General description of discriminating quantum operations*

Zhang Ke-Jia(张可佳)[a)b)†], Zhu Ping(朱 萍)[b)], Gao Fei(高 飞)[a)],
Guo Fen-Zhuo(郭奋卓)[b)], Qin Su-Juan(秦素娟)[a)], and Wen Qiao-Yan(温巧燕)[a)]

[a)] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

[b)] *School of Science, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

(Received 25 March 2011; revised manuscript received 26 May 2011)

The discrimination of quantum operations plays a key role in quantum information and computation. Unlike discriminating quantum states, it has some special properties which can be carried out in practice. In this paper, we provide a general description of discriminating quantum operations. Concretely speaking, we describe the distinguishability between quantum operations using a measure called operator fidelity. It is shown that, employing the theory of operator fidelity, we can not only verify some previous results to discriminate unitary operations, but also exhibit a more general discrimination condition. We further apply our results to analysing the security of some quantum cryptographic protocols and discuss the realization of our method using well-developed quantum algorithms.

Keywords: operator discrimination, quantum cryptograph, quantum computation

PACS: 03.67.Ac, 03.65.Ta, 03.67.Dd, 03.67.Hk **DOI:** 10.1088/1674-1056/20/10/100304

1. Introduction

Quantum nonorthogonality, which is considered to be one of the most basic features of quantum mechanics, is widely used in quantum information and quantum computation. Recently, nonorthogonality has been implicated in the study of the discrimination of quantum states, and many useful results have been reported.[1−9] It is well known that complete discrimination between two nonorthogonal states is impossible, even when arbitrarily large but finite copies of states are available.[7] Starting from this simple situation, some measures have been defined to try to quantify the degree of distinguishability between quantum states. For example, the fidelity of two quantum states is used to determine whether they can be discriminated.[8,9]

Similar problems can be considered for quantum operations, which include all physically realizable operations in quantum mechanics such as unitary operations, quantum measurements, quantum channels, etc. Research on the discrimination of quantum operations has received much attention.[10−21] It is now clear that the discrimination of quantum operations is closely related to quantum state discrimination when the device is probed only once.[10,11] However, there exist some special and interesting properties between them.[12−21] In the research, some efficient measures to quantify the degree of distinguishability between quantum operations have also been provided. For example, the generalization of numerical range for a linear operation can be usually used to discriminate unitary operations.[20,21] In addition, some experimental results about the discrimination of unitary operations have been reported.[22−24] These excellent results motivate us to consider the question of "whether the conclusions can be extended into the situation where the quantum operations are not unitary."

In this paper, we provide a new tool named operator fidelity to discriminate quantum operations. With this tool we can verify some previous results to dis-

*Project supported by the National Natural Science Foundation of China (Grant Nos. 60873191, 60903152, 61003286, 60821001, and 61070251), the Program for New Century Excellent Talents in University (Grant No. NCET-10-0260), the Specialized Research Fund for the Doctoral Program of Higher Education (Grant Nos. 200800131016 and 20090005110010), the Beijing Nova Program (Grant No. 2008B51), the Key Project of the Chinese Ministry of Education (Grant No. 109014), the Beijing Natural Science Foundation (Grant No. 4112040), and the Fundamental Research Funds for the Central Universities (Grant Nos. BUPT2011YB01 and BUPT2011RC0505).

†Corresponding author. E-mail: zhangkejia.bupt@gmail.com

© 2011 Chinese Physical Society and IOP Publishing Ltd

criminate unitary operations.[13−16] A general discrimination condition will be proposed when the operations are both not unitary. In Section 2, we introduce the basic methods to discriminate quantum operations and the definition of operator fidelity mentioned above. In Section 3, we utilize the operator fidelity to study the discrimination problem and obtain the general parallel and sequential discrimination schemes. In Section 4, we provide some useful results which can be used in quantum key distribution (QKD), quantum secret sharing (QSS), quantum secure direct communication (QSDC), etc. We also analyse the realization of our method in practice. A short conclusion is given in Section 5.

