基于椭圆曲线密码体制的一种具有前向安全的数字签名方案

詹雄泉, 洪景新
(厦门大学计算机科学系, 福建 厦门 361005)

摘要: 为了解决普通数字签名密钥被泄漏的局限性, 作者提出一种椭圆曲线数字签名方案, 并基于前向安全理论提出一种具有前向安全的数字签名方案. 新方案中用于数字签名的私钥由一个单向函数控制并随时间的推移按时间段不同不断地改变, 而其相对应的公钥却保持不变, 因此即使在某一时间段签名密钥被泄漏, 攻击者依然无法仿造先前时间段的签名, 从而保证了以前时间段签名的安全性. 文中还分析了新方案的安全性, 并证明了方案的有效性.

关键词: 椭圆曲线; 前向安全; 数字签名
中图分类号: TP 309 文献标识码: A 文章编号: 0438-0479(2005)02-0189-04

随着计算机与通信事业的发展, 如何保证信息传输的安全, 成为电子商务发展的首要问题. 数字签名技术是利用数学变换将一份明文信息或档案文件映射成另一份叫做签名文件的文件, 是为了使接收方能够向第三方证明其收到的消息的真实性而采取的一种加密措施[1]. 不同于传统的签名方式, 数字签名是基于公钥密码体制, 依据一定的加密算法构造而成的. 它是参与者身份的惟一证明, 是解决网络通信中特有的安全问题的有效方法[2,3].

数字签名方案可采用公钥密码体制, 也可采用私钥密码体制, 其实质都是对密钥的使用. 公钥密码体制往往是基于数学上的 NP 问题而设计的, 是一种非对称密码体制, 通信双方不需要提前协商加密秘钥, 从而有效地防止了信息传输中潜在的危险[4]. 基于椭圆曲线密码体制的数字签名方案, 是利用椭圆曲线上的点构成的 Abel 加法群构造离散对数问题. 将椭圆曲线中的加法运算与离散对数中的模乘运算相对应, 将椭圆曲线中的乘法运算与离散对数中的模幂运算相对应, 就可以建立基于椭圆曲线的对应的密码体制[5,6]. 但现实情况中, 可能由于系统的安全漏洞或人为泄漏等原因而引发签名秘钥被盗用, 从而致使签名被伪造, 便成为安全问题中的难题. 本文基于特征为 2^n 的域 $GF(2^n)$ 上的非超奇异椭圆曲线[7] 密码体制的数字签名理论, 提出一种具有前向安全的数字签名方案.

收稿日期: 2004-05-14
基金项目: 福建省科技项目基金(2002H021)资助
作者简介: 詹雄泉(1980—), 男, 硕士研究生.

1 椭圆曲线的定义及其签名算法(ECDSA)

1.1 有限域 $GF(2^n)$ 上的非超奇异椭圆曲线

椭圆曲线是指由三次方程

$$y^2+axy+by=x^3+cx^2+dx+e$$

所确定的平面曲线, 其中 $a, b, c, d, e \in F_p$, 通常 F_p 为一素数域, 记为 F_p, 简称椭圆曲线为 $E(F_p)$. 满足上式的序偶 $(x, y) \in F_p \times F_p$ 称为 F_p 域上 $E(F_p)$ 的点, 如果 F_p 的特征不等于 2 和 3, 则对应上式的经过简化的椭圆曲线方程的一般形式为:

$$y^2 \equiv x^3+ax+b \pmod p,$$

这里 p 是素数, $a, b \in F_p$, 且它们满足: $4a^3+27b^2 \pmod p \neq 0$, 用 $Ep(a, b)$ 表示模 p 的椭圆群, 其元素是满足上面方程的小于 p 的非负整数对 (x, y) 以及无穷远点 O.

基于域 $GF(2^n)$ 上的非超奇异椭圆曲线方程为:

$$y^2+xy=x^3+ax+b,$$

这里 $a, b \in GF(2^n)$, $b \neq 0$, 定义 $E(GF(2^n))$ 是满足上述方程的点 $(x, y) \in GF(2^n) \times GF(2^n)$ 和曲线上无穷远点 O 的所组成的集合.

