基于 EPR 态的量子代理签名方案 *

常祖领[1], 周景贤[1], 张 [illegible][2], 温巧燕[2]
(1. 郑州大学 数学系, 郑州 450001; 2. 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: 提出了一种量子代理签名方案,利用量子力学中 Einstein-Podolsky-Rosen(EPR)的纠缠特性并结合经典编码方法来实现对量子比特串的签名和验证。在本方案中,原始签名人可以将自己的签名权委托给代理签名人,而量子密钥分配和一次一密保证了新方案的无条件安全性。研究表明新方案满足不可伪造性、不可否认性和可追踪性。

关键词: 量子签名; 代理签名; 量子密码; EPR 态
中图分类号: TP309 **文献标志码**: A **文章编号**: 1001-3695(2010)02-0675-03
doi:10.3969/j.issn.1001-3695.2010.02.075

Quantum proxy signature scheme based on EPR state

CHANG Zu-ling[1], ZHOU Jing-xian[1], ZHANG Jie[2], WEN Qiao-yan[2]
(1. *Dept. of Mathematics, Zhengzhou University, Zhengzhou* 450001, *China*; 2. *State Key Laboratory of Networking & Switching Technology, Beijing University of Posts & Telecommunications, Beijing* 100876, *China*)

Abstract: This paper presented a quantum proxy signature scheme which allowed users to obtain the signature and verify of a quantum bit sequence by using the entanglement characteristic of the EPR state and the way of classical encode. In this new scheme, the original signer could delegate his or her signing rights to proxy signer. Guaranteed the unconditionally security of this scheme by quantum key distribution and one time pad. Results show that this new scheme satisfy non-counterfeit, non-disavowal and traceability.

Key words: quantum signature; proxy signature; quantum cryptography; EPR state

0 引言

Bennett 等人[1]于 1984 年提出了量子密码的概念,并给出了第一个量子密码协议——BB84 协议。自此之后,量子密码学成为信息安全领域一个热门的研究课题,它利用量子力学的原理证明安全地分发秘密,包括量子密钥分发(QKD)[2,3]、量子安全直接通信(QSDC)[4]、量子秘密共享(QSS)等。

Ekert[5]于 1991 年提出基于 EPR 的量子密钥分配协议(E91),充分利用了量子系统的纠缠特性,通过纠缠量子系统的非定域性来传递量子信息,取代了 BB84 协议中用来传递量子位的量子信道,因而可以更加灵活地实现密钥分配。由于 EPR 纠缠对万备简单、存储方便、通信高效等优良特性,近年来对它的研究和应用逐渐深入和广泛。温晓军等人[6]利用 EPR 粒子的纠缠特性及隐形传态的特点提出两种可脱离对第三方依赖的信息签名协议;闫丽华等人[7]提出了利用两个 EPR 态作为量子信道隐形传递任意三原子 W 态的方案。另外,在文献[8~11]中对纠缠态均有深入的研究。

像经典保密通信一样,量子保密通信也涉及到了签名的问题。通信和量子计算机的研究取得了迅速的进展,特别是量子计算机的出现使得对量子比特签名成为重要的课题。2001 年,Gottesman 等人[12]首先提出了基于量子力学的数字签名协议,具有绝对安全性。随后, Lu 等人[13]和 Shoo 等人[14]依据量子单向函数分别完成了对一般量子态和已知量子态的签名和验证;2001 年,Zeng 等人[15]提出了一个仲裁量子签名方案。其中签名和验证过程都需要借助一个可信第三方才可以完成。最近,杨宇光等人[16]提出了一种门限代理签名方案,由于代理签名组与原始签名者享用同一个密钥,这将导致最终生成的签名是可否认的。

为克服之前相关方案的不足,本文提出了一个新的量子代理签名方案。该方案使用 EPR 纠缠离子对作为信息载体,利用了一次一密保证无条件安全性,并且代理签名只能由代理签名人生成,具有不可否认性。另外,本方案不需要可信中心存在。

1 预备知识

$\{|0\rangle,|1\rangle\}$是一组标准正交基,称其为 Z 基,简记为 B_Z 定义:

$$|+\rangle=(1/\sqrt{2})(|0\rangle+|1\rangle)$$
$$|-\rangle=(1/\sqrt{2})(|0\rangle-|1\rangle) \quad (1)$$

