文章编号:1000－2367(2017)03－0014－10 DOI:10.16366/j.cnki.1000－2367.2017.03.002

量子系统自测试研究

高飞,王玉坤,秦素娟,温巧燕

(北京邮电大学 网络与交换技术国家重点实验室,北京 100876)

摘 要:量子系统自测试研究如何利用量子系统本身来测试其可信性,即根据量子设备的经典输入输出之间的统计关系来确认设备中所制备的量子态和所执行的量子测量.在经典世界中,要实现这种"设备自己测试自己"的目标并不可行,但量子力学中的非局域性却使这种自测试成为可能.量子系统自测试是设备无关量子密码协议的理论基础.综述了量子系统自测试领域的研究进展.具体来说,首先详细介绍了由两粒子最大纠缠态(即单态)及相应量子测量所构成的两方量子系统的自测试,包括测试 1 对量子态的 CHSH 方案、Mayers-Yao 方案、(2,2,2,2)通用方案、$(N,N,2,2)$链式 Bell 方案,和测试 2 对量子态的双 CHSH 方案、魔方方案等.在此基础上,简要介绍了两方部分纠缠态及多方量子系统的自测试方案.最后对量子系统自测试未来的发展进行了展望.

关键词:自测试;量子密码;设备无关;最大纠缠态

中图分类号:TN918;O413 **文献标志码**:A

近年来,随着量子通信和量子计算的不断发展,量子信息技术已经越来越被人们所熟悉,特别是量子通信卫星、京沪干线等项目的实施,预示着量子通信技术即将走向我们的日常生活.

所有量子信息处理任务都需要用到量子设备.因此,量子设备的可信性,即它是否在按照设备提供商所声称的量子形式工作,对能否顺利完成量子信息处理任务至关重要.然而,由于量子态的微观性和量子器件的专业性,判断量子设备是否可信并不容易.量子系统自测试就是解决该问题的有效方法,它利用量子力学中特有的非局域性,可实现用量子系统本身来测试其可信性,目前已经成为国内外学者研究的热点.

自测试的可行性研究起源于 1990 年,人们发现 Clauser-Horn-Shimony-Holt(CHSH)不等式[1]的最大违背即预示着设备中的态为两粒子最大纠缠态,即单态(Singlet State)[2－4].然而直到 2004 年,Mayers 和 Yao 提出对单态的另一种自测试方案后[5－6],自测试才受到学者们的广泛关注.自测试的主要思想是把量子系统看成黑盒子,不对设备内部的参数(如具体的态、测量)做任何假设(这样就可以免疫所有设备不完美或不可信因素).在此框架下利用量子系统中的测量设备对其制备的量子态进行多次测量,通过观测输入和输出之间的条件概率分布,进而推断出设备中的态和测量是否与预期相一致.

目前,自测试的研究已经取得了很大的进展.按照系统中量子态的不同,自测试可以分为对单态[2－6]、图态[7]、任意维度两粒子部分纠缠态[8－9]、三粒子 W 态[10]及相关测量所构成系统的自测试.对于同一种量子态,也存在不同的测试方案,且每种方案中往往对应不同的测量.比如对单态来说,存在 CHSH 方案、Mayers-Yao 方案、(2,2,2,2)通用方案[11]和$(N,N,2,2)$链式 Bell 方案[12].此外,也可以对多对同样的量子态同时进行自测试,如 N 对单态同时自测试[13].最后,人们也研究了对黑盒有部分约束条件时的自测试,例如在量子系统维度已知情形下的自测试[14－16]和测量设备可信时的自测试[17].

设备可信性问题在量子密码(目前的"量子通信"主要指量子保密通信,为了体现其保密功能,后文多用"量子密码"一词来代替)中体现得尤为突出.量子密码的一个主要应用是量子密钥分配,因其具有高安全性

收稿日期:2017-02-23;**修回日期**:2017-03-29.

基金项目:国家自然科学基金(61572081;61672110;61671082)

作者简介:高飞(1980－),男,河北石家庄人,北京邮电大学教授,博士生导师,长江学者,研究方向为量子密码与量子信息,E-mail:gaof@bupt.edu.cn.

通信作者:王玉坤,E-mail:wykun06@gmail.com.

而广受关注. 对用户来说，其量子密钥分配系统都是从设备提供商处购买而来的. 试想一下，如果设备提供商蓄意制造了“不诚实”的量子设备，它不按照正确的协议执行密钥分配，而是偷偷把设备提供商预存在里面的随机数作为密钥输出给用户，那么用这种设备进行的密钥分配将毫无安全性可言. 因此，对量子密码设备的可信性测试势在必行. 幸运的是，基于量子系统自测试的思想，可以设计出设备无关量子密码协议. 比如在设备无关量子密钥分配协议[18]中，即使设备提供商不可信，用户仍然可以确保利用其设备产生的密钥是安全的. 其本质在于，用户对量子设备进行自测试，并在测试通过的条件下以其输出作为密钥，这种情况下的密钥就一定是可信的. 目前，除了量子密钥分配，人们还在设备无关框架下设计了随机数生成[19]、纠缠目击[20]及维度目击等[21]多种协议.

1　自测试的定义

在这里基于两方设备进行描述，对于多方设备可以简单地类推得到. 设实验两方为 Alice 和 Bob，见图 1. 每方可以通过输入不同的值来选择设备中不同的测量方式，并在测量后记录测量结果（即设备的输出）. 通常用 x 和 a 表示 Alice 的输入和输出，用 y 和 b 表示 Bob 的输入和输出，其中 $a,b,x,y\in\{0,1\}$. 如果用数字来分别代表双方输入的取值个数和输出的取值个数，则上述双方各有两个输入、每个测量各有两个输出结果的情形可简记为(2,2,2,2)情形.

在自测试中，对 Alice 和 Bob 设备的内部参数不做任何假设（完全不知道设备内部的构造，比如到底里面制备了什么态、执行了什么测量等）. 除此之外，一般假设 Alice 和 Bob 的输入是独立同分布的（即随机且相互独立），且他们两方是类空间隔的（可以简单地理解为，由于不存在超光速通信，一方设备的输出与另一方设备的输入之间没有任何关系）.

