_i\rangle_A|\phi_j\rangle_B,$$

$$i,j=1,2,3,4\}G\tilde{T}^{-1}(\tilde{\eta}), \tag{3.10}$$

where $G_{16\times 4}$ is the matrix representation of states $\{|\tilde{\psi}_i(\tilde{\theta})\rangle_A|\tilde{\psi}_i(\tilde{\xi})\rangle_B\}$ on the bases $\{|\phi_i\rangle_A|\phi_j\rangle_B\}$, which are lexicographically ordered, i.e., $|0000\rangle,|0001\rangle,\ldots,|1111\rangle$ in Hilbert space $\mathcal{H}^{\otimes 2}\otimes\mathcal{H}^{\otimes 2}$. We denote $G\tilde{T}^{-1}(\tilde{\eta})=(\omega_1,\omega_5,\omega_9,\omega_{13})$. States $|\omega_i\rangle$ are orthogonal in the space spanned by $\{|\tilde{\psi}_i(\tilde{\theta})\rangle_A|\tilde{\psi}_i(\tilde{\xi})\rangle_B\}$. Denote $\tilde{G}^{-1}=(\omega_1,\omega_2,\ldots,\omega_{16})$, where states $\{|\omega_j\rangle,\ 1\leqslant j\leqslant 16,\ j\notin\{1,5,9,13\}\}$ are selected in the subspace orthogonal to that spanned by $\{|\omega_i\rangle,\ i=1,5,9,13\}$. With Eq. (3.10), we let

$$D^{-1}(\tilde{\theta},\tilde{\xi})\{|\phi_i\rangle_A|\phi_j\rangle_B\}=\{|\phi_i\rangle_A|\phi_j\rangle_B\}\tilde{G}^{-1}. \tag{3.11}$$

Thus we represent $D(\tilde{\theta},\tilde{\xi})$ as matrix $\tilde{G}$ on the orthogonal bases $\{|\phi_i\rangle_A|\phi_j\rangle_B\}$. Similar to Eq. (3.7), define $D_K=D_1(\tilde{\theta},\tilde{\xi}_{K-1})D_2(\tilde{\theta},\tilde{\xi}_{K-2})\cdots D_{K-1}(\tilde{\theta},\tilde{\theta})$ $(\tilde{\theta}=\tilde{\xi}_1)$, where $D_j(\tilde{\theta},\tilde{\xi})$ compresses the information of partite systems A_j,A_{j+1} to A_j, and $\tilde{\xi}_{j+1}$ is uniquely determined by $X(\tilde{\theta},\tilde{\xi}_j)=\tilde{T}^\dagger(\tilde{\xi}_{j+1})\tilde{T}(\tilde{\xi}_{j+1})$. D_K acts as follows:

$$D_K|\psi_i(\tilde{\theta})\rangle^{\otimes K}=|\psi_i(\tilde{\xi}_K)\rangle_{A_1}|00\rangle^{\otimes(K-1)}. \tag{3.12}$$

We can also define the similar operation $D_K(\tilde{\theta},\tilde{\xi})$ that compresses the information of K input copies into one for a k-partite system, where $\tilde{\theta}=(\theta_i^{(j)},\mu_i^{(j)},i=2,3,\ldots,2^k;j=1,2,\ldots,i-1)$. With lemma 1 we can realize D_K via universal logic gates.

For operation D_K, we may introduce a new gate called the Controlled-D_K gate, which can transfer the complicated orthogonal bases to lexicographically ordered ones of a multipartite system. In the information compression process, we perform a Controlled-D_K gate on the controlled partites with

P as the controller. In the information decompression process, a Controlled-D_K^+ gate is needed. With all these operations and controlled operations, we can express the orthogonal bases and transfer them to those suitable for the realization of quantum cloning and identification via universal quantum logic gates.

