

一个基于椭圆曲线的前向安全的签密方案

蔡庆华

(安庆师范学院 计算机与信息学院, 安徽 安庆 246011)

摘要: 签密就是能够在一个逻辑步骤内完成数字签名和加密两项功能, 比传统的先签名后加密有更高的效率。在椭圆曲线密码体制下, 提出一个具有公开可验证性的和前向安全的签密方案, 并分析了该方案的安全性, 解决了签密方案设计上的一个公开问题。文中方案可以应用于许多特殊场合, 如电子现金、匿名认证等, 实现了前向安全性。

关键词: 签密方案; 椭圆曲线密码体制; 数字签名; 前向安全性; 公开可验证性

中图分类号: TP309

文献标识码: A

文章编号: 1673-629X(2007)12-0132-04

A Signcryption Scheme with Forward Security Based on ECC

CAI Qing-hua

(Computer Science Department, Anqing Teachers' College, Anqing 246001, China)

Abstract: Signcryption is a new cryptographic technology, which simultaneously fulfills both the function of digital signature and public key encryption in a logically single step, and more efficient than traditional "signature followed by encryption" approach. A signcryption scheme with forward security based on ECC is presented. The security of the scheme is also analyzed. An open problem on the design of signcryption is solved. With all the feature, this work is attractive for many specialized applications, such as electronic cash, anonymity authentication, and achieves forward security.

Key words: signcryption scheme; elliptic curve cryptosystem; digital signature; forward security; public verifiability

0 引言

随着计算机运算速度的迅速提高和计算能力的日益强大, 信息的安全显得更加重要。为确保信息安全, 在一些使用密钥长度较短的应用中, 迫切需要新的密码体制^[1]来实现。同时, 移动终端的存储及数据处理能力也不断提升, 使以前认为计算较复杂的密码体制的应用成为可能。椭圆曲线密码体制是一种基于代数曲线的公钥密码体制, 它具有密钥比特数少和在与基于乘法群的密码体制相同条件下能够提供更高安全性的特点。由于椭圆曲线密码体制不是建立在一个大整数分解及素数域乘法群离散对数的数学难题上, 而是建立在更难的椭圆曲线离散对数的问题之上, 所以它的安全性更高。

签密是 Zheng Y 于 1997 年提出的一种新的密码学构件, 它能在一个逻辑步骤内同时完成数字签名和公钥加密, 比先签名再加密^[2]的常规消息传递的代价

小得多, 非常适合大量数据的安全认证。

下面是 Zheng Y 在 CRYPTO'97 中首次提出并命名的签密方案。公开参数为 $(p, q, g, H(\cdot), E, D)$, 其中 p, q 为大的强素数且 $q \mid p-1$, g 为 Zp^* 上的 q 阶元, (E, D) 为对称加解密算法, 其密钥长度为 $|k|$ 比特且 $D_k(E_k(m)) = m$, $H: \{0, 1\}^* \rightarrow |k|$ 为单向无碰撞 Hash 函数。收发方 A, B 各自在 Zq^* 上随机选取 x_A, x_B 作为其各自私钥, 并各自计算其对应公钥 $y_A = g^{x_A} \pmod{p}$, $y_B = g^{x_B} \pmod{p}$, 并在一证书中心为其公钥申请对应的公钥证书。现设 A 要向 B 发送消息 m 。将原方案分为签密阶段和打开签密阶段。

签密过程: 发方 A 随机选取 $x(1 < x < q)$, $k_1, k_2 = H(y_B^x \pmod{p})$, $c = E_{k_1}(m)$, $r = H(k_2, m)$, $s = x/(r + x_A) \pmod{p}$, 签密结果为 (c, r, s) 。 k_1, k_2 表示消息的连接, 发方通过公开信道发给收方 B 。

打开签密: 收方收到 (c, r, s) , 计算 $k_1, k_2 = H(y_A \times g^r \pmod{p})$, $m = D_{k_1}(c)$, 验证 $H(k_2, m)$ 是否和 r 相等。若相等则接收消息 m , 否则丢弃 m 。

目前签密方案得到广泛的研究, 但是现已提出的多数签密方案均具有这样或那样的不足。Zheng Y 所给出的两个签密方案均被指出不满足签名的公开可验

收稿日期: 2007-03-07

基金项目: 安徽省自然科学基金项目(KJ2007B043); 安徽省高校青年教师资助项目(2007JQL122)