2. Preliminaries

Here some useful results and notations to operator fidelity are introduced. We denote the d-dimensional Hilbert space by H_d. The notation $Q(d)$ represents the set of quantum operations acting on H_d; in particular, the notation $U(d)$ represents the unitary operation set.

First, we will review the basic methods to discriminate quantum operations. Given the fact that two orthogonal states can be discriminated perfectly, the discrimination of quantum operations is defined below.

Definition 1 Two quantum operations U_0 and U_1 are said to be perfectly discriminated (with a single run allowed) if there exists an input state named the detected state $|\phi\rangle$ such that $U_0|\phi\rangle \perp U_1|\phi\rangle$.

Obviously, we can rewrite the condition as follows:

$$L = \langle\phi|U_0^\dagger U_1|\phi\rangle = 0, \langle\phi|\phi\rangle = 1. \tag{1}$$

In order to discriminate quantum operations, a direct method is to traverse the entire space to find a suitable detected state. Besides, we can reuse the quantum device to solve the problem, i.e., we can discriminate the quantum operations once (DQOO) or discriminate the quantum operations several times (DQOS). The case of DQOS means a quantum device can be used in many essentially different ways such as in parallel, in sequence, or in any other scheme allowed by quantum mechanics. Up to now, the parallel and the sequential schemes have been considered as two sufficient ways to solve the discrimination problem. The two schemes are reviewed as follows.

Definition 2 (Parallel Scheme) Let $U_0, U_1 \in Q(d)$, there exist an integer N and a detected state $|\phi\rangle \in \mathscr{H}_d$ such that $U_0^N|\phi\rangle \perp U_1^N|\phi\rangle$.

Definition 3 (Sequential Scheme) Let $U_0, U_1 \in Q(d)$, there exist a set of auxiliary operations $X_1, \ldots, X_N \in U_d$ and a detected state $|\phi\rangle \in \mathscr{H}_d$ such that $U_0X_{N-1}\cdots X_1U_0 \perp U_1X_{N-1}\cdots X_1U_1$.

The parallel and the sequential schemes provide the basic ways to consider the discrimination of quantum operations. The two schemes for unitary operations have been discussed in Ref. [13]. In the present paper, we extend them to a general case where the quantum operations are not only unitary.

Second, we provide some useful results on the operator fidelity. This can be seen as a function to measure the orthogonality between quantum operations. The preferred definition is given as follows.

Definition 4 Let $U_0, U_1 \in Q(d)$, the definition of operator fidelity can be expressed as:

$$F = \frac{1}{d}|\mathrm{Tr}(U_0^\dagger U_1)| = |\overline{\mathrm{Tr}}(U_0^\dagger U_1)|. \tag{2}$$

Operator fidelity has attracted much interest.[25−27] As referred to in Ref. [26], L is called the Loshmidt echo to evaluate the response to perturbations. Intuitively, L and F are considered as two different metrics which characterize the stability of a quantum system to perturbations. We know that the perfect discrimination of quantum operations is equal to $L = 0$, but if we describe the discrimination problem by F, some similar and useful results may be presented. In the following paragraphs, we just discuss the discrimination problem with F and introduce a general idea to discriminate operations. Furthermore, we describe the operator fidelity with some well-developed quantum algorithms such as the deterministic quantum computation with one quantum bit (DQC1).

3. General description of discriminating quantum operations

Now we use operator fidelity to analyse the description problem and provide some results which can be seen as a general description of discriminating quantum operations. Theorem 1 provides an efficient condition to achieve perfect discrimination. Theorem 2 shows a general result to discriminate quantum operations in practice. In the proof of Theorem 2, we can

obtain a general parallel scheme. Naturally, a new sequential scheme can be derived from Theorem 3.

