一种前向安全性的可证实代理数字签名方案

梁雨平[1],汤小华[1,2]

(1.黄冈师范学院 计算机系,湖北 黄冈 438000;
2.武汉理工大学 计算机学院,湖北 武汉 430070)

摘 要:现有的代理数字签名方案都是基于离散对数问题和大数因子分解问题的方案。文中提出的数字签名方案的思想包括签名方案的前向安全性、代理签名的不可抵赖性。该方法是一种基于椭圆曲线离散对数问题的代理签名方案。文中对方案的复杂性和安全性进行了分析,分析结果表明该方法安全可行,同时也扩展了椭圆曲线密码的密码功能。

关键词:数字签名;椭圆曲线;前向安全签名

中图分类号:TP309.7 **文献标识码**:A **文章编号**:1673-629X(2007)07-0142-03

A Certifiable Representative Digital Signature Approach Based on Forward Security

LIANG Yu-ping[1], TANG Xiao-hua[1,2]

(1. School of Computer Science and Technology, Huanggang Normal University, Huanggang 438000, China;
2. School of Computer Science and Technology, Wuhan University of Technology, Wuhan 430070, China)

Abstract: The present representative digital signature approaches are based on discrete logarithm problem and large number factor decomposition. The idea of the digital signature approach proposed in this paper includes the forward security and non-refutation of representative signature. The approach is based on elliptic curve discrete logarithm problem. The paper made an analysis on the complexity and security of the proposed signature approach. The analytical result shows that the approach is safe and feasible, and it extends the cipher function of elliptic curve codes.

Key words: digital signature; elliptic curve; forward security signature

0 引 言

签名代表了签名人的一种权利。在数字签名方案中,这种权利体现为签名人对自己私钥的拥有及使用。在通常的手写签名意义下,这种权利的实现需要签名人直接在被签文件上签名。这种签名不能转让,但在实际应用中存在代理签名的问题。经过代理签名的文件和本人签名同样具有实效。因此在数字签名方案中存在这样的问题:原始签名人如何将签名的权利委托给一个被称为代理签名的人,同时又不暴露自己的私钥;如何验证签名的正确性;如何解决代理签名的时效性。

一个代理签名方案至少需要三种不同类型的人参与,即原始签名人、代理签名人和代理签名的验证人。为简单起见,文中用 A 表示原始签名人,用 B 表示代理签名人和用 C 表示代理签名的验证人。一个代理签名方案又至少包括四个过程、即初始化过程,数字签名权利的委托过程、代理签名的产生过程和代理签名的验证过程。

1 具有前向安全性的数字签名的密钥进行过程

1.1 前向安全性的提出

普通数字签名具有如下局限性:若签名的密钥被泄露,则这个签名者所有的签名都有可能泄露。这个局限性影响了签名应该提供的不可否认性。实际上,签名者否认他自己签名最简单的方法就是在 Internet 上匿名公开自己的密钥,然后声明计算机遭到了入侵。代理签名的人可能变动,如果签名不具有时效性,可能出现两个代理签名同时有效。其中,只有一个合法。因此,在文中提出一个具有时效性的密钥方法,为代理签名提供更有效的安全保障。

收稿日期:2006-10-18

基金项目:湖北省教育厅优秀中青年人才项目(2000B47001)

作者简介:梁雨平(1970-),男,湖北麻城人,副教授,研究方向为计算机图形图像处理,计算机网络技术。

1.2 构造过程

具有时效性的代理数字签名方案实现的一个关键是密钥进化。系统建立初期用户注册获得一个证书[1,2],得到公钥 PK 和相应的密钥 SK。将公钥的有效期范围分为 T 个时段,分别记为 1,2,3,…,T。在有效期内,公钥 PK 是固定的,而密钥随时段不断进化更新。以 SK_i 记 i 时段的秘密钥,进入时段 i 时,首先计算 $SK_i = f(SK_{i-1})$,这里 f 是一个单向函数,求得 SK_i 后立即删除 SK_{i-1},这样即使当攻击者在 T 时段攻入系统获得了 SK_i 或被不信任的代理者公布了 SK_{i-1},在第 T 时段内不可能获得。密钥的进化如下所示:

$$SK_0 \xrightarrow{f} SK_1 \xrightarrow{f} SK_2 \xrightarrow{f} \cdots \xrightarrow{f} SK_T$$