B. Representation of unitary evolution and realization via universal gates

Suppose that $\Omega^k=\{|\Omega_i\rangle, i=1,2,\ldots,2^k\}$ are the bases which are lexicographically ordered in Hilbert space $\mathcal{H}^{\otimes k}$. For the given probability matrix Γ, with a D_K gate, we can represent the orthogonal bases $\{\{|\alpha_i\rangle|P_0\rangle\}, \{|\tilde{\varphi}_j\rangle|P_1\rangle\}, i, j=1,2,\ldots,2^k\}$ [of Eq. (2.16) for probabilistic identification] and $\{\{|\alpha_i\rangle|\varphi_1\rangle^{\otimes(N-M)}|P_0\rangle\},\{|\beta_j\rangle\}\}, i,j=1,2,\ldots,2^k\}$ [of Eq. (2.1) for probabilistic cloning] as

$$\{\{D_M^{-1}|\Omega_i\rangle|\Omega_1\rangle^{\otimes(M-1)}|P_0\rangle\},\{|\Omega_j\rangle|\Omega_1\rangle^{\otimes(M-1)}|P_1\rangle\}, \quad i,j=1,2,\ldots,2^k\}, \tag{3.13}$$

$$\{\{D_M^{-1}|\Omega_i\rangle|\Omega_1\rangle^{\otimes(N-1)}|P_0\rangle\},\{D_N^{-1}|\Omega_j\rangle|\Omega_1\rangle^{\otimes(N-1)}|P_1\rangle\}, \quad i,j=1,2,\ldots,2^k\},$$

where the first expression is for identification and the second is for cloning. With a controlled-D_M gate and a controlled-D_N gate, we can transfer these orthogonal bases into

$$\{\{|\Omega_i\rangle_{A_1}|P_0\rangle\},\{|\Omega_j\rangle_{A_1}|P_1\rangle\}, i,j=1,2,\ldots,2^k\} \otimes|\Omega_1\rangle_{A_2,A_3,\ldots,A_K}^{\otimes(K-1)}, \tag{3.14}$$

where $K=M$ is for identification and $K=N$ is for cloning. On these new orthogonal bases, the evolution $\hat{U}$ is a unitary controlled operation on a composite system of A_1 and probe P with the composite system of subsystem $A_2, A_3, \ldots, A_K$ as the controller. If the controller is in state $|\Omega_1\rangle_{A_2,A_3,\ldots,A_K}^{\otimes(K-1)}$, we perform operation $\hat{U}$ on the composite system of A_1P. Otherwise we make no operation. Denote $|P_0\rangle=|0\rangle_P$, $|P_1\rangle=|1\rangle_P$, on the bases $\{\{|\Omega_i\rangle_{A_1}|0\rangle_P\}, \{|\Omega_j\rangle_{A_1}|1\rangle_P\}, i,j=1,2,\ldots,2^k\}$; U can be represented as $U=\tilde{V}S\tilde{V}^\dagger$ [Eq. (2.9)]. $\tilde{V}$ corresponds to the operation

$$\hat{V}_{A_1}\hat{I}_P|\Omega_1\rangle^{\otimes(K-1)\otimes(K-1)}\langle\Omega_1|+\hat{J}, \tag{3.15}$$

where $\hat{J}=\Sigma_{|\{\Omega_{i_j}\}\rangle\neq|\Omega_1\rangle^{\otimes(K-1)}}\hat{I}_{A_1P}|\{\Omega_{i_j}\}\rangle\langle\{\Omega_{i_j}\}|$ with $|\{\Omega_{i_j}\}\rangle=|\Omega_{i_1}\rangle|\Omega_{i_2}\rangle\cdots|\Omega_{i_{K-1}}\rangle$, $K=M$ is for identification, and $K=N$ for cloning. The matrix corresponding to the operation $\hat{V}_{A_1}$ on the bases $\{|\Omega_i\rangle_{A_1}\}$ is V. $\hat{I}_P$ represents unit operation of a probe system. On the new orthogonal bases $\{\{|\Omega_i\rangle_{A_1}|P_0\rangle, |\Omega_i\rangle_{A_1}|P_1\rangle\}, i=1,2,\ldots,2^k\}$, we express

$$S=\begin{pmatrix} F & -E \\ E & F \end{pmatrix}$$

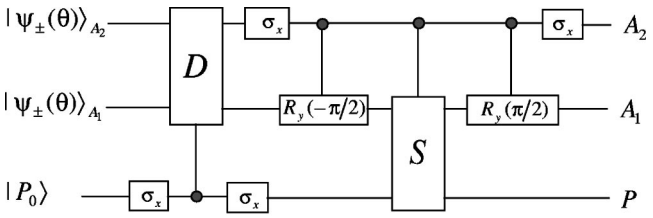

FIG. 2. The networks of probabilistic identification for a one-partite system. $|\psi_\pm(\theta)\rangle_{A_i}$ are to-be-identified states and $|P_0\rangle$ is the probe.

