文章编号:1001 - 9081(2007)10 - 2475 - 03

基于 BB84 与椭圆曲线的数字签名方案

简 丽[1,2],杨 春[1],何 军[3]
(1. 四川师范大学 计算机软件实验室,成都 610068; 2. 四川师范大学 计算机科学学院,成都 610068;
3. 四川大学 计算机学院,成都 610065)
(chunyang_2000@263. net)

摘 要:利用 BB84 协议在量子密钥分配过程中的安全性与椭圆曲线加密体制在经典加密算法中的优越性相结合,提出了一种基于 BB84 协议和椭圆曲线的数字签名方案,该方案利用量子密钥作为会话密钥从而使得签名过程高效、简易,此会话密钥在密钥分配过程中具备的可证明安全性与椭圆曲线加密体制的安全性相结合对该数字签名方案提供了双重安全保护,同时可以达到互相认证的效果。

关键词:量子密码;BB84 协议;数字签名;Hash 函数
中图分类号: TP309 **文献标志码**:A

Digital signature project based on BB84 and elliptic curve cryptography

JIAN Li[1,2], YANG Chun[1], HE Jun[3]
(1. *Laboratory of Computer Software, Sichuan Normal University, Chengdu Sichuan* 610068, *China*;
2. *College of Computer Science, Sichuan Normal University, Chengdu Sichuan* 610068, *China*;
3. *School of Computer, Sichuan University, Chengdu Sichuan* 610065, *China*)

Abstract: Based on the quantum key distribution protocol of BB84 and elliptic curve cryptography, a new digital signature scheme was proposed. This project used the quantum key as conversation key to make the signature process be highly effective and simple. The certifiable security of this conversation key in the key distribution process combined with the elliptic curve encryption system has provided the dual safekeeping of security to the new scheme and simultaneously achieved mutually authenticated effect.

Key words: quantum cryptography; BB84 protocol; digital signature; Hash function

0 引言

随着计算机和通信技术的不断发展,网络已成为全球信息基础设施的主要组成部分。网络安全正被人们日益关注,而网络安全的核心在于加密技术与理论的安全性保证。传统的加密算法是基于数学的原理,原则上,以任何数学技巧为基础的密码算法都是可以攻破的。量子密码学是密码学与量子力学结合的产物,其安全性由 Hersenberg 测不准原理[1], 量子不可克隆定理以及量子相干性来保证的[2],且具有可证明的安全性[3-5],同时对窃听者的窃听行为也容易进行检测。数字签名由公钥密码发展而来,是实现电子交易安全的核心技术之一,它在身份认证、数据完整性、不可否认性以及匿名性等方面有着重要的应用。绝大部分使用公开密钥密码编码学进行加密和数字签名的产品和标准都使用 RSA 算法。然而安全使用 RSA 所要求这种密码体制的比特长度最近几年已经增加许多,从而对于安全使用 RSA 的增加了处理负荷。因此作者利用椭圆曲线加密(Elliptic Curve Cryptosystem, ECC)[6]在公钥密码体制中安全性高、计算量小、处理速度快、存储空间占用小带宽要求低等优点,并与量子密钥分发(Quantum Key Distribution, QKD)[7]在密钥分配过程时具有可证明的安全性及对窃听者监听的可行性相结合,提出了一种基于量子椭圆曲线数字签名方案(Quantum Elliptic Curve Digital Signature Algorithm,QECSA),其基本原理是:在双方通信之前,发送方 Alice 对所要传输的数据进行 Hash 运算得到信息摘要,同时使用自身 ECC 私钥对信息摘要进行加密的数字签名,然后通过对称量子密钥对明文信息和摘要数字签名进行加密,接收方 Bob 则通过 ECC 公钥和量子密钥对 Alice 的数字签名进行验证。