作者简介: 蔡庆华(1974-), 男, 安徽太湖人, 硕士, 副教授, 从事密码学和网络安全方面的研究。

证性和前向安全性。文献[3]基于离散对数的签名体制设计了一个可以实现前向安全性的签密方案,该方案却不能提供公开可验证性。文献[4]基于离散对数方案设计了一个具有公开可验证性和前向安全性的签密方案。鉴于签密方案广泛的应用前景,而椭圆曲线密码系统(ECC)具有密钥短、运算快等特点,文中基于此在 ECC 理论上建立相应的签密方案。

1 椭圆曲线密码体制

1.1 椭圆曲线加密方案

椭圆曲线域参数是指构造一个椭圆曲线密码系统所需要的参数集,包括:有限域 $GF(P)$, 椭圆曲线 E , 基点 G (椭圆曲线上的一个点), 基点的阶 n , 椭圆曲线群的阶 $\#E$, 相关因子 $h = \#E/n$ 。椭圆曲线的域参数是公开的, 由通信各方共享。对于有限域是特征为 2 的有限域 F_{2^m} , 椭圆曲线域参数是一个七元组 $(m, f(x), a, b, G, n, h)$, 其中 m 是有限域的尺寸, $f(x)$ 是域中多项式, a, b 决定椭圆曲线 $E: y^2 + xy = x^3 + ax^2 + b$, G 表示曲线 E 的一个基点, n 是 G 的阶, 即 $nG = O$, h 表示椭圆曲线群的阶与 n 的商, 即 $h = \#E(F_{2^m})/n$, 记为比例因子, 下面给出加解密过程。

(1) 加密(以 A 给 B 发送消息 $M = (M_1 || M_2)$ 为例, 设 B 的私钥为 k_b , 对应的公钥为 Q_B)。

① A 随机选取正整数 $k (k \in [1, n-1])$;

② A 计算 $c_0 = kG; kQ_B = (x, y)$, 若 $x = 0$ 或 $y = 0$ 返回第 ① 步, 直到 $x \neq 0, y \neq 0$ 。

③ 计算 $c_1 = M_1 x \bmod n$

④ 计算 $c_2 = M_2 y \bmod n$

⑤ A 发送密文 $C = (c_0, c_1, c_2)$ 给 B 。

(2) 解密。

B 收到密文 C 后,

① 计算 $k_b c_0 = (x, y)$;

② 计算 $c_1 x^{-1} \bmod n, c_2 y^{-1} \bmod n$, 进而得到 (M_1, M_2) 。

(3) 方案分析。

A 发送 $C = (c_0, c_1, c_2)$ 给 B , B 能得到 (x, y) , 因为: $(x, y) = kQ = kkbG = kbkG = kbc_0$

B 能获得 $M = (M_1 || M_2)$ 。因为: $c_1 = x M_1 \bmod n, c_2 = y M_2 \bmod n, c_1 x^{-1} \bmod n = x^{-1} x M_1 \bmod n = M_1, c_2 y^{-1} \bmod n = y^{-1} y M_2 \bmod n = M_2$

任何中间偷听者仅能获得 C , 如果没有 B 的私钥 k_b 是不能解密得到 M 的。

1.2 椭圆曲线签名算法 ECDSA

椭圆曲线密码系统(ECC)具有密钥短、运算快等

特点, 所以很有必要在 ECC 理论上建立相应的签名方案。由 D. Johnson, A. Menezes 和 S. Vanstone 提出的椭圆曲线数字签名算法(ECDSA)使得伪造签名等同于破解椭圆曲线离散对数问题, 该方案体现出 EGC 算法的许多优势, 下面给出该算法。

设椭圆曲线公钥密码系统参数为 (F_q, E, g, n, a, b, h) , 其中 F_q 是有限域, E 是 F_q 上的椭圆曲线, g 是 E 上的一个基点, n 是椭圆曲线 E 的阶, a, b 是椭圆曲线 E 的系数, h 为安全的单向 Hash 函数。

1) 密钥生成。

用户 A 随机选择一个整数 x , 作为私钥, 公钥是 $y = xg$ 。

2) 签名过程。

(1) 用户 A 随机选取一个整数 k , 其中 $1 < k < n$, 计算 $kg = (x_1, y_1), r_1 = x_1 \bmod n$;