每轮实验中，Alice 和 Bob 记录自己的输入和相应的输出结果. 在很多轮实验之后，Alice 和 Bob 可以得到联合概率分布 $p(a,b|x,y)$. 假设设备中的量子态为 ρ，4 个测量分别为 $A_x=\pi^x_{a-0}+\pi^x_{a-1}$，$B_y=\pi^y_{b-0}+\pi^y_{b-1}$，其中 π^x_a 表示 Alice 一侧输入为 x 输出为 a 的测量算子，π^y_b 表示 Bob 一侧输入为 y 输出为 b 的测量算子. 则根据量子力学可知 $p(a,b|x,y)=\mathrm{tr}(\rho\pi^x_a\pi^y_b)$.

显然，经典统计到量子系统的映射是一对多的，即同一个概率分布可能对应多组不同的量子态及投影测量. 自测试期望在量子理论下可以由 $p(a,b|x,y)$ 直接“唯一”确定量子设备中态和测量，其中“唯一”是在局域同构映射(Local Isometry) $\Phi=\Phi_A\otimes\Phi_B$ 等价的意义下来说的. 也就是说，假设被测试态是两粒子单态 $|\varphi^+\rangle_{AB}=(|00\rangle+|11\rangle)/\sqrt{2}$，测量是$(\vec{\sigma}_x)_A\otimes(\vec{\sigma}_y)_B$，自测试意味着从 $p(a,b|x,y)$ 可以推断出设备中的态 $|\psi\rangle_{AB}$ 一定是一个在局域同构映射下与 $|\varphi^+\rangle_{AB}$ 等价的态，而设备中的测量 $A_x\otimes B_y$ 一定是在同一个局域同构映射下与$(\vec{\sigma}_x)_A\otimes(\vec{\sigma}_y)_B$ 等价的测量，即存在一个局域同构映射 $\Phi=\Phi_A\otimes\Phi_B$ 使得

$$\Phi(|\psi\rangle_{AB})=|J_k\rangle_{AB}\,|\varphi^+\rangle_{AB}, \tag{1}$$

$$\Phi(A_xB_y|\psi\rangle_{AB})=|J_k\rangle_{AB}(\vec{\sigma}_x\otimes\vec{\sigma}_y)\,|\varphi^+\rangle_{AB}, \tag{2}$$

其中 $|J_k\rangle_{AB}$ 代表无用的量子态，并不关心它是什么态.

值得注意的是，尽管自测试并不能真正唯一确定设备中的态和测量，但在上述“局域同构映射意义下的唯一确定”就足以保证该设备能够可信地完成量子信息处理任务. 比如在设备无关量子密钥分配中，上述态和测量带来的密钥一定是可信的.

2　量子单态自测试

2.1　局域同构映射

这里首先介绍用交换(Swap)操作来构建局域同构映射的思想. 虽然并没有证据表明这种构建方法是唯一的，但目前所有关于单态的自测试方案均利用该结构（如图 2）. 图 2 中的局域同构映射以附加粒子为控制位，以被测量子态为目标位，用控制操作 Z'_A，X'_A，Z'_B，X'_B 将被测系统中的态和测量交换到附加系统中. 文献[5,11]指出，如果图 2 中的控制操作是酉操作，并且满足

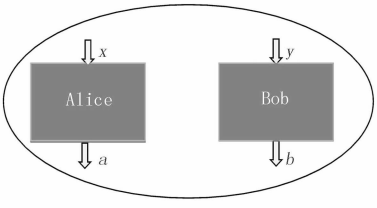
$$Z'_A|\psi\rangle=Z'_B|\psi\rangle, \tag{3}$$

$$X'_B \mid \psi\rangle = Z'_B \mid \psi\rangle, \tag{4}$$

$$X'_A Z'_A \mid \psi\rangle = -Z'_A X'_A \mid \psi\rangle, \tag{5}$$

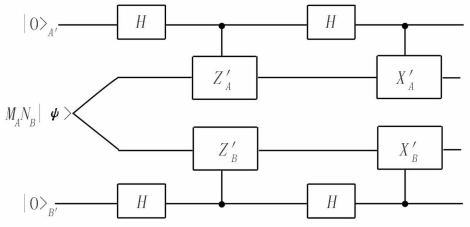
$$X'_B Z'_B \mid \psi\rangle = -Z'_B X'_B \mid \psi\rangle, \tag{6}$$

则量子单态和对应的测量便可以实现自测试. 也就是说,若能由统计到的概率分布构建出满足(3)~(6)式的控制操作 $X'_{A/B}$ 和 $Z'_{A/B}$,则该概率分布便可作为一种自测试方案.



该系统由两个黑盒子构成,自测试的目的就是测试黑盒子内部的量子态制备和测量装置.

图1 需要自测试的量子系统



$|\psi\rangle$是系统中的态,M_A和N_B分别为系统中两方的测量,$|0\rangle_{A'}$与$|0\rangle_{B'}$为附加粒子,H为二维空间上的Hadamard操作;Z'_A,X'_A,Z'_B,X'_B为与测量M_A和N_B有关的控制操作. 值得注意的是这里的局域同构映射实际上是一个虚拟的协议,主要用于证明过程,而做自测试时不需要执行该映射,只需统计输入和输出的概率分布即可.

图2 局域同构映射

下面将沿这种思路来介绍几种对单态的自测试方案.

2.2 CHSH 方案

CHSH 方案考虑(2,2,2,2)情形,记 Alice 和 Bob 两方执行的测量分别为 A_0,A_1 和 B_0,B_1. 执行多轮实验之后,根据观察到的输入输出概率分布,双方容易得到4个测量期望值:$\langle A_x B_y\rangle = \sum_{a,b,x,y} (-1)^{a\oplus b} P(a,b \mid x,y)$,其中 $a,b,x,y \in \{0,1\}$. 如果 CHSH 测试使得

$$S = \langle A_0 B_0\rangle + \langle A_0 B_1\rangle + \langle A_1 B_0\rangle - \langle A_1 B_1\rangle = 2\sqrt{2} \tag{7}$$

成立,则存在图 2 所示的局域同构映射,可交换出单态和 $(\sigma_x)_A$,$(\sigma_z)_A$,$(1/\sqrt{2})(\sigma_x+\sigma_z)_B$,$(1/\sqrt{2})(\sigma_x-\sigma_z)_B$ 4 个测量. 也就是说,在局域同构映射等价的意义下,可以确定系统中的量子态就是单态,而测量就是上述 4 个测量.

