

一种基于椭圆曲线的代理多重盲签名方案

左黎明, 刘二根, 汤鹏志

(华东交通大学 基础科学学院, 江西 南昌 330013)

摘 要: 提出了一种新的基于椭圆曲线离散对数问题的代理多重盲签名方案, 讨论了椭圆曲线离散对数问题的可能攻击方法. 该方案可以有效地防止成员的欺诈行为. 签名者可以通过验证操作发现伪签名, 所有签名参与者还可验证签名者公钥的有效性以防止成员内部的欺诈行为. 方案充分利用椭圆曲线密码体制密钥小、速度快等优点, 降低了通信成本, 因而更具有安全性和实用性.

关键词: 数字签名; 多重盲签名方案; 椭圆曲线

中图分类号: TP393.08

文献标识码: A

文章编号: 1000-7180(2010)09-0069-04

A Proxy Blind Multi-signature Scheme Based on the Elliptic Curve

ZUO Li-ming, LIU Er-gen, TANG Peng-zhi

(School of Natural Science, East China Jiaotong University, Nanchang 330013, China)

Abstract: A new proxy blind multi-signature scheme based on the intractability of the elliptic curve discrete logarithm problem is proposed. Some methods of attack to the discrete logarithm problem are discussed. The scheme can avoid the cheating from the signers efficiently. The signatory can validate the last signature to discover fake signature, at the same time all members can deal with the emergency according to the error message in time, it also can validate the validity of signatory's public key avoid the cheating by inner users. The scheme takes full advantage of elliptic curve cryptosystem, such as shorter private key, higher signature efficiency and reduces the cost of communication, so it is security and practical.

Key words: digital signature; blind multi-signature scheme; elliptic curve

1 引言

代理多重盲签名方案一般建立在一种公钥系统基础之上,而这种公钥系统的安全性依赖于某种数学难题的求解困难性. Chaum 盲签名机制是第一个盲签名机制,它是基于 RSA 的. 一种安全的代理多重盲签名机制必须是既能抵抗自适应的并行攻击,而且又要保证不能被非法复制,目前已经出现了多种代理签名和代理多重盲签名机制^[1-3],大多依赖于求解大数分解问题和一般有限域离散对数问题(DLP)的难度,而基于半环上的代数分解问题和椭圆曲线域离散对数问题(ECDLP)求解困难性的方

案有许多优点,因此这种数字签名方案将逐步取代各种基于大数分解问题和一般有限域离散对数问题的数字签名方案,文献[1]给出的协议由于计算过程相当繁琐,实际上很难实现,文献[2]中方案无法抵御用户合谋攻击,本文提出了一种新的基于椭圆曲线域离散对数问题(ECDLP)的代理多重盲签名方案.

2 多重数字签名与代理签名

2.1 多重数字签名

在数字签名过程中,有时需要多个用户对同一消息进行签名和验证,因此有人提出了一组用户对

收稿日期: 2009-07-15; 修回日期: 2009-09-15

基金项目: 国家自然科学基金项目(10661007); 江西省自然基金项目(2007GZS1054); 江苏省教育厅青年科学基金项目(GJJ09129)

同一消息进行签名的多重数字签名(Digital Multisignature)的概念. 多重代理签名的基本方案一般分为两类^[1]: 一类为有序多重数字签名(Sequential Multisignature)方案, 另一类称为广播多重数字签名方案(Broadcasting Multisignature). 还有其他一些复杂的多重数字签名方案, 通常是按照签名的先后和签名发挥作用的顺序来构造的, 主要有基于图结构的多重数字签名(Map Multisignature)、基于树结构的多重数字签名(Tree Multisignature)、基于环结构的多重数字签名(Ring Multisignature)等. 这些签名方案主要是根据应用的不同需求而设计的, 而且规定了协议交互验证过程, 因此非常复杂, 但是这些复杂的签名方案也是基本类型的复合.