Theorem 1 If $U = U_0^\dagger U_1$ is a normal quantum operation acting on $\mathscr{H}_d$, and satisfies $F = 0$, then there exists a state $|\phi\rangle \in \mathscr{H}_d$ such that $U_0|\phi\rangle \perp U_1|\phi\rangle$.

Proof In order to prove this fact, we first analyse the quantum operations with four different eigenvalues, and this proposition can be easily extended to the case of high dimension. We set

$$\begin{aligned} U = U_0^\dagger U_1 = a|\varphi_1\rangle\langle\varphi_1| + b|\varphi_2\rangle\langle\varphi_2| \\ + c|\varphi_3\rangle\langle\varphi_3| + d|\varphi_4\rangle\langle\varphi_4|, \end{aligned} \tag{3}$$

where $|\varphi_1\rangle, |\varphi_2\rangle, |\varphi_3\rangle$, and $|\varphi_4\rangle$ are the eigenstates of U with the eigenvalues a, b, c, and d, and they also make up the orthogonal basis of $\mathscr{H}_d$. Then we have

$$\mathtt{Tr}(U) = a + b + c + d = 0. \tag{4}$$

Suppose there exists a quantum state satisfying the constraint condition

$$|\phi\rangle = \lambda_1|\varphi_1\rangle + \lambda_2|\varphi_2\rangle + \lambda_3|\varphi_3\rangle + \lambda_4|\varphi_4\rangle, \tag{5}$$

what we want to do is to recognize whether there exists an array of $\{\lambda_1, \lambda_2, \lambda_3, \lambda_4\}$ to satisfy $\mathrm{Tr}(U|\phi\rangle\langle\phi|) = a\lambda_1^2 + b\lambda_2^2 + c\lambda_3^2 + d\lambda_4^2 = 0$. Considering all the necessary conditions, one has the equations as follows:

$$\begin{cases} a\lambda_1^2 + b\lambda_2^2 + c\lambda_3^2 + d\lambda_4^2 = 0, \\ \lambda_1^2 + \lambda_2^2 + \lambda_3^2 + \lambda_4^2 = 1, \\ a + b + c + d = 0. \end{cases} \tag{6}$$

Obviously $a = b = c = d = 0$ satisfies the equation; however the detected state can be arbitrarily chosen in this case. So a more general and significant case should be considered, i.e., at least two of a, b, c, and d are nonzero. Without loss of generality, we let $a \neq 0$, which leads to

$$\begin{cases} (a-b)\lambda_2^2 + (a-c)\lambda_3^2 + (a-d)\lambda_4^2 = 0, \\ a + b + c + d = 0. \end{cases} \tag{7}$$

We can easily obtain $\lambda_1 = \lambda_2 = \lambda_3 = \lambda_4 = \frac{1}{2}$ to satisfy the condition. Of course, this is not the only possible choice, but it is sufficient to prove the conclusion.

Now we have that for two quantum operations U_0 and U_1, if $U = U_0^\dagger U_1$ is Hermitian and $F = 0$, the two operations must be distinguishable. However, this conclusion is sufficient but not necessary.

Example Let $U_0, U_1 \in Q(4)$ such that $U_0^\dagger U_1 = \frac{1}{2}(|00\rangle\langle 00| - |11\rangle\langle 11| + |01\rangle\langle 01| + |10\rangle\langle 10|)$.

On the one hand, by taking $|\phi\rangle = |00\rangle$ we can have $\mathtt{Tr}(U|\phi\rangle\langle\phi|) = \frac{1}{2}$; when we choose $|\phi\rangle = |11\rangle$, we can obtain $\mathtt{Tr}(U|\phi\rangle\langle\phi|) = -\frac{1}{2}$. Obviously we can choose $|\phi\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ to make $\mathtt{Tr}(U|\phi\rangle\langle\phi|) = 0$. Therefore, the two operations can be discriminated perfectly. On the other hand, we know $F = \mathrm{Tr}(U)/4 = \frac{1}{4} \neq 0$. This makes the above conclusion sufficient but not necessary. But for the discrimination of quantum operations, the condition is effective enough.