易知:$\{|+\rangle,|-\rangle\}$也是一组正交基,称为 X 基,简记为 B_X。根据式(1)有

收稿日期: 2009-06-02; **修回日期**: 2009-07-06 **基金项目**: 国家自然科学基金资助项目(60873191,60821001);高等学校博士学科点专项科研基金资助课题(200800131016);北京市科技新星计划项目(2008B51);教育部科学技术研究重点项目(109014);北京市自然科学基金资助项目(4072020);现代通信国家重点实验室基金资助项目(9140C1101010601);ISN 开放基金

作者简介:常祖领(1976-),男,河南新乡人,副教授,硕导,博士,主要研究方向为信息安全、代数编码、信息论等;周景贤(1981-),男,河南信阳人,硕士研究生,主要研究方向为信息安全、量子密码(jingxian629@163.com);温巧燕(1959-),女,教授,博导,主要研究方向为信息安全、计算机安全、量子密码等.

$$|0\rangle=(1/\sqrt{2})(|+\rangle+|-\rangle)$$
$$|1\rangle=(1/\sqrt{2})(|+\rangle-|-\rangle) \quad (2)$$

定义 2-量子比特的四个 Bell 态如下：

$$|\phi^+\rangle=(1/\sqrt{2})(|00\rangle+|11\rangle)$$
$$|\phi^-\rangle=(1/\sqrt{2})(|00\rangle-|11\rangle)$$
$$|\Psi^+\rangle=(1/\sqrt{2})(|01\rangle+|10\rangle)$$
$$|\Psi^-\rangle=(1/\sqrt{2})(|01\rangle-|10\rangle) \quad (3)$$

假设 EPR 对的纠缠态如下：

$$|\Psi\rangle=(1/\sqrt{2})(|0_A0_B\rangle)+|1_A1_B\rangle)=$$
$$(1/\sqrt{2})(|+_A+_B\rangle+|-_A-_B\rangle)$$

由于 EPR 对的纠缠特征，当粒子 A 处于状态$|0\rangle$时，粒子 B 必定也处于状态$|0\rangle$；而当粒子 A 处于状态$|1\rangle$时，粒子 B 也必定处于状态$|1\rangle$，其概率均为 50%。在对粒子 A 和 B 的测量过程中，若测得粒子 A 的结果是$|0\rangle$（或$|1\rangle$）态，即使没有测量粒子 B 也可以断定其状态必定为$|0\rangle$（或$|1\rangle$），而不管两个粒子相距多远。但是一旦这个量子系统被测量，两粒子间的纠缠性将不复存在。

2　量子代理签名方案

方案的参与方有三方，即原始签名人 Alice、代理签名人 Bob 和签名验证人 Charlie。方案主要由以下四个阶段组成：初始化阶段、代理生成阶段、代理签名生成阶段和验证阶段。

在初始化阶段，参与方之间各自相互生成共享密钥，并由 Bob 生成 EPR 纠缠对备用。对每一次签名，由原始签名人 Alice生成代理委托证书 w，并根据代理委托证书 w 对收到的粒子进行测量，将测量结果加密后发送给验证人 Charlie。在签名阶段，代理签名人 Bob 根据消息 m，对自己的粒子进行测量，同样将测量结果加密后发送给 Charlie。最后，验证人 Charlie 解密收到的结果，根据相应的验证式验证签名是否有效。本文方案的详细描述的直观过程如图 1 所示。

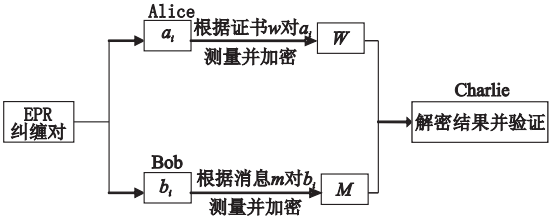

图1　代理签名的直观过程（其中$i=1,2,\cdots,n$）

2.1　初始化阶段

1）密钥分配　生成 $2n$ bit 长的密钥 k_{AB}、k_{AC}、k_{BC}。其中 k_{AB}、k_{AC}和 k_{BC}分别是 Alice 和 Bob、Alice 和 Charlie 及 Bob 和 Charlie 之间的密钥。为确保密钥的无条件安全性，k_{AB}、k_{AC}和 k_{BC}可以通过量子密码的方法获得。本方案运用 BB84 协议来获取 k_{AB}、k_{AC}和 k_{BC}，原因是 BB84 协议简单而且容易实现。