简言之,单态的自测试可以由一个单一的值得到,即 $S=2\sqrt{2}$. 而在量子系统中,要使 $S=2\sqrt{2}$,必有 $\langle A_0 B_0\rangle = \langle A_1 B_0\rangle = 1/\sqrt{2}$,$\langle A_1 B_0\rangle = -\langle A_1 B_1\rangle = 1/\sqrt{2}$ 成立. 利用此关系,可以构建出图 2 所示的局域同构映射,其中的控制操作为 $Z'_A = A_0$,$X'_A = A_1$,$Z'_B = \dfrac{B_0 - B_1}{\sqrt{2}}$,$X'_B = \dfrac{B_0 + B_1}{\sqrt{2}}$.

2.3 Mayers-Yao 方案

原始的 Mayers-Yao 方案基于(3,3,2,2)情形,即 Alice 和 Bob 双方各有 3 个测量. 后来文献[8]指出一方的第 3 个测量并不是必需的,此方记为 Alice. 这里将介绍(2,3,2,2)这种简化版的情形.

记 Alice 和 Bob 两方执行的测量分别为 A_0,A_1 和 B_0,B_1,B_2. 执行多轮实验之后,如果观察到的输入输出概率分布满足如下条件:

$$\langle\psi \mid A_0 B_0 \mid \psi\rangle = \langle\psi \mid A_1 B_1 \mid \psi\rangle = 1, \tag{8}$$

$$\langle\psi \mid A_0 B_1 \mid \psi\rangle = \langle\psi \mid A_1 B_0 \mid \psi\rangle = 0, \tag{9}$$

$$\langle\psi \mid A_0 B_2 \mid \psi\rangle = \langle\psi \mid A_1 B_2 \mid \psi\rangle = 1/\sqrt{2}, \tag{10}$$

则存在图 2 所示的局域同构映射,可交换出单态和 $(\sigma_x)_A$,$(\sigma_z)_A$,$(\sigma_x)_B$,$(\sigma_z)_B$,$(1/\sqrt{2})(\sigma_x+\sigma_z)_B$ 5 个测量. 也就是说,在局域同构映射等价的意义下,可以确定系统中的量子态就是单态,而测量就是上述 5 个测量.

为了得到局域同构映射中的控制操作,可以将(8)式和(9)式变形为 $A_0 \mid \psi\rangle = B_0 \mid \psi\rangle$,$A_1 \mid \psi\rangle = B_1 \mid \psi\rangle$. 由(10)式可得出反对易关系 $A_0 A_1 \mid \psi\rangle = -A_1 A_0 \mid \psi\rangle$,$B_0 B_1 \mid \psi\rangle = -B_1 B_0 \mid \psi\rangle$. 此时不难发现 A_0,A_1,B_0,B_1 恰好满足(3)~(6)式,因此可以直接定义为控制操作 $Z'_A = A_0$,$X'_A = A_1$,$Z'_B = B_0$,$X'_B = B_1$.

2.4 (2,2,2,2)通用方案

结合 CHSH 方案及 Mayers-Yao 方案，文献[11]给出了在(2,2,2,2)情形下可实现单态自测试的所有测量的集合.

记 Alice 和 Bob 两方执行的测量分别为 A_0，A_1 和 B_0，B_1. 执行多轮实验之后，如果观察到的输入输出概率分布满足如下 8 个条件中的任何一个：

$$\sum_{(x,y)\neq(i,j)} \arcsin(E_{xy}) - \arcsin(E_{xy}) = \xi\pi, (i,j) \in \{0,1\}, \xi \in \{1,-1\}, \tag{11}$$

其中 $E_{xy} = \langle A_x B_y \rangle$，并有 $\arcsin(E_{xy})_{x,y\in\{0,1\}} \in [-\frac{\pi}{2}, \frac{\pi}{2}]$，且至多只有一对$(x,y)$ 使得 $\alpha_{xy} = \arccos(E_{xy}) = 0$ 或 π，则存在图 2 所示的局域同构映射，可交换出单态和相应的 4 个测量(4 个测量的具体形式随着参数的不同而变化，但都是 3 个 Pauli 算子 σ_x，σ_y，σ_z 的线性组合). 也就是说，在局域同构映射等价的意义下，可以确定系统中的量子态就是单态，而测量就是上述 4 个测量.

满足(11) 式后可以根据测量操作$\{A_0, A_1, B_0, B_1\}$ 建立满足关系式(3) ～ (6) 式的酉的控制操作. 以条件 $\alpha_{00} + \alpha_{10} = \alpha_{01} - \alpha_{11}$ 为例，其控制操作为

$$Z'_A = A_0, \tag{12}$$

$$X'_A = \frac{A_1 - \cos(\alpha_{00} + \alpha_{10}) A_0}{\sin(\alpha_{00} + \alpha_{10})}, \tag{13}$$

$$Z'_B = \frac{\sin(\alpha_{01}) B_0 - \sin(\alpha_{00}) B_1}{\sin(\alpha_{01} - \alpha_{00})}, \tag{14}$$

$$X'_B = \frac{\sin(\alpha_{00}) B_1 - \sin(\alpha_{01}) B_0}{\sin(\alpha_{01} - \alpha_{00})}. \tag{15}$$

2.5 $(N,N,2,2)$链式 Bell 方案

链式 Bell 方案[12]考虑 $(N,N,2,2)$ 情形，记 Alice 和 Bob 两方执行的 N 个测量分别为 $A_1, A_2, \cdots, A_N$ 和 $B_1, B_2, \cdots, B_N$. 此时的目的是要自测试系统中的量子态和这 $2N$ 个测量. 执行多轮实验之后，如果观察到的输入输出概率分布满足如下条件：

$$\mathcal{R}^n_{ch} = \sum_{i-1}^{n} (\langle A_i B_i \rangle + \langle A_{i+1} B_i \rangle) = 2n\cos\frac{\pi}{2n}, \tag{16}$$

则存在图 2 所示的局域同构映射，可交换出单态和相应的 $2N$ 个测量(这些测量平均分布在 Bloch 球面上，这里不再给出它们的具体形式). 也就是说，在局域同构映射等价的意义下，可以确定系统中的量子态就是单态，而测量就是上述 $2N$ 个测量.

我们知道最大两粒子纠缠态及平均分布在 Bloch 球面上的测量可以使得 N 方链式 Bell 不等式 $\mathcal{R}^n_{ch} = \sum_{i-1}^{n} (\langle A_i B_i \rangle + \langle A_{i+1} B_i \rangle) \leq 2n\cos\frac{\pi}{2n}$ 的等号成立. 事实上也可以证明使该不等式达到最大违背的态和测量操作是唯一的. 证明过程基于 Bell 算子的和方(Sum-Of-Square)分解[12,24]. 利用 SOS 分解的谱，可以构建如图 2 所示的控制操作. 具体的证明过程见文献[12]，这里只简单介绍其用到的 SOS 工具及具体的控制操作.