1 量子密钥分配

1.1 量子态

在经典数字系统中表述数据及存储信息的最小单元是比特位,与经典比特位类似,量子信息科学中的基本单元是量子位[8](qubit),量子位可能存在的两种态分别为 0 和 1,这两态可视为经典信息中的 0,1 态,然而不像经典信息位只能用 0 或 1 表示信息,量子位可存在 0,1 的中间态。

1.2 BB84 量子密钥协议

目前应用较多的量子密钥分配协议有:基于非正交量子态编码的 BB84 协议[9]和 B92 协议[10],基于 EPR 效益的 EPR 协议[11]。由于 BB84 协议效率高且易实现,该协议已在 125

收稿日期:2007 - 05 - 21;**修回日期**:2007 - 07 - 26。
基金项目:四川省科技厅科技计划资助项目(2007H12-010);四川省软件重点实验室资助课题(SCSL 06006)。
作者简介:简丽(1983 -),女,四川仁寿人,硕士研究生,主要研究方向:信息安全、量子信息技术; 杨春(1970 -),男,四川绵阳人,教授,主要研究方向:信息安全、分布式计算、并行计算; 何军(1970 -),男,四川绵阳人,副教授,主要研究方向:计算机网络、分布信息系统、量子信息技术。

km 光纤信道中实现了密钥的分配及传输[12]，因此本文采用 BB84 协议获取 QECSA 量子会话密钥。BB84 协议采用四个量子态实现量子密钥分配，应用 Hilbert 空间中的两组不同的正交基，它们分别是由$|\nearrow\rangle$（位 1）和$|\nwarrow\rangle$（位 0）组成的圆极化基，由$|\uparrow\rangle$（位 1）和$|\rightarrow\rangle$（位 0）线极化基；在 Hilbert 空间中，BB84 采用完全不同的正两组交态字母表表示量子态，分别为圆极化量子字母表 A ⊙和线极化量子字母表 A ⊕。为了确保通信的安全性并可检测到 Eve 的偷听，在 BB84 中 Bennett 和 Brassard 要求 Alice 应等概率的随机选取 A ⊙和 A ⊕制备量子位并分别采用单向量子信道和双向经典信道来完成量子密钥分配。

2 QECSA 方案

2.1 初始化

1）首先 Alice 和 Bob 通过量子信道和经典信道遵循 BB84 协议标准来交换量子随机密钥 $K_{(a,b)}$，此密钥被 Alice 和 Bob 共同拥有。BB84 协议采用单光子的偏振态进行编码，偏振态是由一个二维的 Hilbert 空间的两组正交基制备得出的。线极化基 A ⊕，A ⊕ = $\{|\uparrow\rangle, |\rightarrow\rangle\}$；圆极化基 A ⊙，A ⊙ = $\{|\nearrow\rangle |\nwarrow\rangle\}$，而偏振态满足如下条件：

$$|\nearrow\rangle = \frac{|\uparrow\rangle + |\rightarrow\rangle}{\sqrt{2}}, |\nwarrow\rangle = \frac{|\uparrow\rangle - |\rightarrow\rangle}{\sqrt{2}} \quad (1)$$

$$\langle\uparrow|\rightarrow\rangle = \langle\nwarrow|\nearrow\rangle = 0 \quad (2)$$

$$\langle\rightarrow|\rightarrow\rangle = \langle\uparrow|\uparrow\rangle = \langle\nwarrow|\nwarrow\rangle = \langle\nearrow|\nearrow\rangle = 1 \quad (3)$$

$$\langle\nwarrow|\rightarrow\rangle = \langle\nwarrow|\uparrow\rangle = \langle\nearrow|\rightarrow\rangle = \langle\nearrow|\uparrow\rangle = 1/2 \quad (4)$$

若是用圆极化基测量由线性基制备的偏振态，将以等概率得出随机的结果，反之亦然。另一方面，若选用的测量基与原先制备量子态时选用的基完全一致，那么将会得到确定的结果。Alice 和 Bob 根据 BB84 协议的基本步骤来完成在量子信道中的密钥传输。