1.3 基于离散对数知识具有时效性的密钥管理方案

本方案的密钥生成是基于离散对数知识的。

(1)签名者初始密钥的生成。

设 p,q 为大素数,令 $N = pq$,构造群 $G = < g >$,使其阶数为 N,即 $\mathrm{ord}(g) = N$;将签名密钥的有效性分为 T 个时段,任选 $X_0 \in R^2N$,令 $Y_T = gx_0^{2T}$,该系统签名者的公钥 $PK = \{g, n, Y_T\}$,签名者的初始秘密钥 $SK_0 = \{x_0\}$,即签名者的签名秘密钥和公开钥的初始对 $(X_{s0}, ys) = (SK_0, PK)$,其中 $X_{s0} = X_0, ys = y_T$。

(2) 签名者密钥的进化。

系统一旦进入 $i(1 \leqslant i \leqslant T)$ 时段,签名者使用拥有的 $i-1$ 时段的密钥 $sk_{i-1} = \{x_{i-1}\}$,计算 $X_i = X_{i-1}^2 \bmod N$ 及 $y^i = g^{xi}$,则由归纳法可知 $X_i = X_0^{2i} \bmod N$,此时立刻从系统中完全删除 $i-1$ 时段的密钥 $sk_{i-1} = \{x_{i-1}\}$,保密 i 时段的密钥 $sk_i = \{x_i\}, y_i, y_T$。由求离散对数问题的困难性可知,由 y_i, y_T 无法获得 X_0,X_{i-1}。

2 基于椭圆曲线的代理签名方案

在上节详细介绍了具有时效性的密钥管理方案,不论是原始签名者,还是代理签名者都可采用。下面介绍代理签名方案。

定义　$p > 3$ 是素数。$\mathbf{Z}_p$ 上的同余方程

$$y^2 \equiv x^3 + ax + b \pmod p \tag{1}$$

的所有解 $(x,y) \in \mathbf{Z}_p \times \mathbf{Z}_p$,连同一个特殊的点 θ 即无穷远点,共同构成 $\mathbf{Z}_p$ 上的椭圆曲线 $y^2 \equiv x^3 + ax + b$,其中 $a,b \in \mathbf{Z}_p$ 是满足 $4a^2 + 27b^3 \neq 0$ 的常量。

E 上的加法定义如下(这里的所有运算都在 $\mathbf{Z}_p$ 中):假设 $P(x_1,y_1)$ 以及 $Q = (x_2,y_2)$ 都是 E 上的点。如果 $x_1 = x_2$ 且 $y_2 = -y_1$,则 $P = Q = \theta$;否则 $P + Q = (x_3,y_3)$,其中

$$x_3 = \lambda^2 - x_1 - x_2$$

$$y_3 = \lambda(x_1 - x_3) - y_1$$

$$\text{且 } \lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} & P = Q \end{cases} \tag{2}$$

密码体制 1　椭圆曲线数字签名算法。

设 p 是一个素数或 2 的幂次方,E 是定义在 $\mathbf{F}_p$ 上的椭圆曲线。设 A 是 E 上阶数为 q 的一个点,使得 $< A >$ 上的离散对数问题是难处理的。设 $p = \{0,1\}^*$,$A = \mathbf{Z}_q^* \times \mathbf{Z}_q^*$,定义

$$K = \{(q,p,E,A,m,B): B = mA\}$$

其中 $1 \leqslant m \leqslant q-1$,值 q,p,E 和 A 是公钥,m 为私钥。

对于 $K = (q,p,E,A,m,B)$ 和一个秘密的随机数 k,$1 \leqslant k \leqslant q-1$,定义 $\mathrm{sig}_K(x,k) = (r,s)$