as $S=\mathrm{diag}(K_1,K_2,\ldots,K_{2^k})$, where

$$K_i=\begin{pmatrix} \sqrt{1-m_i} & -\sqrt{m_i} \\ \sqrt{m_i} & \sqrt{1-m_i} \end{pmatrix}.$$

So we obtain

$$\hat{S}=\prod_{i=1}^{2^k} P_{2i,2^{k+1}}P_{2i-1,2^{k+1}-1}\Lambda_k^{A_1P}(K_i) \times P_{2i-1,2^{k+1}-1}P_{2i,2^{k+1}}|\Omega_1\rangle^{\otimes(K-1)\otimes(K-1)}\langle\Omega_1|+\hat{J}, \tag{3.16}$$

where $K=M$ is for identification and $K=N$ is for cloning. We have shown in lemma 1 that the unitary operations U_0, $P_{2i-1,2^{k+1}-1}$, $P_{2i,2^{k+1}}$, and $\hat{V}_{A_1}$ can be decomposed into the product of basis operations such as C-NOT and $\Lambda_k(\hat{u})$. The decomposition of $\Lambda_k(\hat{u})$ has been completed by Barenco *et al.* [23]. Thus we complete the decomposition of the unitary evolution via universal quantum logic gates, so as to realize probabilistic cloning and identification of a k -partite system.

In the following we will give some examples. First we shall be concerned with quantum probabilistic identification of a one-partite system, provided with M initial copies. With the given maximum probability $\gamma_1=\gamma_2=1-\cos^M 2\theta$, we obtain

$$\tilde{V}=\frac{1}{\sqrt{2}}(I^A+i\sigma_y^A)I^P=R_y^A\left(\frac{\pi}{2}\right)I^P, \quad m_1=1,$$

$$m_2=\frac{1-\cos^M 2\theta}{1+\cos^M 2\theta}, \quad K_1=\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$

$$K_2=\begin{pmatrix} \sqrt{\dfrac{2\cos^M 2\theta}{1+\cos^M 2\theta}} & -\sqrt{\dfrac{1-\cos^M 2\theta}{1+\cos^M 2\theta}} \\ \sqrt{\dfrac{1-\cos^M 2\theta}{1+\cos^M 2\theta}} & \sqrt{\dfrac{2\cos^M 2\theta}{1+\cos^M 2\theta}} \end{pmatrix},$$

where

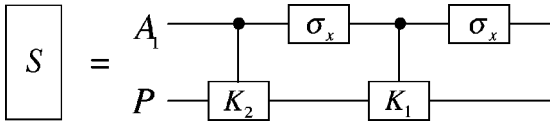

FIG. 3. The networks of an S gate for a one-partite system.

$$R_y(\chi)=\begin{pmatrix} \cos\frac{\chi}{2} & \sin\frac{\chi}{2} \\ -\sin\frac{\chi}{2} & \cos\frac{\chi}{2} \end{pmatrix}.$$

The network of quantum probabilistic identification for a one-partite system via universal logic gates is shown in Fig. 2 ($M=2$).

The S gate in Fig. 2 is illustrated in Fig. 3.

For a two-partite system, with the given maximum probability matrix Γ which satisfies the inequality $X^{(M)}-\Gamma\geqslant 0$, we obtain

$$\hat{S}=\sigma_x^1\sigma_x^2\Lambda_2(K_1)\sigma_x^2\sigma_x^1\sigma_x^1\Lambda_2(K_2)\sigma_x^1\sigma_x^2\Lambda_2(K_3)\times\sigma_x^2\Lambda_2(K_4)|00\rangle^{\otimes(M-1)\otimes(M-1)}\langle 00|+\hat{J}.$$

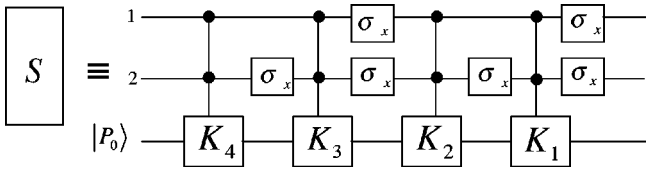

FIG. 5. The networks of an S gate for a two-partite system.