2）Alice 选取适当的有限域 F_q 和椭圆曲线 E，在 $E(F_q)$ 中选一个周期很大的点，如选了一个点 $P = (X_p, Y_p)$，它的周期为一个大的素数 n，记 $\prod(P) = n$（素数）。

Alice 执行下列计算：

① 在区间[1, $n-1$]中随机选取一个整数 d；

② 计算点 $Q = dP$（d 个 P 相加）；

③ 公开自己的公钥 ——（$E(F_q)$，P，n，Q），此时记 Alice 的公钥为 K_P；

④ 其私钥为整数 d!，此时记私钥为 K_S。

2.2 签名过程

签名过程如下：

1）数字签名发送方 Alice 准备好要传送的明文 M；

2）Alice 对明文信息进行 Hash 运算，得到一个信息摘要即 $H_{ash}(M) = IA$；Hash 函数两个重要特性是：①输出一般相对较短，通常为 128 位；②Hash 函数具有抗碰撞性，从而保证了两个不同的数据不会产生相同的摘要，即当 $x \neq y$ 时，$H_{ash}(x) \neq H_{ash}(y)$。故攻击者不能根据截获到的散列值，构造出欺骗明文并通过鉴别；

3）Alice 用其 ECC 的私钥 K_S 对 IA 进行加密，从而得到发送方的数字签名记为 $E_{KS}(IA) = DS$，并将其附在明文信息 M 之后；

4）Alice 利用之前通过量子信道和接收方 Bob 建立的量子密钥对数字签名和明文信息共同加密可得到一个密文信息，记为 $E_{K(a,b)}(M + DS) = C$，此时 Alice 将此密文信息 C 通过经典信道发送给 Bob；

5）Bob 收到 Alice 传来的密文信息后，首先利用之前和 Alice 建立的量子密钥 $K_{(a,b)}$ 解密信息，记为 $D_{K(a,b)}(C) = M + DS$，解密后 Bob 可得到明文消息 M 和发送方数字签名 DS；

6）Bob 用 Alice 的椭圆曲线加密公钥 K_P 对她的数字签名进行解密 $D_{KP}(DS) = IA$，从而得到信息摘要 IA，同时实现了双向认证的效果；

7）Bob 用相同的 Hash 算法对收到的明文再进行一次 Hash 运算 $H_{ash}(M) = IA*$，得到一个新的信息摘要 $IA*$；

8）Bob 将收到的信息摘要 IA 和新产生的信息摘要 $IA*$ 进行比较。由于单向 Hash 函数具有良好的抗碰撞性，所以如果两份信息摘要内容一致，则可以说明收到的信息没有被修改过。从而确定该信息是否是发送方的数字签名。

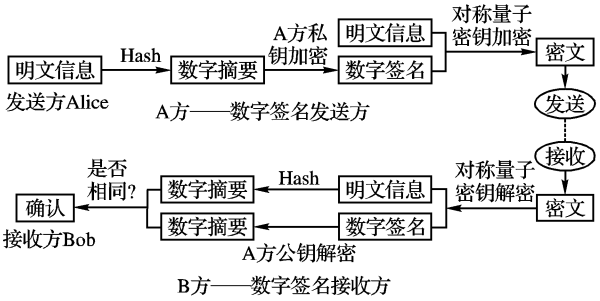


图 1 实施签名的过程

3 安全性分析

1）量子密钥在分配过程中的安全性

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，然而量子力学中的 Hersenberg 测不准原理、单光子不可分割性和量子不可克隆原理保证了通信双方量子密钥的安全性和可靠性。极化光子的非正交态的不可克隆原理保证 Eve 无法从密钥的产生和分发过程中得到任何有用信息。这是因为如果假设 Eve 所准备的测量仪器的标准状态是$|m\rangle$，若想在不破坏量子态的情况下识别$|0\rangle$和$|l\rangle$，则需满足如下的么正变换：

