一种基于秘密共享的量子强盲签名协议

温晓军[1,2,3],田 原[1],牛夏牧[1]
(1.哈尔滨工业大学信息对抗研究所,黑龙江哈尔滨 150001;
2.中国科学院研究生院 信息安全国家重点实验室,北京 100049;
3.北京交通大学网络舆情安全研究中心,北京 100044)

摘 要: 提出了一种基于秘密共享原理的量子强盲签名协议.每一组 GHZ(Greenberger-Horne-Zeilinger)中的三个光子依次分发给消息拥有者 Alice、签名者 Trent 及验证者 Bob,Alice 测量自己的光子将消息盲化,Trent 测量自己的光子对盲消息进行签名,而 Bob 根据手中光子的测量结果及量子态的关联性验证签名,但其行为受到量子指纹及审计程序的约束.本协议实现了签名的盲性以及消息拥有者无法被追踪,其安全性不受攻击者所拥有的计算资源的影响.

关键词: 强盲签名; 秘密共享; 量子密码
中图分类号: TN918.1 **文献标识码:** A **文章编号:** 0372-2112 (2010) 03-0720-05

A Strong Blind Quantum Signature Protocol Based on Secret Sharing

WEN Xiao-jun[1,2,3], TIAN Yuan[1], NIU Xia-mu[1]
(1. *Information Countermeasure Technique Research Institute, Harbin Institute of Technology, Harbin, Heilongjiang* 150001, *China*;
2. *Graduate School of Chinese Academy of Sciences, State Key Laboratory of Information Security, Beijing* 100049, *China*;
3. *Network Opinion Security Research Center, Beijing Jiaotong University, Beijing* 100044, *China*)

Abstract: A strong blind quantum signature protocol was presented based on secret sharing. In this protocol, the three photons of each GHZ (Greenberger-Horne-Zeilinger) triplet are delivered to the message owner Alice, signatory Trent and verifier Bob respectively. Alice measures her photon to blind her message while Trent measures his photon to sign the blinded message, and then Bob verifies the signature according to the measuring results of his photon under the relationship of GHZ states. However, Bob's actions are restricted by the quantum fingerprints and the audit program. Our protocol ensures that the signature is blind and the message owner is untraceable. Moreover, its security was not influenced by the computational resource of attackers.

Key words: strong blind signature; secret sharing; quantum cryptography

1 引言

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.正是这种新的需求,推动了盲签名技术的发展.盲签名[1]是一种特殊的数字签名,是指签名者并不知道所签文件或消息的具体内容,而文件或消息的拥有者又可以得到签名者关于真实文件或消息的签名.基于盲签名的特点,盲签名技术在电子选举、电子现金等应用中对保护用户的匿名性方面起着重要作用:在电子选举系统中,需要管理中心为选票签名而令选票有效,但又必须保证投票人投票内容的隐私;在电子现金系统中,需要银行为电子现金签名,而又要求保证消费者消费内容的匿名性.基于以上实际需求,这两类系统都需要用到盲签名技术.

传统的盲签名方案大多是基于大数因子分解、离散对数、二次剩余等计算复杂性问题,然而这些方案并不能被证明是无条件安全的.随着计算能力的不断提高,这些算法或协议将变得不安全.而量子密码技术则是基于量子物理学的基本原理,其安全性是建立在 Heisenberg 测不准原理及量子不可克隆定理基础上的,特别是一些量子密钥分配协议如 BB84,B92 协议已经被证明是无条件安全的[2].