其中

$$kA = (u,v)$$

$$r = u \bmod q \tag{3}$$

$$s = k^{-1}(\mathrm{SHA}-1(x) + mr) \bmod q$$

(如果 $r = 0$ 或者 $s = 0$,应该为 k 另选一个随机数)。

对于 $x \in \{0,1\}^*$ 和 $r,s \in \mathbf{Z}_q^*$,验证是通过下面的计算机完成的:

$$w = s^{-1} \bmod q$$

$$i' = w\ \mathrm{SHA}-1(x) \bmod q$$

$$j = wr \pmod q \tag{4}$$

$$(u,v) = iA = jB$$

$$\mathrm{ver}_K(x,(r,s)) = \text{true} \Leftrightarrow u \bmod q = r$$

签名方案步骤如下:

Step1:初始化过程。假定 E 是定义在有限域[2,3] F 上的一条椭圆曲线,$P \in E$ 是 E 中一个阶为 N 的点,将 E,N 和 P 公开,进一步假定 A 为原始签名人,A 的私钥为 K_A,公钥为 P_A,私钥 K_A 保密,公钥 P_A 公开。公钥 P_A 和私钥 K_A 之间有关系:$P_A = K_AP$。

Step2:委托过程。原始签名人 A 为了将其签名的权利委托给代理签名人 B,同时又不暴露自己的私钥 K_A,A 首先选取随机数 K_0,并计算 K_0P,记 $Q_0 = k_0p = (x_0,y_0)$,其中 $x_0,y_0 \in F$,然后 A 计算:

$$R_0 \equiv x_0 \bmod N \text{ 和 } Q \equiv (K_A + r_0k_0) \bmod N \tag{5}$$

然后 A 将用 B 的公钥加密,得到 $M = E(D(Q,K_{SA}),K_{PB})$。最后将 (M,θ_0) 公开发送给 B。称 (M,θ_0) 为 A 发送给 B 的委托信息。B 收到一组委托信息 (M,θ_0) 后,先用 B 的私钥解密 $\overline{m} = D(E(M,K_{SB},K_{PA})$,并且验证 $Q_p = P_A + r_0Q_0$。

如果等式(5) 成立,则委托过程成立,A,B 两方都

得到认证。如果等式(5) 不成立,则委托过程失败。

Step3:代理签名的产生过程。对任何消息 $m(o < m < n)$,A 的代理签名人B 可以按照下面的方法产生关于消息的代理签名。B 首先选取随机数K,$o < K < n$,然后计算 K_P,记 $K_P = (x,y)$,其中 $x,y \in F$,接着 B 计算:①$r \equiv x \bmod N$;②$S \equiv k^{-1}(m + rQ_0)\ m_0 \bmod N$,则$(m,r,s,Q_0)$ 一起构成了代理签名人及消息的代理签名。

Step4:验证过程。任何一个验证人 C 收到代理签名(m,r,s,Q_0) 后,利用原始签名人的公钥 P_A,进行下列计算:

①$c \equiv s^{-1} \bmod N$;

②$u_1 \equiv mc \bmod N$;

③$u_2 \equiv rc \bmod N$;

④ 计算 $u_1 p + u_2(PA + r_0 Q_0)$;设 $u_1 p + u_2(PA + r_0 Q_0) = (x,y)$;

⑤ 计算 $x \bmod N$,如果 $r = x \bmod N$,则代理签名得到认证。

在整个代理签名方案中,A,B 的密钥管理是前提,要充分考虑时效性。同时在委托过程中 A,B 双方要认证对方身份是否合法。验证过程严格要求计算步骤执行。文中验证过程的安全性证明可参考文献[4]。

