电子信息工程、管理工程 文章编号: 1000-8608(2007)03-0424-05

基于 EPR粒子对的信息签名协议

温晓军*[1], 刘 云[1], 张鹏云[2]

(1. 北京交通大学 电子信息工程学院, 北京 100044;
2. 大连理工大学 物理系, 辽宁 大连 116024)

摘要: 研究了利用 Einstein-Podolsky-Rosen (EPR) 对的纠缠特性进行量子数字签名的方案,提出了一个基于测量结果比较的签名协议以及一个基于隐形传态的签名协议. 在基于测量结果比较的签名协议中,通信双方测量各自的 EPR并将测量结果与消息 M进行比较可以实现 M的签名和验证,同时通过量子单向函数来保证协议的安全. 在基于隐形传态的签名协议中,消息发送者将 M通过隐形传态传递给接收者来实现对 M签名并验证,其安全性由量子隐形传态的物理特性来保证. 这两种协议均可以脱离可信赖的第三方,且通信过程中不需要密钥,具有无条件安全性.

关键词: 量子信息; 签名协议; EPR对
中图分类号: TN918.91; TN201 文献标识码: A

0 引 言

根据签名的鉴定方式,数字签名协议可分成两类: (1) 直接的签名鉴定方法; (2) 间接的签名鉴定方法. 直接的鉴定方法由收方执行,简称真实数字签名. 间接的鉴定方法由第三方执行,他充当仲裁者的角色,因而也称为仲裁数字签名[1].

直接的数字签名方法采用较多的是对称加密技术和非对称加密技术,它们明显的弱点都是完全依赖密钥的安全性,另外发送方还有可能称私钥丢失从而否认自己的签名. 在非对称加密技术中为了解决公共密钥的存储问题,需要建立一个可信赖的密钥分配中心(KDC)来完成个人信息及其密钥的确定工作,密钥分配中心就是一个第三方成员,所以在数字签名方案中通常都要依赖第三方来保证签名的公正性. 然而,也正是因为第三方成员的存在,既降低了系统的效率又增加了不安全因素.

与经典密码学一样,量子保密通信也同样涉及量子信息签名问题. 最近,量子通信和量子计算机的研究进展迅速,量子密钥分配(quantum key distribution, QKD)[2,3]和量子秘密共享(quantum secret sharing, QSS)[4,5]技术已经在实验上取得成功,量子消息认证(quantum message authentication, QMA)[6]及量子信息签名(quantum signature, QS)[7]也成为学术界重视的课题. 经典密码学(仅区别于量子密码术,包括传统密码学和现代密码学)中的数字签名大多是基于计算上安全的,如 ElGamal和 DSA签名方案的安全性都是主要基于有限域上离散对数问题的难解性. 随着计算机技术的发展和计算能力的提高,如量子计算机的出现,将轻易地攻破这些经典的签名方案,而量子信息签名却是基于量子物理特性的具有无条件安全性的信息安全技术.

曾贵华等[8,9]研究了基于 GHZ三重态粒子的量子信息签名方案,但该方案属于仲裁签名方案,需要一个可信赖的系统管理员参与,并且在通信

收稿日期: 2005-11-25; 修回日期: 2007-03-15.
基金项目: 国家自然科学基金资助项目(10505005, 60572035);通信与信息系统北京市重点实验室资助项目(JD100040513).
作者简介: 温晓军* (1971-), 男, 博士, 副教授, 大连理工大学 1997届硕士, E-mail: szwxjun@sina.com; 刘 云(1955-),女,教授,博士生导师.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

过程中需要密钥来加密信息. 作者在以前的研究工作中提出了基于量子纠缠交换 (quantum entanglement swapping, QES) 的信息签名方案[10],但因为纠缠交换需要较多的粒子参加,所以通信效率较低,且通信过程中也需要使用密钥. 另外,根据当前的技术水平, GHZ三重态粒子在制备、存储、测量等技术上都不如 EPR粒子对容易实现. 本文利用 EPR粒子的纠缠特性及隐形传态 (teleportation) 的特点提出两种可脱离对第三方依赖的信息签名协议,该协议在通信过程中不需要使用密钥,具有无条件的安全性,并且发送方事后不能否认自己的签名.