(2) m 为消息, 计算 $e = h(m)$;

(3) 计算 $s = k^{-1}(e + r_1 x_1) \bmod n$;

(4) m 的签名为 (s, r_1) ;

3) 签名的验证。

(1) 计算 $e = h(m)$;

(2) $u = s^{-1}e, v = s^{-1}r_1$;

(3) $(x_2, y_2) = ug + vy, r_2 = x_2 \bmod n$;

(4) 如果 $r_1 = r_2$, 则接受这个签名。

1.3 基于椭圆曲线的基本签密算法

数字签密由一对算法 (S, U) 构成, 其中 S 称为签密算法, U 为解签密算法。 (S, U) 满足下列条件:

1) 解签密惟一性: 给定任意长度的消息 m , 算法 S 签密消息 m 并输出签密文 c 。一旦输入 c , 算法 U 解签 c 并无二义地恢复消息 m 。

2) 安全性: (S, U) 同时实现加密方案的安全特性和签名方案的安全特性。这些性质主要包括消息内容的机密性、不可伪造性和不可否认性。

3) 有效性: 在同样条件下, 签密方案的计算和通信代价小于常规的“先签名再加密”方案。

下面给出一基于椭圆曲线的基本签密算法, 除签密算法 S 和解签密算法 U 外, 还有系统参数产生过程。

(1) 系统参数。

构造椭圆曲线^[5,6] $E: y^2 = x^3 + ax + b (a, b \in F_q)$, 该曲线是非超奇异的。选择一个公开的基点 $G \in E(F_q)$, q 是椭圆曲线的阶。

用户 A 的密钥 $x_a \in \{1, 2, \dots, q-1\}$, $P_a = x_a G$ 为其公钥; 用户 B 的密钥 $x_b \in \{1, 2, \dots, q-1\}$, $P_b = x_b G$ 为其公钥。 $E(k, m)$ 和 $E^{-1}(k, c)$ 是一对单钥加/解密算法^[3] (如 DES 或 AES), 分别表示用密钥 k 加密消息 m 和解密密文 c 。 $KH_k(m)$ 为带密钥 k 的哈希函

数^[4,7]。

(2) 签密算法 S。

发送者 Alice 选择一个随机数 x , 然后计算参数 c 和 r :

$$xP_b = (k_1, k_2), c = E(k_1, m), r = KH_{k_2}(m)$$

当 $r + x_a \equiv 0 \pmod q$ 时, Alice 选择另一随机数 x , 并重新计算相应参数, 直到 $r + x_a \not\equiv 0 \pmod q$ 后计算: $s = x/(r + x_a) \pmod q$, 然后将 (c, r, s) 发送给 Bob。

(3) 解签密算法 U。

Bob 计算 $(P_a + rG)sx_b = (k_1, k_2)$ 和 $m = E^{-1}(k_1, c)$

当且仅当 $KH_{k_2}(m) = r$ 时接受 m 。

2 一个具有前向安全的签密算法

本方案包括 4 个过程: 系统初始化过程; 发送者 A 产生签密文阶段; 接收者 B 解密与验证签密文阶段; 仲裁者验证签密文阶段。适合于应用在移动通信中发送端计算能力有限的设备上, 如移动终端。

在系统初始化过程中, 由仲裁者 V (即收发双方都信任的公平第 3 方) 产生公开的椭圆曲线参数, 并由参与成员自行产生私钥和公钥对, 而仲裁者对公钥给予公证。在发送者产生签密文阶段, 发送者对明文 M 签字加密产生签密文件送给接收者。在接收者解密与验证签密文阶段, 接收者解密签密文并验证签字。在仲裁者验证签密文阶段, 接收者可将签字与解密后的明文请求仲裁者仲裁此明文的签字是否为发送者发出的。

(1) 系统初始化过程。

选取有限域 F_q 上的一条椭圆曲线 $E: y^2 = x^3 + ax + b (a, b \in F_q)$, 该曲线是非超奇异的。在 $E(F_q)$ 上选择一个公开的基点, q 是椭圆曲线的阶。 (E, D) 为对称加解密算法, 其密钥长度为 k 比特, 且 $Dk(EK(m)) = m$ 。 H : 为一个公开的将椭圆曲线上的点映射为 Z_q 的单向无碰撞哈希函数^[7]。设用户 A 欲对消息 m 进行签密, 假设接收方为 B。发送方 A 的私钥为 x_A , 其对应的公钥为 $Y_A = x_A G$ 。接收方 B 的私钥为 x_B , 其对应的公钥为 $Y_B = x_B G$ 。