N 方链式 Bell 不等式中的 Bell 算子为 $r^{\max}_n = \sum_{i-1}^{n} (A_i B_i + A_{i+1} B_i)$. 因为 $r_s = 2n\cos\frac{\pi}{2n} - r^{\max}_n$ 是半正定的，所以存在和方分解，即存在算子 P_i(是 A_i，B_j，$A_i \otimes B_j$ 的多项式形式，但不一定是半正定的)，使得 $r_s = \sum_i P_i^+ P_i$. 显然使得 $\mathcal{R}^n_{ch}$ 达到最大违背的量子态和测量，必然使得 r_s 分解中的每个多项式为零. 利用 $A_i \mid \psi\rangle$，$B_j \mid \psi\rangle$，$A_i \otimes B_j \mid \psi\rangle$ 之间的关系，可以构建图 2 所示的局域同构映射，从而实现单态及此 $2N$ 个测量的自测试. 其中控制操作为

$$X'_A = \begin{cases} A'_{n/2+1}, n \text{ 为偶数}, \\ \dfrac{A'_{(n+1)/2} + A'_{(n+3)/2}}{2\cos(\pi/2n)}, n \text{ 为奇数}, \end{cases} \tag{17}$$

$$Z'_A = A_1, \tag{18}$$

$$X'_B=\begin{cases}\dfrac{B'_{n/2}+B'_{n/2+1}}{2\cos(\pi/2n)}, & n\text{ 为偶数},\\ B'_{(n+1)/2}, & n\text{ 为奇数},\end{cases}\tag{19}$$

$$Z'_B=\frac{B'_1-B'_n}{2\cos(\pi/2n)}.\tag{20}$$

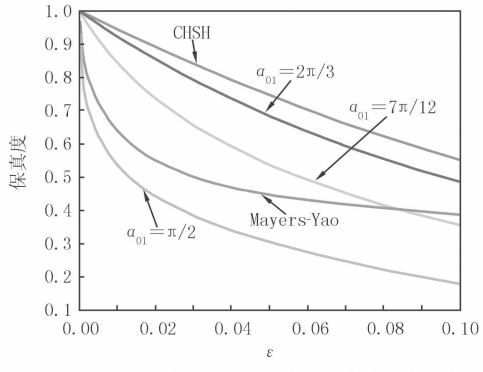
2.6 鲁棒性

鲁棒性指的是在非理想情形(如实验设备不完美、统计误差等因素)对自测试结果的影响程度. 此时实际得到的概率统计值与理想值存在偏差 ε,可表示为 $|\langle\psi|A_xB_y|\psi\rangle-E_{xy}^{ideal}|\leq\varepsilon$. 目前研究鲁棒性分析方案有两种,一种是基于 NPA 半正定方法的数值计算[25],另一种是试图寻找其解析解[26-27]. 通常 NPA 方法更受欢迎,因为解析解的方法要么给出的界过于低,要么对系统有不等式和维度的约束. 这里用基于 NPA 的方法对上述讲到的 CHSH 方案、Mayers-Yao 方案及其他(2,2,2,2)自测试方案进行比较.

已知对于任意两方系统,我们说一个未知量子态 ρ 可以被自测试到量子态 $|\psi\rangle$,则其中必存在一个局域同构映射 Φ. 用保真度 $F=\langle\psi|\rho_{A'B'}|\psi\rangle$ 来度量在映射 Φ 下所交换出的态 $\rho_{A'B'}=\mathrm{tr}_{AB}[\Phi\rho_{AB}\otimes|00\rangle_{A'B'}\langle00|\Phi^{+}]$ 与 $|\psi\rangle$ 之间的近似程度. 由于 Φ 可以分解为测量算子的线性组合,所以 F 即为 $c=(1,\langle A_i\rangle,\langle B_j\rangle,\langle A_iA_j\rangle,\langle B_iB_j\rangle,\langle A_iB_j\rangle,\cdots)$ 的线性组合. 此时鲁棒性问题将转化为以下半正定优化问题:

$$\begin{aligned}&\min\quad F(c)\\ &\text{s.t.}\quad \Gamma\geq0\\ &\qquad|\langle\psi|A_xB_y|\psi\rangle-E_{xy}^{ideal}|\leq\varepsilon,\\ &\qquad\langle A_xB_y\rangle=\mathrm{tr}(\rho_{AB}A_x\otimes B_y).\end{aligned}\tag{21}$$

此优化问题是一个无限层析的过程,其中 Γ 是由所有统计值 $(1,\langle A_i\rangle,\langle B_j\rangle,\langle A_iA_j\rangle,\langle B_iB_j\rangle,\langle A_iB_j\rangle,\langle A_iB_jA_k\rangle,\cdots)$ 构成的半正定矩阵. 每次层析时 Γ 对应不同的矩阵,如第一层层析时,Γ 是由统计值 $(1,\langle A_i\rangle,\langle B_j\rangle)$ 构成的半正定矩阵;第二层层析时,Γ 是由统计值 $(1,\langle A_i\rangle,\langle B_j\rangle,\langle A_iA_j\rangle,\langle B_iB_j\rangle,\langle A_iB_j\rangle)$ 构成的半正定矩阵,以此类推. 具体的构造方法见文献[22]. 下面基于第二层加部分第三层层析结果,给出下面的鲁棒性对比图,见图 3.



对比发现CHSH方案是(2, 2, 2, 2)情形下鲁棒性性能最好的方案. 在通用自测试方案中, a_{01}越大, 鲁棒性越好.

图3 不同自测试方案的鲁棒性对比(无量纲图)

3 2 对量子单态自测试

上面介绍的都是对 1 对单态的自测试方案. 实际上,还可以对 2 对单态同时进行自测试. 显然,若这 2 对单态及各自测量构成的系统之间是分离的,即有两个如图 1 所示的系统时,自测试这 2 对单态及对应的测量是很容易实现的. 此时对每个系统分别利用上述对单个单态的自测试方案即可实现此 2 对单态的自测试. 然而当这 2 对单态及各自测量同时存在于图 1 所示的黑盒子中而无法区分时,就变成了对 2 对单态同时进行自测试的复杂情况.

下面将介绍两种对 2 对量子单态自测试的方案[28]. 事实上,任意大的 N 对量子单态也是可以同时实现自测试,文献[13]中给出了 N 对量子态同时实现自测试的充分条件,这里不做介绍.

