基于纯 W-like 态的量子强盲签名协议*

倪 敏, 查新未
(西安邮电学院 理学院, 西安 710061)

摘 要: 按照三体纯态及其纠缠度量得出纯 W-like 态,提出基于纯 W-like 态的量子强盲签名协议。协议中应用量子密钥分发技术、指纹函数、量子一次一密算法,不仅能够有效隐藏用户身份,而且具有无条件安全、复杂度低及效率高的优点,是实现量子强盲签名协议的新途径。

关键词: W-like 态; 强盲签名; 量子密码; 无条件安全
中图分类号: TP301.2 **文献标志码**: A **文章编号**: 1001-3695(2012)10-3817-03
doi:10.3969/j.issn.1001-3695.2012.10.056

Strong blind quantum signature protocol based on pure W-like state

NI Min, ZHA Xin-wei
(*School of Science, Xi'an University of Posts & Telecommunications, Xi'an* 710061, *China*)

Abstract: Aiming at pure three-qubit states and the measure of entanglement, this paper proposed pure W-like state. Based on pure W-like state, this paper proposed a strong blind quantum signature protocol. The protocol adopted the quantum key distribution, the quantum fingerprint and one-time pad. The protocol ensures that the signature is blind and the message owner is untraceable. Moreover, the protocol provides the unconditionally security, lower complexity and best quantum bit efficiency. This protocol is a novel method for constructing the strong blind quantum signature protocol.

Key words: W-like state; strong blind quantum signature; quantum cryptography; unconditional security

量子信息学是量子力学与信息科学相结合的产物,是以量子力学的态叠加原理为基础,研究信息处理的一门新兴前沿科学。量子信息学包括量子密码术、量子通信、量子计算机等几个方面,近年来在理论和实验上都取得了重大的突破。其中发展速度最快的分支学科是量子密码,它是以经典密码学和量子力学为基础,利用量子效应实现无条件安全的信息交互的一种新型密码体制[1]。目前量子密码学的研究主要包括 QKD 量子密钥分配[2~7]、QSS 量子秘密共享[8]、量子身份认证[9]、量子数字签名[10~15]以及量子安全直接通信等领域。与经典密码学一样,量子保密通信也一定会涉及数字签名问题。

数字签名是现代密码体系中一项重要信息安全技术[16],一套数字签名通常定义两种互补的运算,一种用于签名,另一种用于验证。数字签名是加密的过程,数字签名验证是个解密的过程;数字签名可以为被传送的消息提供认证性、完整性和不可抵赖性,从而成为了现代密码体系中一项重要的信息安全技术。然而随着签名技术在电子商务、电子政务领域的深入应用,普通的数字签名已经不能满足一些应用的特殊需要,比如无法保障签名者的匿名性等。针对这些新的需求,极大地推动了盲签名技术的发展。

2001 年,曾贵华等人[17]提出了一个利用 Greenberger-Horne-Zeilinger(GHZ) 三重态的相干特性实现对量子比特串的签名方案,掀起了研究量子签名的浪潮。同年,Gottesman 等人提出了一个基于量子单向函数(quantum one way function)的量子数字签名方案,该协议利用量子单向函数产生公钥,并采用量子交换来验证签名;Lee 等人[18]提出了两个基于消息自动恢复(message recovery)的仲裁量子数字签名方案;2010 年,李伟等人[14]提出了基于纠缠交换的仲裁量子签名方案;田原、温晓军等人[19,20]也对量子签名进行了深入的研究,提出了诸如量子多重签名、量子盲签名等一些新型的量子签名方案。这些针对量子签名的深入研究,都为研究量子盲签名奠定了良好的基础。本协议提出了基于纯 W-like 态[21]的量子强盲签名协议。

1 纯 W-like 态

三体纯态[21,22]一般可以表示为

$$|\varphi\rangle_{ABT}=(a_0|000\rangle+a_1|001\rangle+a_2|010\rangle+a_3|011\rangle+a_4|100\rangle+a_5|101\rangle+a_6|110\rangle+a_7|111\rangle)_{ABT} \tag{1}$$

纠缠度[23]分别为

$$\tau_{A(BT)}=2(1-tr\rho_A^2)=4\begin{bmatrix}|a_0a_5-a_1a_4|^2+|a_0a_6-a_2a_4|^2+\\|a_0a_7-a_3a_4|^2+|a_1a_6-a_2a_5|^2+\\|a_1a_7-a_3a_5|^2+|a_2a_7-a_3a_6|^2\end{bmatrix} \tag{2}$$

$$\tau_{B(AT)}=2(1-tr\rho_B^2)=4\begin{bmatrix}|a_0a_3-a_1a_2|^2+|a_0a_6-a_2a_4|^2+\\|a_0a_7-a_2a_5|^2+|a_1a_6-a_3a_4|^2+\\|a_1a_7-a_3a_5|^2+|a_4a_7-a_5a_6|^2\end{bmatrix} \tag{3}$$