The network of quantum probabilistic identification for a two-partite system is shown in Fig. 4 ($M=2$).

The S gate in Fig. 4 is illustrated in Fig. 5

As to probabilistic cloning, we also begin with a one-partite system. With inequality (2.4), we give the maximum probability $\gamma_{\max}=(1-\cos^M 2\theta)/(1-\cos^N 2\theta)$. Then

$$\tilde{V}=\frac{1}{\sqrt{2}}(I^{A_1}+i\sigma_y^{A_1})|0\rangle_{A_2A_2}\langle 0|I^P=R_y^A\left(\frac{\pi}{2}\right)|0\rangle_{A_2A_2}\langle 0|I^P,$$

$$K_1=\begin{pmatrix} 0 & -1 \\ 1 & 0, \end{pmatrix},$$

$$K_2=\begin{pmatrix} \sqrt{\frac{2(\cos^M 2\theta-\cos^N 2\theta)}{(1-\cos^N 2\theta)(1+\cos^M 2\theta)}} & -\sqrt{\frac{(1+\cos^N 2\theta)(1-\cos^M 2\theta)}{(1-\cos^N 2\theta)(1+\cos^M 2\theta)}} \\ \sqrt{\frac{(1+\cos^N 2\theta)(1-\cos^M 2\theta)}{(1-\cos^N 2\theta)(1+\cos^M 2\theta)}} & \sqrt{\frac{2(\cos^M 2\theta-\cos^N 2\theta)}{(1-\cos^N 2\theta)(1+\cos^M 2\theta)}} \end{pmatrix}.$$

The network of quantum probabilistic clone for a one-partite system is shown in Fig. 6 ($M=2$, $N=3$).

For a two-partite system, with the given maximum probability matrix Γ satisfying $X^{(M)}-\sqrt{\Gamma}X^{(N)}\sqrt{\Gamma}\geqslant 0$, we obtain

$$\hat{S}=\sigma_x^1\sigma_x^2\Lambda_2(K_1)\sigma_x^2\sigma_x^1\sigma_x^1\Lambda_2(K_2)\sigma_x^1\sigma_x^2\Lambda_2(K_3)\times\sigma_x^2\Lambda_2(K_4)|00\rangle^{\otimes(N-1)\otimes(N-1)}\langle 00|+\hat{J}.$$

The network of quantum probabilistic cloning for a two-partite system is shown in Fig. 7 (where $M=2$, $N=3$).

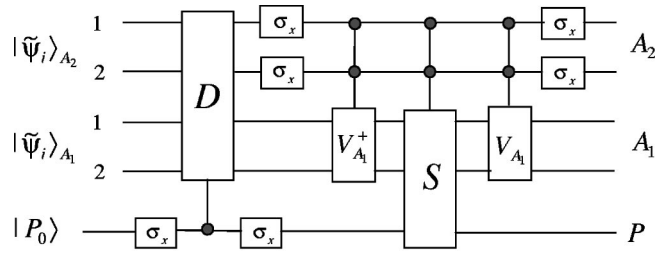

FIG. 4. The networks of probabilistic identification for a two-partite system. $|\tilde{\psi}_i\rangle_{A_j}$ are to-be-identified states.

So far we have realized quantum probabilistic identification and cloning in a k-partite system via universal quantum logic gates, which have important applications in quantum cryptography [24,25], quantum programming [26], and quantum state preparation [27].

C. Robustness of the quantum networks

The robustness properties of the cloning and identifying machines may prove to be crucial in practice. In this subsection, we show whether any errors occur in the input target systems $A_{M+1}, A_{M+2}, \ldots, A_N$, we can detect them without

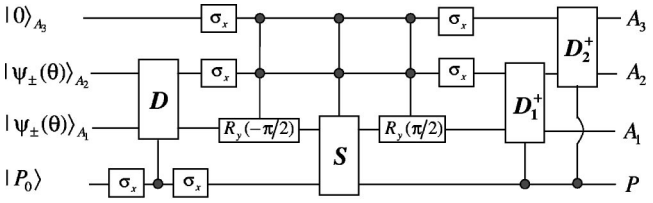

FIG. 6. The networks of probabilistic cloning of a one-partite system. The S gate has been illustrated in Fig. 3. $|\psi_{\pm}(\theta)\rangle_{A_i}$ are to-be-cloned states and $|0\rangle_{A_3}$ is the input target state.

