第 29 卷 第 1 期 量 子 电 子 学 报 Vol.29 No.1
2012 年 1 月 CHINESE JOURNAL OF QUANTUM ELECTRONICS Jan. 2012

DOI: 10.3969/j.issn.1007-5461. 2012.01.011

基于量子隐写术的计算安全比特承诺协议

曹 东 [1,2], 宋耀良 [1]

(1 南京理工大学电子工程与光电技术学院, 江苏 南京 210094 ;
2 南京邮电大学通信与信息工程学院, 江苏 南京 210003)

摘 要: 在量子比特承诺协议中, 目前流行的方案没有很好地解决信道噪声的影响, 实用性不强。根据量子隐写术对信息的隐藏性, 提出一种新的量子比特承诺协议。提出了利用量子信道噪声结合遮盖比特隐藏敏感信息, 同时采用量子纠错码的方法克服信道噪声, 有效地抵抗了第三方窃听攻击和噪声对信息的影响和破坏。通过理论分析与仿真证明该协议的绑定性和完善隐蔽性; 理论证明了方案的有效性, 为量子密码协议的推广应用提供了理论基础。

关 键 词: 量子信息; 量子密码; 比特承诺; 量子隐写术

中 图 分 类 号: O431.2 **文 献 标 识 码:** A **文章编号:** 1007-5461(2012)01-0063-06

Computationally secure bit commitment protocol based on quantum steganography

CAO Dong[1,2], *SONG Yao-liang*[1]

(1 School of Electronic Engineering and Optoelectronic Technology, Nanjing University of Science and Technology, Nanjing 210094, China ;
2 College of Communication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China)

Abstract: In quantum bit commitment (QBC), most existed proposals analyze little of communicating an innocent message over noisy quantum channels. These methods are not practical. Based on the information hiding characteristics of quantum steganography, a novel QBC protocal is proposed. An elegant scheme is presented for disguising secret information as quantum noise, and embedding it in stego qubits which encode into a codeword of quantum error-correcting code. The method is proved secure and effective in the presence of noisy quantum channel and it's a potential eavesdropper. The results of theoretical analysis and numerical simulation show that the proposed scheme has perfect concealing and binding properties. Theoretical analysis proved the validity. The method forms a theoretical basis for the promotion and application of quantum cryptographic protocols.

Key words: quantum information; quantum cryptography; bit commitment; quantum steganography

基金项目: 国家自然科学基金 (61071145, 41074090) 、教育部博士点专项基金 (200802880014) 资助课题

作者简介: 曹 东 (1974 -), 博士生, 讲师, 主要研究领域为量子信息安全。 **E-mail:** caodongcn@gmail.com
导师简介: 宋耀良 (1960 -), 教授, 博士生导师, 研究方向为自适应信号处理, 量子信息, 通信系统理论与设计。
E-mail: ylsong@mail.njust.edu.cn

收稿日期: 2011–05–16; **修改日期:** 2011–07–01

1 引 言

一般而言，比特承诺 (Bit commitment, BC) 是密码学的重要基础协议之一，基本思想是：发送者发送一个证明给接收者作为承诺，内容是一个比特 0 或者 1 (也可以是多个比特的比特串) 。一方面，发送者未打开承诺之前，接收者无法知道发送者承诺的信息，为隐蔽性；另一方面，发送者不能打开一个与最初承诺相反的比特，即发送者无法篡改承诺的比特以欺骗接收者，为绑定性。作为构造密码协议的基本元素，比特承诺可用于构建掷币协议、零知识证明和秘密共享等，在安全多方计算中有着重要应用。

比特承诺的概念最早于 1982 年由 Blum 提出 [1] 。然而，经典比特承诺对承诺者和接收者的计算能力做了限制性假设 [2,3], 这在量子计算环境下很容易遭受攻击而变得不再安全。参照经典比特承诺协议人们提出量子比特承诺方案， Brassard 等根据量子物理法则，第一次完整证明了除非以任意小的概率，协议中的参与者都不可能成功欺骗，并且该协议可以在现有技术基础上实行 [4], Andrew 在希尔伯特空间中概率事件的分析做了一些数学技巧上的改进 [5], 并且证明了对抗相干测量的规范量子茫然传输协议的安全性。随后， Mayers 和 Lo 等相继证明方案不能抵抗量子纠缠攻击即不具有无条件安全性 [6,7] 。转而研究基于有条件安全的量子比特承诺协议， 2008 年 Ramos 等提出无需借助量子内存可在现有技术基础上实现的一种量子比特承诺协议 [8] 。 Magnin 等扩展了 no-go 定理到连续变量协议 [9] 。 Li 等提出 no-go 定理既适用于静态量子比特承诺也适用于非静态情形，并给出相应示例 [10] 。 Chailloux 等提出一种量子比特承诺的优化约束方法，该方法利用量子效应结合弱的抛币协议 [11], 表明任意经典比特承诺协议通过完美抛币协议可获得的欺骗概率小于 3/4 。然而，上述论文主要工作集中在研究协议本身的绑定性和隐蔽性的安全，而对协议在实际应用中信道噪声对协议的影响较少涉及，协议实施过程中通信信道容易遭受到的第三方窃听攻击的问题也未解决。