虽然经典的盲签名的研究比较成熟,但对基于量子密码的盲签名研究却基本处于空白.不过,自 2001 年

收稿日期:2008-10-22;修回日期:2009-06-28
基金项目:国家自然科学基金(No.60832010,60671064,60703011);国家 863 计划(No.2007AA01Z458);高等学校博士学科专项科研基金资助课题(No.RFDP:20070213047);2008 年信息安全国家重点实验室开放课题基金;中国博士后基金(No.20080440896)

Zeng[3]首次提出利用 GHZ 三体纠缠态的纠缠特性进行量子签名的方案以来,掀起了研究量子签名的热潮,Gottesman[4]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,该方案能够实现多个用户对同一签名消息进行验证;Lee[5]等提出了两个基于消息自动恢复(Message Recovery)的量子数字签名方案,该方案属于仲裁签名方案;Lü[6]提出了一个基于 GHZ 三体纠缠态粒子和量子稳固码的量子签名方案,能对未知的量子态签名;Wen[7]提出了一个能支持多个用户对同一信息进行签名的多重量子签名方案.量子签名的深入研究,为研究量子盲签名奠定了良好的基础.

基于电子选举中的安全性需求,本文提出了一种量子强盲签名协议.在本协议中,签名者(选票管理中心)必须对每张选票进行签名,但并不知道它所签名消息的具体内容,且不能抵赖自己的签名;消息的拥有者(选民)无法被追踪.该协议借鉴了量子秘密共享的思想,其安全性不受通信方以及攻击者所拥有的计算资源的限制.

2　基本原理

GHZ 三体纠缠态是一个三光子系统的最大纠缠态,假设三个光子分别由 Alice、Bob 和 Trent 三方所拥有.利用 $B_z=\{|0\rangle,|1\rangle\}$作为基矢,GHZ 态表示如下:

$$|\psi\rangle=\frac{1}{\sqrt{2}}(|0_a0_b0_t\rangle+|1_a1_b1_t\rangle) \tag{1}$$

其中,脚标 a,b,t 分别表示由 Alice、Bob 和 Trent 拥有的三个光子.

定义二维 Hilbert 空间中的两个共轭正交坐标系 H_x 和 H_y,其对应的基矢分别为 $\boldsymbol{B}_x=\{|+x\rangle,|-x\rangle\}$,$\boldsymbol{B}_y=\{|+y\rangle,|-y\rangle\}$.用基矢 $\boldsymbol{B}_z$ 表示基矢 $\boldsymbol{B}_x$ 和基矢 $\boldsymbol{B}_y$,得到:

$$|+x\rangle=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle),|-x\rangle=\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle) \tag{2}$$

$$|+y\rangle=\frac{1}{\sqrt{2}}(|0\rangle+i|1\rangle),|-y\rangle=\frac{1}{\sqrt{2}}(|0\rangle-i|1\rangle) \tag{3}$$

由式(2)很容易得到:

$$|0\rangle=\frac{1}{\sqrt{2}}(|+x\rangle+|-x\rangle),|1\rangle=\frac{1}{\sqrt{2}}(|+x\rangle-|-x\rangle) \tag{4}$$

代入式(1)后,则 GHZ 态可表示为:

$$\begin{aligned}|\psi\rangle=\frac{1}{2}[&(|+x\rangle_a|+x\rangle_b+|-x\rangle_a|-x\rangle_b)|+x\rangle_t\\&+(|+x\rangle_a|-x\rangle_b+|-x\rangle_a|+x\rangle_b)|-x\rangle_t]\end{aligned} \tag{5}$$

式(5)说明光子 a,b,t 之间存在着量子关联性,因此我们可联合对光子 a 和 b 的测量结果来判定光子 t 的量子态.例如,Alice 和 Bob 共同采取以$\{|+x\rangle,|-x\rangle\}$为本征态的正交测量 $\sigma_x^A\otimes\sigma_x^B$ 测量手中的光子,其中 $\sigma_x=|+x\rangle\langle+x|-|-x\rangle\langle-x|$.若得到测量结果相同,则表明 t 光子量子态必为$|+x\rangle$;若测量结果相反,则 t 光子量子态必为$|-x\rangle$.其它情形下的量子关联性如表 1 所列.

