第41卷第10期 中国科学技术大学学报 Vol. 41, No. 10
2011年10月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Oct. 2011

文章编号:0253-2778(2011)10-0924-04

广播多重量子数字签名方案的设计与分析

杨亚涛[1],薛 霆[1,2],李子臣[1]

(1.北京电子科技学院,北京 100070;2.西安电子科技大学通信工程学院,陕西西安 710071)

摘要:提出了一种广播多重量子数字签名方案,通过执行CNOT操作来对所要签名的信息进行加密,并利用幺正变换来实现信息的签名和验证.分析表明,本方案不受签名者多少的限制,具有可验证性,安全性高且技术实现简单,是一种可实现的广播多重量子数字签名方案.

关键词:量子签名;广播多重签名;幺正变换;CNOT操作

中图分类号:TP393.08 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2011.10.013

Design and analysis of broadcasting multiple quantum digital signature scheme

YANG Yatao[1], XUE Ting[1,2], LI Zichen[1]

(1. *Beijing Electronic Science and Technology Institute*, *Beijing* 100070, *China*;
2. *Communication Engineering Institute*, *Xidian University*, *Xi'an* 710071, *China*)

Abstract: A broadcast multiple quantum digital signature scheme was proposed, which encrypted messages to be signed by conducting CNOT operation, and used unitary transformation to realize information signature and validation. Analysis shows that, the scheme is not affected by the restrictions of the number of signers, capable of verifiability, high safety and simple technical implementation, and is thus a realizable broadcasting multiple quantum digital signature scheme.

Key words: quantum signature; broadcasting multi-signature; unitary transformation; CNOT operation

0 引言

经典数字签名中,常常需要多个用户对同一个消息进行签名和认证.能够实现多个用户对同一消息进行签名的数字签名称为多重数字签名.根据签名过程的不同,多重数字签名方案可分为两类:一类为有序多重数字签名方案[1-2],另一类为广播多重数字签名方案.

1994年,Harn首次设计了一种广播多重数字签名方案[3-4].Harn广播多重签名方案包含:系统初始化、单用户签名产生过程、单用户签名验证过程、多重签名产生过程和多重签名验证过程.在整个方案中包含:消息发送者 U_I,签名者 U_i,签名收集者 U_c,和签名验证者 U_v. U_I 将消息 m 同时发送到 U_i 进行签名,其中 U_i 为第 i 个签名者.U_i 将签名信息发送到签名收集者 U_c,U_c 收到签名信息后验证签名的有效性,如果有效,对签名进行计算整理产生多重签名,然后将整理后的多重签名发送到 U_v 进行验证.其中 U_I 不参加数字签名.

量子密码学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.研究方向主要包括量子密钥分配(QKD)[5-6]、量子安全直接通信(QSDC)[7]、量子秘密共享(QSS)、量子数字签名以及量子身份认证(QIA)[8-9]等方面.

2001年,我国学者曾贵华教授首次提出了量子数字签名[10]的概念,并提出了基于GHZ三重态粒

收稿日期:2011-04-28;**修回日期**:2011-06-21

基金项目:国家自然科学基金(61070219),北京电子科技学院信息安全重点实验室课题(YZDJ1004)资助.

作者简介:杨亚涛(通讯作者),男,1978年生,博士/讲师.研究方向:信息安全与密码学.E-mail:yyt2011@gmail.com

子的一种量子仲裁的量子数字签名方案.但该方案属于仲裁签名(arbitrated signature)方案,需要一个可信赖的系统管理员参与且只支持一个签名用户.同年,以色列学者 Gottesman 等提出了一种利用量子单向函数产生公钥,并采用量子 Swap-test 来验证签名的方案[11],该方案能够实现多个用户对同一签名消息进行验证,可惜无法实现多个用户对同一消息进行签名,而且该方案只完成了对经典比特串的签名,属于原理性签名方案.

本文提出了一种量子广播数字签名方案,借助 CNOT 操作来加密签名信息,采用幺正变换来生成签名信息,同时依赖于量子密钥分配的无条件安全性来保证方案的安全性.本方案根据经典情形下的广播多重签名的模型,实现了多个用户对同一消息的签名.方案中签名收集者收集各个签名者的签名信息,合并生成多重签名,最后的签名验证者对多重签名信息进行验证.本方案安全性高,实现简单.