3.1 双 CHSH 方案

双 CHSH 方案[27]考虑(4,4,4,4)情形,记 Alice 和 Bob 两方执行的 4 个测量分别为 A_0,A_1,A_2,A_3 和 B_0,B_1,B_2,B_3,每个测量有 4 个输出结果,即 $x,y,a,b\in\{0,1,2,3\}$. 此时的目的是要自测试系统中的量子态 $|\psi\rangle_{AB}=[\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)]^{\otimes2}$ 和这 8 个测量.

双 CHSH 的思想是将输入及输出分成两部分,每部分都可以完成一个 CHSH 测试. 具体来说,输入输

出可以分成如下两部分，

$$x = 2x_{\mathrm{I}} + x_{\mathrm{II}}, y = 2y_{\mathrm{I}} + y_{\mathrm{II}}, \tag{22}$$

$$a = 2a_{\mathrm{I}} + a_{\mathrm{II}}, b = 2b_{\mathrm{I}} + b_{\mathrm{II}}, \tag{23}$$

其中下标I和II代表两个子系统. 此时测量算子也可分解为如下形式：

$$\prod_{a|x-0} := \pi_{z-a_{\mathrm{I}}}^{A_{\mathrm{I}}} \pi_{z-a_{\mathrm{II}}}^{A_{\mathrm{II}}}, \prod_{a|x-1} := \pi_{x-a_{\mathrm{I}}}^{A_{\mathrm{I}}} \pi_{z-a_{\mathrm{II}}}^{A_{\mathrm{II}}}, \tag{24}$$

$$\prod_{a|x-2} := \pi_{z-a_{\mathrm{I}}}^{A_{\mathrm{I}}} \pi_{x-a_{\mathrm{II}}}^{A_{\mathrm{II}}}, \prod_{a|x-3} := \pi_{x-a_{\mathrm{I}}}^{A_{\mathrm{I}}} \pi_{x-a_{\mathrm{II}}}^{A_{\mathrm{II}}}, \tag{25}$$

类似地，对 Bob 一侧的测量算子也是如此.

执行多轮实验之后，如果观测到(26)～(27)式的统计关系，则存在局域同构映射 $\Phi = (S_{\mathrm{I}}S_{\mathrm{II}})_A \otimes (S_{\mathrm{I}}S_{\mathrm{II}})_B$，可交换出 2 对单态和相应的 8 个测量. 也就是说，在局域同构映射等价的意义下，可以确定系统中的量子态就是 2 对单态，而测量就是上述 8 个测量.

$$\frac{1}{2}(\langle Z'_1 + Z''_1\rangle\langle V'_3 + W'_3\rangle + \langle X'_1 + X''_1\rangle\langle V'_3 - W'_3\rangle) = 2\sqrt{2}, \tag{26}$$

$$\frac{1}{2}(\langle Z'_2 + Z''_2\rangle\langle V'_4 + W'_4\rangle + \langle X'_2 + X''_2\rangle\langle V'_4 - W'_4\rangle) = 2\sqrt{2}, \tag{27}$$

其中 Z'_A, X'_A 为 Alice 测量 $A_x, x = \{0,3\}$ 的算子的线性组合，Z''_A, X''_A 为 Alice 测量操作 $A_x, x = \{2,1\}$ 的算子的线性组合，V'_3 为 Bob 测量操作 $B_y, y = \{0,2\}$ 的算子的线性组合，V'_4 为 Bob 测量操作 $B_y, y = \{0,1\}$ 的算子的线性组合，W'_3 为 Bob 测量操作 $B_y, y = \{3,1\}$ 的算子的线性组合，W'_4 为 Bob 测量操作 $B_y, y = \{3,2\}$ 的算子的线性组合.

具体的 S 操作为：

$$S_{\mathrm{I}}S_{\mathrm{II}} \mid 00\rangle_{A'} = \prod_{0|0} \mid 00\rangle_{A'} + (\prod_{0|3} - \prod_{1|3} + \prod_{2|3} - \prod_{3|3}) \mid 01\rangle_{A'} + (\prod_{0|3} + \prod_{1|3} - \prod_{2|3} - \prod_{3|3}) \mid 10\rangle_{A'} + (\prod_{0|3} + \prod_{1|3} - \prod_{2|3} + \prod_{3|3}) \mid 11\rangle_{A'}. \tag{28}$$

3.2　魔方方案

下面介绍魔方(Magic Square)方案. 魔方是一个非常著名的假心灵感应游戏[29－30]. 在这个非局域游戏中，量子参与方总可以取得胜利，就像是有心灵感应一样. 而经典的参与方只有一定的概率能取得胜利.

魔方方案[27]考虑(3,3,4,4)情形，记 Alice 和 Bob 两方执行的 3 个测量分别为 A_0, A_1, A_2 和 B_0, B_1, B_2，每个测量有 4 个输出结果，即 $x, y \in \{0,1,2\}, a, b \in \{0,1,2,3\}$. 此时的目的是要自测试系统中的量子态 $\mid \psi\rangle_{AB} = [\frac{1}{\sqrt{2}}(\mid 00\rangle + \mid 11\rangle)]^{\otimes 2}$ 和这 6 个测量.

执行多轮实验之后，如果观测到的概率统计分布与(29)式中的量子态及(30)～(33)式中的测量对应的测量结果相一致，则存在局域同构映射 $\Phi = (S)_{AA'} \otimes (S)_{BB'}$，可交换出 2 对单态和相应的 6 个测量. 也就是说，在局域同构映射等价的意义下，可以确定系统中的量子态就是 2 对单态，而测量就是上述 6 个测量.

$$\mid \psi\rangle = \mid \Phi^+\rangle_{A_{\mathrm{I}}B_{\mathrm{I}}} \otimes \frac{\mid \Phi^+\rangle + \mid \psi^+\rangle}{\sqrt{2}}_{A_{\mathrm{II}}B_{\mathrm{II}}}, \tag{29}$$

$$\prod_{c|0} = \pi_{z-c_{\mathrm{I}}} \otimes \pi_{z-c_{\mathrm{II}}}, \tag{30}$$

$$\prod_{c|1} = \pi_{x-c_{\mathrm{I}}} \otimes \pi_{x-c_{\mathrm{II}}}, \tag{31}$$

$$\prod_{0,1|2} = \mid \chi_+\rangle\langle\chi_+ \mid, \tag{32}$$

$$\prod_{2,3|2} = \mid \chi'_+\rangle\langle\chi'_+ \mid, \tag{33}$$

其中 $\mid \chi_+\rangle = \frac{1}{\sqrt{2}}(\mid \Phi^-\rangle \pm \mid \psi^+\rangle)$，$\mid \chi'_+\rangle = \frac{1}{\sqrt{2}}(\mid \Phi^+\rangle \pm \mid \psi^-\rangle)$ 且 $c = a, b$ 分别表示 Alice 和 Bob 侧的测量.