From Theorem 1, the perfect discrimination of two quantum operations can be achieved if $F = 0$. But in practice, the discrimination system should be affected by the intrinsic error associated with the quantum device and the random error associated with the environment. If the error margin ε has been provided, we are able to implement the quantum devices repeatedly to discriminate the two quantum operations. In other words, if $F < 1$, we can find a finite N to make $F^N \leq \varepsilon$; this is equal to $F^N \to 0$, and $N \to \infty$. In the following paragraphs, we will redescribe the parallel and the sequential discrimination schemes by the above idea when the two quantum operations are both not unitary.

Lemma 1 Let U be a normal quantum operation, then there exists a state ρ such that $|\mathrm{Tr}(U\rho)| = |\nu_{\min}|$, where $\nu_{\min}$ is an eigenvalue of U which has the minimum module.

Proof From the above condition, we can set

$$\begin{aligned} U = v_{\max}\sum_{k=1}^{m}|\nu_k\rangle\langle\nu_k| + v_{\min}\sum_{k=m+1}^{m+n}|\nu_k\rangle\langle\nu_k| \\ + \sum_{k=m+n+1}^{d}\nu_k|\nu_k\rangle\langle\nu_k|, \end{aligned} \tag{8}$$

where $v_{\max}$ and $v_{\min}$ are the eigenvalues of U with the maximum and the minimum modules respectively, and the others are represented by u_k $(k = m + n + 1, \ldots, d)$. Here the eigenstates $\{|\nu_k\rangle\}$ form a d-dimensional orthonormal basis in $\mathscr{H}_d$.

We construct a state as follows:

$$\rho = \sum_{k,k'=m+1}^{m+n} a_{kk'}|\nu_k\rangle\langle\nu_{k'}|. \tag{9}$$

Due to $\mathrm{Tr}(\rho) = 1$, we need to require that

$$\sum_{k=m+1}^{m+n} a_{kk} = 1. \tag{10}$$

With this constructed state, we can easily obtain $\mathrm{Tr}(U\rho) = \nu_{\min}$. Of course, the conclusion can be extended to the case where U is not positive.

Theorem 2 Let $U_0, U_1 \in Q(d)$ which satisfy $U = U_0^\dagger U_1$ that is normal. If there exists an eigenvalue of U whose module is less than d, then we can find a state ρ such that U_0 and U_1 can be discriminated.

Proof Firstly, we can obtain the conclusion that $\mathrm{Tr}(U^{\otimes N}) = (\mathrm{Tr}(U))^N$ for any integer N. In order to simplify this conclusion, we first consider the simplest case of $U \in \mathscr{Q}(2)$. Without loss of generality, we let

$$U = \lambda_1|0\rangle\langle 0| + \lambda_2|1\rangle\langle 1|, \tag{11}$$

so that $\mathrm{Tr}(U) = \lambda_1 + \lambda_2$. In this case we obviously obtain

$$\begin{aligned} U^{\otimes 2} = {} & \lambda_1^2|00\rangle\langle 00| + \lambda_1\lambda_2|01\rangle\langle 01| \\ & + \lambda_1\lambda_2|10\rangle\langle 10| + \lambda_2^2|11\rangle\langle 11|, \end{aligned} \tag{12}$$

then $\mathrm{Tr}(U^{\otimes 2}) = \lambda_1^2 + \lambda_1\lambda_2 + \lambda_1\lambda_2 + \lambda_2^2 = (\lambda_1 + \lambda_2)^2$.

Because the trace of a normal operation depends on the spectral decomposition, the case of $N(N \geq 2)$ can be clearly recognized, i.e., $\mathrm{Tr}(U^{\otimes N}) = (\lambda_1 + \lambda_2 + \cdots + \lambda_N)^N$.