1　基于测量结果比较的签名协议

假设 Alice和 Bob共享 n个 EPR粒子对,每一个粒子对处于如下 Bell态:

$$|\Psi^+\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \quad (1)$$

1.1　协议初始化

(1) 假定 Alice要发送的真实消息 $M = \{M(1), M(2), \cdots, M(n)\}$(二进制序列);

(2) Alice制备 n对处于 $|\Psi^+\rangle$ 态的 EPR粒子,记为 $\{\Psi(1)^+, \Psi(2)^+, \cdots, \Psi(n)^+\}$;

(3) 为了防止被 Eve篡改真实消息 M, Alice和 Bob共同选择一个量子单向函数 (quantum one-way function) H,因为对消息 M,计算 $H(M)$是容易的,但由 $H(M)$计算 M却是困难的. Alice将消息 M作变换得到 $H(M)$,量子单向函数的使用方法参见文献 [7].

1.2　签名过程

(1) Alice将每对 EPR粒子中的一个按顺序分发给 Bob;

(2) Alice采用 $\{|0\rangle_A, |1\rangle_A\}$基测量自己留下的一半粒子,测量结果记为 $A = \{A(1), A(2), \cdots, A(n)\}$;

(3) Alice将测量结果与真实消息 M进行比较,比较的结果以 $S = \{S(1), S(2), \cdots, S(n)\}$来表示,如果某一位上对应的 $M(i)$和 $A(i)$的值相同,则 $S(i)$记为 0,否则记为 1; S即为消息 M的签名. 假设真实消息 $M = \{101001\}$, Alice测量 EPR粒子的结果为 $A = \{110010\}$,则消息签名 $S = \{011011\}$;

(4) Alice将 $\{H(M), S\}$发送给 Bob.

1.3　验签过程

Bob可以直接验证 Alice的消息签名,以下步骤实现验签过程:

(1) Bob接收到 Alice发来的粒子后采用 $\{|0\rangle_B, |1\rangle_B\}$基进行测量,测量结果记为 $B = \{B(1), B(2), \cdots, B(n)\}$;

(2) Bob接受 Alice发来的签名信息,对照 $S = \{S(1), S(2), \cdots, S(n)\}$和自己的测量结果 $B = \{B(1), B(2), \cdots, B(n)\}$可以计算出 $M' = \{M'(1), M'(2), \cdots, M'(n)\}$; 如果不存在干扰对手 Eve,根据 EPR粒子的纠缠特性, Bob的测量结果应与 Alice一样,在上述例子中 $B = \{110010\}$,由 $S = \{011011\}$可得到 $M' = \{101001\}$;

(3) Bob对 M'使用量子单向函数进行变换得到 $H(M')$;

(4) Bob比较 $H(M)$与 $H(M')$,若 $H(M) = H(M')$,则确认 $S = \{S(1), S(2), \cdots, S(n)\}$为消息 M的有效签名,反之则拒绝.

1.4　安全性分析

假设 Alice没有对消息 M作量子单向函数变换,如果对手 Eve截获了消息 M及签名 S,则可以篡改 M同时也篡改 S而不被发现.

例如: 真实消息 $M = \{101001\}$, Alice测量 EPR粒子的结果为 $A = \{110010\}$,消息签名 $S = \{011011\}$. Eve将 M篡改为 $\{111000\}$,同时 S改为 $\{001010\}$,则 $B = \{110010\} = A$, Bob发现不了签名已经被 Eve篡改.

为了防止 Eve的攻击,在本协议中 Alice对消息 M进行量子单向函数 H变换, Eve截获的不是真实消息而是 $H(M)$,由于 Eve不可能从 $H(M)$得到 M,他篡改 S将很容易被发现.

2　基于隐形传态 (teleportation) 的签名协议

2.1　基本原理

1993年, Bennett等提出了第一个量子隐形传态方案[11],并在 1997年由奥地利学者实验成功[12]. 其主要思想是,利用 EPR纠缠粒子对能将某个物体的未知量子态传送给信息的接收方而不

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

传递物体的本身. 本文将未知量子态改为已知量子态,将要发送的信息“调制” 到被发送的量子态中,接收方经过相应的变换可以“解调” 出该信息,从而实现信息的签名与验证.

如图 1所示,假设 Alice要发送的携带消息 M 的粒子的态为

$$|J\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle_M + b|1\rangle_M) \tag{2}$$

其中 $b=1$和 $b=-1$分别对应消息 $M(i)=0$和 $M(i)=1$.