收稿日期: 2012-02-20; **修回日期**: 2012-03-31 **基金项目**: 国家自然科学基金资助项目(10902083); 陕西省自然科学基金资助项目(2009JM1007)

作者简介: 倪敏(1983-),女,陕西咸阳人,硕士研究生,主要研究方向为量子信息、量子安全通信(minni1983@163.com);查新未(1957-),男,陕西西安人,教授,主要研究方向为量子光学、量子信息与量子通信.

$$\tau_{T(AB)} = 2(1 - tr\rho_C^2) = 4\begin{bmatrix} |a_0a_5 - a_1a_4|^2 + |a_0a_3 - a_1a_2|^2 + \\ |a_0a_7 - a_1a_6|^2 + |a_3a_4 - a_2a_5|^2 + \\ |a_4a_7 - a_5a_6|^2 + |a_2a_7 - a_3a_6|^2 \end{bmatrix} \quad (4)$$

$$\tau_{ABT} = |4H\det(t_{ijk})| \quad (5)$$

其中
$$H\det(t_{ijk}) = (a_0a_7 + a_1a_6 - a_2a_5 - a_3a_4)^2 + 4(a_0a_6 - a_2a_4)(a_3a_5 - a_1a_7) \quad (6)$$

众所周知,可将 W 态表示为

$$|W\rangle_{ABT} = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)_{ABT} \quad (7)$$

很容易得到

$$\tau_{ABT} = 0, \tau_{A(BT)} = \tau_{B(AT)} = \tau_{T(AB)} = \frac{8}{9}$$

进而可得到纯 W-like 态:

$$|\phi\rangle_{ABT} = \frac{1}{2\sqrt{6}}(3|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - 3 - |111\rangle)_{ABT} \quad (8)$$

从式(8)可以发现,如果 Alice、Bob 及 Trent 分别通过 D-basis $= \left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$测量纯 W-like 态的第一个、第二个和第三个粒子,那么它们的测量结果之间满足 $R_B = R_A \oplus R_T$。

因此,可以将上述原理应用到强盲签名协议中:假定消息的拥有者 Alice、签名者 Trent 及验证者 Bob 分别拥有纯 W-like 态的光子 A、T、B,则消息拥有者 Alice 测量自己的光子可以传递消息;签名者 Trent 测量自己的光子则可以对该消息进行签名,由于签名者 Trent 只获取了一个光子的状态信息,签名者无法知道消息的内容而使签名具有盲性;验证者 Bob 结合自己和签名者 Trent 的测量信息可以推断出消息的内容并进行验证。

基于上述原理提出基于纯 W-like 态的量子强盲签名协议。

2 量子强盲签名协议

强盲签名协议中,消息拥有者将消息 M 盲化为 M',签名者所签消息是经过盲化后的消息 M',因此即使签名者保留消息 M 和签名 sig(M')的相关数据,仍然难以找出消息拥有者和签名信息的内在联系,无法对消息 M 的拥有者进行追踪。在电子投票系统中,为了确保投票者的匿名性及保密性,将强盲签名协议用于电子投票系统中。

该协议由初始化、盲签名及验证签名三个阶段完成。

2.1 初始化

1)制备投票信息

Alice 将要发送的投票信息 M 转换为 N bit,即

$$M = \{m(1), m(2), \cdots, m(i), \cdots, m(N)\} \quad i = 1, 2, \cdots, N$$

2)建立安全的量子信道

a)制备纯 W-like 态。Trent 制备 N 组纯 W-like 态并表示为 $\{|\phi(1)\rangle_{ABT}|\phi(2)\rangle_{ABT}\cdots|\phi(i)\rangle_{ABT}\cdots|\phi(N)\rangle_{ABT}\}$。其中,$|\phi(i)\rangle_{ABT} = \frac{1}{2\sqrt{6}}(3|000\rangle + |001\rangle + |010\rangle - |011\rangle + |100\rangle - |101\rangle - |110\rangle - 3|111\rangle)_{ABT}$, $i = 1, 2, \cdots, N$。