1　量子广播多重数字签名方案

广播多重数字签名方案的参与对象为消息发送者 U_1,签名者 U_i,签名收集者 U_c,和签名验证者 U_v.在本方案中,设 Alice 为消息发送者,Bob 为签名验证者,Charlie 为签名收集者,$U_1,U_2,\cdots,U_i$ 为签名者.方案分 5 个阶段,分别为系统初始化、单用户签名产生阶段、单用户签名验证阶段、合并多重签名生成阶段和合并多重签名验证阶段.

1.1　系统初始化

①密钥分发:Alice,U_i 和 Charlie 通过量子信道和经典信道遵循 BB84 协议来获得各自的密钥.其中 K_{AU_i},K_{CU_i} 为密钥.分别为 Alice 和 U_i,U_i 和 Charlie 之间的密钥.

②Alice 欲给经典二进制信息 $M(i)$ 进行签名,首先制备 i 粒子序列 $\psi_i=[P_1,P_2,\cdots,P_i]$,粒子状态分别为$|0\rangle(|1\rangle)$,与要签名的消息比特一一对应,例如,若 $M(i)=\{01011100\}$,则 ψ_i 的状态为$|\psi_i\rangle=\{|0\rangle,|1\rangle,|0\rangle,|1\rangle,|1\rangle,|1\rangle,|0\rangle,|0\rangle\}$.并制备 N 个 EPR 纠缠对 $S=[(P_1(1),P_1(2));(P_2(1),P_2(2));\cdots;(P_N(1),P_N(2))]$,纠缠态如下:

$$|\delta_{xy}\rangle=\frac{1}{\sqrt{2}}(|0\rangle_x|0\rangle_y+|1\rangle_x|1\rangle_y),$$

其中 $N=i$.

③Alice 通过受控非门(CNOT)操作来对粒子序列 ψ_i 进行加密.例如,Alice 对粒子 p_i 和 ψ_i 执行 CNOT 操作,其中 c_i 代表控制粒子,p_i 代表受控粒子,Alice 随机选取 x_i 或者 y_i 作为控制粒子,表达如下:

$$C_{c_ip_i}|\delta_{x_iy_i}\rangle|m_i\rangle_{p_i}=\frac{1}{\sqrt{2}}(|00m_i\rangle+|11\overline{m_i}\rangle)_{x_iy_ip_i}$$

其中,$m_i=1-\overline{m_i}$;并把加密后的粒子序列 ψ_i 传给 U_i,同时使用密钥 K_{AU_i} 加密一个信息,告诉 U_i 所选用的控制粒子 c_i.

1.2　单用户签名产生阶段

①U_i 收到粒子序列后,对每一个粒子执行 CNOT 操作来恢复出消息.例如:使用 K_{AU_i} 解密后得知 Alice 所选用的控制粒子为 x_i,则执行 CNOT 操作后系统状态为

$$C_{c_ip_i}\frac{1}{\sqrt{2}}(|00m_i\rangle+|11\overline{m_i}\rangle)_{x_iy_ip_i}=|\delta_{xy}\rangle_{x_iy_i}|m_i\rangle_{p_i}$$

U_i 采用 B_Z 基$\{|0\rangle,|1\rangle\}$测量 ψ_i 中的每一个粒子,所得测量结果恰好是信息 $M(i)$.

②U_i 将 $M(i)$的每一比特与密钥 K_{CU_i}的每一位作比较,进行如下异或操作:如果某一位相等,则记作“0”,否则记作“1”.例如,$M(i)=(010110)$,$K_{CU_i}=(110010)$,$M(i)\oplus K_{CU_i}=(100100)$.

③U_i 利用 $M\oplus K_{CU_i}$ 和 N 粒子序列 ψ_i,为消息 $M(i)$生成一个量子态$|\phi\rangle$.

$$|\phi\rangle=|\varphi_{K_{CU_1},M(1)}\rangle\otimes|\varphi_{K_{CU_2},M(2)}\rangle\otimes\cdots\otimes|\varphi_{K_{CU_i},M(i)}\rangle$$

其中量子比特$|\varphi_{M(i)\oplus K_{CU_i},M(i)}\rangle$处于下面的态之一:

$$|\varphi_{0,0}\rangle=|0\rangle$$

$$|\varphi_{1,0}\rangle=|1\rangle$$

$$|\varphi_{0,1}\rangle=(|0\rangle+|1\rangle)/\sqrt{2}$$

$$|\varphi_{1,1}\rangle=(|0\rangle-|1\rangle)/\sqrt{2}$$

$M(i)$的值决定基:如果 $M(i)$是 0,那么用 Z 基$\{|0\rangle,|1\rangle\}$编码;如果 $M(i)$是 1,那么用 X 基$(|0\rangle\pm|1\rangle)/\sqrt{2}$编码,形成单光子的 M 序列.