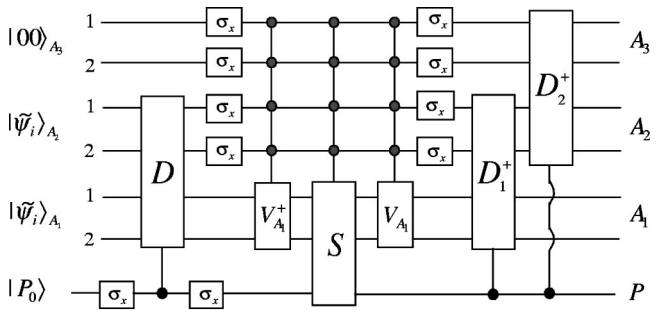

FIG. 7. The networks of probabilistic cloning for a twopartite system. The S gate has been illustrated in Fig. 5. $|\tilde{\psi}_i\rangle_{A_j}$ are to-be-cloned states and $|00\rangle_{A_3}$ is the input target state.

destroying the to-be-cloned states in systems A_1, $A_2, \ldots, A_M$, and the to-be-cloned states can be recycled.

The input target state with errors may be generally expressed as

$$\rho_{A_{M+1},A_{M+2},\ldots,A_N} = \left((1-\delta_1)|\Omega_1\rangle\langle\Omega_1| + \delta_1 \sum_{i=2}^{2^k} \epsilon_i |\Omega_i\rangle\langle\Omega_i| \right)^{\otimes(N-M)}, \tag{3.17}$$

where $\Sigma_{i=2}^{2^k}|\epsilon_i| = 1$ and δ_1 is the error rate, or

$$|\phi\rangle_{A_{M+1},A_{M+2},\ldots,A_N} = \left(\sqrt{1-|\delta_2|^2}|\Omega_1\rangle + \delta_2 \sum_{i=2}^{2^k} \tau_i |\Omega_i\rangle \right)^{\otimes(N-M)}, \tag{3.18}$$

where $\Sigma_{i=2}^{2^k}|\tau_i|^2 = 1$ and $|\delta_2|^2$ is the error rate. Equation (3.17) expresses the errors caused by the decoherence due to the environment. Equation (3.18) represents the errors in state preparation. The errors occur in the $(N-M)$ input target systems for cloning with the approximate rate $(N-M)\delta_1$ $[(N-M)|\delta_2|^2]$, which cannot be omitted in practice when N is relatively large.

After the cloning process, if measurement of probe P results in $|0\rangle_P$, the cloning attempt should be regarded as a failure in a normal sense. However, it may be caused by errors.

If errors caused by the decoherence occur in any input target systems, at least one system occupies state $|\Omega_i\rangle$, $i \neq 1$. According to Eqs. (3.15) and (3.16), the controlled operations $\hat{V}_{A_1}$, $\hat{S}$, and Controlled-D_K^+ gate in the information decompression, function as unit evolutions, in other words, only Controlled-D_K gate in the information compression works. Thus the to-be-cloned state remains undestroyed. According to Eq. (2.1) and the above discussion, the input target states remain unchanged if probe P is in $|0\rangle_P$, whenever the clone fails or errors occur. These two cases can be checked out by measuring the output target states.

If the errors are caused by state preparation, after the evolution of the system, the output target system corresponding to $|0\rangle_P$ is the superposition of two different terms. We measure the output target states, and if they result in $|\Omega_1\rangle^{\otimes(N-M)}$, the clone really fails. Otherwise, the errors work and the to-be-cloned state remains undestroyed.

To the two error situations mentioned above, we can reinput the to-be-cloned system to the cloning machines at the location immediately behind the Controlled-D_K gate (the first operation of the cloning machine) and clone again.

IV. CONCLUSIONS

In summary, we have considered the realization of quantum probabilistic identifying and cloning machines by physical means. We showed that the unitary representation and the Hamiltonian of probabilistic cloning and identifying machines are determined by the probabilities of success. The logic networks have been obtained by decomposing the unitary representation into universal quantum logic operations. We have discussed the robustness of the networks and found that if error occurs in the input target system, we can detect it and the to-be-cloned states can be recycled. Our method is suitable for a k-partite system, such as a quantum computer, and may be generalized to general state-dependent cloning and identification.

