基于量子密码的签名方案

曾贵华[1],马文平[2],王新梅[2],诸鸿文[1]
(1. 上海交通大学电子工程系,上海 200030;2. 西安电子科技大学 ISN 理论与关键技术国家重点实验室,陕西西安 710071)

摘 要: 本文首次研究了量子签名问题,并提出了一个基于对称密码体制的量子签名方案. 所提出的量子签名方案利用量子力学中的 Greenberger-Horne-Zeilinger (GHZ) 三重态的相干特性实现对量子比特串的签名和验证.

研究表明本文提出的量子签名方案具有可证明安全性.

关键词: 量子签名; 量子密码; 数字签名

中图分类号: TN918.1 **文献标识码**: A **文章编号**: 0372-2112 (2001) 08-1098-03

Signature Scheme Based on Quantum Cryptography

ZENG Gui-hua[1], MA Wen-ping[2], WANG Xin-mei[2], ZHU Hong-wen[1]
(1. *Electrical engineer department of Shanghai Jiaotong university, Shanghai* 200030, *China*;
2. *National Key lab. on ISN, Xidian university, Xi'an, Shanxi* 710071, *China*)

Abstract: In this paper, the principle of the quantum signature has been investigated, and a quantum signature scheme has been proposed. The presented scheme is based on the correlation of the Greenberger-Horne-Zeilinger (GHz) triplet state. Results show that the proposed quantum signature scheme is provable secure.

Key words: quantum signature; quantum cryptography; digital signature

1 引言

利用量子物理现象或效应对信息进行保密通信,是 1969 年哥伦比亚大学的 S. Wiesner 首先提出的[1]. 遗憾的是他的这一思想当时没有被人们接受. 十年后,IBM 公司的科学家 C. H. Bennett 和加拿大 Montreal 大学的密码学家 G. Brassard 重新捡起这一工作,并在此基础上提出了量子密码 (Quantum cryptography) 的概念[2]. 1984 年 Bennett 和 Brassard 提出了国际上第一个量子密钥分发协议,即著名的 BB84 协议[2]. 1989 年,IBM 公司和 Montreal 大学合作首次完成了量子密码中的第一个实验,对 BB84 协议从实验上做了验证[3],该实验利用光子在自由空间中传输来传递信息. 这个实验的通信距离虽然只有 32cm,但具有极其重要的意义. 1997 年,美国洛斯阿拉莫斯将光子在自由空间中的通信距离延伸到了 205m. 量子密码的第一个实验完成后不久,人们便开展了光纤中的实验研究. 最近英国电信局 (British Telecom) 将光纤中通信距离延长到超过 30 公里[4]. 目前更大的计划在欧洲进行,人们 (特别是美国政府和军方) 期望在不久的将来量子密码得以实用化.

量子密码以量子力学为基础,这一点不同于以往的以数学为基础的密码体制. 由于量子密码的安全性得到了测不准原理或量子相干性的保证,这种体制具有可证明的安全性,同时还能对窃听者的行为很容易地进行检测. 这些特性使得量子密码具有以往密码体制所没有的优势,因而量子密码引起了国际密码学界和物理学界的高度重视. 到目前为止,人们在量子密码学理论和实验研究方面获得了一系列的研究成果,主要包括以下几个方面: (1) 量子密码信息理论基础; (2) 量子密钥管理; (3) 量子秘密共享; (4) 量子比特承诺及其应用; (5) 量子认证; (6) 量子多方计算; (7) 量子密码检测理论等. 所有这些方面的研究都是与经典密码 (这里'经典'相对于'量子'而言) 类比而进行的,也就是说,为了实现某个协议或某个算法,人们试图利用某个 (或多个) 量子效应或原理来实现. 这与经典密码中的方法类似: 为了实现某种协议或某个算法,人们试图利用某个 (或多个) 数学原理或理论来实现.

在量子保密通信的过程中,象经典保密通信一样也会涉及到签名的问题,但这个方面还没有人研究. 在现实世界里,签名是一件重要的事情,例如在商务、外交、军事等许多方面都需要对文件签字后方可生效. 传统的方法是采用手写签字,计算机出现后,人们提出数字签字的概念. 所谓数字签字就是对数字文件进行数字化签字,从而使数字文件具有法律效应. 最近量子通信和量子计算机的研究取得了迅速的进展[5],特别是量子计算机,它的出现使得对量子比特签名成为重要的课题;同时即使没有量子计算机,量子签名也是非常重要的,因为量子签名利用量子效应或原理实现,象密钥分发一样具有经典签名所没有的优势. 考虑到这些方面,本文首次研究了量子签名问题,包括方案的算法原理,物理原理等方面,并提出了一个量子签名算法,讨论它的安全性.