表 1　GHZ 态中光子的量子关联性

	$\|+x\rangle_b$	$\|-x\rangle_b$	$\|+y\rangle_b$	$\|-y\rangle_b$
$\|+x\rangle_a$	$\|+x\rangle_t$	$\|-x\rangle_t$	$\|-y\rangle_t$	$\|+y\rangle_t$
$\|-x\rangle_a$	$\|-x\rangle_t$	$\|+x\rangle_t$	$\|+y\rangle_t$	$\|-y\rangle_t$
$\|+y\rangle_a$	$\|-y\rangle_t$	$\|+y\rangle_t$	$\|-x\rangle_t$	$\|+x\rangle_t$
$\|-y\rangle_a$	$\|+y\rangle_t$	$\|-y\rangle_t$	$\|+x\rangle_t$	$\|-x\rangle_t$

从上述分析可知:以共轭子空间表示的 GHZ 三体纠缠态中,仅获取一个光子的状态信息,另外两个光子的状态信息不能被确定;但如果同时获取到两个光子的状态信息,第三个光子的状态的信息可被准确确定,而且无需借助任何其它的测量手段.GHZ 三体纠缠态的这种关联特性可以应用在秘密共享中,即将秘密信息拆分成若干个部分,由若干个参与者共同管理,单个参与者无法恢复秘密消息,只有若干参与者一同协作才能恢复出秘密消息[8].

由此,我们可以将上述原理应用到盲签名方案中:假定由消息的拥有者、签名者及验证者共享每组 GHZ 三体纠缠态光子,则消息拥有者测量自己的光子可以传递消息;签名者测量自己的光子则可以对该消息进行签名,由于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;验证者合并自己和签名者的测量信息可以推断出消息的内容并进行验证.

3　协议描述

假设 Alice 为任意一位消息的拥有者(选民),Trent 代表选票管理中心,Bob 为消息及签名的验证者.协议实现的功能如下:Alice 对她的投票信息 M 进行盲化得到 M',Trent 对盲信息 M' 进行签名得到 $sig(M')$,Bob 验证 M 及 $sig(M')$的有效性,但难以找出 M 和 $sig(M')$之间的内在联系,从而无法对 Alice 进行追踪.

3.1　协议初始化

(1)制备投票信息

Alice 将要发送的投票信息 M 转化为 N-bit,即

$$M=\{m(1),m(2),\cdots,m(i),\cdots,m(N)\},i=1,2,\cdots,N \tag{6}$$

(2)建立安全的量子信道

Step 1 制备三体纠缠态光子序列. Trent 制备 Q ($Q > N$)组量子态为$|\psi\rangle_{abt}$的 GHZ 态光子并表示成$\{|\psi(1)\rangle_{abt}, |\psi(2)\rangle_{abt}, \cdots, |\psi(i)\rangle_{abt}, \cdots, |\psi(Q)\rangle_{abt}\}$,其中

$$|\psi(i)\rangle_{abt} = \frac{1}{\sqrt{2}}(|0_a 0_b 0_t\rangle + |1_a 1_b 1_t\rangle), i = 1,2,\cdots,Q \tag{7}$$

Step 2 分发三体纠缠态光子. 对每一个 GHZ 态光子组,Trent 留下光子 t_i 在自己手上,然后把光子 a_i 和光子 b_i 分别分发给 Alice 和 Bob.

Step 3 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. 首先由 Trent 从自己手中的光子序列中随机挑出 Q-N 个光子并随机选择 $+x$ 方向或 $-x$ 方向进行测量(以 $+x$ 方向测量为例,选择特定的测量工具可使该光子塌缩到$|+x\rangle$态,则测量结果为$|+x\rangle$,其他方向类似),然后宣布这些光子在序列中的编号及测量结果;最后 Alice 和 Bob 依次在 $+x$ 方向或 $-x$ 方向测量自己手中对应编号的光子. 三方公开比较测量结果,如果这些结果的关联性满足表 1 所示,则认为不存在截断重发和中间人攻击. 剩下的 N 组三体纠缠态光子由通信三方共享,此时 Alice,Bob 及 Trent 之间建立了安全的量子信道.

(3)分发量子密钥

Trent 与 Bob 共享一个 N-bit 量子密钥 K,分发密钥的方法采用著名的 BB84 协议.