From Lemma 1 we know that there exists a state ρ_0 such that $|\mathrm{Tr}(U\rho_0)| = |\nu_{\min}|$. Then we can obtain

$$\begin{aligned} F^N &= |(\mathrm{Tr}(U\rho_0))^N/d^N| = |\mathrm{Tr}(U^{\otimes N}\rho_0^{\otimes N})/d^N| \\ &= |\nu_{\min}/d|^N, \end{aligned} \tag{13}$$

because the module of $\nu_{\min}$ is less than d, we can obtain $F^N \to 0$, and $N \to \infty$, and the detected state can be made by $\rho = \rho_0^{\otimes N}$.

In fact, the proof of Theorem 2 shows us a more general parallel scheme for the discrimination between two quantum operations which are both not unitary (the unitary case can be certainly included with $|v|_{\min} \leq 1$). A similar consideration can be also promoted in the sequential scheme.

Theorem 3 Let $U_0, U_1 \in Q(d)$ which satisfy $U = U_0^\dagger U_1$ that is normal. Then there exist a finite integer $N > 1$ and a sequence of quantum operations $X_1, X_2, \ldots, X_{N-2}, X_{N-1}$ such that $W_0^\dagger W_1$ is normal, where $W_0 = U_0 X_{N-1} U_0 X_{N-2} \cdots X_2 U_0 X_1 U_0$, and $W_1 = U_1 X_{N-1} U_1 X_{N-2} \cdots X_2 U_1 X_1 U_1$. If there exists an eigenvalue of U whose module is less than d, we can find a state ρ such that U_0 and U_1 can be discriminated.

The proof can be easily performed with an arbitrary choice of $X_1, X_2, \ldots, X_{N-1}$. The unitary case can be seen in Ref. [13]. From the above discussion, it has been seen that if we use operator fidelity to describe the discrimination problem, we can obtain some general discrimination ideas. In practice, any quantum operation acting on $\mathscr{H}_d$ is able to satisfy $v_{\min} < d$, so that the above conclusion can be seen as a general idea to discriminate quantum operations. From this point of view, the classic parallel and sequential schemes to unitary operations can be considered as special cases.

In the following paragraphs, we will discuss the potential application in some quantum secure problems and introduce a quantum algorithm to estimate the operator fidelity in practice.

4. Application and implementation

From the above conclusions, we obtain a general idea to discriminate quantum operations. In real quantum computation and quantum information, unitary operation is usually considered as the most basic resource. At the same time, some complex quantum operations can be divided into a series of unitary operations acting on $\mathscr{H}_2$. So the discrimination of unitary operations acting on $\mathscr{H}_2$ is significant. Here, we study this special discrimination problem and its application in quantum cryptograph protocols. We also introduce a well-developed quantum algorithm named DQC1 to estimate the distinguishability between different quantum operations.

Theorem 4 Let $U_0, U_1 \in U(2)$, $F = 0$ is a sufficient and necessary condition to discriminate U_0 and U_1.

Proof We know that numerical range is an effective tool to discriminate unitary operations and it has been used in many researches.[15−18] Here we want to compare operator fidelity with numerical range and verify this fact. Without loss of generality, we set two unitary operators to be distinguished in the following forms:

$$U_0 = \begin{pmatrix} \cos\theta & \sin\theta\, \mathrm{e}^{\mathrm{i}\,\omega} \\ \sin\theta\, \mathrm{e}^{-\mathrm{i}\,\omega} & -\cos\theta \end{pmatrix},$$

$$U_1 = \begin{pmatrix} \cos(\theta+\varepsilon) & \sin(\theta+\varepsilon)\, \mathrm{e}^{\mathrm{i}(\omega-\tau)} \\ \sin(\theta+\varepsilon)\, \mathrm{e}^{-\mathrm{i}(\omega-\tau)} & -\cos(\theta+\varepsilon) \end{pmatrix}.$$