本文给出量子计算环境下一种比特承诺协议，并证明了该协议具有绑定性和完善隐蔽性，本文构建的量子比特承诺协议利用量子隐写技术，采用遮盖隐写方法有效地抵抗了第三方的攻击或窃听，有效地利用信道噪声掩盖和隐藏了敏感信息，同时在通信中采用量子纠错码编码信息有效抵抗信道噪声的影响，避免了噪声对信息的破坏。在安全性和抗窃听方面均优于其他各类比特承诺方案。

2 基于量子隐写术的比特承诺协议

早期的量子比特承诺协议 [4~10] 只是考虑其绑定性和隐蔽性，并未深入研究客观存在的量子信道噪声，以及考虑窃听者对协议实施的影响。本文的协议兼顾考虑了信道噪声和攻击者存在的因素，基于量子隐写术 [12,13] 构造一种量子计算安全的比特承诺协议。

隐写术是将待隐藏的秘密信息嵌入到普通消息中的方法，本文采用将量子信息隐匿到量子纠错码的码字中构成量子隐写术，假设传输通过的信道为一般的退极化信道，发送者把信息伪装成信道错误，通过共享密钥接收者可以很容易恢复隐匿信息，而窃听者却无法将信息从噪声中分离出来，在他看来是一片噪声而已，采用量子隐写术的方法可以很好地抵抗第三方攻击和窃听，因为对于窃听者而言面临两方面的困难，一是很难有效侦测到信道上正在传输秘密信息，二是即使怀疑已有秘密信息在传送由于没有共享密钥所以也无法读取。

系统模型中假设信道为退极化信道，协议实现之前对系统作如下初始化：

Alice 选取 n 个量子比特的直积态 $|\varphi_1\varphi_2\cdots\varphi_i\cdots\varphi_n\rangle(\varphi_i\in\{0,1\},i=1,2,\cdots n)$ 向 Bob 发送用于测试信道状态，以获得量子信道状态信息 (Quantum channel state information, QCSI) 。此处考虑退极化信道，得到信道对通过它的量子比特退极化概率，即单量子比特被信道作用后变换为完全混合态 $I/2$ 。

Bob 根据接收到的测试量子比特，获得退极化概率 p 。 Bob 根据此信道状态制备一串随机量子态 $|\varphi_{\rm B}\rangle=|b_1b_2\cdots b_k\rangle$, 采用恰当的量子纠错码 (此处采用稳定码) 编码量子态

$$|\varphi_{\rm B}\rangle_{\rm L}|b_1b_2\cdots b_k\rangle_{\rm L}=\prod_{j=1}^{k}(-1)^{b_j}\bar{Z}_j\Big[\sum_{M\in S}M|00\cdots0\rangle\Big]\ , \tag{1}$$

无差错地传送给 Alice 。同时将 QCSI (概率 p) 反馈给 Alice 。

Alice 根据接收到来自 Bob 的 QCSI (概率 p), 设置隐写概率 q, 满足 diamond 范数 [14~16]

$$\mathrm{dist}(D_{p_{\rm Eve}}^{\otimes N}-D_p^{\otimes N})=||D_{p_{\rm Eve}}^{\otimes N}-D_p^{\otimes N}||_\diamond=\sum_{i=0}^{N}\left(\begin{array}{c}N\\i\end{array}\right)|p_{\rm Eve}^i(1-p_{\rm Eve})^{N-i}-p^i(1-p)^{N-i}|\le\xi\ . \tag{2}$$