$|0\rangle|m\rangle \rightarrow |0\rangle|m_0\rangle$；$|1\rangle|m\rangle \rightarrow |1\rangle|m_1\rangle$。

两边取内积：

$$\langle 0|1\rangle\langle m|m\rangle = \langle 0|1\rangle\langle m_0|m_1\rangle \quad (5)$$

因此，当量子态没被破坏时，两种情况下测量仪器的最后状态相同，Eve 从编码的比特上得不到任何信息。当然，更常见的测量过程是破坏原来的量子态，使它从$|0\rangle$变为$|0*\rangle$从$|1\rangle$变为$|1*\rangle$。

测量过程可表示为：

$|0\rangle|m\rangle \rightarrow |0*\rangle|m_0\rangle$；$|1\rangle|m\rangle \rightarrow |1*\rangle|m_1\rangle$。

两边取内积：

$$\langle 0|1\rangle\langle m|m\rangle = \langle 0*|1*\rangle\langle m_0|m_1\rangle \quad (6)$$

即：$$\langle 0|1\rangle = \langle 0*|1*\rangle\langle m_0|m_1\rangle \quad (7)$$

$\langle m_0|m_1\rangle$ 的最小值应对应于 Eve 能完全区分这两个状态的情况。这时得到$\langle 0*|1*\rangle = 1$，因此可得出，当 Eve 对传输量子态测量后，$|0\rangle$和$|1\rangle$变成了两个相同的状态。因此，在非正交态的不可克隆原理保证下，单粒子极化光子的密

钥产生和分发是绝对安全的。所以即使在通信的第四步密文信息被截获,但因为截获者根本不可能知道解密的量子密钥从而也无法获取明文信息。

2) 签名的不可伪造性

在该方案中对签名的不可伪造作出了双重保证,首先通信双方在建立量子密钥 $K_{(a,b)}$ 的过程中可知道对方的身份,因为 $K_{(a,b)}$ 只有通信的双方才拥有,所以消息的接受者能肯定消息的唯一发送者。同时因为只有发送者本人才知道自己的椭圆曲线加密的私有密 K_S,因此只有消息的发送者才能对消息做唯一签名。

3) 签名的不可重用性

在该方案中采用的单向 Hash 算法使签名成为消息的函数同时由于单向 Hash 函数具有良好的抗碰撞性 $H_{ash}(x) \neq H_{ash}(y)$,保证了签名不可能被转换为其他的文件,从而确定了签名的不可重用性。

4) 签名的不可抵赖性

Alice 用自己的私钥加密信息摘要得数字签名 DS, Bob 直接利用 Alice 的公钥就可以独立的验证发送者的签名,同时 Bob 也不能否认他收到了发送者的签名,因为只有 Bob 本人拥有解开密文信息的量子密钥。

5)任何想获取量子密钥的试图都不可能成功。

因为本方案中第三方不能从通信双方公开参数中获取通信双方密钥,特别是当通信者采用一次一密方式加密时系统将是无条件安全的。

4　结语

本文利用量子密码在量子信道密钥分配中的安全性及椭圆曲线加密体制在经典秘密通信中的优越性,将二者相结合,提出了一种在经典信道中基于量子密钥的数字签名方案,该方案有可证明的安全性,同时也保证了签名的不可伪造性和不可抵赖性。不足之处是目前量子密钥分配还存在着很多制约因素,最主要的是传输距离、噪声干扰的限制。但相信随着科学技术的不断发展,量子密钥有望突破一些在自由空间和光纤信道中的传输困难而得到良好的分配和传输。也可能将会与经典安全通信中的优秀算法、方案相结合从而为信息安全提供更强有力的工具。

参考文献:

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

[2] WOOTERS W K, ZUREK W H. A single quantum cannot be cloned [J]. Nature, 1982,299: 802 -803.

[3] L üTKENHAUS N. Security against eavesdropping in quantum cryptography[J]. Physics Review A, 1996, 54(1):97 -111.