Here we introduce parameters ε and τ to demonstrate the difference. Then we can have

$$U_0^\dagger U_1 = \begin{pmatrix} a + b\,\mathrm{e}^{\mathrm{i}\,\tau} & c\,\mathrm{e}^{\mathrm{i}(\omega-\tau)} - d\,\mathrm{e}^{\mathrm{i}\,\omega} \\ -c\,\mathrm{e}^{-\mathrm{i}(\omega-\tau)} + d\,\mathrm{e}^{-\mathrm{i}\,\omega} & a + b\,\mathrm{e}^{-\mathrm{i}\,\tau} \end{pmatrix},$$

where $a = \cos\theta\cos(\theta+\varepsilon)$; $b = \sin\theta\sin(\theta+\varepsilon)$; $c = \cos\theta\sin(\theta+\varepsilon)$; $d = \sin\theta\cos(\theta+\varepsilon)$. So the operator fidelity can be easily expressed as follows:

$$F = |\mathrm{Tr}(U_0^\dagger U_1)/2| = |a + b\cos\tau|. \tag{14}$$

From the point of view of numerical range, perfect discrimination of unitary operations depends on the complex hull that the eigenvalues of $U_0^\dagger U_1$ surround. If the complex hull includes the origin, the two unitary operations can be distinguished perfectly. For the above unitary operations, the eigenvalues of $U_0^\dagger U_1$ are $\lambda_1 = a + b\cos\tau + b\cos\tau|\sin\tau|\,\mathrm{i}$ and $\lambda_2 = a + b\cos\tau - b\cos\tau|\sin\tau|\,\mathrm{i}$. If the two unitary operations can be discriminated, the connection between the eigenvalues should cross the origin, i.e., the three points should be collinear. So ε should satisfy the condition that $a + b\cos\tau = 0$, i.e. $F = 0$. It is clear that the operator fidelity is equivalent to numerical range in the discrimination of unitary operations acting on $\mathscr{H}_2$, which is obviously correct.

In fact, from the analysis of discriminating unitary operations acting on $\mathscr{H}_2$, some interesting conclusions can be proposed.

Conclusion 1 If U_0 and U_1 are two real different unitary operations acting on $\mathscr{H}_2$ which satisfy $F = 0$, the detected state can be found by the accurate form of $U = U_0^\dagger U_1$.

Proof Without loss of generality, we set

$$U = U_0^\dagger U_1 = \begin{pmatrix} \cos\beta & \sin\beta \\ \sin\beta & -\cos\beta \end{pmatrix}.$$

We suppose a quantum state with the form of $|\varphi\rangle = a|0\rangle + b|1\rangle$. With a series of mathematical derivation, we can find $a = \frac{1}{\sqrt{2}}(\sin\frac{\beta}{2} + \cos\frac{\beta}{2})$ and $b = \frac{1}{\sqrt{2}}(\sin\frac{\beta}{2} - \cos\frac{\beta}{2})$, which is a solution of $\langle\varphi|U_0^\dagger U_1|\varphi\rangle = 0$.

Conclusion 2 The perfect discrimination of

$$U_0 = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\,\alpha} & 0 \\ 0 & 1 \end{pmatrix}, \quad U_1 = \begin{pmatrix} \mathrm{e}^{\mathrm{i}\,\beta} & 0 \\ 0 & 1 \end{pmatrix}$$

will be achieved if $U = U_0^\dagger U_1$ is Hermitian.

Proof With the condition that $U = U_0^\dagger U_1$ is Hermitian, we can see $\alpha - \beta = k\pi, k \in N$, and $F = 1 + \cos(\alpha - \beta)$. Because the two unitary operations are different, we know that k should be odd, i.e., $\cos(\alpha - \beta) = -1$, and $F = 0$. From Conclusion 1, the result is true.