ACKNOWLEDGMENTS

We thank Dr. L.-M. Duan for helpful discussion. This work was supported by the National Natural Science Foundation of China.

APPENDIX A

In this appendix, we determine M and N and derive the representation of U. U is a unitary matrix, that is,

$$UU^\dagger = U^\dagger U = I_{2n}. \tag{A1}$$

Equation (A1) can be proved equivalent to the following two equations:

$$N = -(\sqrt{\Gamma})^{-1} C M, \tag{A2}$$

$$MM^\dagger = I_n - C^\dagger X^{-1} C. \tag{A3}$$

It is obvious that $I_n - C^\dagger X^{-1} C$ is a symmetric matrix. According to Eq. (2.6), we yield

$$I_n - C^\dagger X^{-1} C = (I_n + C^\dagger \Gamma^{-1} C)^{-1}. \tag{A4}$$

For Γ positive definite, $C^\dagger \Gamma^{-1} C$ is semipositive definite. Thus $I_n + C^\dagger \Gamma^{-1} C$ is positive definite and its reversed matrix $I_n - C^\dagger X^{-1} C$ is also positive definite.

$I_n - C^\dagger X^{-1} C$ can be represented as the following:

$$I_n - C^\dagger X^{-1} C = V \,\mathrm{diag}(m_1, \ldots, m_n) V^\dagger, \tag{A5}$$

where V is unitary. Together with Eq. (A3), M is determined by

$$M=-V\,\mathrm{diag}(\sqrt{m_1},\ldots,\sqrt{m_n})V^{\dagger}. \tag{A6}$$

Furthermore, we can also prove several useful conclusions to replace the submatrices of U in Eq. (2.8),

$$C^{\dagger}A^{-1}=V\,\mathrm{diag}(\sqrt{1-m_1},\ldots,\sqrt{1-m_n})V^{\dagger}, \tag{A7}$$

$$\sqrt{\Gamma}A^{-1}=V\,\mathrm{diag}(\sqrt{m_1},\ldots,\sqrt{m_n})V^{\dagger}, \tag{A8}$$

$$N=-(\sqrt{\Gamma})^{-1}CM=V(\sqrt{1-m_1},\ldots,\sqrt{1-m_n})V^{\dagger}. \tag{A9}$$

Hence, we get

$$U=\begin{pmatrix} V & 0\\ 0 & V\end{pmatrix}\begin{pmatrix} F & -E\\ E & F\end{pmatrix}\begin{pmatrix} V^{\dagger} & 0\\ 0 & V^{\dagger}\end{pmatrix}, \tag{A10}$$

where $E=\mathrm{diag}(\sqrt{m_1},\ldots,\sqrt{m_n})$, $F=\mathrm{diag}(\sqrt{1-m_1},\ldots,\sqrt{1-m_n})$.

According to Eq. (A5) and $I_n-C^{\dagger}X^{-1}C>0$, we yield

$$m_i>0,\quad i=1,2,\ldots,n.$$

On the other hand, Eq. (A5) can be rewritten as

$$C^{\dagger}X^{-1}C=V\,\mathrm{diag}(1-m_1,\ldots,1-m_n)V^{\dagger}.$$

For X positive definite, $C^{\dagger}X^{-1}C$ is semipositive definite. So $1-m_i\geqslant 0$, that is, $m_i\leqslant 1$, $i=1,\ldots,n$. Combining the results above, we get the range of m_i as

$$0<m_i\leqslant 1,\quad i=1,2,\ldots,n. \tag{A11}$$

APPENDIX B

Here we diagonalize $\hat{U}$.