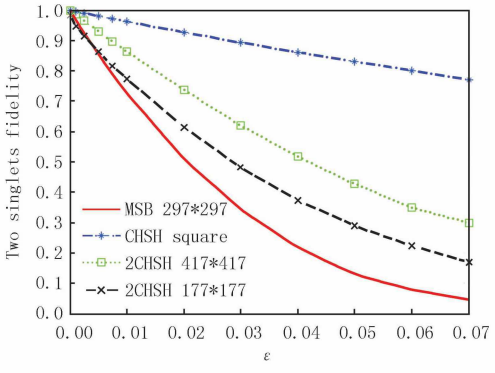
具体的 S 操作为：

$$S \mid \psi\rangle \otimes \mid 0,0\rangle = \sum_{i,j=0}^{1} (S^{i,j} \otimes I) \mid \psi\rangle \otimes \mid i,j\rangle, \tag{34}$$

其中 $S^{0,0}=\prod_{0|0}, S^{0,1}=\prod_{0|3}-\prod_{1|3}+\prod_{2|3}-\prod_{3|3}, S^{1,0}=\prod_{0|3}+\prod_{1|3}-\prod_{2|3}-\prod_{3|3}, S^{1,1}=\prod_{0|3}-\prod_{1|3}-\prod_{2|3}+\prod_{3|3}$.

3.3 鲁棒性

图 4 给出双 CHSH 方案和魔方方案的鲁棒性,并将它们与两个独立的 CHSH 测试方案(即两个态是完全分离,利用两次 CHSH 实现其自测试的情形)的鲁棒性进行比较. 显然,两个独立 CHSH 测试方案的鲁棒性更好(由蓝色星点图给出),这是因为用户已经知道被测试的两对态是分离的. 双 CHSH 方案的鲁棒性由红绿色方点图及黑色叉点图线给出(基于不同层的 Γ 矩阵),魔方方案的鲁棒性由红色实线给出. 之所以其中 Γ 矩阵的大小不同是因为双方的测量基个数不同,在考虑到层次分析第三层时,对应的 Γ 矩阵的大小也不同. 尽管 Γ 矩阵的大小不同,还是可以看出双 CHSH 方案的鲁棒性优于魔方方案.



其中MSB为魔方方案的鲁棒性,绿线和黑线均为双CHSH的鲁棒性,297*297,417*417和177*177代表对应的Γ矩阵的大小.

图4 双CHSH方案和魔方方案的鲁棒性(无量纲图)

4 非单态系统的自测试

事实上除了上述单态自测试之外,还存在很多其他的量子态及对应的测量操作构成的量子系统可以实现自测试,在这里将对目前已知的可实现自测试的量子态进行介绍.

4.1 基于 qubit 自测试的扩展

单态实际上为两-qubit 最大纠缠态,在其上发展起来的自测试方法本质上是基于 qubit 的. 事实上这种成熟的 qubit 自测试的技术,可以扩展到由两方 qubit 或多个-qubit 构成的系统上. 因此部分两粒子纠缠态和高维多 qubit 量子态的自测试也就变得容易了. 如目前已知的图态[7],ω 态的自测试[10],其参与方局域同构映射的构造都如图 2 中的参与方所示,只是其中的控制操作的定义和参与方的个数有所不同罢了.

这里以两粒子部分纠缠态为例,考虑(2,2,2,2)情形,记 Alice 和 Bob 两方执行的 2 个测量分别为 A_1, A_2 和 B_1, B_2. 此时的目的是要自测试系统中的量子态 $|\psi\rangle_\theta=\cos(\theta)|00\rangle+\sin(\theta)|11\rangle$ 和这 4 个测量. 执行多轮实验之后,如果观察到的输入输出概率分布满足如下条件:

$$I_\alpha=\alpha\langle A_0\rangle+\langle A_0B_0\rangle+\langle A_0B_1\rangle+\langle A_1B_0\rangle-\langle A_1B_1\rangle=\sqrt{8+2\alpha^2}, \tag{35}$$

则存在图 2 所示的局域同构映射,可交换出量子态 $|\psi\rangle_\theta$ 和相应的 4 个测量(这些测量平均分布在 Bloch 球面上,这里不再给出它们的具体形式). 也就是说,在局域同构映射等价的意义下,可以确定系统中的量子态就是 $|\psi\rangle_\theta(\sin(2\theta)=\sqrt{(4-\alpha^2)/(4+\alpha^2)})$,而测量就是上述 4 个测量.

利用上述提到的 SOS 分解方法,可以推导出使得 I_α 达到最大违背值的量子态及测量操作必满足以下关系式

$$A_0|\psi\rangle=B_0|\psi\rangle, \tag{36}$$

$$\sin(\theta)A_1(I+B_0)|\psi\rangle=\cos(\theta)B_1(I-A_0)|\psi\rangle. \tag{37}$$

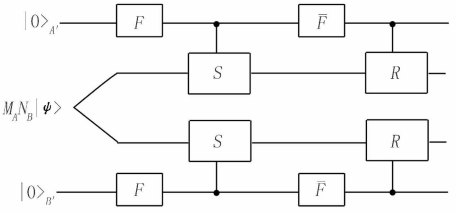
由此可以定义出如图 2 所示的局域同构映射操作,只是此时其中的控制操作为 $Z'_A=A_0, X'_A=A_1; Z'_B=\frac{B_0+B_1}{2\cos(u)}, X'_B=\frac{B_0-B_1}{2\sin(u)}$,其中 $\tan(u)=\sin(2\theta)$.