In fact, discriminating two unitary operations acting on a single qubit (this is equal to acting on $\mathscr{H}_2$) when the device is probed only once, is very useful in solving some quantum secure problems. We know that the most important step in quantum key distribution (QKD)[28−35] and quantum secure direct communication (QSDC)[36−40] is to encode secret bits. The protocol that encodes a secret bit into unitary operations can be simplified as follows. The sender Alice encodes the secret bit into U_0 or U_1 and transfers the secret information to Bob. In the channel, there exists an eavesdropper named Eve. If U_0 and U_1 can be discriminated once, Eve may extract the secret with the intercept-resend attack. In view of this, Alice and Bob should choose unitary operations which cannot be discriminated once to encode secret bits. We can also use this tool to discuss the security of some communication protocols such as those using Pauli operations to encode information. The conditions we provided above may help us to realize this property directly. The idea to discriminate unitary operations can also be used in the QSS.[19,41,42] The discrimination of quantum operations has potential applications in future research.

We use F to describe the above discrimination problem for the added reason is that it can be estimated in real quantum computation. Then we may introduce the quantum algorithm DOC1 to estimate F.

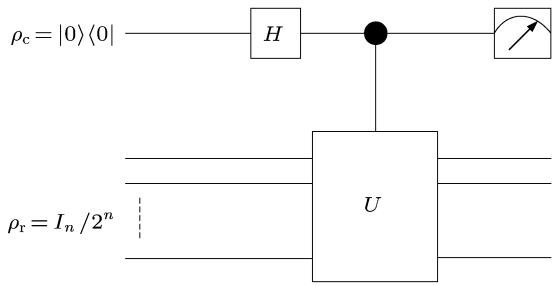


Fig. 1. Algorithm DQC1 for estimation of F.[43] Here U represents $U_0^\dagger U_1, d = 2^n$. Repeated running of the circuit and measurement of qubit c in Pauli $X(Y)$ basis yields an estimate of the corresponding expectation value, from which one can derive the real (imaginary) part of F.

5. Conclusion

In conclusion, we provide a new method to discriminate quantum operations. We use operator fidelity to describe the distinguishability between quantum operations and obtain the general parallel and sequential discrimination schemes. These results can

be used in the discrimination of unitary operations, when we restrict the premise. We also introduce some conclusions which can be used to analyse the security of quantum cryptograph protocols. Finally, a well-developed quantum algorithm called DOC1 is used to estimate the operator fidelity, i.e., the distinguishability can be measured in real quantum computation. We unify the discrimination of quantum states and quantum operations in this paper, because the essence of discrimination of quantum operations (just like that of quantum states) also depends on the orthogonality. It is hoped that some significant results can be obtained using operator fidelity in further research; the new method merits further attention.

References

[1] Qiu D and Li L 2010 *Phys. Rev.* A **81** 042329

[2] Kleinmann M, Kampermann H and Bruss D 2010 *Phys. Rev.* A **81** 020304

[3] Assalini A, Cariolaro G and Pierobon G 2010 *Phys. Rev.* A **81** 012315

[4] Hayashi A, Hashimoto T and Horibe M 2008 *Phys. Rev.* A **78** 012333

[5] Herzog U 2009 *Phys. Rev.* A **79** 032323

[6] Kimura G, Miyadera T and Imai H 2009 *Phys. Rev.* A **79** 062306

[7] Audenaert K M R, Calsamiglia J, Muñoz-Tapia R, Bagan E, Masanes L, Acin A and Verstraete F 2007 *Phys. Rev. Lett.* **98** 160501

[8] Wootters W K 1981 *Phys. Rev.* D **23** 357

[9] Braunstein S L and Caves C M 1994 *Phys. Rev. Lett.* **72** 3439

[10] D'Ariano G M, LoPresti P and Paris M G A 2001 *Phys. Rev. Lett.* **87** 270404

[11] Piani M and Watrous J 2009 *Phys. Rev. Lett.* **102** 250501

[12] A quantum device is reusable, the input state for quantum devices can be chosen freely and there are many different schemes (in parallel or in sequential) to use a quantum device.