(2) A 对消息 m 计算其签密步骤。

发送方 A 选择一随机数 $x \in Z_q^*$, 计算: $k_1 = xG$ 和 $k_2 = H(xY_B)$, 然后对明文 m 用加密算法 E 密钥 k_2 加密得密文: $c = E_{k_2}(m)$ 。然后对密文计算下式进行签名:

$$r = H(mk_1);$$

$$R = rG;$$

$$s = x(r + x_A) - 1 \pmod q;$$

最后 A 将 m 的签密消息 (c, R, s) 通过公共信道发送给接收方 B。

(3) 接收者 B 的解签密算法。

当接收者 B 收到签密消息 (c, R, s) 后, 按下式计算: $k_1 = (Y_A + R)s$; $k_2 = H(x_B k_1)$ 得到解密密钥 k_2 , 然后对密文解密: $m = D_{k_2}(c)$ 得到明文 m 。最后验证等式 $R = H(m, k_1)G$ 是否成立, 若成立则认为 m 是 A 向 B 签发的消息; 否则拒绝接收明文 m 。

(4) 公开验证。

若发方 A 否认他曾向 B 发送过关于 m 的签密组或任意第三方 V 要证实 (c, R, s) 确为对 m 的签密消息, 则 B 向 V 提交 (m, R, s) 。V 计算 $k_1 = (Y_A + R)s$, $r = H(mk_1)$, 验证是否有 $R = rG$ 成立, 若是则 V 认为 m 确为 A 向 B 签发的消息。

3 签密算法的分析

本方案基于椭圆曲线密码体制, 具有较短的密钥长而不失安全性, 同时该签密方案把签名和加密结合在一起, 从而在效率上较传统的分两步实现的方法提高许多。该方案具有签密的唯一性、机密性、不可伪造性和不可否认性和前向安全性等安全特性。

定理 1 上述签密算法满足解签密的唯一性。

证明: 因为 R 是同一个, 如果解签密不唯一, 则存在 m' 和 m'' 满足: $H(m'k_1) = H(m''k_1)$, 这与 H 为一个单向杂凑函数相矛盾。

定理 2 在求解 ECDLP 困难的假定下, 上述签密算法满足机密性。

证明: 对消息 m 的签密算法中, 对称加密密钥为 $k_2 = H(xY_B) = H(x_B k_1)$, 在求解椭圆曲线的离散对数问题困难假设和 x 保密情况下, 除发送方和接收方外, 其它用户是不可能解出密钥 k_2 的, 因而也就不可能解密出消息 m 。

定理 3 上述签密算法满足不可伪造性。

证明: 不可伪造性是指任何外部攻击者或内部攻击者都不能伪造一个来自发方的关于某个消息的签密。一个外部攻击者要假冒签名者进行签密, 因为他不知道 x_A , 故无法构造合法的能通过 B 验证的 s , 从而不可伪造合法签密。若内部攻击者 B 向第三方称 (m', R, s) 为来自 A 的签密, 其中 R, s 为 B 伪造的数据。为了 m 使伪造数据通过第三方验证, 他必须由 $R = rG$ 来确定 R 与 r , 其中 $r = H(mk_1)$ 确定。而 $k_1 = (Y_A + R)s$, 即 k_1 的计算又用到 R 的信息。故 B 不能伪造发送者 A 的一个合法签密。

定理 4 上述签密算法满足不可否认性, 这是由

于该签密方案是公开可验证的。

定理 5 上述签密算法满足前向安全性。

证明:因为任何人虽然均可截获在公开信道上传输的签密 (c, R, s) ,但由于 r 是隐藏在 $R = rG$ 中,这样即使 x_A 丢失,他也不会从 $s = x(r + x_A)^{-1} \bmod q$ 中得到 x ,这样只能从 $k_2 = H(x_B k_1)$ 中计算 k_2 ,这是 ECDLP 问题。因此敌手不能计算加密密钥 k_2 。