Bob制备一对 EPR粒子 (AB)处于 Bell态:

$$|U_{00}\rangle_{AB} = \frac{1}{\sqrt{2}}(|00\rangle_{AB} + |11\rangle_{AB}) \tag{3}$$

则 3个粒子的混合态为

$$|J_0\rangle = |J\rangle_M \otimes |U_{00}\rangle_{AB} = \frac{1}{2}[|0\rangle_M(|00\rangle_{AB} + |11\rangle_{AB}) + b|1\rangle_M(|00\rangle_{AB} + |11\rangle_{AB})] \tag{4}$$

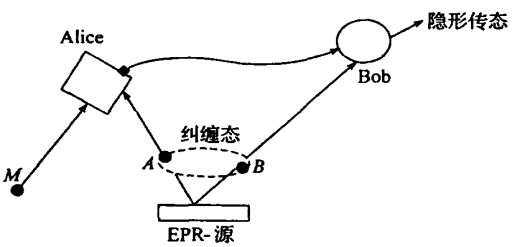

图 1 量子态隐形传态模型

Fig. 1 Model for teleporting a quantum state

按照约定前 2个量子比特属于 Alice,而第 3个量子比特则属于 Bob, Alice对她的量子位进行一个 C_{NOT}门变换,得到

$$|J_1\rangle = \frac{1}{2}[|0\rangle_M(|00\rangle_{AB} + |11\rangle_{AB}) + b|1\rangle_M(|10\rangle_{AB} + |01\rangle_{AB})] \tag{5}$$

然后 Alice对第 1个量子位作 Hadamard变换,得到

$$|J_2\rangle = \frac{1}{2\sqrt{2}}[(|0\rangle + |1\rangle)_M(|00\rangle_{AB} + |11\rangle_{AB}) + b(|0\rangle - |1\rangle)_M(|10\rangle_{AB} + |01\rangle_{AB})] \tag{6}$$

这一状态表达式能够写成以下形式

$$|J_2\rangle = \frac{1}{2\sqrt{2}}[|00\rangle_{MA}(|0\rangle + b|1\rangle)_B + |01\rangle_{MA}(|1\rangle + b|0\rangle)_B + |10\rangle_{MA}(|0\rangle - b|1\rangle)_B + |11\rangle_{MA}(|1\rangle - b|0\rangle)_B] \tag{7}$$

Alice对 $|J_2\rangle$中的前两个量子位进行一次测量 (恰好为 4个 Bell态之一,记为 $|U_{00}\rangle$, $|U_{01}\rangle$, $|U_{10}\rangle$, $|U_{11}\rangle$),$|J_2\rangle$将等概率地塌缩到上式的 4个叠加态之一上. 于是,Bob拥有的量子位也相应地变化为以下 4种状态之一:

$$|U_{00}\rangle_{MA} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle + b|1\rangle)_B \equiv \boldsymbol{I}|J\rangle_B,$$

$$|U_{01}\rangle_{MA} \rightarrow \frac{1}{\sqrt{2}}(|1\rangle + b|0\rangle)_B \equiv \boldsymbol{X}|J\rangle_B,$$

$$|U_{10}\rangle_{MA} \rightarrow \frac{1}{\sqrt{2}}(|0\rangle - b|1\rangle)_B \equiv \boldsymbol{Z}|J\rangle_B,$$

$$|U_{11}\rangle_{MA} \rightarrow \frac{1}{\sqrt{2}}(|1\rangle - b|0\rangle)_B \equiv \boldsymbol{Y}|J\rangle_B \tag{8}$$

其中

$$\boldsymbol{I} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \boldsymbol{X} \equiv \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \boldsymbol{Z} \equiv \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix},$$
$$\boldsymbol{Y} = \boldsymbol{ZX} \equiv \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \tag{9}$$

当 Alice把她的两个量子位态的测量结果告诉 Bob时,Bob进行相应的逆变换,即 $\boldsymbol{I}^{-1}$、$\boldsymbol{X}^{-1}$、$\boldsymbol{Z}^{-1}$、$\boldsymbol{Y}^{-1}$,就可以使携带 M信息的量子态在 B粒子上再现出来,于是 Bob测量自己的粒子可以得出 $b=1$或 $b=-1$,并置换出对应的消息 $M(i)=0$或 $M(i)=1$.

2.2 签名协议初始化

(1) 假定 Alice要发送的真实消息 $M=\{M(1), M(2), \cdots, M(n)\}$(二进制序列);

(2) Alice根据 $M(i)$制备 n个处于 $|J\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle_M + b|1\rangle_M)$的量子位,记做 $\{J_M(1), J_M(2), \cdots, J_M(n)\}$,其中 $b=1$和 $b=-1$分别对应消息 $M(i)=0$和 $M(i)=1$;

(3) Bob制备 n对处于 $|U_{00}\rangle$态的 EPR粒子,记为 $\{U_{AB}(1), U_{AB}(2), \cdots, U_{AB}(n)\}$.