2 算法描述

数字签名包括两类[6]: 真实签名 (*True signature*) 和仲裁签名 (*Arbitrated signature*). 其中在真实签名中,实现过程不依赖

收稿日期: 2000-04-14; 修回日期: 2001-04-09
基金项目: 本文为国家自然科学基金 (No. 69803008)

于仲裁,只在有争议的时候才需要仲裁,而在仲裁签名中,其实现过程依赖于仲裁. 本文利用量子力学中的 GHZ 三重态实现量子仲裁签名,这是一个基于对称密钥体制的量子签名方案,该算法需要一个可信赖的系统管理员 Trent. 算法按如下步骤实现对量子比特串的签名和验证.

2.1 初始化

(1) Alice 和 Bob 各自获得秘密钥 K_a, K_b,这里 K_a, K_b 分别是 Alice 和 Trent 及 Bob 和 Trent 之间的密钥. K_a 和 K_b 可以通过量子密码的方法获得,从而使 Alice 和 Bob 获得的密钥具有无条件安全性. 本方案中我们选用著名的 BB84 协议来获取 K_a, K_b,理由是 BB84 协议简单而且容易实现.

(2) Alice 向系统提出申请. 当 Alice 和 Bob 之间需要通信时,Alice 或 Bob 首先向 Trent 提出申请.

(3) Trent 分发 GHZ 粒子. 收到申请后,Trent 制备 GHZ 三重态序列,并将每一个 GHZ 三重态$|\Psi\rangle$中的两个粒子分别分发给参与通信的两方 Alice 和 Bob(亦可采用其他分发方式),使 Trent,Alice 和 Bob 各持有每一个 GHZ 三重态的一个粒子,这三个粒子是纠缠的,在未测量之前三粒子的状态不能决定. GHZ 三重态有八个可能的量子态,本方案中选取如下的态:

$$|\Psi\rangle = (1/\sqrt{2})(|0\ 0\ 0\rangle + |1\ 1\ 1\rangle). \tag{1}$$

以上过程中,第 1 步在系统建立时完成,第 2、3 步在通信时于签名之前完成.

2.2 签名过程

(1) Alice 制备与消息 M 对应的量子比特串. 设 Alice 要发送的消息为 M,对应的量子比特串为

$$|\Psi_M\rangle = \{|\Psi_1\rangle, |\Psi_2\rangle, \cdots, |\Psi_n\rangle\} \tag{2}$$

用本征态$|0\rangle$,$|1\rangle$表示,则

$$|\Psi_i\rangle = \alpha_i|0\rangle + \beta_i|1\rangle \tag{3}$$

于是 Alice 的量子消息可表示为

$$|\Psi_M\rangle = \{\alpha_1|0\rangle + \beta_1|1\rangle, \alpha_2|0\rangle + \beta_2|1\rangle, \cdots, \alpha_n|0\rangle + \beta_n|1\rangle\} \tag{4}$$

式中 α_i、β_i 为复数, $\|\alpha_i\|^2 + \|\beta_i\|^2 = 1$, $i = 1, 2, \cdots, n$.

(2) Alice 加密量子比特$|\Psi_N\rangle$. 将 Alice 的密钥 K_a 转化为测量基序列 M_{K_a},转化的方式可按文献[7]的方法实现. 转化后得到的测量基序列为一个量子力学算符集:

$$M_{K_a} = \{M^1_{K^1_a}, M^2_{K^2_a}, \cdots, M^n_{K^n_a}\}, \tag{5}$$

式中 $M^i_{K^i_1}$依赖于 K^i_1, $i = 1, 2, \cdots, n$,这里我们假定 K_a 中有 n 个比特. 用 M_{K_a} 作用于消息量子比特串$|\Psi_m\rangle$后得到

$$|\phi\rangle = M_{K_a}|\Psi\rangle = \{|\phi_1\rangle, |\phi_2\rangle, \cdots, |\phi_n\rangle\} \tag{6}$$

式中$|\phi_i\rangle = M_{K_a}|\Psi_i\rangle$,表示$|\phi\rangle$中的第 i 个量子比特.