公式 (1) 中的 $\mathrm{dist}(D_{p_{\rm Eve}}^{\otimes N}-D_p^{\otimes N})$ 表示退极化信道分别对应错误概率 $p_{\rm Eve}$ 和 p 时对于 N 长量子比特作用的差异。其中信道中的攻击者 Eve 能够观测的退极化信道错误概率 $p_{\rm Eve}=p+\delta p=p+q(1-4p/3)$, 实际上是 Alice 在原有信道上加入隐写构造的隐写信道，即需要满足 $\delta p<\xi\sqrt{p(1-p)/N}$ 和 $q=\delta p/(1-4p/3)$, ξ 为一小正数。

在退极化信道模型下，根据信道特征 [12]

$$D_{\rm channel}\rho=(1-4p/3)\rho+(4p/3)(1/4)(\rho+X\rho X+Y\rho Y+Z\rho Z)=(1-4p/3)\varsigma\rho+(4p/3)\Xi\rho\ , \tag{3}$$

其中 $\varsigma\rho=\rho$, $\Xi\rho=(1/4)(\rho+X\rho X+Y\rho Y+Z\rho Z)$ 。 N 量子比特中有 Q 个量子比特处于完全混合态，对应隐写概率 q 的关系满足

$$q=\left(\begin{array}{c}N\\Q\end{array}\right)(4p/3)^Q(1-4p/3)^{N-Q}\ , \tag{4}$$

至此，初始化完成。下面给出量子比特承诺协议模型。

1) 承诺阶段

Step 1 Alice 生成要承诺的量子比特 $|\varphi_{\rm A}\rangle$, 结合 Bob 发送来的随机量子比特串 $|\varphi_{\rm B}\rangle$ (已将 $|b_1b_2\cdots b_k\rangle_{\rm L}$ 译码), 合并为直积态 $|\varphi_{\rm AB}\rangle=|\varphi_{\rm A}\rangle\otimes|\varphi_{\rm B}\rangle$ 。

Step 2 Alice 将 $k+1$ 长量子比特 $|\varphi_{\rm AB}\rangle$ 编码为 $[[M,\ k+1]]$ 量子纠错码。

Step 3 Alice 另选 $\kappa_{\rm c}$ 个 '遮盖量子比特' (实际上不包含有效信息), 采用 $[[N,\ \kappa_{\rm c}]]$ 量子纠错码编码到 N 个量子比特，满足 $N\gg M$ 。

Step 4 使用随机密钥 x, Alice 从 N 个量子比特中随机选取包含 M 个量子比特的子集 (共有 $C(N,\ M)$ 种) 之一，用 Step 2 中的包含 $k+1$ 个隐写量子比特的 M 长码字交换这一子集，并且随机选取这个子集之外的少量具有完全混合态量子比特中的 m 个量子比特，满足 $Q=M+m$, 并且精确匹配公式 (3) 的分布。

Step 5 Alice 根据 $2M$ 比特共享密钥，对 M 个交换量子比特实施退极化操作 (线路实现见图 1) 。即应用随机选取的 Pauli 矩阵 I, X, Y 或 Z 其中之一，分别作用于每个交换量子比特，其中 I 表示单位矩阵， X 表示比特翻转操作， Z 表示相位翻转操作， Y 表示比特和相位翻转操作。 $\rho\to\Xi\rho$, 则

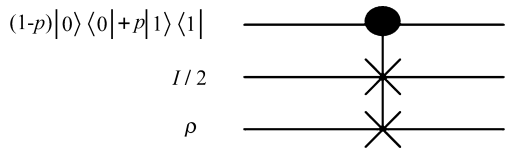

Fig.1　Circuit implementation of the depolarizing channel[17]

$$\Xi\rho=(1/4)(\rho+X\rho X+Y\rho Y+Z\rho Z)\ , \tag{5}$$

这些量子比特对于没有共享密钥的 Eve 来说呈现出完全混合态。

Step 6 Alice 发送经过操作后的码字 N 到 Bob 。

2) 打开阶段

Step 1 Alice 发送随机密钥 x 和 $2M$ 比特共享密钥到 Bob 。 Bob 根据密钥得到子集 M 量子比特，译码得 $|\varphi'_{\mathrm{AB}}\rangle$ 。

Step 2 Bob 提取 $|\varphi'_{\mathrm{AB}}\rangle$ 中的随机量子比特串 $|\varphi'_{\mathrm{B}}\rangle$ 对照 $|\varphi_{\mathrm{B}}\rangle$ 验证其是否相等，是，则 Bob 接收 $|\varphi_{\mathrm{A}}\rangle$ 。