4 结束语

当签密方案采用小的安全参数时(公共模数为 512 位),与常规的先签名后加密的方法比较,签密的计算代价降低为 58%,消息扩展率为 70%;当采用长的安全参数时(公共模数为 1536 位),签密的计算代价降低为 50%,消息扩展率为 91%,签密的节省代价正比于安全参数的长度,当取较大安全参数时安全性能更佳^[8]。

由于签密方案仅需执行一步操作就能实现签名与加密的功能,因而能高效地实现安全、认证的信息传输。文中提出的新的基于椭圆曲线的签密方案,具有机密性、不可伪造性、不可否认性,而且具有前向安全性和公开可验证性等安全特征,在效率上较传统的分两步实现的方法有显著提高,因而在现实环境中,将具有良好的应用前景,特别适用于移动通信的应用场合,以实现移动通信中收发双方相互的认证,而公平第 3

方,即仲裁者可以仲裁发送方和接收方通信中发生的争议。下一步的研究将是如何去设计更高效的签密方案,以进一步提高其应用前景和应用价值。

参考文献:

- [1] 王继林. 公钥体制下的匿名问题研究[D]. 西安:西安电子科技大学,2003.
- [2] Zheng Y. Digital Signcryption or How to Achieve Cost (Signature & Encryption)[C]//In Advances in Cryptology - Crypto' 97. Lecture Notes in Computer Science 1294. Berlin: Springer,1997.
- [3] Jung H, Lee D, Lim J, et al. Signcryption Scheme with Forward Security [C]//Proceedings of WISA 2001. [s. l.]: Springer - Verlag,2001.
- [4] 李艳平,谭示崇,王育平. 一个公开可验证和前向安全的签密方案[J]. 计算机应用研究,2006(9):98-99.
- [5] 李新明,李子臣. 改进的认证密钥交换协议[J]. 河南科技大学学报:自然科学版,2003,24(3):58-59.
- [6] 张雁,林英,郝林. 椭圆曲线公钥密码体制的研究热点综述[J]. 计算机工程,2004,30(3):127-129.
- [7] 卢开澄. 计算机密码学——计算机网络中的数据保密与安全[M]. 北京:清华大学出版社,2003:282-297.
- [8] Zheng Y. Digital signcryption and its application in the efficient public solutions[C]//Proceeding of Information Security Workshop(ISW' 97). Berlin: Springer Verlag, 1997: 291 - 312.

(上接第 131 页)

若非法用户盗取了用户 yanxin 的口令和密码,而不知道其私钥,在私钥框中随机输入私钥,将不能看到其消息。

在实际系统中应将私钥设置为不可见的,或者以通常的若干个 '*' 方式显示。

6 结束语

本方案在加密和数字签名上的算法和相关技术等,都是经过比较后选择的,并结合了现有校园网络安全的情况,充分证实方案所具有的优越性和可行性。在当今还没有一个较 RSA 密码系统更为优秀的密码系统出现之前,可以有效地改进 RSA 加密算法的速度也是解决当今密码学主要的一个研究方向。

目前大学校园无纸化办公已成为一种趋势,无纸化办公能否顺利地进行,已经引起人们的高度重视。将文中所采用的方案与无纸化办公实现无缝连接还有

许多工作要做。

参考文献:

- [1] 贺刚. 数字签名在校园办公网上的实现[J]. 湖北民族学院学报:自然科学版,2004,22(2):69-71.
- [2] 周芳,宫晓曼,腾荣华. 对校园网络安全的研究[J]. 江西科技师范学院学报,2004(5):90-92.
- [3] 程线,戴国梁. 论校园网系统建设安全性及相应策略[J]. 湖南广播电视大学学报,2004(2):24-26.
- [4] 刘涛. 基于校园网的成绩 MIS 数字签名的研究与设计[J]. 微机发展,2005,15(11):24-26.
- [5] Stallings W. 密码编码学与网络安全——原理与实践[M]. 第 3 版. 刘玉珍,王国娜,傅建明等译. 北京:电子工业出版社,2004.
- [6] Bishop M. 计算机安全学——安全的艺术与科学[M]. 王立斌,黄征等译. 北京:电子工业出版社,2004.
- [7] 贾俊敏,王纪卿,孔英会,等. 电子交易系统中文本安全传输方案研究[J]. 电力系统通信,2005,26:33-35.