有序多重数字签名方案中, 按照应用要求在逻辑上设置好一条签名链, 规定好了对信息数字签名的顺序, 首先消息发送者将信息传给签名链中的第一个签名者, 第一个签名者进行数字签名之后将信息发送给签名链中的下一个签名者, 下一个签名者对上一个签名者的数字签名进行验证, 如果发现签名有效, 继续用自己的私钥签名, 并将信息传给下一个签名者, 否则拒绝签名, 中止协议. 依次类推, 直到最后信息接收者进行最后的签名验证.

在广播多重签名方案中, 信息发送者对所有签名人均同时发送信息, 每个签名人对同样的信息进行签名, 最后所有带签名的信息都提交给一个签名收集者, 签名收集者整理后发送给信息接收者进行签名验证.

2.2 代理签名与代理多重盲签名体制

设 A, B 是数字签名机制 $(M, S, K, \text{SIG}, \text{VER})$ 的两个用户, 他们的密钥对分别为 $(x_A, y_A), (x_B, y_B)$. 如果有以下条件成立^[2]:

(1) A 利用他的密钥 x_A 计算出一个数 σ , 并且将 σ 秘密地交给 B ;

(2) 任何人(包括 B) 在试图求出 x_A 时, σ 都不会对他有任何帮助;

(3) B 可以用 σ 和 x_B 生成一个新的签名密钥 $\sigma_{A \rightarrow B}$;

(4) 存在一个公开的验证算法 $\text{ver}_{A \rightarrow B}$, 使得对任何 $s \in S$ 和 $m \in M$, 都有以下成立: $\text{ver}_{A \rightarrow B}(y_A, s, m) = \text{True} \leftrightarrow s = \text{sig}(\sigma_{A \rightarrow B}, m)$;

(5) 任何人在试图求出 x_A, x_B, σ 和 $\sigma_{A \rightarrow B}$ 时, 任何数字签名 $\text{sig}(\sigma_{A \rightarrow B}, m)$ 都不会对他产生任何帮助.

那么我们称用户 A 将他的(部分)数字签名权

力委托给了用户 B , 并且称 A 为 B 的原始签名人, 称 B 为 A 的代理签名人, 称 σ 为委托密钥, 称 $\sigma_{A \rightarrow B}$ 为代理签名密钥, 称以 $\sigma_{A \rightarrow B}$ 作为签名密钥对消息 $m \in M$ 生成的数字签名 $\text{sig}(\sigma_{A \rightarrow B}, m)$ 为 A 的代理签名(Proxy Signature), 能够生成代理签名的数字签名体制被称为代理签名体制^[2-5].

对于原始签名人而言, 他事先并不知道他的代理签名人要什么样的文件信息进行数字签名, 因此从一定意义上而言, 代理签名具有盲签名的一些特点, 即原始签名人并不知道要签名的文件内容. 但是代理签名与盲签名也有不同的特点, 代理签名人可以知道要签名的文件内容, 并对其进行签名. 由此过程可以看出, 代理签名人可以与其他恶意攻击者对原始签名人进行串谋攻击^[5]. 有些情况下, 对于代理签名人, 也必须对其隐瞒要签名的文件内容. 如果将信息在多个签名者之间来回地签名、验证, 必然将影响整个通讯网络的效率, 降低整个网络协议的安全系数, 因此如果所有的签名人都委托同一个代理签名人, 从逻辑上看, 整个签名过程要多人参与, 但实际上除了初始化委托密钥外, 整个签名过程只需代理签名人即可完成, 因此效率将大大提高.

设 $A_i (1 \leq i \leq n)$ 是某个数字签名体制 $(M, S, K, \text{SIG}, \text{VER})$ 的 n 个用户, 对任意 $1 \leq i \leq n$, 记 A_i 的公钥密钥对为 (x_i, y_i) . 假设对任意 $A_i (1 \leq i \leq n)$ 都将其数字签名权利委托给一个代理签名人 B (记 B 得到的代理签名密钥为 $\sigma_i (1 \leq i \leq n)$, r 为盲化因子. 如果代理签名人 B 对某个信息 $m \in M$ 生成了一个多重盲签名 $(s, r) = \text{sig}(\sigma_1, \sigma_2, \dots, \sigma_n, m)$, 使得验证这个多重签名的有效性时, 必须使用所有用户 A_i 的公开密钥 $y_i (1 \leq i \leq n)$, 那么称 (s, r) 为一个由 B 代表 $A_i (1 \leq i \leq n)$ 生成的代理多重盲签名. 能够产生代理多重盲签名的数字签名体制 $(M, S, K, \text{SIG}, \text{VER})$ 称为代理多重盲签名体制^[1, 5-6].