[4] L üTKENHAUS N . Estimates for practical quantum cryptography [J]. Physics Review A , 1999, 59: 3301 -3319.

[5] BRASSARD G, L üTAKENHAUS N, MOR T, *et al*. Security aspects of practical quantum cryptography[DB/OL]. [2007 -05 -01]. http: //arxiv. org/df?quant -ph/9911054.

[6] HANKERSON D, MENEZES A, CANSTONE S. Guide to elliptic curve cryptography[M]. Heidelberg: Springer, 2004.

[7] BENNETT C H , BRASSARD G, BREIDBART S, *et al*. Quantum cryptography , or unforgeable subway tokens[C]// Advances in Cryptology: Proceedings of Crypto 82. New York: Plenum Press, 1982: 267 -275.

[8] CLAUSER J F . Experimental distinction between the quantum and classical field-theoretic predictions for the photoelectric effect[J]. Physical Review Letters, 1974, D9, 853 -860. .

[9] BENNETT C H, BRASSARD G. An update on quantum cryptography[C]// Advances in Cryptology: Proceedings of Crypto 84. Berlin: Springer-Verlag, 1984: 475 -480.

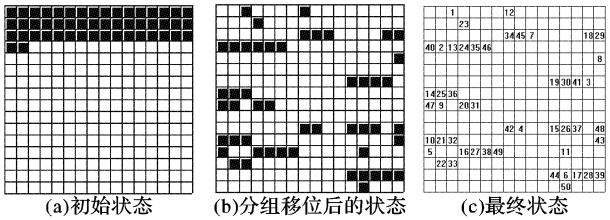
[10] BENNETT C H, BESSETTE F, BRASSARD G, *et al*. Experimentalquantum cryptography[J]. Journal of Cryptology, 1992, 5(1):3 -28.

[11] BENNETT C H, WIESNER S J . Communication via one-and two-particle operators on Einstein-podolsky-rosen states[J]. Physical Review Letters, 1992, 69: 2881 -2884.

[12] 郭光灿. 量子密码——新一代密码技术[J]. 物理与工程, 2005, 15(4):1 -4, 8.

(上接第 2474 页)

后的状态,通过两大类型的变换,从而可以形象地看出水印嵌入位置和顺序的变化过程。



(a)初始状态　(b)分组移位后的状态　(c)最终状态

图 4　实验结果

以载体图像大小为 128 × 128,水印大小为 200,给定的密钥 K 为 Z15SG94C 为例:载体图像的 DCT 块大小为 16 × 16 = 256,嵌入水印需用 50 个 DCT 块,水印嵌入的初始位置设定如图 4(a)。分组移位操作后,结果如图 4(b)所示。保持水印位置不变,利用混洗算法将嵌入的顺序打乱,得到的结果见图 4(c)。

5　结语

本文提出的基于密钥的分组移位和混洗算法对于产生随机分散的水印嵌入和提取位置比较有效,可以广泛用于数字水印系统嵌入位置的选取上。其中,分组移位算法也可用于水印图像的置乱。在水印系统中,嵌入位置用本文提出的算法,水印图像置乱用分组移位算法,就可实现水印系统的单密钥体制。

参考文献:

[1] 刘德鹏, 蔡翔云. 水印对象的混沌置乱算法[J]. 云南大学学报: 自然科学版, 2006, 28(S1): 145 -148.

[2] 李敏, 费耀平. 基于置乱变换的多重数字水印盲算法[J]. 计算机工程, 2006, 32(16): 122 -124.

[3] 陈波, 谭运猛, 吴世忠. 信息隐藏技术综述[J]. 计算机与数字工程, 2005, 33(2): 21 -27.

[4] KWOK S H. Watermark-based copyright protection system security [J]. Communications of the ACM, 2003, 46(10): 98 - 101.

[5] YIN ZH, WANG K. Improvements of the definition of image fidelity [C]// Proceedings of the 12th International multi-Media Modelling Conference proceedings. New York: IEEE Press, 2006, 1: 426 -429.