3 协议的安全性分析

3.1 隐蔽性

定理 1 基于隐写术的量子比特承诺方案是完善隐蔽的，即在打开之前接收方无法获得任何承诺信息。

证明：承诺阶段 Step 3 采用纠错编码 $[[N,\kappa_{\mathrm{c}}]]$, Bob 得到的码字 N 对应的消息 κ_{c} 本身是遮盖消息不含信息，所以即使成功译码也不能得到承诺信息，此处编码主要起辅助扩充密钥空间作用和隐写作用；从 N 个量子比特中随机选取包含 M 个量子比特的子集共有 $C(N,M)$ 种，实施退极化操作需要 $2M$ 个比特作标签，所以相对于 N 长比特共需要的密钥数为 $\log_2(C(N,M))+2M$ 。所以可以得到相对密钥率的分布函数 $K=[\log_2(C(N,M))+2M]/N$ (已知其中 $M/N=4q/3$) 如下

$$K=\log_2\frac{N!}{M!(N-M)!}+\frac{8q}{3}\approx\log_2\frac{\sqrt{2\pi N}(N/e)^N}{\sqrt{2\pi M}(M/e)^M\sqrt{2\pi N-M}(N-M/e)^{N-M}}+\frac{8q}{3}\approx$$

$$\log_2\left\{\left(\frac{3-4p}{\delta p}\right)^{\frac{4\delta p}{3-4p}}\left[\frac{3-4p(1+\delta p)}{3-4p}\right]^{\frac{4p(1+\delta p)-3}{3-4p}}\right\}. \tag{6}$$

K 的分布见图 2 。在具有相同密钥率 K 的情况下 δ_p 和 p 满足图 3 所示的关系，当 N 逐渐增大时，协议所形成的密钥空间对 Bob 来说依概率具有计算复杂性意义上的完全不确定度，所以本协议具有完善隐蔽性。

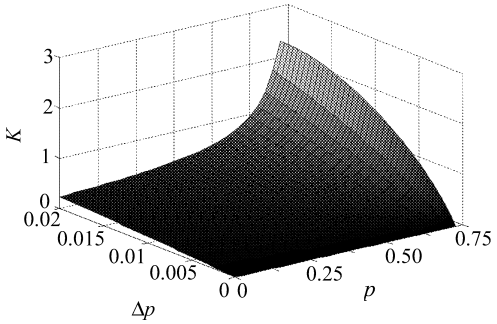

Fig.2 Distribution of the relative key rate

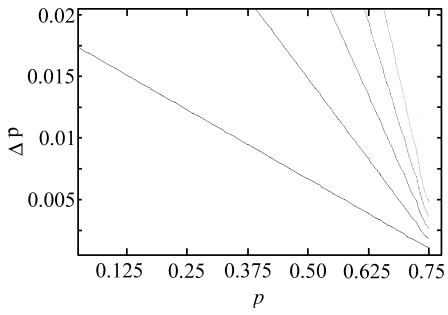

Fig.3 Distribution relationship between δ_{p} and p

3.2 绑定性

定理 2 第 2 节的量子比特承诺方案中的承诺者无法在打开承诺阶段改变自己的承诺比特而不被接收者发现，即承诺者不可能作弊成功。

证明：在初始化阶段， Bob 制备随机量子态 $|\varphi_{\mathrm{B}}\rangle=|b_1b_2\cdots b_k\rangle$ 并发送给 Alice, Alice 将其和承诺比特合并后发送给 Bob, 如果 Alice 在打开阶段作弊，则 Bob 必然发现 $|\varphi_{\mathrm{B}}\rangle$ 已经改变，所以承诺者不可能作弊成功。

3.3 抵抗信道攻击

为抵抗 Eve 的信道窃听，一般采用的方法是对信息加密之后通过信道发送 [18], 这一类安全基于公钥密码或对称密码的安全性，前提其实已经暗含 Alice 和 Bob 的通信已经被 Eve 发觉。本协议运用适宜的隐写概率有效地利用信道噪声掩盖传输的信息，可以避免引起 Eve 的怀疑，从而巧妙抵抗第三方攻击。