b)分发光子。通过多步传输[24]和分块传输[25],Trent 将光子 A 和 B 分别发送给 Alice 和 Bob,而把光子 T 留在自己手上;随后 Trent 准备有效的单粒子 $Q_A = \{Q_A^1 Q_A^2 \cdots Q_A^N\}$, $Q_B = \{Q_B^1 Q_B^2 \cdots Q_B^N\}$,其中 Q_A、$Q_B \in \{|+\rangle |-\rangle\}$,并将这些单粒子分别插入序列 A 和 B,用于检测量子信道的安全性。

c)检测量子信道。为了防止截断重发攻击或中间人攻击,必须对量子信道进行安全性检测。当 Trent 证实 Alice 和 Bob 已经收到各自的粒子后,它将向 Alice 和 Bob 公布测量基; Alice 和 Bob 分别通过相应测量基测量自己手中的粒子,Trent 通过比较测量结果便能评估信道是否安全。如果测量结果的错误率未超出预先规定的门限值,则认为不存在截断重发和中间人攻击,此时 Alice、Bob 和 Trent 之间建立了安全的量子信道。

3)分发量子密钥

采用著名的 BB84 协议分发密钥,Trent 与 Bob 共享一个 N bit量子密钥 K。

2.2 盲签名阶段

a) Alice 根据投票信息 $m(i)$ 测量自己手中的光子 A_i,测量规则为

$$\text{Alice 测量方向} = \begin{cases} |+\rangle & m(i) = 0 \\ |-\rangle & m(i) = 1 \end{cases} \quad (9)$$

但 Alice 不公开测量结果,消息 M 被盲化为 M'。

b) Bob 随机选择 $|+\rangle$ 或 $|-\rangle$ 测量自己手中对应的光子 $B(i)$,测量结果记为

$$B(i) = \begin{cases} 0 & |B(i)\rangle = |+\rangle \\ 1 & |B(i)\rangle = |-\rangle \end{cases} \quad (10)$$

所有光子 $B(i)$ 的测量结果表示为

$$B = \{B(1), B(2), \cdots, B(i), \cdots, B(N)\} \quad i = 1, 2, \cdots, N$$

c)依照强盲签名的特性,签名者 Trent 应无法获得验证者 Bob 的测量结果,所以 Bob 必须将测量结果 B 用量子指纹函数[26]进行变换:

$$|f(x)\rangle = \frac{1}{\sqrt{m}}\sum_{i=1}^{m}|i\rangle|E_i(x)\rangle \quad (11)$$

其中:$x \in \{0,1\}^n$ 为经典比特串,$E: x \in \{0,1\}^n \to \{0,1\}^m$ 为纠错码(如 Justesen 码),$c > 1$ 且 $m = cn$。变换后的量子指纹函数表示为 $f(B)$。Bob 用与 Trent 共享的密钥 K 对它进行加密,加密后的状态记为 $|H\rangle = E_K^1|f(B)\rangle$,其中,$E^1$ 表示量子态加密算法[27],之后 Bob 将 H 发送给 Trent。

d) Trent 测量自己手中的光子 $T(i)$, $T(i)$ 的状态为

$$T(i) = \begin{cases} 0 & |T(i)\rangle = |+\rangle \\ 1 & |T(i)\rangle = |-\rangle \end{cases} \quad (12)$$

所有光子 $T(i)$ 的测量结果表示为

$$T = \{T(1), T(2), \cdots, T(i), \cdots, T(N)\} \quad i = 1, 2, \cdots, N$$

e) Trent 将测量结果 T 用密钥 K 进行加密,得到对盲消息 M'的签名:$\text{sig}(M') = E_k^2(T)$,其中 E^2 表示一次一密算法。由于签名者 Trent 是对盲化后的消息 M'进行签名,而且它并不知道 M 的内容,因此签名 sig(M')具有盲性。

f) Trent 将 sig(M')发送给 Bob。

2.3 验证签名阶段

a) Bob 用与 Trent 共享的密钥 K 解密 sig(M')可得到 Trent 的测量结果 T。

b) Bob 根据自己手中的测量结果 B 和 Trent 的测量结果 T 之间满足的关系 $R_B = R_A \oplus R_T$,可以推导出消息拥有者 Alice 的秘密信息 M。

3　性能分析及安全性分析

3.1　性能分析

在上述强盲签名协议中,由于消息拥有者 Alice 将消息 M 盲化为 M',因此签名者 Trent 是对消息 M'进行签名,也就是说签名者并不知道所签消息的具体内容使签名具有盲性;验证者 Bob 根据自己手中的测量结果 B 和 Trent 的测量结果 T 之间满足的关系可以推导出 Alice 的秘密信息 M;而且在该协议中,Alice 将自己的秘密信息 M 盲化为 M'后没有留下任何个人信息的情况下退出,即使 Bob 和 Trent 保留 sig(M')及其他相关数据,仍然很难找出 M 和 sig(M')之间的内在关系,不可能对消息 M 的拥有者 Alice 进行追踪,所以说该协议可实现对消息拥有者隐私信息的保护。