3.2 盲签名阶段

Step 1 Alice 根据投票信息 $m(i)$测量自己手中的光子 a_i,但不公开测量结果,消息 M 被盲化为 M'. 测量规则如下:

$$\text{Alice 测量方向} = \begin{cases} +x, & m(i) = 0 \\ -x, & m(i) = 1 \end{cases} \tag{8}$$

Step 2 *Bob* 随机选择 $+x$ 方向或 $-x$ 方向去测量自己手中对应的光子 b_i,测量结果记为

$$b(i) = \begin{cases} 0, & |b_i\rangle = |+x\rangle \\ 1, & |b_i\rangle = |-x\rangle \end{cases} \tag{9}$$

所有光子 b_i 的测量结果表示为:

$$B = \{b(1), b(2), \cdots, b(i), \cdots, b(N)\}, i = 1,2,\cdots,N \tag{10}$$

Step 3 为了给 Trent 事后审计提供依据,Bob 必须将测量结果 B 用量子指纹函数[9]进行变换:

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

其中 $x \in \{0,1\}^n$ 为经典比特串,$E: \{0,1\}^n \to \{0,1\}^m$ 为纠错码(如 Justesen 码),$c > 1$ 且 $m = cn$.

变换后的量子指纹表示为$|f(B)\rangle$,Bob 用与 Trent 共享的密钥 K 将它进行加密,加密后的状态记为:

$$|H\rangle = E_K^1(|f(B)\rangle) \tag{12}$$

其中 E^1 表示量子态加密算法[10]. Bob 将$|H\rangle$发送给 Trent.

Step 4 Trent 在收到$|H\rangle$之后,测量自己手中对应 GHZ 三体纠缠态光子组中的光子 t_i,t_i 的状态为$|+x\rangle$或$|-x\rangle$,用经典 bit 表示为:

$$t(i) = \begin{cases} 0, & |t_i\rangle = |+x\rangle \\ 1, & |t_i\rangle = |-x\rangle \end{cases} \tag{13}$$

所有光子 t_i 的测量结果表示为:

$$T = \{t(1), t(2), \cdots, t(i), \cdots, t(N)\}, i = 1,2,\cdots,N \tag{14}$$

Step 5 Trent 将 T 用 K 进行加密,得到对盲消息 M'的签名:

$$sig(M') = E_K^2(T) \tag{15}$$

其中 E^2 表示一次一密算法. 此时 Trent 并不知道 M 的内容,签名 $sig(M')$具有盲性.

Step 6 Trent 将 $sig(M')$发送给 Bob.

3.3 验证签名阶段

Step 1 Bob 用和 Trent 共享的密钥 K 解密 $sig(M')$得到 Trent 的测量结果 T.

Step 2 Bob 根据 T 和自己手中的测量结果 B 以及 GHZ 三体纠缠态光子的量子态的关联性(参见表 1)可以推导出 Alice 的秘密信息 M.

例如 当 $i = 2$,Alice 的投票信息 $m(2) = 0$,则 Alice 对手中的光子 a_2 做 $+x$ 方向测量;如果 Bob 选择 $+x$ 方向对自己手中的光子 b_2 进行测量,则 Trent 手中对应光子 t_2 的量子态必为$|+x\rangle$. 因此,Bob 根据手中对应光子 b_2 的量子态以及 Trent 的测量结果 t_2 可以推断出 Alice 的投票信息 $m(2) = 0$.

Step 3 Bob 公布投票结果 M,同时公布自己手中光子序列的测量结果(记为 B')供事后审计用.

3.4 审计阶段

一个完整的盲签名过程包括 Alice 对消息的盲化、Trent 进行盲签名以及 Bob 验证三个阶段. 然而为了防止 Bob 的欺骗行为,本协议专门设计了审计阶段. 之所以称之为审计阶段,是指在一次完整的盲签名过程之后,由选票管理中心 Trent 根据实际需要决定是否对 Bob 验证过程的合法性进行审核,审计过程如下:

Step 1 Trent 审查公布的投票结果 M、Bob 公布的测量结果 B'以及自己的测量结果 T 三者之间是否满足表 1 所示的关联性. 如果满足则进入 Step2,否则审计不通过.

