

一种基于椭圆曲线的指定验证人代理签名

沈丽敏, 张福泰

(南京师范大学 数学与计算机科学学院, 江苏 南京 210097)

[摘要] 将 Schnorr 签名方案和椭圆曲线数字签名方案 (ECDSA) 相结合, 给出了一个 ECDSA 的改进方案. 该方案避免了 Z_n 中的求逆运算, 从而提高了效率, 并且通过对该方案的详细安全性分析, 证明了它是安全的. 而后给出了一个基于该改进方案的指定验证人代理签名新方案, 并对这个新方案的复杂性和安全性进行了分析, 指出它是安全的、更快速的.

[关键词] 椭圆曲线, 数字签名, 适应性选择消息攻击, 指定验证人代理签名

[中图分类号] TP 309 [文献标识码] A [文章编号] 1672-1292(2008)01-0069-06

A Designated-Verifier Proxy Signature Scheme Based on Elliptic Curve

Shen Lining Zhang Futai

(School of Mathematics and Computer Science, Nanjing Normal University, Nanjing 210097, China)

Abstract This paper presents an improved elliptic curve digital signature (ECDSA) scheme which combines the Schnorr signature scheme with ECDSA. This scheme is more efficient by avoiding the calculation of inverse element over the field Z_n . And the detailed security analysis of the scheme shows that it is secure. Then a designated-verifier proxy signature scheme based on the improved ECDSA scheme is proposed. The computational complexity as well as the security of the newly proposed scheme are also analyzed. The analyses show that the scheme is not only secure but also efficient in computation.

Key words elliptic curve, digital signature, adaptively chosen-message attack, designated-verifier proxy signature

自 1976 年 Diffie 和 Hellman 首先提出公钥密码体制的概念^[1]以来, 到目前为止, 人们对公钥加密和数字签名的研究已有 30 年, 取得了丰富的研究成果. 目前在理论上和技术上较成熟的公钥密码体制主要有 3 类: 基于整数分解的、基于有限域上离散对数问题 (DLP) 的和基于椭圆曲线离散对数问题 (ECDLP) 的. 研究表明, 基于 ECDLP 的椭圆曲线密码 (ECC) 比基于整数分解的 RSA 和基于 DLP 的 ElGamal 等系统在实现和应用上具有安全性更高、计算量更小、速度更快的优点.

近 10 年来, 许多适用于各种实际应用的特殊数字签名相继被提出, 例如: 代理签名、群签名、指定验证人签名等. 其中, 代理签名的概念是由 Mambo, Usuda, Okamoto^[2]于 1996 年提出的. 代理签名解决了数字签名权力委托的问题, 即原始签名人 A 将签名的权力委托给代理签名人 B, 同时又不暴露自己的私钥.

代理签名人利用原始签名人给他的委托信息能够代表原始签名人生成数字签名, 并且任何具有原始签名人公钥的人都可以验证这种签名的真实性, 并能和原始签名人的直接签名相区别. 一个代理签名方案涉及 3 种不同类型的参与者: 原始签名人、代理签名人、代理签名的验证人. 代理签名方案一般包括 4 个阶段: 系统初始化、签名权力的委托、代理签名的产生和验证. 文献 [2-3] 指出了代理签名方案的一些安全性要求, 例如: 可验证性、可鉴别性、不可伪造性 (强不可伪造性)、可区分性、可注销性、不可否认性、防止签名的滥用等 7 个基本性质. 由于代理签名在移动通信、电子商务、电子拍卖等许多方面有着重要的应

收稿日期: 2007-03-16
基金项目: 国家自然科学基金 (60673070)、江苏省自然科学基金 (BK2006217) 和西安电子科技大学教育部计算机网络与信息安全重点实验室开放课题 (20040105) 资助项目.
作者简介: 沈丽敏 (1978-), 女, 讲师, 研究方向: 信息安全与密码学等. E-mail: shln_nnu@yahoo.com.cn
通讯联系人: 张福泰 (1965-), 教授, 博士生导师, 研究方向: 信息安全及电子商务等. E-mail: zhangfuta@njnu.edu.cn

用,所以代理签名一经提出便受到广泛的关注.

在现实生活中,如网络金融业务的签名、电子投标、某些数字公文的签署等往往要求签名只能由某些指定的接收者来验证并确认签名的有效性.指定验证人签名^[4]的概念正是为满足这种实际需要而提出的.指定验证人的签名方案主要应用于对消息 m 产生的签名能且只能由指定的验证人验证并且相信签名的有效性,而其他人却无法验证签名是否有效.这是因为,对于指定验证人而言,他能够在没有原始签名人参与的情况下,对不同的消息 m' ,再结合所能得到的公共信息,能够伪造出和消息 m' 的原始签名不可区分的签名.结合指定验证人签名和代理签名的优点,文献[3]提出了指定验证人的代理签名方案,它可以有效地解决电子商务中的一些实际应用问题.一个指定验证人的代理签名方案同样涉及 3 种不同类型的参与者:原始签名人、代理签名人、指定验证人.由于指定验证人的代理签名方案结合了这两种签名的特点,所以除了要满足代理签名所需满足的安全性要求外,还需满足指定的可验证性以及指定的不可否认性.