④对$|\phi\rangle$做幺正变换 W^1,

$$W^1:|\phi\rangle\rightarrow|\phi^1\rangle$$

式中,W^1 定义为

$$W^1=U_1^1V_1^1\otimes U_2^1V_2^1\otimes\cdots\otimes U_i^1V_i^1$$

其中

$$U_i^1=U(M(i)\oplus K_{CU_i}),$$

$$V_i^1=V(M(i)),$$

$$U(0)=|0\rangle\langle0|+|1\rangle\langle1|,$$

$$U(1)=|0\rangle\langle1|-|1\rangle\langle0|,$$

$$V(0)=|0\rangle\langle0|+|1\rangle\langle1|,$$

$$V(1)=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\langle 0|+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\langle 1|$$

得到新的单光子 M 序列 $|\phi^1\rangle$，该序列即为 U_i 的签名信息 $|S_{U_i}\rangle$.

⑤将信息 $(M(i),|S_{U_i}\rangle)$ 传给签名收集者 Charlie.

1.3 单用户签名验证阶段

在这个阶段，签名收集者 Charlie 将验证签名者 U_i 的签名信息，具体步骤如下：

①Charlie 对 $|S_{U_i}\rangle$ 做幺正变换 W^2，

$$W^2:|\phi^1\rangle\rightarrow|\phi^2\rangle$$

W^2 定义为

$$W^2=U_1^2V_1^2\otimes U_2^2V_2^2\otimes\cdots\otimes U_i^2V_i^2$$

其中

$$U_i^2=U(M(i)\oplus K_{CU_i}),V_i^2=V(M(i)),$$

$$U(0)=|0\rangle\langle 0|+|1\rangle\langle 1|,$$

$$U(1)=|0\rangle\langle 1|-|1\rangle\langle 0|,$$

$$V(0)=|0\rangle\langle 0|+|1\rangle\langle 1|,$$

$$V(1)=\frac{1}{\sqrt{2}}(|0\rangle+|1\rangle)\langle 0|+\frac{1}{\sqrt{2}}(|0\rangle-|1\rangle)\langle 1|$$

得到新的单光子 M 序列 $|\phi^2\rangle$.

②对 $|\phi^2\rangle$ 采用 B_Z 基 $\{|0\rangle,|1\rangle\}$ 测量，所得测量结果恰好是明文信息 $M(i)$，若测量结果不相等，则拒绝签名.

1.4 合并多重签名生成阶段

该阶段 Charlie 收集所有个人签名信息 $|S_{U_i}\rangle$ 以构造合并多重签名 $|S_M\rangle$，具体步骤如下：

①Charlie 首先制备 i 个 EPR 纠缠对 $L=[(q_1(1),q_1(2));(q_2(1),q_2(2));\cdots;(q_i(1),q_i(2))]$，纠缠态如下：

$$|\mu_{xy}\rangle=\frac{1}{\sqrt{2}}(|0\rangle_x|0\rangle_y+|1\rangle_x|1\rangle_y).$$

②Charlie 对粒子 X_i 和 $|S_{U_i}\rangle$ 执行 CNOT 操作，其中 x_i 代表控制粒子，u_i 代表受控粒子，表达如下：

$$C_{x_iU_i}|\mu_{xy}\rangle_{x_iy_i}|S_{U_i}\rangle=\frac{1}{\sqrt{2}}(|00S_{U_i}\rangle+|11\overline{S}_{U_i}\rangle)_{x_iy_iU_i},$$

$$S_{U_i}=1-\overline{S}_{U_i};$$

并把加密后的粒子序列 $|S_{U_i}\rangle$ 传给 Bob，除了发送 $|S_{U_i}\rangle$，还将 $M(i)\oplus K_{CU_i}$ 发送给验证者 Bob. 则 $|S_M\rangle$ 表示为

$$|S_M\rangle=\{M(i)\oplus K_{CU_i},|S_{U_i}\rangle\}$$

③Charlie 发送 $(M(i),|S_M\rangle)$ 给 Bob.