4.2 非基于 qubit 系统的自测试

此种高维系统不再是由 many-qubit 构成,如 qudit 系统. 为了能够自测试这样的系统,首先需要解决的两个问题可能是:1)寻找合适的局域同构映射操作;2)定义恰当的 bell 方案,尤其是需要大量输入输出的. 第一点可以由前面 qubit 技术的启发得到下面的图 5,其中 R 及 S 分别定义为形式:$R_{AA'/BB'}|\psi\rangle_{AB}|k\rangle_{A/B}=x^{(k)}_{A/B}$

$|\psi\rangle_{AB}|k\rangle_{A/B}, S_{AA'/BB'}|\psi\rangle_{AB}|k\rangle_{A/B}=z_{A/B}^{(k)}|\psi\rangle_{AB}|k\rangle_{A/B}$. 不幸的是，对于第二点，即使这样的 bell 方案是存在的，找到它也是非常困难的任务. 而且，已经有很多证据证明，即使找到这样的 bell 方案也不一定能够再利用 SOS 分解方法. 如(3,3,2,2)方案的 bell 不等式实际上并没有最优的 SOS 分解. 所以只能通过观测到的统计关系直接推测. 这里简要介绍文献[9]给出的关于量子态 $|\psi_{targ\ et}\rangle=\sum_{i=0}^{d-1}c_i|ii\rangle$ 及测量的自测试方案.

考虑(3,4,d,d)情形，记 Alice 和 Bob 两方执行的 2 个测量分别为 $\{A_0,A_1,A_2\}$ 和 $\{B_0,B_1,B_2,B_3\}$. 此时的目的是要自测试系统中的量子态 $|\psi_{targ\ et}\rangle=\sum_{i=0}^{d-1}c_i|ii\rangle$ 和这 7 个测量. 执行多轮实验之后，可以得到如图 6 所示的统计值. 这样的表格有 xy 个. 实际上根据态的特点，存在一些测量基使得得到的 T_{xy} 是 2 * 2 块对角化的矩阵. 每一块都可以看成 2⊗2 维的空间，Alice 与 Bob 各 2 维. 在这样的测量操作下，被测量子态相邻的两方之间可以看成一个整体，如图 7 所示. 其中每个小 m 块都对应于两粒子部分纠缠态的情形. 当然仅是(0,1),(2,3),……,($d-2$,$d-1$)的划分并不能最终恢复出整个量子态，只有加上交叉项才能恢复出整个需要验证的量子态. 具体地，对于测量 $x,y\in\{0,1\}$，测量结果 a，$b\in\{0,1\},\{2,3\},\cdots,\{d-2,d-1\}$，对应的 T_{xy} 是 2 * 2 块对角化的矩阵，此时 m 块的统计概率值使得偏 Bell 不等式(对不同的块，不等式的参数不同)达到最大违背[9]，由此可知 m 块对应的量子态正比例与 $c_{2m}|2m,2m\rangle+c_{2m+1}|2m+1,2m+1\rangle$. 对于测量基 $x\in\{0,2\}$，$y\in\{2,3\}$，测量结果记为 $a,b\in\{1,2\},\{3,4\},\cdots,\{d-2,0\}$. 类似的，此时 m 块对应的量子态正比例与 $c_{2m+1}|2m+1,2m+1\rangle+c_{2m+2}|2m+2,2m+2\rangle$.



其中F为Fourier变换，$\bar{F}$为逆Fourier变换. 此时附加系统$|0\rangle_{A'}$与$|0\rangle_{B'}$的维度为d，和目标量子态同维.

图5　用于自测试高维bell非最大纠缠态$|\psi_{targ\ et}\rangle$的swap操作

$T_{x,y}:=$

$a\backslash b$	0	1	…	$d-1$
0	$P(0,0\mid x,y)$	$P(0,1\mid x,y)$	…	$P(0,d-1\mid x,y)$
1	$P(1,0\mid x,y)$	$P(1,1\mid x,y)$	…	$P(0,d-2\mid x,y)$
⋮	⋮	⋮	⋮	⋮
$d-1$	$P(d-1,0\mid x,y)$	$P(d-1,1\mid x,y)$	…	$P(d-1,d-1\mid x,y)$

图 6　T_{xy}用于统计输入为$\{x,y\}$输出为$\{a,b\}$的条件概率值

最后通过子系统之间的关系，推得，

$$Z_{A/B}=\sum_{k=0}^{d-1}w^k p_{A/B}^k, \tag{38}$$

$$p_A^k|\psi\rangle=p_B^k|\psi\rangle,\forall k, \tag{39}$$

$$X_A^k P_B^k|\psi\rangle=\frac{c_k}{c_0}(X_B^k)^+ P_B^0|\psi\rangle, \tag{40}$$

其中 X_A^K, X_B^K, Z_A, Z_B 为酉运算，由 Alice 及 Bob 实际采用的测量操作来定义，$\{p_A^k\},\{p_B^k\}$ 为完备的正交投影算符. 此时存在如图 5 所示的局域同构映射，在此映射下量子态变为 $|\psi_{targ\ et}\rangle=\sum_{i=0}^{d-1}c_i|ii\rangle$，测量变为相对应的测量. 此外读者可以参看文献[31]，在该文献中作者指出高维 Magic Square 也可以实现该量子态及测量系统的自测试.

5　结　论

测试量子设备的可信性是各种量子信息处理任务中的重大需求. 量子系统可以实现“设备自己测试自己”，这种测试方法就是自测试. 自测试是设计设备无关量子密码协议及其他量子信息任务的理论基础.

实际上，通过一种自测试方案能确保量子系统中相应的态和测量的可信性，而由这种态和测量可以完成的量子信息任务，就可以看作是设备无关的，或者说是可信的. 相对于各种各样的量子信息处理任务来说，上述量子系统自测试的成果还只是冰山一角. 因此，寻找更多可以完成自测试的态、给出更多不同的自测试方案，具有重要的理论意义和应用价值. 相关成果有助于发现更多可以在设备无关前提下完成的量子信息处理

任务,特别是设备无关量子密码任务.这对于理解量子力学到底能给密码学带来什么样的变革有重要的指引作用,而实现更多量子密码协议也有利于推动量子密码与传统密码的融合.

本文介绍了量子系统自测试的研究进展,包括自测试的概念、单态自测试方案和非单态自测试方案.希望本文可以使读者对量子系统自测试有一个初步的了解,并对相关研究起到一定的启发作用.

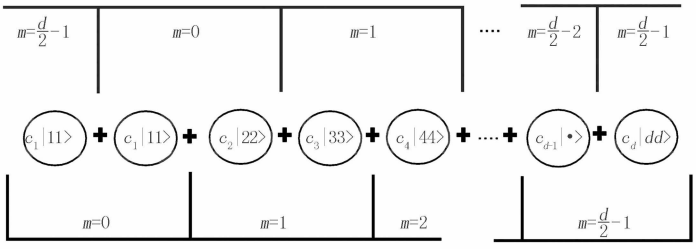


图7 将相邻的两方作为一个子系统,通过验证子系统恢复出整个系统

参 考 文 献

[1] Clauser J F, HorneM A, Shimony A, et al. Proposed Experiment to Test Local Hidden-Variable Theories[J]. Phys Rev Lett, 1969, 23:880.