1.2 基于椭圆曲线的签名算法 ECDSA

选择 $E(GF(2^n))$ 上的一个有理点 P, 称为基点, 求出 P 的阶 n, n 为满足 $nP=O$ 的素数, 根据 SHA-1 选择一个单向安全的 Hash 函数 $h(x)$[8]. 系统的每一用户有一私钥 a, 计算公钥 $P_a=aP$, 假设用户上 A 要对信息 m 签名, 则其 ECDSA 方案可描述如下[9]:

(1) A 随机选择一个整数 k, $1 \leq k \leq n$, 计算 $kP=$

(x, y), $r = x \bmod n$, 若 $r = 0$, 则返回(1);

(2) 计算 $e = h(m)$; $s = (ke + ra)P$;

(3) 以 (r, s) 作为 A 对信息 m 的数字签名.

数字签名验证过程:

(1) 计算 $e = h(m)$;

(2) 计算 $X = e^{-1}(s - rP_a) = (x_1, y_1)$;

(3) 如果 $X = 0$, 则拒绝这个签名; 否则计算 $r_1 = x_1 \bmod n$, 若 $r_1 = r$, 则接受这个签名.

2 前向安全数字签名

前向安全方案的目的是为了克服普通数字签名所具有的局限性, 在普通数字签名中, 若签名者的密钥被泄漏, 那么这个签名者所有签名都有可能泄漏, 包括过去的和将来的签名[10]. 这个局限性影响了签名所应该具有的不可否认性. 实际上, 签名者否认自己签名的最简单方法是在网上匿名公开自己的密钥, 然后声明自己的计算机遭到了入侵. 前向安全方案的目标就是即使在某一时间段签名密钥被泄漏, 攻击者依然无法仿造先前时间段的签名, 从而保证了以前时间段签名的安全性, 使得当密钥泄漏以后尽可能减少损失并控制损失. 与一般签名方案不同, 前向安全的数字签名的私钥是随时间的推移按时间段不同不断地进行改变, 而其相对应的公钥却保持不变. 一般情况下, 在系统建立初期, 用户先注册一个证书, 得到公钥 P_K 和相应的私钥 SK_0, 保存此私钥, 将密钥的有效期分为 T 个时间段, 分别记为 1, 2, …, T. 在有效期内, 公钥 P_K 是固定不变的, 而私钥随时间段不断更新, 以 SK_i 表示时间段 i 的私钥. 进入时间段 i 时, 首先要进行从 SK_{i-1} 到 SK_i 变换, 计算公式为 $SK_i = f(SK_{i-1})$, 其中 f 是个单向函数, 在生成 SK_i 后就立即删除 SK_{i-1}, 这样即使攻击者在 i 时间段侵入了计算机获得了 SK_i, 也无法获得 SK_{i-1}, SK_{i-2}, …, SK_0, 因为他要面临求解离散对数的难题, 从而保证了之前签名的安全性. 图 1 显示了私钥在不同时间段的变化过程.

$$SK_0 \xrightarrow{f} \underset{SK_1}{\text{时段 1}} \xrightarrow{f} \underset{SK_2}{\text{时段 2}} \xrightarrow{f} \cdots\cdots \xrightarrow{f} \underset{SK_T}{\text{时段 } T}$$

图 1 私钥的更新变换过程

Fig. 1 The updated process of the private key

3 基于非超奇异椭圆曲线的前向安全数字签名方案

基于上述前向安全数字签名的理论, 本节及下一节将讨论在当前椭圆曲线的数字签名文案和基于身份的椭圆曲线数字签名方案中应用前向安全数字签名理论的方法.

选择 $E(GF(2^n))$ 上的一个有理点 $P(x, y)$, 作为基点, 求出 P 的阶 n, n 为满足 $nP = O$ 的素数, 根据 SHA-1 选择一个单向安全的 Hash 函数 $h(x)$.

3.1 签名者初始密钥对的生成

(1) 将签名密钥的有效期分为 T 个时间段, 选择一大素数 p 和随机数 SK_0, $1 < SK_0 < p$;

(2) 计算 $P_K = SK_0^{n^T} P$;

(3) 公开系统公钥 $\{p, T, P_K\}$, 初始密钥 SK_0 应保密.

3.2 签名者私钥的更新算法

当系统进入 i 时间段时, $1 \leqslant i \leqslant T$, 签名者使用拥有的 $i-1$ 时间段的密钥 SK_{i-1} 计算 $SK_i = SK_{i-1}^{n} \bmod p$, 删除系统中 $i-1$ 时间段的密钥 SK_{i-1}, 保密新生成的 i 时段的密钥 SK_i.