2）EPR 纠缠对的生成　Bob 制备 n 个 EPR 纠缠对$|\Psi\rangle=\{|\Psi_1\rangle,|\Psi_2\rangle,\cdots,|\Psi_n\rangle\}$。每个 EPR 对中的两个粒子是纠缠的，在未测量之前两粒子的状态不能确定。EPR 态有四种可能的量子态。本方案中选取如下的态：

$$|\Psi_i\rangle=(1/\sqrt{2})(|0\rangle_{a_i}|0\rangle_{b_i}+|1\rangle_{a_i}|1\rangle_{b_i}) \quad i=1,2,\cdots,n \quad (4)$$

其中：a_i 和 b_i 对应于第 i 个纠缠对的两个粒子。

2.2　代理生成阶段

1）对于每个 EPR 纠缠对，Bob 发送粒子 a_i 给 Alice，自己保留对应的粒子 b_i。

2）收到 $a_i(i=1,2,\cdots,n)$后，Alice 首先生成一个包含签名有效期、原始签名人和代理签名人身份信息的委托证书 w，并将 w 转换为 n 经典比特的序列$\{w(1),w(2),\cdots,w(n)\}$。其中 $w(i)\in\{0,1\}$。然后根据 w 对 $a_i(i=1,2,\cdots,n)$进行测量。测量的方式如下：

若 $w(i)=0$，用基 $B_Z=\{|0\rangle,|1\rangle\}$对 a_i 进行测量；

若 $w(i)=1$，用基 $B_X=\{|+\rangle,|-\rangle\}$对 a_i 进行测量。

其中，两组测量基 B_Z 和 B_X 是非正交的。本方案中，两组基满足：$\langle B_Z|B_Z\rangle=1/\sqrt{2}$。

Alice 记录测量结果作为 $w'=\{w'(1),w'(2),\cdots,w'(n)\}$。其中 $w'(i)\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$，这四种量子态$\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}$可以对应的被编码成两位经典比特，例如：

$$|0\rangle|\rightarrow 00,|1\rangle\rightarrow 11,|+\rangle\rightarrow 10,|-\rangle\rightarrow 01 \quad (5)$$

最终，得到委托证书 w 的盲化形式 $w''=\{w''(1),w''(2),\cdots,w''(n)\}$（$2n$ bit）

3）Alice 用密钥 k_{AC}加密 w''得到秘密委托证书 W。其中 W 被定义如下：

$$W=E_{k_{AC}}\{w''(1),w''(2),\cdots,w''(n)\} \quad (6)$$

4）Alice 发送秘密委托证书 W 给验证人 Charlie。

2.3　签名生成阶段

假设 Alice 需要 Bob 代表自己对消息 m 进行签名 $m=\{m(1),m(2),\cdots,m(n)\}$。其中：

$$m(i)\in\{0,1\};i=1,2,\cdots,n \quad (7)$$

1）Bob 首先根据消息 m 去测量他的粒子 $b_i(i=1,2,\cdots,n)$。若 $m(i)=0$，他用基 $B_Z=\{|0\rangle,|1\rangle\}$来测量；若 $m(i)=1$，他用基 $B_X=\{|+\rangle,|-\}$测量。Bob 记录测量的结果为

$$m'=\{m'(1),m'(2),\cdots,m'(n)\}$$
$$(m'(i)\in\{|0\rangle,|1\rangle,|+\rangle,|-\rangle\}) \quad (8)$$