[13] Duan R Y, Feng Y and Ying M S 2007 *Phys. Rev. Lett.* **98** 100503

[14] Ziman M 2008 *Phys. Rev.* A **77** 062112

[15] Duan R Y, Feng Y and Ying M S 2008 *Phys. Rev. Lett.* **100** 020503

[16] Ji Z F, Feng Y, Duan R Y and Ying M S 2006 *Phys. Rev. Lett.* **96** 200401

[17] Wu X D and Duan R Y 2008 *Phys. Rev.* A **78** 012303

[18] Chiribella G, D'Ariano G M and Perinotti P 2008 *Phys. Rev. Lett.* **101** 060401

[19] Duan R Y, Feng Y and Ying M S 2009 *Phys. Rev. Lett.* **103** 210501

[20] Childs A M, Preskill J and Renes J 2000 *J. Mod. Opt.* **47** 155

[21] Acín A 2001 *Phys. Rev. Lett.* **87** 177901

[22] Laing A, Rudolph T and O'Brien J L 2009 *Phys. Rev. Lett.* **102** 160502

[23] Zhang P, Peng L, Wang Z W, Ren X F, Liu B H, Huang Y F and Guo G C 2008 *J. Phys.* B: *At. Mol. Opt. Phys.* **41** 195501

[24] Yao X W, Zeng B R, Liu Q, Mu X Y, Lin X C, Yang C, Pan J and Chen Z 2010 *Acta Phys. Sin.* **59** 6837 (in Chinese)

[25] Giorda P and Zanardi P 2010 *Phys. Rev.* E **81** 017203

[26] Wang X G, Sun Z and Wang Z D 2009 *Phys. Rev.* A **79** 012105

[27] Lu X M, Sun Z, Wang X G and Zanardi P 2008 *Phys. Rev.* A **78** 032309

[28] Zukowski M, Zeilinger A, Horne M A and Ekert A K 1993 *Phys. Rev. Lett.* **71** 4287

[29] Wang X B 2005 *Phys. Rev. Lett.* **94** 230503

[30] Ma X F, Fung C H F, Dupuis F, Chen K, Tamaki K and Lo H K 2006 *Phys. Rev.* A **74** 032330

[31] Guo G P, Li C F, Shi B S, Li J and Guo G C 2001 *Phys. Rev.* A **64** 042301

[32] Grosshans F 2005 *Phys. Rev. Lett.* **94** 020504

[33] Cabello A 2000 *Phys. Rev.* A **61** 052312

[34] Gao F, Guo F Z, Wen Q Y and Zhu F C 2006 *Phys. Lett.* A **349** 53

[35] Zhang S, Wang J, Zhang Q and Tang Z J 2009 *Acta Phys. Sin.* **58** 73 (in Chinese)

[36] Long G L and Liu X S 2002 *Phys. Rev.* A 65 032302

[37] Deng F G, Long G L and Liu X S 2003 *Phys. Rev.* A 68 042317

[38] Wang C, Deng F G and Long G L 2005 *Opt. Commun.* **253** 15

[39] Lin S, Wen Q Y, Gao F and Zhu F C 2008 *Phys. Rev.* A **78** 064304

[40] Quan D X, Pei C X, Liu D and Zhao N 2010 *Acta Phys. Sin.* **59** 2493 (in Chinese)

[41] Qin S J, Gao F, Wen Q Y and Zhu F C 2007 *Phys. Rev.* A **76** 062324

[42] Qin S J, Gao F, Wen Q Y and Zhu F C 2009 *Quantum Infor. Comput.* **9** 0765

[43] Knill E and Laflamme R 1998 *Phys. Rev. Lett.* **81** 5672