3.3 签名过程

(1) 签名者任意选择随机数 k, $0 < k < n$, 计算 $kP = (x, y)$, $r = x \bmod n$, 若 $r = 0$, 则返回(1);

(2) 计算 $e = h(m)$, $s = (ke + rSK_i^{n^{T-i}})P$;

(3) 以 (r, s) 作为信息 m 的签名发给验证方.

3.4 验证过程

(1) 验证者计算 $e = h(m)$;

(2) 计算 $X = e^{-1}(s - rP_K) = (x_1, y_1)$;

(3) 如果 $X = 0$, 则拒绝这个签名; 否则计算 $r_1 = x_1 \bmod n$, 若 $r_1 = r$, 则接受这个签名.

3.5 方案的有效性证明

事实上, 由归纳法可知,

$$SK_i^{n^{T-i}} = (SK_{i-1}^{n})^{n^{T-i}} = SK_{i-1}^{n^{T-i+1}} = \cdots = SK_0^{n^{T-i+i}} = SK_0^{n^T},$$

则

$$X = e^{-1}(s - rP_K) = e^{-1}((ke + rSK_i^{n^{T-i}})P - rP_K) = e^{-1}((ke + rSK_0^{n^T})P - rSK_0^{n^T}P) = kP = (x, y),$$

因此, 本方案可以有效地工作.

4 基于身份的椭圆曲线前向安全数字签名方案

基于身份的前向安全数字签名的方法是由系统可信任的第三方验证者 Q, 分配给每一个系统用户(如用户 A) 一个惟一的身份号 ID_A. Q 用一种安全的签名方案对 ID_A 签名, 系统初期用户 A 产生自己的私钥, 并

将私钥有效期分为 T 个时间段,并对这个私钥根据不同时间段不断更新,用当前时间段的私钥进行信息签名,在验证时,验证者利用 A 的身份 ID_A 计算出 A 的公钥,再进行通常的认证,该协议由私钥产生、私钥更新、签名和验证 4 个部分组成.选择 $E(GF(2^n))$ 上的一个有理点 $P(x,y)$,作为基点,求出 P 的阶 n,n 为满足 $nP=O$ 的素数,根据 SHA-1 选择一个单向安全的 Hash 函数 $h(x)$.设系统的参数为 $(GF(2^n), E, P, n, h)$.

4.1　系统初始化及私钥的生成

(1) Q 选择选择一大素数 p 和一个随机整数 $k_T(1<k_T<p)$ 作为私钥保存起来,将 $P_T=k_TP$ 作为公钥,是系统的公开参数.

(2) Q 给每一个系统用户分配一个身份号,如用户 A 为 ID_A,用户 A 选择一个随机数 k_A^0,计算 $P_A=k_A^0P=(x_0,y_0)$,$p_A=x_0 \bmod n$;

(3) 计算 $SK_{A0}^{n^T}=h(ID_A)k_A^0 \bmod p$,$SK_{A0}^{n^T}$ 是 A 的初始私钥应该秘密存放;将私钥的有效期分为 T 个时间段;

(4) A 的公钥是 $SK_{A0}^{n^T}P=h(ID_A)k_A^0P=h(ID_A)P_A$.

4.2　私钥的更新算法

当系统进入 i 时间段时,$1\leqslant i\leqslant T$,签名者使用拥有的 $i-1$ 时间段的密钥 SK_{Ai-1} 计算 $SK_{Ai}=SK_{Ai-1}^n \bmod p$,删除系统中 $i-1$ 时间段的密钥 SK_{Ai-1},保密新生成的 i 时段的密钥 SK_{Ai}.

4.3　签名过程

(1) 签名者随机选择一个整数 t,计算 $tP=(x,y)$,$r=x \bmod n$;

(2) 计算 $e=h(m)$,$s=(t+(e\ 8\ r)SK_{Ai}^{n^{T-i}})P$;

(3) 以 (s,r) 作为信息 m 的签名发送给第三方 Q;

4.4　验证过程

(1) 验证者首先计算 A 的公钥 $G=h(ID_A)PA$;

(2) 计算 $e=h(m)$,$u=(e\ 8\ r) \bmod n$;

(3) 计算 $X=s-uG=(x_1,y_1)$;

(4) 如果 $X=0$,则拒绝这个签名;否则计算 $r_1=x_1 \bmod n$,若 $r_1=r$,则接受这个签名.