在现有文献中能够看到的代理签名、指定验证人签名方案大多是基于有限域上离散对数问题的.本文先给出一个改进的椭圆曲线数字签名方案,在此基础上提出一个指定验证人代理签名方案,并对该方案的复杂性和安全性进行了分析.

1 一般的椭圆曲线数字签名 (ECDSA) 及其改进方案

1.1 ECDSA 方案

Johson 和 Menezes^[5]于 1999 年提出了建立在 ECDLP 上的椭圆曲线数字签名算法 (ECDSA). ECDSA 是数字签名算法 (DSA) 在椭圆曲线密码体制上的平移,其安全性是基于 ECDLP 的困难性的,这使得 ECDSA 在实现和应用上都具有较大的速度优势和安全优势.

假设 E 是定义在有限域 F 上的一条椭圆曲线 (椭圆曲线的相关概念参阅文献[6]), $\#(E)$ 表示 E 中元素的个数,大素数 $n \mid \#(E)$, 并设 $P \in E$ 是 E 的一个阶为 n 的点.椭圆曲线离散对数问题 (ECDLP) 可描述为:给定 E 上一点 Q 以及阶为 n 的点 P , 计算一正整数 $a (0 < a < n)$, 使得 $Q = aP$. 这个问题被认为是非常困难的.将 (F, E, n, P, h) 作为系统公开参数,其中 $h(\cdot)$ 是一个安全的散列 (hash) 函数,那么建立在椭圆曲线 E 上的以点 P 为基点的 ECDSA 方案可描述如下^[5]:

(1) 密钥对的产生:用户 A 随机选取正整数 $k_A (0 < k_A < n)$ 作为私钥,然后计算 k_AP , 记 $P_A = k_AP$, 则用户 A 的公私钥对为 (P_A, k_A) .

(2) 签名的产生:对任何消息 $m (0 < m < n)$, 用户 A 首先选取随机数 $k (0 < k < n)$ (称为消息密钥), 然后计算 $kP = (x, y) (x, y \in F)$, $r = x \bmod n$, $e = h(m)$; 最后利用自己的私钥计算 $s = k^{-1}(e + k_A r) \bmod n$. 则对消息 m 的签名为数组 (r, s) .

(3) 签名的验证:对于系统中的任意验证用户 C , 得到系统参数和签名者 A 的公钥 P_A 以及签名 (m, r, s) 后, 判断 $0 < r, s < n$ 是否成立. 若成立, 则计算下列等式: $e = h(m)$, $c = s^{-1} \bmod n$, $u_1 = ec \bmod n$, $u_2 = rc \bmod n$, $u_1P + u_2P_A = (x, y)$, $r' = x \bmod n$. 当且仅当 $r' = r$ 时, 确信 (r, s) 为 A 对消息 m 的有效签名. 反之, 则签名无效.

利用 ElGamal 签名方程, 可以给出以上签名方案的多种变型^[7]. 但是 ECDSA 方案及其各种变型, 均需要计算 Z_n 中的逆元, 因而计算比较复杂. 本文给出了一种改进的 ECDSA 方案, 避免了求逆过程, 从而提高了效率.

1.2 改进的 ECDSA 方案

这里的系统参数若无特殊说明, 则同 1.1 节. 在整个 ECDSA 方案中, 要多次计算椭圆曲线上点的数乘, 如果域 F 的特征为 2 或 3 则可以用射影坐标代替仿射坐标进行计算^[8,9], 这样在点的数乘过程中可以节约大量时间, 从而提高整个方案的效率.

本文将 Schnorr 签名方案和 ECDSA 相结合, 给出一个改进的 ECDSA 方案, 该方案避免了计算 Z_n 中的逆元. 方案具体描述如下:

(1) 用户 A 的公私钥对为 (P_A, k_A) .

(2) 签名的产生:对任何消息 $m (0 < m < n)$, 用户 A 首先选取随机数 $k (0 < k < n)$, 然后计算 $kP =$

(x, y) (若可以采用射影坐标, 则为 $kP = (x, y, z)$, 其中 $x, y, z \in F$), $r = x \bmod n$, $e = h(m, r)$; 最后用户 A 利用自己的私钥计算 $s = k + ek_1 \bmod n$, 则签名消息为一组数 (m, r, e, s) .