1.5 合并多重签名验证阶段

①Bob 收到粒子序列后，对每一个粒子执行 CNOT 操作来恢复出消息，例如：

$$C_{x_iU_i}\frac{1}{\sqrt{2}}(|00S_{U_i}\rangle+|11\overline{S}_{U_i}\rangle)_{x_iy_iU_i}=|\mu_{xy}\rangle_{x_iy_i}|S_{U_i}\rangle$$

②Bob 对 $|S_{U_i}\rangle$ 做幺正变换 W^2，得到新的单光子 M 序列 $|\phi^2\rangle$.

③对 $|\phi^2\rangle$ 采用 B_Z 基 $\{|0\rangle,|1\rangle\}$ 测量，所得测量结果恰好是明文信息 $M(i)$. 若测量结果不相等，则拒绝签名；若相等则接受 $|S_M\rangle$ 为所有用户对 $M(i)$ 的真实多重签名.

2 方案分析

广播多重数字签名不是由签名成员所生成的多个单签名简单累加生成的，而是由每个签名成员生成部分签名，以合并的方式生成多重签名. 其中部分签名的长度固定，不随签名人数的改变而变化. 这就要求参与签名的所有人员都不能篡改和伪造签名. 下面我们从方案的正确性和安全性上来分析本方案.

2.1 正确性分析

CNOT 操作可简单描述如下：若控制比特置为 0，则目标量子比特将保持不变；若控制量子比特置为 1，目标量子比特将翻转. 即 $|A,B\rangle=|A,B\oplus A\rangle$，其中 $\oplus$ 为模二加法. 那么，我们可以得到结论，CNOT 操作就是控制量子比特和目标量子比特作异或运算，并将结果存放在目标量子比特中. 由此我们可以得到下面的结论：

结论 2.1 经过两次 CNOT 操作后，目标量子比特的状态不变.

幺正变换在量子系统的演变中起重要作用. 设有算符 U，U 的共轭转置是 $U^\dagger$，若

$$U^\dagger=U^{-1}$$

则称 U 为幺正变换(算符). 式中，U^{-1} 是 U 的逆算符($UU^{-1}=U^{-1}U=I$)，I 是等同算符. 设 $|s\rangle$ 和 $|t\rangle$ 是空间中任意两个矢量，其内积为 $|s,t\rangle=|s,t\oplus s\rangle$. 以幺正算符 U 作用于 $|s\rangle$ 及 $|t\rangle$ 后得到的矢量是 $U|s\rangle$ 及 $U|t\rangle$，其内积为 $(U|s\rangle,U|t\rangle)$，由 $(U|s\rangle)^\dagger=\langle s|U^\dagger$ 可得

$$(U|s\rangle,U|t\rangle)=\langle s|U^\dagger U|t\rangle=\langle s|t\rangle$$

由这个结论我们得出以下结论：

结论 2.2 空间中任意两个矢量经幺正变换后其内积保持不变.

根据上述两个结论，我们来分析本方案的正确性.

(Ⅰ) 解密签名信息的正确性

本方案中消息发送者 Alice 首先使用 EPR 纠缠对，执行 CNOT 操作将所需要签名的信息进行加密，签名者 U_i 接收到消息以后，再执行一次 CNOT 操作来进行解密. 由结论 2.1，我们就可以正确地解密签名信息.

（Ⅱ）签名信息的可验证性

本方案中签名者将接收到的消息 $M(i)$ 通过编码转化为量子态，并将该量子态经过幺正变换后得到签名信息. 签名验证者接收到签名信息后，再经过一次幺正变换，得到签名者原始的量子态，测量该量子态，测量结果应与恢复出的原始的签名信息 $M(i)$ 一致.

根据结论 2.2，我们可以保证经过两次幺正变换后的量子态保持不变，那么它们的测量结果也不变，这就保证了签名信息的可验证性.