2）Bob 根据式(5)将 m'编码成 m''。类似 w''，m''也为 $2n$ bit 序列。

3）Bob 用密钥 k_{BC}对 m''进行加密得到消息的代理签名 M。其中 M 被定义如下：

$$M=E_{k_{BC}}\{m''(1),m''(2),\cdots,m''(n)\} \quad (9)$$

由于 m''和 k_{BC}都是 $2n$ bit 长，可以采用一次一密作为加密算法来保证无条件安全性。

4）Bob 发送最终的代理签名 M 给验证人 Charlie。

2.4　验证阶段

1）Charlie 收到来自 Alice 的秘密委托证书 W，然后用他的密钥 k_{AC}对其解密得到盲化的证书$\{m''(1),w''(2),\cdots,w''(n)\}$。

2）Charlie 根据式(5)去转换 w''来得到原来的委托证书 w。

3）Charlie 通过委托证书 w 来核对此次签名的各项有效信息，如有效时间、参与者的身份等。如有任何一项不符，则签名停止，宣布此次签名无效；否则，继续下面步骤。

4）Charlie 收到来自 Bob 的代理签名 M，然后用他的密钥 k_{BC}对其解密得到 m''。

5）Charlie 接收 M 作为消息 m 有效地代理签名，当且仅当参数 m、w、m''和 w''满足下列关系：

（a）若 $w(i)=m(i)$，则有 $w''(i)=m''(i)$；

（b）若 $w(i)\neq m(i)$，则有 $w''(i)=m''(i)$ 或 $w''(i)\neq m''(i)$，否则，他拒绝 M。

3　方案分析

3.1　方案的正确性

为了说明方案的正确性,本文给出如下实例:假设 Charlie 收到 Alice 发送的秘密证书 W,解密的结果 $w''=\{w''(1),w''(2),w''(3),w''(4)\}=\{00,10,11,01\}$。那么由式(5),可以得到 Alice 的测量结果 $w'=\{|0\rangle,|+\rangle,|1\rangle,|-\rangle\}$,进而可以知道 Alice 的测量基为 $\{B_Z,B_X,B_Z,B_X\}$;最终由 Alice 的测量规则可得到:$w=\{0,1,0,1\}$。直观还原过程如表 1 所示。

表 1　盲化证书 w''到初始证书 w 的还原过程

n	1	2	3	4
w''	00	10	11	01
Alice's measure result	$\|0\rangle$	$\|+\rangle$	$\|1\rangle$	$\|-\rangle$
Alice's measure base	B_Z	B_X	B_Z	B_X
w	0	1	0	1

假定消息 $m=\{1,1,0,0\}$,根据 Bob 的测量规则及 EPR 离子对的纠缠性,因为 $w(2)=m(2)$,$w(3)=m(3)$,可得到 $m''=\{R,10,11,R\}$。其中 R 为随机的 2 bit 序列。

3.2　安全性分析

3.2.1　抗伪造性

假设敌手 Eve 截取了 Bob 发送给 Alice 的粒子,这时他有两种选择:

a)自己制备新的 n 个 EPR 粒子对,将每个对中的一个粒子发送给 Alice。Eve 冒充 Bob 对消息 m 进行签名。这种攻击虽然没有破坏 EPR 粒子对的纠缠性,但 Eve 也肯定不能取得成功,因为他没有 Bob 与 Charlie 的共享密钥 k_{BC},无法对测量结果进行加密,这样就很容易被 Charlie 识破。

b)不制备新的粒子,直接冒充 Alice 进行接收,并生成对自己有利的委托证书 $\tilde{w}$,同时根据证书对收到的粒子进行测量。他将面临同样的难题:不知道 Alice 与 Charlie 的共享密钥 k_{AC}。若 Charlie 对收到的结果顺利解密,并没有发现异常。那么结果肯定不能通过验证,因为加解密钥不对称必将破坏 EPR 粒子的纠缠性。

同样,Charlie 也不能伪造证书 w 或签名 M。

假设签名验证者 Charlie 是不诚实的,并且试图伪造 Alice 的委托证书 w 或 Bob 的代理签名 M。Charlie 知道密钥 k_{AB} 和 k_{AC},所以可以达到目的。但当发生纠纷时,Alice 和 Bob 可以各自公布他们对自己粒子的测量结果,对 Charlie 的伪造行为进行揭露。因为委托证书 w 和消息 m,与他们的测量结果各自惟一对应。另外,在测量时用到的测量基 B_X 和 B_Z 是非正交的,所以本方案可以抵御特洛伊木马攻击[17]。