定理 3 满足条件

$$||D_{p_{\mathrm{Eve}}}^{\otimes N}-D_p^{\otimes N}||_{\diamondsuit}=\sum_{i=0}^{N}\left(\begin{array}{c}N\\i\end{array}\right)|p_{\mathrm{Eve}}^{i}(1-p_{\mathrm{Eve}})^{N-i}-p^{i}(1-p)^{N-i}|\le\xi \tag{7}$$

的隐写概率 q, 则攻击者无法以任意不可忽略的概率区分信道截获的消息是否含有信息。其中

$$p_{\mathrm{Eve}}=p+\delta p=p+q(1-4p/3)\ , \tag{8}$$

$D_{p_{\mathrm{Eve}}}$ 和 D_p 表示错误概率分别是 p_{Eve} 和 p 时退极化信道作用的超算子。

证明： D 为某任意超算子， $T(H)$ 和 $T(H')$ 分别为作用于希尔伯特空间 H 和 H' 上的线性算子空间。令 D: $T(H)\to T(H')$, 则 diamond 范数 D 为 $||D||_{\diamondsuit}=||I_{T(H)}\otimes D||_1$, 其中

$$||D||_1=\max\Big\{||D(X)||_1:X\in T(H)\ ,\ ||X||_1\le 1\Big\}\ . \tag{9}$$

已知

$$(D_{p_{\mathrm{Eve}}}-D_p)(\rho)=(p-p_{\mathrm{Eve}})\rho+(1/3)(p_{\mathrm{Eve}}-p)(X\rho X+Y\rho Y+Z\rho Z)\ , \tag{10}$$

设 $N=3$ 时最大化范数的密度矩阵

$$\rho=\phi\otimes|\Theta\rangle\langle\Theta|\ ,\ |\Theta\rangle=1/\sqrt{2}(|000\rangle+|111\rangle)\ , \tag{11}$$

则

$$\begin{aligned}&(D_{p_{\mathrm{Eve}}}^{\otimes 3}-D_p^{\otimes 3})(\rho)=[(1-p_{\mathrm{Eve}})^3-(1-p)^3]\rho+[(p_{\mathrm{Eve}}/3)(1-p_{\mathrm{Eve}})^2-(p/3)(1-p)^2]\times\\&(X_1\rho X_1+Y_1\rho Y_1+Z_1\rho Z_1+X_2\rho X_2+\cdots+Z_3\rho Z_3)+[(p_{\mathrm{Eve}}/3)^2(1-p_{\mathrm{Eve}})-(p/3)^2(1-p)]\times\\&(X_1X_2\rho X_1X_2+X_1Y_2\rho X_1Y_2+X_1Z_2\rho X_1Z_2+Y_1X_2\rho Y_1X_2+\cdots+Z_2Z_3\rho Z_2Z_3)+\\&[(p_{\mathrm{Eve}}/3)^3-(p/3)^3](X_1X_2X_3\rho X_1X_2X_3+\cdots+Z_1Z_2Z_3\rho Z_1Z_2Z_3)\ .\end{aligned} \tag{12}$$

所以，得到 3 量子比特时的 diamond 范数为

$$\begin{aligned}||D_{p_{\mathrm{Eve}}}^{\otimes 3}-D_p^{\otimes 3}||_{\diamondsuit}=&|(1-p_{\mathrm{Eve}})^3-(1-p)^3|+9|(p_{\mathrm{Eve}}/3)(1-p_{\mathrm{Eve}})^2-(p/3)(1-p)^2|+\\&27|(p_{\mathrm{Eve}}/3)^2(1-p_{\mathrm{Eve}})-(p/3)^2(1-p)|+27|(p_{\mathrm{Eve}}/3)^3-(p/3)^3|=\\&|(1-p_{\mathrm{Eve}})^3-(1-p)^3|+3|p_{\mathrm{Eve}}(1-p_{\mathrm{Eve}})^2-p(1-p)^2|+\\&3|p_{\mathrm{Eve}}^2(1-p_{\mathrm{Eve}})-p^2(1-p)|+|p_{\mathrm{Eve}}^3-p^3|\ ,\end{aligned} \tag{13}$$

显然，类推可得， N 量子比特时的 diamond 范数为

$$||D_{p_{\mathrm{Eve}}}^{\otimes N}-D_p^{\otimes N}||_{\diamondsuit}=\sum_{i=0}^{N}\left(\begin{array}{c}N\\i\end{array}\right)|p_{\mathrm{Eve}}^{i}(1-p_{\mathrm{Eve}})^{N-i}-p^{i}(1-p^{N-i})|\ . \tag{14}$$