2.2　安全性分析

①敌手 Eve 不可能假冒签名. 在本方案中签名者 U_i 首先需要使用密钥 K_{AU_i} 解密获得 CNOT 操作中控制粒子 c_i，否则将不能获得所需要的签名信息 $M(i)$，而 K_{AU_i} 是通过已被证明为无条件安全的 QKD 协议获得的，因此 Eve 得不到所需要的签名信息. 签名过程中，签名者 U_i 将签名信息 $M(i)$ 的每一比特与密钥 K_{CU_i} 的每一位进行异或操作，并根据该异或结果将原始信息 $M(i)$ 转换为量子态，而编码基的选择由 $M(i)$ 的值决定. 密钥 K_{CU_i} 是通过已被证明为无条件安全的 QKD 协议获得的，所以敌手 Eve 不可能得到原始信息的量子态. 综上，Eve 既得不到所需要的签名信息，也不可能得到原始信息的量子态，所以 Eve 不能假冒签名.

②签名者 U_i 不能否认他的签名. 因为每份签名信息 $M(i)$ 的获得都需要使用他的密钥 K_{AU_i}，而且签名信息 $|S_{U_i}\rangle$ 中也包含着他的密钥 K_{CU_i}，所以签名者无法抵赖他的签名.

③签名收集者 Charlie 和最后验证签名的 Bob 均不能伪造签名. 原始签名信息 $M(i)$ 是由签名者 U_i 使用 K_{AU_i} 解密后得知 Alice 所选用的控制粒子，通过执行 CNOT 操作恢复出来的. Charlie 和 Bob 所获得的签名信息 $M(i)$ 均是通过对 $|\phi^2\rangle$ 进行测量后得到的，并不能直接得到签名信息 $M(i)$. 若他们其中一个伪造签名信息，发生纠纷时，由消息发送者提供原始签名信息 $M(i)$ 与之进行比对.

3　结论

本文提出了一种有效的量子广播多重签名方案，本方案借助 CNOT 操作来加密签名信息，采用幺正变换来生成签名信息，同时依赖于量子密钥分配的无条件安全性来保证方案的安全性. 本方案的原理与运算均基于量子物理特性，其安全系数高、技术实现简单. 不过本方案没有考虑到信道的衰减和窃听者的攻击可能造成的量子态的丢失，这将是下一步的工作方向.

参考文献（References）

[1] Wu T, Chou S. Two-based multi-signature protocols for sequential and broadcasting architectures [J]. Computer Communications, 1996, 9: 851-856.

[2] Li Zichen, Yang Yixian. ElGamal's multisignature digital signature scheme [J]. Journal of Beijing University of Posts and Telecommunications, 1999, 22(2): 30-34.
李子臣，杨义先. ElGamal 多重数字签名方案[J]. 北京邮电大学学报，1999，22(2)：30-34.

[3] Harn L, Xu Y. Design of generalized ElGamal type digital signature schemes based on discrete logarithm [J]. Electronics Letters, 1994, 30(24): 2 025-2 026.

[4] Harn L. New digital signature scheme based on discrete logarithm[J]. Electronics Letters, 1994, 30(5): 396-397.

[5] Bennett C H, Brassard G. An update on quantum cryptography [C]// Advance in Cryptology: Proceedings of Crypto84. Berlin: Springer-VerLag, 1984: 475-480.

[6] Sun Ying, Wen Qiaoyan, Zhu Fuchen. Quantum Secure Communication Based on the Reusable Bases Sequences[J]. Acta Electronica Sinica, 2010, 38(1): 111-116.
孙莹，温巧燕，朱甫臣. 基于可重用基序列的量子安全通信方案[J]. 电子学报，2010，38(1)：111-116.

[7] 高飞，郭奋卓，温巧燕，等. 重新审视量子对话和双向量子安全直接通信的安全性[J]. 中国科学(G 辑：物理学力学 天文学)，2008，38(5)：477-484.

[8] Curty M, Santos D J. Qubit authentication[J]. Phys Rev A, 2002, 66: 022301.

[9] 张兴兰. 基于公钥的单向量子身份认证[J]. 科学通报，2009，10(54)：1 415-1 418.

[10] Zeng Guihua, Ma Wenping, Wang Xinmei, et al. Signature Scheme Based on Quantum Cryptography [J]. Acta Electronica Sinica, 2001, 29(8): 1-3.
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.

[11] Gottesman D, Chuang I. Quantum Digital Signatures [DB/OL]. (2001-11-15)[2011-04-20]. http://arxiv.org/abs/quant-ph/0105032.