2.3 签名过程

(1) Bob将处于 $|U_{00}\rangle$态的 EPR粒子对中的一半发给 Alice,记为 $\{U_A(1), U_A(2), \cdots, U_A(n)\}$;

(2) Alice接收到 EPR粒子后,与相应的 $M(i)$结合并使用 Bell基测量,结果记为 $S=\{U_{MA}(1), U_{MA}(2), \cdots, U_{MA}(n)\}$, S即为消息 M的签名;

(3) Alice将 $\{M, S\}$发送给 Bob.

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

2.4 验签过程

(1) Bob接收 $\{M, S\}$;

(2) Bob 根据 $S = \{U_{MA}(1), U_{MA}(2), \cdots, U_{MA}(n)\}$ 以及式(8)对留给自己的 EPR粒子对中的一半 $\{U_B(1), U_B(2), \cdots, U_B(n)\}$ 作相应的 $\boldsymbol{I}^{-1}$、$\boldsymbol{X}^{-1}$、$\boldsymbol{Z}^{-1}$、$\boldsymbol{Y}^{-1}$之一的变换,得到与携带消息 M的粒子一致的态 $\{J_B(1), J_B(2), \cdots, J_B(n)\}$;

(3) Bob 通过测量 $\{J_B(1), J_B(2), \cdots, J_B(n)\}$得到每个粒子的 b值,从而提取消息 $M' = \{M'(1), M'(2), \cdots, M'(n)\}$,如果 $M = M'$,则确认 $S = \{S(1), S(2), \cdots, S(n)\}$为消息 M的有效签名.

例如: Alice要发送的消息 $M = \{0110\}$,其签名为 $S = \{\{U_{00}, U_{10}, U_{11}, U_{10}\}\}$,则 Bob对自己的粒子依次进行的变换为 $\{\boldsymbol{I}^{-1}, \boldsymbol{Z}^{-1}, \boldsymbol{Y}^{-1}, \boldsymbol{Z}^{-1}\}$,得到态 $\{\frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M), \frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M), \frac{1}{\sqrt{2}}(|0\rangle_M - |1\rangle_M), \frac{1}{\sqrt{2}}(|0\rangle_M + |1\rangle_M)\}$与 M是一致对应的,证明 S为 M的有效签名.

2.5 安全性分析

Eve有一种攻击策略,即拦截了 $\{M, S\}$后,篡改相应的签名 S,但总能被发现. 例如在对某一bit的消息 $M(i)$签名 $S(i) = |U_{01}\rangle$,根据公式, Bob在验证签名提取 $M'(i)$时,需进行 $\boldsymbol{X}^{-1}$操作,假设 $M(i)$的签名被 Eve篡改为 $S(i) = |U_{00}\rangle$,则 Bob在验证时变成 $\boldsymbol{I}^{-1}$操作,这一过程描述如下:

(1) 无 Eve攻击

$$\text{Alice}\ |J\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle_M + b|1\rangle_M) \rightarrow$$

$$\text{Bob}\ |J\rangle_B = \frac{1}{\sqrt{2}}(|1\rangle_B + b|0\rangle_B) \xrightarrow{\text{Bob}\ \boldsymbol{X}^{-1}}$$

$$|J\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B + b|1\rangle_B) \rightarrow b;$$

$$S(i) = |U_{01}\rangle \qquad (10)$$

(2) 有 Eve攻击

$$\text{Alice}\ |J\rangle_M = \frac{1}{\sqrt{2}}(|0\rangle_M + b|1\rangle_M)$$

$$\xrightarrow{\text{Eve}\ \ S(i) = |U_{00}\rangle} \text{Bob}\ |J\rangle_B = \frac{1}{\sqrt{2}}(|1\rangle_B + b|0\rangle_B) \xrightarrow{\text{Bob}\ \boldsymbol{I}^{-1}} |J\rangle_B = \frac{1}{\sqrt{2}}(|1\rangle_B + b|0\rangle_B);$$

$$S(i) = |U_{01}\rangle \qquad (11)$$

因此如果 Eve没有篡改签名, Bob在验证时经过相应的逆变换,即 $\boldsymbol{I}^{-1}$、$\boldsymbol{X}^{-1}$、$\boldsymbol{Z}^{-1}$、$\boldsymbol{Y}^{-1}$,将自己的 B粒子态恢复为

$$|J\rangle_B = \frac{1}{\sqrt{2}}(|0\rangle_B + b|1\rangle_B) \qquad (12)$$

但如果 Eve篡改了签名,则 Bob在验证时虽然还进行 $\boldsymbol{I}^{-1}$、$\boldsymbol{X}^{-1}$、$\boldsymbol{Z}^{-1}$、$\boldsymbol{Y}^{-1}$之一变换,但 B粒子将出现其他的态而被发现. 同理, Eve既然无法篡改签名,也就无法篡改消息 M.