3 代理签名性能分析

3.1 基本性能

(1) 基本不可伪造性。由 shamon 信息理论知[5],在未知关于 $h(m_w)a_1$ 的信息情况下,从等式 $s_1 = ux_A + h(m_w)a_1$ 中不能得到任何关于 X_A 的信息,但若求出 a_1,则可解出 X_A。但从中很难解出 a_1,从而不能伪造 A 的普通签名。

(2) 代理签名的不可伪造性。只有 B 知道 K 的随机独自秘密数,故只有 B 能生成代理签名。

(3) 不可抵赖性。由于任何人都不能伪造 A 的签名,所以 A 不能否认一次有效的签名,因授权给 B,因此只有 B 才能代理 A 签名。

(4) 密钥依赖性。因 A,B 的私钥都具有时效性即 $SK_i = f(SK_{i-1})$,所以密钥之间存在依赖性,但生成后自动消失。

(5) 可注销性。A 的授权消息包括授权时间及代理的有效性。对一个诚实的代理来说,授权消息保证方案的可注销性。目前大多数具有证书的签名方案其可注销性都基于此,但代理人若不诚实,可通过自动更换私钥解决。

3.2 代理签名方案特有的优点

能防止代理签名人滥用自己的签名权。

①签名方案附有授权消息 m_w,ID_A,ID_B,代理签名消息的许可范围,且 m_w 受安全Hash函数保护。这样 B 既不能将自己的代理权转移给他人,又不能对任何消息(如有损 A 利益的消息) 进行签名。

② 证书上的 N 为A 规定B 在T(T 为授权时间及代理的有效期限) 内签名的最大次数。若 B 违反了规定,在进行 $N+1$ 或 $N+1$ 次以上的签名后,由代数知识知,方程组 $n_i u = m_i h(nt_i)X_B + s_i k + h(m_{i1}) + h(m_{i2}) + \cdots + h(m_{iN-2})(i = 1,2,3,\cdots,N)$ 共有 $N+1$ 个未知量,任何人都可以收集 $N+1$ 或 $N+1$ 个以上有效签名,带到方程组里使可解出 X_B(但此对原始签名人毫无影响),故 B 不会冒危险而滥用其代理权。这样,B 在有效期内至多签名 N 次后其代理签名权会终止。

4 结束语

文中提出了一种前向安全性的可证实代理数字签名方案,讨论了该方案的正确性和安全性,分析结果表明该方法有很强的理论和实用价值。

参考文献:

[1] 白国强,黄 谆. 基于椭圆曲线的代理数字签名[J]. 电子学报,2003,31(11):1659-1663.

[2] 李方伟,王 建,陈广辉. 前向安全的基于椭圆曲线密码体制的签密方案[J]. 北京邮电大学学报,2006,29(1):22-25.

[3] 眭新光,罗 慧. 基于S盒的数字图像置乱技术[J]. 中国图像图形学报,2004,9(10):1223-1226.

[4] 秦 波,王尚平,王晓峰,等. 一种新的前向安全可证实数字签名方案[J]. 计算机研究与发展,2003,40(7):1016-1020.

[5] 李淑静,赵远东. 基于椭圆曲线的 ELGamal 加密体制的组合公钥分析及应用[J]. 微计算机信息,2006(12):69-71.

(上接第 141 页)

[2] Denninc D. An Intrusion-detection Model[C]//In IEEE Symposium on Security and Privacy. Oakland, USA:[s.n.], 1986.

[3] 李守国,李 俊. 基于数据挖掘的入侵检测系统设计[J]. 计算机技术与发展,2006,16(4):212-214.

[4] Lee W, Stolfo S J. Data Mining Approaches for Intrusion Detection[C]//In: Proceedings of the 7th USENIX Security Symposium. San Antonio:[s.n.],1998:6-9.

[5] Han Jiawei, Kamber M. 数据挖掘概念与技术[M]. 范 明,孟小峰等译. 北京:机械工业出版社,2001:147-158.