由此当 $||D_{p_{\mathrm{Eve}}}^{\otimes N}-D_p^{\otimes N}||_{\diamondsuit}\le\xi$ 时， $q=\delta p/(1-4p/3)$ 满足 $\delta p<\xi\sqrt{p(1-p)/N}$, 证毕。

在传输过程中即使 Eve 经过长时间的观察产生怀疑，得到的仅仅是码字对应的 κ_{c} 个遮盖量子比特，因为其本身并不包含有效信息所以对安全性不构成威胁。

4　结　论

量子比特承诺协议是设计其他许多量子安全协议的基础，比如量子掷币协议、量子安全多方计算、量子茫然传送和零知识证明等，研究基于计算安全的量子比特承诺协议对设计高性能的安全协议具有重大意

义。本文从量子计算安全的角度，研究了量子比特承诺协议的绑定性和完善隐蔽性，理论证明了协议的安全性，提出了基于量子隐写术的量子比特承诺协议，通过设置精确隐写概率使得在通信过程中呈现在攻击者面前的信道是一片噪声，将信息隐藏到量子纠错码的码字中再通过信道传输，接收者通过共享密钥重新得到隐藏信息，在抵抗信道窃听和第三方攻击方面优于其他各类协议。

参考文献：

[1] Blun M. Coin flipping by telephone [C]. *Proc. IEEE Sprint CompCom*, Las Vegas, 1982: 133-137.

[2] Naor M. Bit commitment using pseudorandomness [J]. *Journal of Cryptology*, 1991, 2(2): 151-158.

[3] Damgard I, Fujisaki E. An integer commitment scheme based on groups with hidden order [C]. *Advances in Cryptology-ASIACRYPT*, New Zealand, 2002, 125-142.

[4] Brassard G, Crepeau C, *et al.* A quantum bit commitment scheme provably unbreakable by both parties [C]. *Proceedings of 34th Annual IEEE Symposium on the Foundations of Computer Science*, Palo Alto, California, USA, 1993: 362-371.

[5] Andrew C C Yao. Security of quantum protocols against coherent measurements [C]. *Proceedings of 26th Annual ACM Symposium on the Theory of Computing*, Las Vegas, Nevada, USA, 1995, 67-75.

[6] Mayers D. Unconditional secure quantum bit commitment is impossible [J]. *Phys. Rev. Lett.*, 1997, 78: 3414-3417.

[7] Lo H K. Insecurity of quantum secure computations [J]. *Phys. Rev. A*, 1997, 56: 1154-1162.

[8] Ramos R V, Mendonca F A. Quantum bit commitment protocol without quantum memory [OL]. http://arxiv.org/abs/0801.0690v1, 2008.

[9] Magnin L, Magniez F, Leverrier A, *et al.* Strong no-go theorem for Gaussian quantum bit commitment [J]. *Phys. Rev. A*, 2010, 81(1): 010302.

[10] Li Q, Li C, *et al.* On the impossibility of non-static quantum bit commitment between two parties [OL]. http://arxiv.org/abs/1101.5684v1, 2011.

[11] Chailloux A, Kerenidis I. Optimal bounds for quantum bit commitment [OL]. http://arxiv.org/abs/ 1102. 1678v1, 2011.

[12] Shaw B A, Brun T A. Quantum steganography [OL]. http://arxiv.org/abs/1006. 1934, 2010.

[13] Shaw B A, Brun T A. Hiding quantum information in the perfect code [OL]. http://arxiv.org/abs/ 1007. 0793, 2010.

[14] Ben-Aroya A, Ta-Shma A. On the complexity of approximating the diamond norm [OL]. http://arxiv.org/abs/0902. 3397v3, 2009.

[15] Watrous J. Semidefinite programs for completely bounded norms [OL]. http://arxiv.org/abs/0901. 4709v2, 2009.

[16] Benenti G, *et al.* Computing the distance between quantum channels: usefulness of the Fano representation [J]. *Journal of Physics B: Atomic, Molecular and Optical Physics*, 2010, 43(21): 215508.

[17] Nielsen M A, Chuang I L. *Quantum Computation and Quantum Information* [M]. Beijing: Higher Education Press, 2003: 379.

[18] Zhang S L, Zhang S, Wang J. Continuous variable quantum dialogue protocol based on squeezed state [J]. *Chinese Journal of Quantum Electronics* (量子电子学报), 2011, 28(3): 335-340 (in Chinese).