在实际应用中,量子信道可能会出现量子噪声,另外 Eve也可能会采取截获 /重发策略来进行攻击. 然而这些都会对 EPR粒子的相干性产生扰动而被发现,通信双方可以用以下简单方法来检测量子信道的安全性:

(1) Alice随机选择第 k个 EPR粒子对,并采用 $\{|0\rangle, |1\rangle\}$基测量粒子 A.

(2) Alice公开宣布她的测量结果.

(3) Bob用同样方法测量对应的粒子 B,如果没有 Eve的存在,两者的测量结果正好相同.

(4) 如果测量结果没有相干性,则量子信道中可能存在窃听. 假设通信各方测量 n对 EPR粒子,其中没有相干性的粒子对数为 m,则 $m/n < c$(阈值)在本协议的适用范围之内.

3 结　论

(1) 与其他签名协议(无论是经典签名协议还是量子签名协议)不同,本方案提出的两种签名协议都不需要依赖第三方(仲裁者),也不需要密钥,因此安全性与通信效率更高;

(2) 基于隐形传态的签名协议与基于测量结果比较的签名协议相比,可以不需要利用量子单向函数加密信息,应用更加方便;

(3) 与量子密钥分配(QKD)一样,本方案提出的两种签名协议具有不同于经典数字签名的无条件安全性,可以用在点对点的量子保密通信中,该协议还同时具有量子身份认证的功能.

参考文献:

[1] WILLIAM S. **Cryptography and Network Security Principles and Practice Second Edition** [M]. Beijing: Tsinghua University Press, 2003: 299-305

[2] SHOR P W, PRESKILL J. Simple proof of security of the BB84 quantum key distribution protocol [J].

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

Phys Rev Lett, 2000, **85**(7): 441–444

[3] HUGHES R J, MORGAN G L, PETERSON C G. Quantum key distribution over a 48 km optical fibre network [J]. **J Mod Opt**, 2000, **47**: 533–547

[4] HILLERY M, BUZEK V, BERTHIAUME A. Quantum secret sharing [J]. **Phys Rev A**, 1999, **59**(3): 1829–1834

[5] GUO G P, GUO G C. Quantum secret sharing without entanglement [J]. **Phys Lett A**, 2003, **310**(4): 247–251

[6] BARNUM H, CREPEAU C, GOTTESMAN D, *et al*. Authentication of quantum messages[C] // **Proceedings of 43rd Annual IEEE Symposium on the Foundations of Computer Science**. Vancouver: IEEE, 2002: 449–458

[7] GOTTESMAN D, CHUANG I. Quantum digital signatures [DB/OL]. [2001-05-08] http://arxiv.org/abs/quant-ph/0105032

[8] 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

[9] ZENG G H, CHRISTOPH K. An arbitrated quantum signature scheme [J]. **Phys Rev A**, 2002, **65**(4): 042312–042317

[10] 温晓军,刘 云,张振江. 基于纠缠交换的量子信息签名方案[J]. 电子与信息学报, 2005, **27**(5): 811–813

[11] BENNETT C H, BRASSARD G, CREPEAU C, *et al*. Teleporting an unknown quantum state via dual classical and Einstein–Podolky–Rosen channels [J]. **Phys Rev Lett**, 1993, **70**(13): 1895–1899

[12] BOUWMEESTER D, PAN J W, MATTLE K, *et al*. Experimental quantum teleportation [J]. **Nature**, 1997, **390**: 575–579

Information signature protocols using Einstein–Podolsky–Rosen pairs

WEN Xiao-jun*[1], LIU Yun[1], ZHANG Peng-yun[2]

(1. School of Electr. Inf. Eng., Beijing Jiaotong Univ., Beijing 100044, China;
2. Dept. of Phys., Dalian Univ. of Technol., Dalian 116024, China)

Abstract Two quantum digital signature schemes using the entanglement character of Einstein–Podolsky–Rosen (EPR) pairs were researched, and a protocol based on comparing the measurement result and the other protocol based on teleportation were proposed. In the first protocol, the communicators measured their EPR and compared the measurement results with the message M to implement signature and verification, in the meantime using quantum one-way function to guarantee its security. In the second protocol, the sender sent M to the receiver via quantum teleportation to implement signature and verification, whose security was guaranteed by the physical characteristics of quantum teleportation. These two protocols did not need a third party who was worthy of being trusted, neither need any keys in the communication process. Furthermore, they had unconditional security.

Key words quantum information; signature protocol; EPR pairs

?1994-2015 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net