Step 2 Trent 将 Bob 公布的测量结果 B'用式(11)所示量子指纹函数进行变换,得到$|f(B')\rangle$.

Step 3 Trent 把在盲签名阶段 Step3 中收到的$|H\rangle$

解密得到$|f(B)\rangle$.

Step 4　Trent 比较$|f(B)\rangle$与$|f(B')\rangle$是否相等,如果相等则通过审计,反之则审计不通过.

值得注意的是由于量子测量的统计特性,比较两个量子态$|f(B)\rangle$与$|f(B')\rangle$是否相等不像在经典情形下那么直接.这里,Trent 可以使用 Buhrman[9] 提出的量子交换测试电路(Quantum Swap Test Circuit,QSTC)来进行比较.

4　协议特性及安全性分析

如前所述,强盲签名协议要求签名必须实现盲性和对消息拥有者的不可追踪性这两种特性;和所有经典签名协议一样,本协议必须能够防止消息被篡改;另外作为基于量子密码的盲签名方案,它还必须同时具有无条件安全性.

4.1　协议的强盲签名特性

在本协议的签名阶段中,Trent 签名时无法知道 Alice 的投票信息.因为 Alice 根据投票信息 M 测量自己手中的光子而并未公开其测量结果,而 Bob 发给 Trent 的只是自己的测量结果的指纹,而不是 Bob 的测量结果本身,由于指纹函数的单向性,Trent 也无法知道 Bob 的测量结果.根据秘密共享的原理,Trent 签名时只知道一方的消息(自己的测量结果)将无法知道 Alice 的投票信息.因此 Trent 的签名具有盲性.

本协议中,投票消息 M 的拥有者 Alice 通过测量 GHZ 三体纠缠态粒子组中的一个,将消息传递给验证者 Bob 后退出,由于她未留下任何个人特征信息,比如使用密钥等,Bob 和 Trent 难以找出 M 和盲签名 $sig(M')$之间的内在联系,因此 Alice 无法被追踪.

4.2　协议的经典安全性

(1)消息及签名的安全

投票消息 M 通过 GHZ 三体纠缠态粒子间的关联性传递给验证者 Bob,因此它不会被攻击者截获与篡改.Trent 对盲消息的签名 $sig(M')$则采用 E^2(一次一密算法)加密,因此签名也是安全的.

(2)协议的防欺骗性

结合实际应用,在本协议定义的模型中,选票管理中心 Trent 是值得信赖的.为了防止验证者 Bob 的不诚实,Trent 签名之前预先要求 Bob 留下其测量结果的指纹.Bob 有以下两种欺骗策略:

(a) 假定 Bob 在 Trent 签名(测量)之前伪造假的测量结果及指纹以实现对投票结果进行篡改,但此时 Bob 只有自己一方的测量信息,根据第 2 节阐述的量子秘密共享原理,Bob 的行为将破坏 GHZ 三体纠缠态粒子间的关联性.

(b) 假定 Bob 在 Trent 签名(测量)之前发送真的测量结果的指纹,而在验证阶段使用假的测量结果以实现对投票结果进行篡改,很明显,这无法通过审计阶段的指纹校验.

综上所述,Bob 的欺骗行为均会在审计阶段被发觉.

4.3　协议的无条件安全性

本协议从密钥分发、加密算法以及传输信道这几个环节实现了无条件安全性.

(1)密钥分发的无条件安全性

协议中唯一使用的由验证者 Bob 和选票管理中心 Trent 共享的量子密钥 K 采用 BB84 协议进行分发,这已经被证明是无条件安全的[2].

(2)加密算法的无条件安全性

用来加密量子指纹的 E^1 为量子态加密算法[10]和用来加密 Trent 测量结果的一次一密算法 E^2 均被证明是无条件安全的.