(3) Alice 测量粒子对. Alice 将要发送的量子比特串中的每一个粒子态$|\Psi_i\rangle$, $i = 1, 2, \cdots, n$ 与自己的每一个 GHZ 粒子结合,然后 Alice 根据相应粒子的状态从四维 Hilbert 空间中的 Bell 基$\{|\Psi^+_{12}\rangle, |\Psi^-_{12}\rangle, |\Phi^-_{12}\rangle, |\Phi^+_{12}\rangle\}$中选取合适的测量基对粒子对进行测量. Alice 将量子消息中每一个粒子对应的测量基组成的序列记为 R_a.

(4) Alice 获得签名 S_a. 用 K_a 加密 R_a 和$|\phi\rangle$得到

$$S_a = K_a(|\Psi_i\rangle, |\phi\rangle) \tag{7}$$

式中$|\Psi_i\rangle = \{|\Psi^+_{12}\rangle, |\Psi^-_{12}\rangle, |\Phi^-_{12}\rangle, |\Phi^+_{12}\rangle\}$,这里 S_a 即为量子消息$|\Psi_m\rangle$的签名.

(5) Alice 发送签名 S_a. 完成上述步骤后,Alice 将 S_a 发送给 Bob,其中包括了 R_a.

2.3 验证过程

本方案的验签过程需要系统管理员 Trent 的参与. 以下步骤实现验签过程.

(1) Bob 随机测量自己的 GHZ 粒子. 收到 Alice 发送来的消息,Bob 用沿 x 方向的测量基测量自己的每一个 GHZ 粒子,获得结果$|+x\rangle$或$|-x\rangle$,Bob 将对每一个粒子的测量结果构成的序列用 R_b 表示,用 K_b 加密 R_b, S_a,$|\Psi_M\rangle$得到

$$y_b = K_b(|x_i\rangle, S_a, |\Psi_M\rangle) \tag{8}$$

式中$|x_i\rangle = \{|+x\rangle, |-x\rangle\}$. 然后 Bob 将 y_b 发送给 Trent.

(2) Trent 获取参数 γ. Trent 收到 y_b 后用 K_b 解密获得 S_a、$|\Psi_m\rangle$、R_b,然后对 S_a 用 K_a 解密得到$|\phi'\rangle$. 借助于密钥 K_a, Trent 通过下面的条件获取参数 γ:

$$\gamma = \begin{cases} 1 & |\phi'\rangle = M_{k_a}|\Psi_m\rangle \\ 0 & |\phi'\rangle = M_{k_a}|\Psi_m\rangle \end{cases} \tag{9}$$

(3) Trent 测量 GHZ 粒子. 根据 Alice 和 Bob 的测量结果,即 R_a、R_b, Trent 选择相应的测量基测量相应的 GHZ 粒子. 测量完成后获得 R_t,然后 Trent 将 R_a, R_b, R_t 及 S_a 用 K_b 加密得到

$$y_{tb} = K_b(R_a, R_b, R_t, \gamma, S_a) \tag{10}$$

再将 y_{tb}送给 Bob.

(4) Bob 解密 y_{tb}. 解密后 Bob 得到 R_a、R_b、R_t、S_a 及参数 γ.

(5) Bob 验证签名. 这一步由两步完成,首先 Bob 根据解密后得到的参数来做初步判定:若 $\gamma = 0$ 则拒绝;若 $\gamma = 1$,Bob 根据 R_a、R_b、R_t 及 GHZ 三重态的相干性获得量子消息$|\Psi'_M\rangle$,若$|\Psi'_M\rangle = |\Psi_M\rangle$接受,否则拒绝.

以下我们对上述的验签过程对应的物理原理做简单描述. 在量子比特的传输及验签过程中采用 GHZ 三重态实现,实际上是采用了多粒子的 Teleperation 量子信息传输效应. 不失一般性,下面只须讨论$|\Psi_M\rangle$中的任意一个量子比特$|\Psi_i\rangle$与 Alice 的相应一个 GHZ 粒子结合成为的粒子对并传输和验签的情况,其它粒子对都是同样处理. 当 Alice 将其 GHZ 粒子与量子比特$|\Psi_i\rangle = \alpha_i|0\rangle_a + \beta_i|1\rangle^a$ 进行量子力学结合,然后用 Bell 基测量他的粒子对后,得到

$$|\Psi_\pm\rangle_{Aa} = (1/\sqrt{2})(|0\ 0\rangle_{Aa} + |1\ 1\rangle_{Aa}) \tag{11}$$

$$|\Phi_\pm\rangle_{Aa} = (1/\sqrt{2})(|0\ 1\rangle_{Aa} + |1\ 0\rangle_{Aa}) \tag{12}$$