S can be rewritten as

$$S=TKT^{\dagger}, \tag{B1}$$

where $K=\mathrm{diag}(K_1,K_2,\ldots,K_n)$,

$$K_i=\begin{pmatrix} \sqrt{1-m_i} & -\sqrt{m_i}\\ \sqrt{m_i} & \sqrt{1-m_i}\end{pmatrix},$$

T is a unitary matrix which interchanges the rows of K, and $T^{\dagger}$ interchanges the columns. Denoting

$$L_j=\frac{1}{\sqrt{2}}\begin{pmatrix} 1 & -i\\ -i & 1\end{pmatrix},$$

$j=1,2,\ldots,n$, $\tilde{L}=\mathrm{diag}(L_1,L_2,\ldots,L_n)$, we have

$$K=\tilde{L}\,\mathrm{diag}(e^{i\theta_1},e^{-i\theta_1},\ldots,e^{i\theta_n},e^{-i\theta_n})\tilde{L}^{\dagger}, \tag{B2}$$

where θ_j, and $j=1,2,\ldots,n$ is determined by

$$e^{i\theta_j}=\sqrt{1-m_j}+i\sqrt{m_j},\quad \left(0<\theta_j\leqslant\frac{\pi}{2}\right). \tag{B3}$$

According to Eqs. (2.9), (B1), and (B2), U is completely diagonalized as the following:

$$U=O\,\mathrm{diag}(e^{i\theta_1},e^{-i\theta_1},\ldots,e^{i\theta_n},e^{-i\theta_n})O^{\dagger}, \tag{B4}$$

where $O=\tilde{V}T\tilde{L}$.

[1] W. K. Wootters and W. H. Zurek, Nature (London) **299**, 802 (1982).
[2] H. P. Yuen, Phys. Lett. A **113**, 405 (1986).
[3] G. M. D'Ariano and H. P. Yuen, Phys. Rev. Lett. **76**, 2832 (1996).
[4] H. Barnum, C. M. Caves, C. A. Fuchs, R. Jozsa, and B. Schumacher, Phys. Rev. Lett. **76**, 2818 (1996).
[5] M. Koashi and N. Imoto, Phys. Rev. Lett. **81**, 4264 (1998).
[6] D. Dieks, Phys. Lett. **92A**, 271 (1982); Phys. Lett. A **126**, 303 (1987).
[7] C. H. Bennett, Phys. Today **48** (10), 24 (1995).
[8] V. Bužek and M. Hillery, Phys. Rev. A **54**, 1844 (1996).
[9] N. Gisin and S. Massar, Phys. Rev. Lett. **79**, 2153 (1997).
[10] D. Bruß, D. P. DiVincenzo, A. Ekert, C. A. Fuchs, C. Macchiavello, and J. A. Smolin, Phys. Rev. A **57**, 2368 (1998).
[11] D. Bruss, A. Ekert, and C. Macchiavello, Phys. Rev. Lett. **81**, 2598 (1998).
[12] R. F. Werner, Phys. Rev. A **58**, 1827 (1998).
[13] M. Keyl and R. F. Werner, J. Math. Phys. **40**, 3283 (1999).
[14] S. Massar and S. Popescu, Phys. Rev. Lett. **74**, 1259 (1995).
[15] R. Derka, V. Bužek, and A. Ekert, Phys. Rev. Lett. **80**, 1571 (1998).
[16] M. Hillery and V. Bužek, Phys. Rev. A **56**, 1212 (1997).
[17] A. Chefles and S. M. Barnett, Phys. Rev. A **60**, 136 (1999).
[18] L.-M. Duan and G.-C. Guo, Phys. Lett. A **243**, 261 (1998).
[19] L.-M. Duan and G.-C. Guo, Phys. Rev. Lett. **80**, 4999 (1998).
[20] C.-W. Zhang, C.-F. Li, and G.-C. Guo, Phys. Lett. A **261**, 25 (1999).
[21] V. Bužek, S. L. Braunstein, M. Hillery, and D. Bruß, Phys. Rev. A **56**, 3446 (1997).
[22] D. Deutsch, Proc. R. Soc. London, Ser. A **400**, 97 (1985); **425**, 73 (1989).
[23] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, T. Sleator, J. A. Smolin, and H. Weinfurter, Phys. Rev. A **52**, 3457 (1995).
[24] C. H. Bennett, G. Brassard, and N. D. Mermin, Phys. Rev. Lett. **68**, 557 (1992).
[25] S. M. Barnett and S. J. D. Phoenix, Phys. Rev. A **48**, R5 (1993).
[26] M. A. Nielsen and I. L. Chuang, Phys. Rev. Lett. **79**, 321 (1997).
[27] M. Brune, S. Haroche, J. M. Raimond, L. Davidovich, and N. Zagury, Phys. Rev. A **45**, 5193 (1992).