(3)传输信道的无条件安全性

本协议在初始化阶段建立了安全的量子信道,在签名及验证的过程中,通过对 GHZ 光子组的测量,实现了信息在量子信道中的瞬间传递.这种传递是不受距离和时间限制的,且不会为任何障碍所阻隔,因此具有无条件安全性.

需要说明的是,无条件安全性并非是指绝对的安全,而是指与当前计算资源无关的,基于量子态物理特性的安全,其安全性是由 Heisenberg 测不准原理,未知量子态不可克隆定理等来保证的.

5　结论

结合电子选举的实际需求,本文提出了一种基于秘密共享的量子强盲签名协议.本协议能够实现签名者对消息进行盲签名,同时消息的拥有者无法被追踪,充分保护了消息的匿名性.与经典的盲签名协议相比,本文提出的协议不受通信方所具备的计算能力的限制,即使攻击者拥有无比强大的计算资源也无法攻破本协议,因此具有无条件安全性.一旦量子信息技术进入工程时代,本协议能够在基于量子密码的电子选举或电子政务中发挥作用.

参考文献:

[1] Fan C I, Lei C L. Efficient blind signature scheme based on quadratic residues[J]. Electronic Letters, 1996, 32(9): 811 – 813.

[2] Shor P W, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol[J]. Physical Review Letters, 2000, 85(2): 441 – 444.

[3] 曾贵华,马文平,王新梅,诸鸿文.基于量子密码的签名方

案[J].电子学报,2001,29(8):1098 – 1100.
ZENG Gui-hua, MA Wen-ping, Wang Xin-mei, Zhu Hong-wen. Signature scheme based on quantum cryptography[J]. Acta Electronica Sinica, 2001, 29(8): 1098 – 1100. (in Chinese)
[4] Gottesman D, Chuang I. Quantum digital signatures[DB/OL]. http://arxiv.org/abs/quant-ph/0105032.pdf, 2001 – 05 – 08.
[5] Lee H, Hong C, Kim H, et al. Arbitrated quantum signature scheme with message recovery[J]. Physics Letters A, 2004, 321(5 – 6): 295 – 300.
[6] Lü X, Feng D G. An arbitrated quantum message signature scheme[A]. CIS2004, Lecture Notes in Computer Science 3314 [C]. Heidelberg: Springer, 2004. 1054 – 1060.
[7] Wen X J, Liu Y, Zhang P Y. Digital multi-signature based on the controlled quantum teleportation [J]. Wuhan University Journal of Natural Science, 2007, 12(1): 029 – 032.
[8] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing [J]. Physical Review A, 1999, 59(3): 1829 – 1834.
[9] Buhrman H, Cleve R, Watrous J, et al. Quantum fingerprinting [J]. Physical Review Letters, 2001, 87, 167902 – 167904.
[10] Zhou N R, Zeng G H. A realizable quantum encryption algorithm for qubits[J]. Chinese Physics, 2005, 14(11): 2164 – 2169.

作者简介:

温晓军 男,1971 年生,江西赣州人,副教授,中国电子学会高级会员,毕业于北京交通大学通信与信息系统专业,获博士学位,现为哈尔滨工业大学计算机科学与技术博士后流动站研究人员.研究方向为量子密码与信息安全. E-mail: szwjun@sina.com

田 原 男,1984 年生,内蒙古呼伦贝尔人,硕士研究生.现就读于哈尔滨工业大学深圳信息安全技术研究中心,在职军人,中国人民解放军 61938 部队助理工程师,研究方向为量子密码与信息安全.
E-mail: tianyuan0522@gmail.com

牛夏牧 男,1961 年生,辽宁锦州人,教授、博士生导师.现任哈尔滨工业大学信息对抗技术研究所所长,哈尔滨工业大学深圳信息安全技术研究中心主任.SCI 国际会议-图像压缩与数字水印分会主席,国际 SPIE 学会会员,国际 IEEE 学会会员,美国 ACM 学会会员,中国电子学会高级会员.研究方向为信息安全.
E-mail: xiamu.niu@ict.edu.cn