1)盲性

该协议的盲性主要从以下两个环节体现:

a)在协议的签名阶段中,Alice 根据投票信息测量自己手中的光子,但并不公开测量结果,此时秘密信息 M 盲化为 M'。

b)签名者 Trent 无法获知验证者 Bob 的测量结果和消息拥有者 Alice 的投票信息。原因是:一方面在于验证者 Bob 对自己手中的测量结果 B 实行了指纹函数变换和加密算法,也就是说 Trent 得到的信息是经过加密的信息,无法得知 Bob 的原始测量结果;另一方面,在签名的初始阶段 Alice 就将秘密信息 M 盲化为 M'。因此,签名者 Trent 的签名具有盲性。

2)不可追踪

签名初始阶段消息拥有者 Alice 将秘密信息 M 盲化为 M'后即退出后续签名过程,几乎没有留下任何个人特征信息,比如使用密钥等,那么验证者 Bob 和签名者 Trent 难以找出秘密消息 M 的拥有者和盲签名 sig(M')之间的内在联系,因此 Alice 无法被追踪。

3.2　安全性分析

a)信道安全性分析。投票消息 M 通过 W-like 态粒子间的关联性传递给验证者 Bob,传递信息过程中会对信道的错误率进行检测,如果错误率在规定门限值内,信息有效签名过程继续;一旦错误率超过规定门限值,便舍弃本次投票结果。

b)协议的防欺骗性。在整个投票过程中,如果有攻击者截获或窜改消息,将无法满足关系 $R_B = R_A \oplus R_T$;同时,联系实际认为投票管理中心(签名者)Trent 是值得信任的。为了防止 Bob 有欺骗行为在签名阶段使用了指纹函数(单向函数)和加密算法,那么当 Bob 有任何欺骗行为时,三方的测量结果都将无法满足关系 $R_B = R_A \oplus R_T$。

c)签名的安全性。Trent 对盲消息的签名 sig(M')采用了 E^2(一次一密算法)加密,一次一密加密算法是最安全的加密算法,因此签名也是安全的。

3.3　协议的无条件安全性分析

协议中采用了著名的 BB84 协议进行量子密钥的分发,同时使用了量子指纹函数加密及一次一密算法加密。BB84 协议、量子指纹函数及一次一密加密算法均已被证明是无条件安全的,因此本协议具有无条件安全性。注:这里所说的无条件安全主要是指与当前计算资源无关,基于量子态物理特性的安全,并非绝对的安全。

3.4　复杂度分析

协议中认为 Trent 是值得信赖的,那么一旦 Bob 有不诚实行为,将很容易破坏纯 W-like 态粒子之间的纠缠关系 $R_B = R_A \oplus R_T$,这样就很容易揭发 Bob 的欺骗行为。因此,该协议在保证正确无误传递投票信息的前提下只需要验证关系式 $R_B = R_A \oplus R_T$ 即可,复杂度低。

3.5　效率分析

从初始化过程的步骤 b)可以看到,Trent 制备 N 组纯 W-like 态,需要 $2N$ 个光子用于信道安全检测,也就是说,总共有 $3N$ bit 用于共享 Trent 的 N bit 信息,那么该协议中用于验证签名信息的效率可达到 1/3。

相同条件下,如果采用 GHZ 态传递相同信息效率为 1/12,使用 GHZ-like 态的效率也仅为 1/5。显然,相同条件下使用纯 W-like 态传递信息的效率最高;而且本文使用的纯 W-like 态也可以防范木马攻击[28]。

4　结束语

强盲签名要求签名者对秘密信息进行盲签名,即签名者无法获知所签消息的具体内容,所以必须要保护消息拥有者的匿名性和保密性。针对这一情况并结合电子选举的实际要求,本文提出了一种基于纯 W-like 态的强盲签名协议。协议充分利用纯 W-like 态的优势,实现了签名者在不了解所签消息具体内容的前提下完成对消息的盲签名,充分保护了消息的匿名性,安全性高。

参考文献:

[1] NICOLAS G, GREGOIRE R, WOLFGANG T, *et al*. Quantum cryptography[J]. Reviews of Modern Physics, 2002, 74(1): 145-195.