3 基于椭圆曲线的代理多重盲签名协议

3.1 协议初始化

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. 若签名者 A 随机选择一个整数 x_A 作为私钥, 则其公钥是 $y_A = x_A g$.

$A_i (1 \leq i \leq n), B, C$ 是数字签名机制 $(M, S, K, \text{SIG}, \text{VER})$ 的多个用户, $A_i (1 \leq i \leq n)$ 的密钥

对为 (x_i, y_i) , B 和 C 的密钥对分别为 (x_B, y_B) 、 (x_C, y_C) . $A_i (1 \leq i \leq n)$ 为 B 的原始签名人, B 为 $A_i (1 \leq i \leq n)$ 的代理签名人, $\sigma_i (1 \leq i \leq n)$ 为委托密钥, $\tilde{\sigma}$ 为代理签名密钥, $y_{\tilde{\sigma}} = k\tilde{\sigma}$ 为代理签名公钥, m 为需签名文件信息, $h(x)$ 为一种散列算法, $\parallel$ 表示连接运算. C 要求 B 对消息 m 利用 $\tilde{\sigma}$ 进行盲签名.

3.2 $A_i (1 \leq i \leq n)$ 对 B 的委托过程

A_i : 选取一随机数 $t_i \in [2, n-1]$, 计算 $T_i = t_i g$, $\tilde{h}_i = h(T_i \parallel y_i)$, $\sigma_i = \tilde{h}_i x_i + t_i \pmod{n}$; $A_i \rightarrow B: (\sigma_i, T_i, \tilde{h}_i)$;

B : 验证每个等式 $\sigma_i g \equiv \tilde{h}_i y_i + T_i \pmod{n}$ 且 $T_i \neq T_j (1 \leq i, j \leq n)$, 若不成立, 则要求对应的 A_i 重发. 若成立则计算代理签名密钥 $\tilde{\sigma} = \sum_{i=1}^n \sigma_i + x_{B y_B} \pmod{n}$, 代理签名公钥 $y_{\tilde{\sigma}} = \tilde{\sigma} g = (\sum_{i=1}^n \sigma_i + x_{B y_B}) g$;

B : 计算散列值 $\tilde{h}_1 = h(T_1 \parallel \sigma_1 \parallel y_1 \parallel y_{\tilde{\sigma}})$, $\tilde{h}_i = h(\tilde{h}_{i-1} \parallel T_i \parallel \sigma_i \parallel y_i) (2 \leq i \leq n)$, $\tilde{h} = \sum_{i=1}^n \tilde{h}_i \pmod{n}$;

$B \rightarrow A_i: \tilde{h}_i$;

3.3 代理盲签名的生成过程

$B \rightarrow C$: 选取一个随机数 $v \in [2, n-1]$, 计算 $\tilde{v} = \tilde{h} g$, 将 $(\tilde{v}, \tilde{h})$ 发送给 C ;

C : 选择一个随机数 $a \in [2, n-1]$, 计算 $r = \tilde{v} + ag \pmod{n}$, $\tilde{r} = r^{-1} m \pmod{n}$, 对消息 m 盲化;

$C \rightarrow B$: C 发送 $\tilde{r}$ 给 B ;

$B \rightarrow C$: 利用代理签名密钥 $\tilde{\sigma}$ 对 $\tilde{m}$ 进行盲签名, 计算 $\tilde{s} = \tilde{\sigma} \tilde{v} + \tilde{r} \tilde{h} \tilde{v} \pmod{n}$, 将 $\tilde{s}$ 发送给 C ;

C : 计算 $s = \tilde{s} r \tilde{v}^{-1} + am \pmod{n}$, 则 $(r, s, T_1, T_2, \dots, T_n)$ 是对 m 的签名.