[2] Summers S J, Werner R F. Maximal violation of Bell's inequalities is generic in quantum field theory[J]. Commun Math Phys, 1987, 110: 247.

[3] Popescu S, Rohrlich D. Which states violate Bell's inequality maximally? [J]. Phys Lett A 1992, 169:411.

[4] Tsirelson B, Hadronic S. Some results and problems on quantum Bell-type inequalitie[J]. J Supp, 1993, 8:329-345.

[5] Mayers D, Yao A. Self testing quantum apparatus[J]. Quant Inf Comp, 2004, 4: 273-286.

[6] Franz T, Furrer F, Werner R F. Extremal Quantum Correlations and Cryptographic Security[J]. Phys Rev Lett, 2011, 106:250502.

[7] McKague M. Self-testing graph states[EB/OL]. [2017-01-09]. http://arxiv.org/abs/1010.

[8] Yang T H, Navascues M. Robust self-testing of unknown quantum systems into any entangled two-qubit states[J]. Phys Rev A, 2013, 87: 050102.

[9] Coladangelo A, Goh K T, Scarani V. All Pure Bipartite Entangled States Can be Self-Tested[EB/OL]. [2017-01-09]. http://arxiv.org/abs/1611.08062v1.

[10] Wu X Y, Cai Y, Yang T H, et al. Robust self-testing of the three-qubit W state[J]. Phys Rev A, 2014, 90:042339.

[11] Wang Y K, Wu X Y, Scarani V. All the self-testings of the singlet for two binary measurements[J]. New J Phys, 2016, 18:025021.

[12] Šupic I, Augusiak R, Salavrakos A, et al. Self-testing protocols based on the chained Bell inequalities[J]. New J Phys, 2016, 18: 035013.

[13] McKague M. Self-testing in parallel[J]. New J Phys, 2016, 18:045013.

[14] Li H W, Pawlowski M, Yin Z Q, et al. Semi-device-independent randomness certification using $n\to 1$ quantum random access codes[J]. Phys Rev A, 2012, 85:052308.

[15] Wang Y K, Qin S J, Song T T, et al. Effects of relaxed assumptions on semi-device-independent randomness expansion[J]. Phys Rev A, 2014, 89:032312.

[16] Lo H K, Curty M, Qi B. Measurement-Device-Independent Quantum Key Distribution[J]. Phys Rev Lett, 2012, 108:130503.

[17] Šupic I, Hoban M J. Self-testing through EPR-steering[J]. New J Phys, 2016, 18 (7):075006.

[18] Acín A, Brunner N, Gisin N, et al. Device-Independent Security of Quantum Cryptography against Collective Attacks[J]. Phys Rev Lett, 2007, 98:230501.

[19] Pironio S, Acín A, Massar S, et al. Random numbers certified by Bell's theorem[J]. Nature, 2010, 464:1021.

[20] Bancal J D, Gisin N, Liang Y C, et al. Device-Independent Witnesses of Genuine Multipartite Entanglement [J]. Phys Rev Lett, 2011, 106:250404.

[21] Gallego R, Brunner N, Hadley C, et al. Device-Independent Tests of Classical and Quantum Dimensions[J]. Phys Rev Lett, 2010, 105: 230501.

[22] Cirel'son B S. Quantum generalizations of Bell's inequality[J]. Lett Math Phys, 1980, 4:93.

[23] Landau L. Empirical two-point correlation functions[J]. Found Phys, 1988, 18:449.

[24] Bamps C, Pironio S. Sum-of-squares decompositions for a family of CHSH-like inequalities and their application to self-testing[J]. Phys Rev A, 2015, 91:052111.

[25] Navascués M, Pironio S, Acin A. A convergent hierarchy of semi-definite programs characterizing the set of quantum correlations[J].

Phys Rev Lett，2007，98：010401 .
[26] McKague M，Yang T H，Scarani V J. Robust self-testing of the singlet[J]. Phys. A：Math. Theor，2012，45：455304.
[27] Kaniewski J. Analytic and (nearly) optimal self-testing bounds for the Clauser-Holt-Shimony-Horne and Mermin inequalities[J]. Phys Rev Lett. ，2016，117：070402.
[28] Wu X Y，Bancal J D，McKague M，et al. Device-independent parallel self-testing of two singlets[J] . Phys Rev A，2016，93：062121.
[29] Mermin N D. Simple unified form for the major no-hidden variables theorem[J]. Phys Rev Lett，1990，65：3373-3376.
[30] Rosset D，Branciard C，Barnea T J，et al. Nonlinear bell inequalities tailored for quantum networks[J]. Phys Rev Lett，2016，116：010403.
[31] McKague M. Self-testing high dimensional states using the generalized magic square game，[EB/OL]. [2017-01-09] . http：//arxiv. org/abs/1605. 09435v1 .

Research of Self-testing of Quantum System

Gao Fei，Wang Yukun，Qin Sujuan，Wen Qiaoyan

(State key Laboratory of Networking and Switching Technology，Beijing University of Posts and Telecommunications，Beijing 100876，China)

Abstract：Self-testing refers to the possibility of characterizing uniquely the state and the measurements contained in quantum devices. It is based on the observed classical input-output statistics. This is a formidable task and is impossible in the classical world；however in quantum physics，the peculiar phenomena of non-locality can make this task possible. Self-testing provides fundamental basis for device independent quantum cryptography protocols. In this paper，we will summarize the progress made in self-testing research. Firstly，we will introduce some self-testing criterion for the quantum system constructed by two-qubit maximum entangled state (singlet) and the corresponding measurements. The criterion including both of two scenarios，one copy of singlet and two parallel of singlets. For one copy of singlet，there are CHSH criteria，Mayers-Yao criteria，(2，2，2，2) universal criteria and (N，N，2，2) Chain-Bell criteria；while for the two parallel of singlets，there are double-CHSH criteria and Magic Square Criteria. Then we will show how expand our analysis of the singlet to the case of any entangled two qubits and high dimensional states briefly. In the end of the paper，we look forward to the future of self-testing.

Keywords：self-testing；quantum cryptography；device-independent；entanglement

[责任编辑　陈留院]