量子比特$|\Psi_i\rangle_4$ 的引入及 Alice 对粒子对的测量对原来的 GHZ 三粒子态产生影响,使其成为四粒子态,并且粒子状态为

$$\begin{aligned} |\Psi\rangle_4 = (1/2)\{&|\Psi_+\rangle_{Aa}(\alpha_i|00\rangle_{tb} + \beta_i|11\rangle_{tb}) \\ &+ |\Psi_-\rangle_{Aa}(\alpha_i|00\rangle_{tb} + \beta_i|11\rangle_{tb}) \\ &+ |\Phi_+\rangle(\beta_i|00\rangle_{tb} + \alpha_i|11\rangle_{tb}) + |\Phi_+\rangle_{Aa}(\beta_i|00\rangle_{tb} + \alpha_i|11\rangle_{tb}) \end{aligned} \tag{13}$$

若为 Alice 的结果为$|\Psi_+\rangle_{Aa}$或$|\Psi_-\rangle_{Aa}$,则 Bob 的单粒子的密度矩阵(GHZ 粒子)为

$$\rho_b = |\alpha_i|^2|0\rangle_{bb}\langle 0| + |\beta_i|^2|1\rangle_{bb}\langle 1| \tag{14}$$

若为 Alice 的结果为$|\Phi_+\rangle_{Aa}$或$|\Phi_-\rangle_{Aa}$,则 Alice 的单粒子密度矩阵为

$$\rho_b = |\beta_i|^2|0\rangle_{bb}\langle 0| + |\alpha_i|^2|1\rangle_{bb}\langle 1| \quad (15)$$

但两种情况中,即使 Bob 获得了 Alice 的结果 R_a^i(与$|\Psi_i\rangle$对应的 Bell 测量基),也只能获得量子比特$|\Psi_i\rangle$的部分信息. 因为 Alice 的测量导致了三粒子 GHZ 态解纠缠,但 Trent 和 Bob 的粒子形成一对纠缠态,且量子比特$|\Psi_i\rangle$已传输到这个纠缠态上,这对纠缠态可表示为

$$|\Psi\rangle_{tb} = \alpha|00\rangle + \beta|11\rangle \quad (16)$$

Bob 的测量能确定$|\Psi\rangle_{AB}$的部分信息,另一部分必须使用 Trent 的测量结果 R_t^i 才能获得,也就是说,要获得$|\Psi_i\rangle$的完全信息,需要同时有 R_a、R_t 和 R_b,这是由 GHZ 三重态的相干性所决定的. 当这些条件均具备时,可由如下方式获得

$$\begin{aligned}
&|\Psi_+\rangle_{Aa}|+x\rangle_t \to I, |\Phi_+\rangle_{Aa}|+x\rangle_t \to \sigma_x,\\
&|\Psi_+\rangle_{Aa}|-x\rangle_t \to \sigma_z, |\Phi_+\rangle_{Aa}|-x\rangle_t \to \sigma_x\sigma_z,\\
&|\Psi_-\rangle_{Aa}|+x\rangle_t \to \sigma_z, |\Phi_-\rangle_{Aa}|+x\rangle_t \to \sigma_x\sigma_z,\\
&|\Psi_-\rangle_{Aa}|-x\rangle_t \to I, |\Phi_-\rangle_{Aa}|-x\rangle_t \to \sigma_x,
\end{aligned} \quad (17)$$

由上述描述的 GHZ 三重态的特性可知,当 R_a、R_b、R_t 不能满足其相干性时,验签过程不可能通过.

因为 Bob 获得信息 M 必须得到系统管理员 Trent 的测量结果 R_t,因此本算法除了可以实现上述描述的量子签名外,还可实现不可否认量子签名,即 Bob 要获得签字,必须首先获得签字方的同意. 不可否认签字也是签名中的一个重要协议,它可以防止 Bob 否认收到签字消息.