3.4 代理盲签名的验证过程

验证 $sg = ry_{\tilde{\sigma}} + rm$. 若成立, 则接受 $(r, s, T_1, T_2, \dots, T_n)$ 是对 m 的签名. 否则拒绝.

3.5 协议分析

(1) 不可伪造性: 由于只有 B 才能生成 $\tilde{\sigma}$, 所以除 B 以外(包括每个 A_i), 任何人都不能伪造签名, 因此只有 B 才能构造出 $\tilde{\sigma}$. 如果怀疑签名被伪造, 参与各方可直接验证 $sg = r[\sum_{i=1}^n (\tilde{h}_i y_i + T_i) + ny_B^2 + m] \pmod{n}$.

(2) 可区分性: 最终的签名为 $(r, s, T_1, T_2, \dots, T_n)$, 由三部分组成, 一部分是普通的签名信息 s , 一部分是数 r , 另一个部分是由被代理人 A_i 产生的数 T_i , 只要每个被代理人开始选的随机数不同, 就可以保证代理签名具有区分性.

(3) 不可抵赖性: 由代理签名的不可伪造性和代理签名的可区分性可以知道, 通过所有被代理人共同协作, 验证 $\tilde{h}_i$, 并计算出 $\tilde{h}$, 因此 B 对签名是不能抵赖的.

(4) 可注销性: 只要有某个被代理人 A_i 宣称 T_i 失效, 则所有与之相关的签名均失效. 身份证实性和密钥依赖性显然是显然的.

(5) 代理盲签名的验证过程正确性证明如下:

$$\begin{aligned} sg &\equiv (\tilde{s} r \tilde{v}^{-1} + am) g \\ &\equiv ((\tilde{\sigma} \tilde{v} + r^{-1} m \tilde{h} \tilde{v}) r \tilde{v}^{-1} + am) g \\ &\equiv (\tilde{\sigma} r \tilde{v} \tilde{v}^{-1} + \tilde{h} m + am) g \\ &\equiv (\tilde{\sigma} r + \tilde{h} m + am) g \\ &\equiv \tilde{\sigma} r g + \tilde{h} m g + am g \\ &\equiv r y_{\tilde{\sigma}} + \tilde{h} m g + am g \\ &\equiv r y_{\tilde{\sigma}} + (\tilde{v} \tilde{h} g + ag) m \\ &\equiv r y_{\tilde{\sigma}} + (\tilde{v} + ag) m \\ &\equiv r y_{\tilde{\sigma}} + rm \pmod{n} \end{aligned}$$

4 与协议相关的一些问题

目前针对 ECDLP 的攻击方法有以下几种^[7-8]:

(1) 椭圆曲线域上 pohlig-hellman 离散对数算法; (2) 椭圆曲线域上 pollard-p 离散对数算法; (3) 基于有限循环群理论的椭圆曲线域离散对数算法; (4) 椭圆曲线域 Shark 离散对数算法. 但是对于超奇异椭圆曲线(设 F_q 的特征为 p , E/F_q 的 q 阶 Frobenius 变换的迹 t 是 p 的倍数时, E 称为超奇异的), 采用 MOV 算法和 FR 算法等亚指数概率攻击算法可以很好地求解此类曲线的 ECDLP. 另外, 还有一类特殊椭圆曲线是异常(anomalous)椭圆曲线(设 $q = p^m$, $p \neq 2, 3$ 为素数, E/F_q 由方程 $y^2 = x^3 + ax + b$ 定义, 阶为 p , 当 $p = q$ 时, 异常曲线上的 p 阶 Frobenius 变换的迹 $t = 1$), 使用 Semaev-Smart-Satoh-Araki 算法可以较好地求解此类曲线的 ECDLP.