3.2.2　不可否认性

Alice 不能否认他对签名权进行了委托:a)Alice 将发送 $W=E_{k_{AC}}\{w''(1),w''(2),\cdots,w''(n)\}$ 给 Charlie,其中用到的密钥 k_{AC} 只有 Alice 和 Charlie 知道;b)在收到 W 后 Charlie 可以对其解密,进而直接恢复出委托证书 w,其中包含有 Alice 的身份信息。所以 Alice 不可能否认他对签名权的委托。

同样,Bob 也不可能否认他对消息 m 的签名。因为 Bob 需要发送最终签名 M 给 Charlie,其中用到的密钥 k_{BC} 只有 Bob 和 Alice 知道;另外,也可以查看委托证书 w,因为 Bob 的身份信息也被包含在内。

4　结束语

本文基于 EPR 纠缠态,提出了一个量子代理签名方案。在新方案中,原始签名人 Alice 通过生成委托证书 w,并根据 w 去测量收到的粒子,来实现签名权的委托。验证人 Charlie 能够恢复出委托证书 w,同时根据 EPR 粒子的纠缠特性验证 Bob 的签名 M。

为了防止攻击者窜改委托证书 w 或签名 M,本方案使用 BB84 协议以及一次一密算法来保证方案的无条件安全性。同时,要求使用委托证书来防止不诚实的 Alice 否认对签名权的委托,或不诚实的 Bob 对签名的否认。本方案具有无条件安全性及较高的通信效率,并且在当前的技术及实验条件下完全能够实现。

参考文献:

[1] BENNETT C H, BRASSARD G. Quantum cryptography public-key distribution and coin tossing[C]//Proc of IEEE International Conference on Computers, Systems and Signal Processing. India: Bangalore Press,1984:175-179.

[2] BENNETT C H. Quantum cryptography using any two nonorthogonal states[J]. Phys Rev Lett,1992,68(21):3121-3124.

[3] DENG F G,LONG G L. Controlled order rearrangement encryption for quantum key distribution[J]. Phys Rev A,2003,68(4)2315- 1-4.

[4] LUCAMARINI M, MANCINI S. Secure deterministic communication without entanglement[J]. Phys Rev Lett,2005,94(14):140501-1-4.

[5] EKERT A K. Quantum cryptography based on Bell's theorem[J]. Phys Rev Lett,1991,67(6):661-664.

[6] 温晓军,刘云,张鹏云. 基于 EPR 粒子对的信息签名协议[J]. 大连理工大学学报,2007,47(3):424-428.

[7] 闫丽华,高云峰,赵建刚. 利用两个纠缠对隐形传递任意三原子 W 态[J]. 原子与分子物理学报,2008,25(6):1387-1403.

[8] SUDHEESH C, LAKSHMIBALA S, BALAKRISHNAN V. Dynamics of quantum observables in entangled states[J]. Physics Letters A, 2009,373(32):2819-2874.

[9] WANG Shu-mei, MA Hong-yang. Quantum secure communication network on EPR states[C]//Proc of International Conference on Network and Parallel Computing. 2008:545-548.

[10] WEN Jia-yan, QIU Dao-wen. Adiabatic quantum evolution for preparation of quantum entanglement states[C]//Proc of the 27 th Chinese on Control Conference. 2008:177-181.

[11] SHI Guo-fang, XI Xiao-qiang, TIAN Xiu-lao, *et al*. Bidirectional quantum secure commication based on a shared private Bell state[J]. Optics Communications,2009,282(12):2460-2463.

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

[13] LU Xin, FENG Deng-guo. Quantum digital signature based on quantum one-way functions[R/OL]. (2003). http://arxiv.org/abs/quant-ph/0403046.

[14] 邵博闻,欧海文. 基于量子单向函数的量子门限签名方案[J]. 微计算机信息,2007(18):60-62.

[15] 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):1-3.

[16] 杨宇光,温巧燕. 具有门限共享验证的门限代理量子签名方案[J]. 中国科学 G 辑:物理学 力学 天文学,2008,38(7):834-843.

[17] ZENG G H. Security of quantum cryptography algorithm against Trojan horse attacking[J]. Journal of Software,2004,15(8):1259-1264.

[18] 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.