4.5　方案的有效性证明

事实上,由归纳法可知,

$$SK_{Ai}^{n^{T-i}}=SK_{Ai-1}^{n^{T-i+1}}=\cdots=SK_{A0}^{n^{T-i+i}}=SK_{A0}^{n^T},$$

则

$$X=s-uG=(t+(e\ 8\ r)SK_{Ai}^{n^{T-i}})P-u(h(ID_A)P_A)=tP+(e\ 8\ r)SK_{A0}^{n^T}P-(e\ 8\ r)SK_{A0}^{n^T}P=tP=(x,y).$$

因此,本方案可以有效地工作.

5　新方案的安全性分析

本方案是基于有限域 $GF(2^n)$ 上非超奇异椭圆曲线数字签名的一种改进,其安全性是在非超奇异椭圆曲线密码体制的安全性基础上,进一步依赖于计算离散对数的难度.因而,它比基于有限域上的离散对数问题的公钥体制更安全,是值得信赖的.除非能破解离散对数问题,否则即使攻击者在 i 时间段侵入了系统获得了私钥 SK_i,也无法获得 $SK_{i-1}, SK_{i-2}, \cdots, SK_0$.另外,攻击者试图伪造当前时间段的签名所面临的椭圆曲线离散对数问题,难度远大于求解一般离散对数的问题.同样,攻击者要想从签名者的公钥中求解出私钥相当于求解离散对数问题,而要从签名者公开传送的密文中求解出签名也是一个求解离散对数的问题.

6　结　论

本文在因子分解、离散对数问题的困难假设下,给出一种椭圆曲线密码体制的数字签名方案,然后基于此方案提出一种具有前向安全数字签名方案,最后用新方案给出了一种基于身份的椭圆曲线前向安全数字签名方案,并有力地保证了新方案的安全性和有效性,因此,将新方案应用于电子商务等领域,具有广泛的应用前景.

参考文献:

[1] 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.

[2] 赖溪松. 计算机密码学及其应用[M]. 北京:国防工业出版社, 2001. 1—30.

[3] 黄元飞, 陈麟, 唐三平. 信息安全与加密解密核心技术[M]. 上海:浦东电子出版社, 2001.

[4] IEEE 1363. Standard specifications for public-key cryptography[S]. 2000.

[5] Johson D, Menezes A. The Elliptic Curve Digital Signature algorithm[C]. Technical Report, CORR 99—31, Canada: Department of Combinatories and Optimization, University of Waterloo, 1999.

[6] William Stallings. 密码编码学与网络安全:原理与实践(第 2 版)[M]. 杨明, 胥光辉, 齐望东, 等译. 北京:电子工业出版社, 2001.

[7] Pohlig S, Hellman M. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance [J]. IEEE Trans Inform Theory, 1978, 24: 106

— 110.

[8] Naor M, Yung M. Universal one-way hash functions and their cryptographic applications[A]. Johnson, D. S. ed. Proceedings of the 21st Annual ACM Symposium on Theory of Computings (STOC' 89)[C]. Seattle, WA, New York: ACM Press, 1989. 33—43.

[9] Yen S M, Laih C S. Improved digital signature algorithm [J]. IEEE Tran. On Computers, 1995, 44(5): 729—730.

[10] Bellare M, Miner S K. A forward-secure digital signature scheme[A]. Proc. of the CRYPTO' 99[C]. Berlin: Springer-Verlag, 1999. 431—448.

A Forward-secure Digital Signature Scheme of ECC (Elliptic Curve Cryptography) Cryptography

ZHAN Xiong-quan, HONG Jing-xin

(Dept. of Computer Science, Xiamen University, Xiamen 361005, China)

Abstract: In order to overcome the limitations of the ordinary digital signatures, this paper advances an ECC digital signature scheme, and then puts forward a new forward-secure digital signature scheme, which is based on the elliptic curve cryptosystem. In the new scheme, the digital signature's private key is under the control of some one-way function and continually changed in different durations with time going by, but its public key remains the same. So the attacker still could not fake the signature of the past time even if the private key in signature is leaked out in some period of time. In this way this scheme makes sure of the security of signature of former phases. It analyzes the security of the scheme and proves the scheme's validity.

Key words: ECC (elliptic curve cryptography); forward-secure; digital signature