通过以上的分析, 要保证椭圆曲线密码系统的安全性, 就是要使所选取的曲线能抵抗上述的关于 ECDLP 求解算法的攻击, 目前如何选取最合适的曲线是一个理论难题, 在本方案的实现中, 参考 IEEE1636 标准和 NIST 推荐的参数来产生一条椭圆曲线^[7-8]:

(1) 为了对抗 Pollard- ρ 算法攻击, 所选取 EC 的阶 $\#E(\text{GF}(q))$ 的分解式中应该包含一个较大素因子, 应不小于 160bit;

(2) 为了抗击 Weil 对和 Tate 对的攻击, 对于 $1 \leq k \leq 30$, n 不能除 $q^k - 1$, 不宜选取超奇异椭圆曲线;

(3) 为了抗击 Semaev-Smart-Satoh-Araki 算法的攻击, 所选曲线的阶不能等于该曲线所定义的有限域的阶, 即 $\#E(F_q) \neq q$, 不宜选取异常椭圆曲线和二元曲线;

(4) 若选取二进制域 $\text{GF}(2^n)$, 度 n 最好为素数.

椭圆曲线密码体制应用中的大量运算是倍乘(数乘), 为了提高程序的运行速度, 在实现中, 椭圆曲线上点的运算采用了复乘(Complex Multiplication)算法.

5 结束语

本文构造出一种多重代理盲数字签名方案^[9], 从分析得出, 它比文献[1, 4]中提出的基于一般域上的 DLP 和大数分解问题的多重代理盲签名方案更安全有效, 计算复杂性更小, 易于在电子商务和电子政务系统中使用. 使用椭圆曲线域上的离散对数问题构造数字签名方案, 相对大数分解问题具有更快的速度. 下一步研究的重点是在实际应用中结合个人数字证书和 CA 中心构造协议.

参考文献:

- [1] Lu R, Cao Z, Zhou Y. Proxy blind multi-signature scheme without a secure channel[J]. Applied Mathematics and

Computation, 2005, 164(4): 179 - 187.

- [2] Hsu C L, Tsai K Y, Tsai P L. Cryptanalysis and improvement of non-reputable threshold multi proxy multi signature scheme[J]. The Journal of Systems and Software, 2007, 177(2): 543 - 549.
- [3] Mambo M, USuda K, Okamoto E. Proxy signatures: delegation of the power to sign messages[J]. IEICE Transaction on Fundamentals of Electronic Communications and Computer Sciences, 1996, E79-A(9): 1338 - 1354.
- [4] Lu E, Hwang M S, Huang C J. A new proxy signature scheme with revocation[J]. Applied Mathematics and Computation, 2005, 161(3): 799 - 806.
- [5] Pointcheva D, Stern J. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361 - 396.
- [6] 王洪涛, 李大兴, 魏传瑾. 更为有效的代理数字签名方案[J]. 微电子学与计算机, 2007, 24(6): 146 - 149.
- [7] 王洪涛, 李大兴, 周大水. 一种新的基于椭圆曲线的代理盲多重签名[J]. 微电子学与计算机, 2007, 24(2): 160 - 163.
- [8] 张龙军, 沈钧毅, 赵霖. 椭圆曲线密码体制安全性研究[J]. 西安交通大学学报, 2001, 35(10): 1038 - 1041.
- [9] 左黎明. 一种基于椭圆曲线的多重数字签名方案[J]. 华东交通大学学报, 2009, 26(1): 39 - 41.

作者简介:

左黎明 男, (1981-), 硕士, 讲师, CCF 会员. 研究方向为网络信息安全、非线性系统.

刘二根 男, (1968-), 硕士, 教授. 研究方向为图论及其应用.

汤鹏志 男, (1965-), 硕士, 教授. 研究方向为网络信息安全.

(上接第 68 页)

- [8] 徐跃, 杨英强. 输入输出调谐的低相位噪声 CMOS 压控振荡器[J]. 微电子学与计算机, 2009, 26(6): 50 - 53.

作者简介:

魏伟伟 男, (1985-), 硕士研究生. 研究方向为模拟集成电路的设计.

于海勋 男, 教授, 硕士研究生导师. 研究方向为电子设计自动化和电子技术与应用.

李卫民 男, 研究员, 硕士研究生导师. 研究方向为超大规模集成电路的设计与测试.

文武 男, 高级工程师. 研究方向为射频与模拟集成电路的设计与测试.