[2] 林青群,王发强,米景隆,等. 基于随机相位编码的确定性量子密钥分配[J]. 物理学报, 2007, 56(10): 5796-5801.

[3] MINK A, TANG Xiao, MA Li-Jun, *et al*. High speed quantum key distribution system supports one-time pad encryption of real-time video [J]. Quantum Information and Computation IV, 2006, 6244 (62440M): 62440M1-62440M7.

[4] 马海强,李亚玲,赵环,等. 基于双偏振分束器的量子密钥分发系统[J]. 物理学报, 2005, 54(11): 5014-5017.

[5] DENG Fu-guo, LI Xi-han, ZHOU Hong-yu, *et al*. Improving the security of multiparty quantum secret sharing against Trojan horse attack [J]. Physical Review A, 2005, 72(4): 044302-044306.

[6] WAKS E, INOUE K, SANTORI C, *et al*. Secure communication: quantum cryptography with a photon turnstile[J]. Nature, 2002, 420 (6917): 762-766.

[7] CHAUM D. Blind signature for untraceable payments[C]//Advances in Cryptology: Proceedings of Crypto. 1983: 199-203.

[8] 孙莹,杜建忠,秦素娟,等. 具有双向认证功能的量子秘密共享方案[J]. 物理学报, 2008, 57(8): 4689-4694.

[9] HARN L. Cryptanalysis of the blind signature based on the discrete logarithm problem [J]. Electronic Letters, 1995, 31 (14): 1136-1137.

[10] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letter, 2000, 85 (2): 441-444.

[11] GOTTESMAN D, CHUANG I. Quantum digital signatures[EB/OL]. (2001-12-15). http://arxiv.org/abs/quant-ph/0105032.

(下转第 3845 页)

(上接第 3819 页)

[12] ZENG Gui-hua, KEITE C H. Arbitrated quantum-signature scheme [J]. Physical Review A, 2002, 65(4): 042312-042316.

[13] NGUYEN B A. Quantum dialogue [J]. Physical Letters A, 2004, 328(1): 6-10.

[14] 李伟, 范明钰, 王光卫. 基于纠缠交换的仲裁量子签名方案[J]. 物理学报, 2011, 60(8): 080302-1-080302-7.

[15] 温晓军, 刘云. 一种可实现的量子有序多重数字签名方案[J]. 电子学报, 2007, 35(6): 1079-1083.

[16] MAYERS D M. Unconditional security in quantum cryptography [J]. Journal of the ACM, 2001, 48(3): 351-406.

[17] 曾贵华, 马文平, 王新梅, 等. 基于量子密码的签名方案[J]. 电子学报, 2001, 29(8): 1098-1100.

[18] LEE H, HONG Chang-ho, KIM H, *et al*. Arbitrated quantum signature scheme with message recovery [J]. Physical Letters A, 2004, 321(5-6): 295-300.

[19] 田原, 温晓军, 公延军. 应用量子盲签名和群签名的电子支付系统[J]. 计算机工程与应用, 2011, 47(19): 108-112.

[20] 温晓军, 田原, 牛夏牧. 一种基于秘密共享的量子强盲签名协议[J]. 电子学报, 2010, 38(3): 720-724.

[21] 查新未, 张淳民. 三体纯态的纠缠度及其分类[J]. 西安交通大学学报, 2006, 40(2): 243-245.

[22] 查新未. 量子纯态纠缠态的构成与纠缠度[J]. 西安邮电学院学报, 2003, 8(1): 56-58.

[23] 查新未, 张淳民. 量子纠缠态及可分离态判据[J]. 西安交通大学学报, 2003, 37(7): 769-770.

[24] LONG Gui-lu, LIU Xiao-shu. Theoretically efficient high-capacity quantum-key-distribution scheme [J]. Physical Review A, 2002, 65(3): 032302-032305.

[25] DENG Fu-guo, LONG Gui-lu, LIU Xiao-shu. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block [J]. Physical Review A, 2003, 68(4): 042317-042323.

[26] BUHARMAN H, CLEVE R, WATROUS J, *et al*. Quantum fingerprinting [J]. Physical Review Letters, 2001, 87(16): 167902-167906.

[27] ZHOU Nan-run, ZENG Gui-hua. A realizable quantum encryption algorithm for qubits [J]. Chinese Physics, 2005, 14(11): 2164-2169.

[28] BOILEAU J C, LAFLAMME R, LAFOREST M, *et al*. Robust quantum communication using a polarization-entangled photon pair [J]. Physical Review Letter, 2004, 93(22): 220501-220504.