3 安全性分析

量子攻击策略不可能成功. 假设 Eve 试图通过量子的方法进行攻击. 在这种方案中,Eve 可以采取假冒 Alice 或 Bob 的攻击方式. 量子密码中假冒攻击的方式很多,如完全截断攻击方案、截获/重发攻击方案、纠缠态攻击方案等. 在完全截断攻击方案中,Eve 截获 Trent 送给 Alice 的 GHZ 粒子,假冒 Alice 进行发送;或者 Eve 截获 Trent 送给 Bob 的 GHZ 粒子,假冒 Bob 进行接收. 但这些攻击方法都是不可能成功的,因为 Eve 没有 Alice 和 Bob 与 Trent 的共享密钥,同时将破坏 GHZ 三重态的相干性. 在截获/重发攻击方案中,Eve 想截获 Trent 发送给 Alice 或 Bob 的粒子,对她截获的粒子测量,然后将其中一个粒子发送给 Alice 或 Bob,并希望由此获得 Alice(Bob)与 Trent 间的有关信息,以便进行攻击. 研究表明,该方案中对截获/重发攻击方案是安全的,因为敌手的这种攻击方法同样将破坏 GHZ 三重态的相干性,从而使 Alice 和 Bob 可通过量子方法检测出攻击的存在,这种攻击方法的不可成功性在量子密钥分发协议中进行过研究. 在纠缠态攻击方案中也是不可能成功的,文献[8]证明了 GHZ 三重态的纠缠态攻击不可能成功,因为敌手的攻击必然导致对合法通信者间量子态的扰动. 实际上,即使敌手的纠缠态攻击能过成功,敌手也不可能伪造 Alice 或 Bob,因为她没有他们的密钥 K_a, K_b.

经典攻击策略亦不可能成功. 下面从三个方面讨论:

(1)不诚实的 Alice 或 Bob 的欺诈不可能成功. 假设 Bob 是不是诚实的,他想伪造签名,如果他能成功的话,他能篡改 Alice 的信息,从而为自己谋利. 遗憾的是 Bob 不可能成功,因为 Bob 收到的签名是由 Alice 和 Trent 间的共享密钥加密而成,并且这里可采用一次一密算法,从而具有无条件安全性.

(2) Alice 不可能抵赖,因为签名 S_a 中包含了她的密钥. 同时 Bob 不可能否认收到签名,因为验签过程需要 Trent 的帮助. 为了加强 Bob 的不可否认性,本方案还可做进一步修改如下:在验签过程中,Trent 将发送给 Bob 的 y_{ta} 修改为:

$$y_{tb} = K_b(R_a, R_b, R_t, \alpha, S_a') \quad (18)$$

其中 $S_a' = K_a(R_a, |\phi\rangle, y_b)$,然后将 y_{tb} 送给 Bob,同时 S_a' 做为签名. 这样签名中包括了 Bob 的密钥 K_b.

(3)任何想获取 K_a 或 K_b 的试图都不可能成功. 因为本方案中公开的参数为 S_a, y_b, y_{tb}, Eve 不能从这些参数中获取 Alice 和 Bob 的密钥,特别是当通信者采用一次一密方式加密时(在量子密码中这种方式不是难事),系统将是无条件安全的.

4 结论

本文首次研究了量子签名,并提出了一个利用 GHZ 三重态实现量子签名的方案,该方案具有可证明的安全性. 象量子密钥分发一样,量子签名具有经典签名所无法达到的安全性. 该方案适合在小型网络系统中使用,因为该方案需要通信者与系统管理员之间的共享密钥. 一个缺陷是该方案不能象经典签字一样能实现多人次验签(实际上在经典的单钥体制签字系统中也不能多人次验签).

参考文献:

[1] Wiesner S. Conjugate coding [J]. Sigact News, 1983, 15(1): 78 - 88.

[2] Bennett C H, Brassard G. An update on quantum cryptography [A]. Advances in Cryptology: Proceedings of Crypto 84 [C]. Springer-Verlag, 1984, 475 - 480.

[3] Bennett C H, Bessette F, Brassard G, Salvail L, Smolin J. Experimental quantum cryptography [J]. Journal of Cryptology, 1992, 5: 3 - 28.

[4] Marand C, Townsend P D. Quantum key distribution over distance as long as 30km [J]. OpticsLetter 1995, 20: 1695 - 1698.

[5] DiVincenzo D P. Quantum Computation [J]. Science, 1995, 270: 255 - 261.

[6] Schneier B. Applied cryptography: protocols, Algorithms, and Source Code in C [M]. John Wiley & Sons, Inc., 1994.

[7] Zeng G, Zhang W. Identity verification in quantum key distribution [J]. Physical Review A 2000, 61: 022303/1 - 5.

[8] Hillery M, Buzek V, Berthiaume A. Quantum secret sharing [J]. Phyical Review A 1999, 59: 1829 - 1835.

作者简介:

曾贵华 1966 年出生,上海交通大学教授. 1997 年毕业于中科院上海光学精密机械研究所,获博士学位;1997 年 12 月在西安电子科技大学从事量子密码学与网络安全的博士后研究工作,发表论文 51 篇,其中已被 SCI 收录 15 篇. 研究方向有:量子信息系统、网络信息安全.