(3) 签名的验证: 对于系统中的任意验证用户 C , 得到系统参数、签名者 A 的公钥 P_A 以及签名 (m, r, e, s) 后, 判断 $0 < r, s < n$ 是否成立. 若成立, 则计算下列等式: $e = h(m, r)$, $sP - eP_A = (x, y)$, $r' = x \bmod n$. 当且仅当 $r' = r$ 时, 确定 (m, r, e, s) 为 A 的有效签名. 反之, 则签名无效.

这个改进后的方案避免了求逆运算, 因此比 ECDSA 方案要简单快速.

1.3 改进方案的安全性分析

有关随机预言模型及引理的知识详见文献 [10].

1.3.1 无消息 (no message) 攻击

引理 1 设 (G, Σ, \mathcal{V}) 是一个带有安全参数 k 的数字签名方案, A 是概率多项式时间图灵机, 仅以公开参数为输入, 它可以向随机预言器询问 Q 次. 假设在时间 T 内, A 以 $\varepsilon \geq 7Q/2^k$ 的概率输出一个有效签名 $(m, \sigma_1, h, \sigma_2)$. 那么存在一个可控制 A 的多项式时间图灵机, 可以在时间 $T' \leq 84480TQ/\varepsilon$ 内, 输出两个有效签名 $(m, \sigma_1, h, \sigma_2)$ 和 $(m, \sigma_1, h', \sigma_2')$, 其中 $h \neq h'$. (证明见 [10].)

定理 1 假设攻击者 A 在时间 T 内, 在无消息攻击 (攻击者只拥有签名人的公钥) 下以 $\varepsilon \geq 7Q/n$ 的概率对本方案实施存在性伪造, 则可以在时间 $84480TQ/\varepsilon$ 内解决椭圆曲线上离散对数问题.

证明 设椭圆曲线的离散对数问题的输入为 (F, E, n, P, h) . 如果签名方案的攻击者能够伪造一个有效的签名 $(m, \sigma_1, h, \sigma_2)$, 那么利用引理 1 控制攻击者困难问题解决者可以输出两个有效签名 (m, r, e, s) 和 (m, r, e', s') , 其中 $e \neq e'$. 根据签名方案, 可以得到 $s - s' = r(e - e')k_1 \bmod n$, 从而可以通过计算 $k_1 = r^{-1}(s_1 - s_2)(e_1 - e_2)^{-1} \bmod n$ 得到 P_A 的椭圆曲线的离散对数 k_1 , 即解决了椭圆曲线上的离散对数问题. 从而本文提出的方案对无消息攻击是安全的.

1.3.2 适应性选择消息攻击

引理 2 设 A 是概率多项式时间图灵机, 仅以公开参数为输入, 它可以向随机预言器询问 Q 次, 还可以询问 R 次签名. 假设在时间 T 内, A 以 $\varepsilon \geq 10(R+1)(R+Q)/2^k$ 的概率输出一个有效签名 $(m, \sigma_1, h, \sigma_2)$. 如果在不知道私钥的情形下, (σ_1, h, σ_2) 能够以不可区分的概率分布被模拟, 那么存在另一可控制 A 的多项式时间图灵机, 可以在时间 $T' \leq 120686TQ/\varepsilon$ 内, 通过模拟, 输出两个有效签名 $(m, \sigma_1, h, \sigma_2)$ 和 $(m, \sigma_1, h', \sigma_2')$, 其中 $h \neq h'$. (证明见 [10].)

定理 2 假设攻击者 A 在时间 T 内, 在适应性选择消息攻击下以 ε 的概率对本方案实施存在性伪造, 设 A 向随机预言器询问 Q 次, 向签名人询问 R 次签名. 假设 $\varepsilon \geq 10(R+1)(R+Q)/n$, 那么可以在时间 $120686TQ/\varepsilon$ 内解决椭圆曲线上离散对数问题.

证明 如果可以证明: 由签名者产生的 (r, e, s) 能够在不知道私钥的情形下被模拟, 而且模拟的分布与签名方案中产生的 (r, e, s) 的分布是不可区分的, 那么直接利用引理 2 就可以得到结论 (证明过程如定理 1).

引理 3 本方案中, 签名可以被模拟者 S 在不知道私钥的情形下, 以不可区分的概率分布进行模拟. 即下列分布是相同的:

$$\delta = \left\{ (r, e, s) \left| \begin{array}{l} k \in Z_n^* \\ e \in Z_n \\ hP = (x, y) \\ r = xm \bmod n \\ s = k + ek_1 \bmod n \end{array} \right. \right\} \quad \text{和} \quad \delta' = \left\{ (r, e, s) \left| \begin{array}{l} k \in Z_n^* \\ e \in Z_n \\ s = k \\ sP - eP_A = (x, y) \\ r = xm \bmod n \end{array} \right. \right\}.$$

证明 首先从签名集合中选择三维组 $(\varepsilon, \beta, \gamma)$, 令 $\varepsilon \in Z_n^*$, $\gamma \in Z_n$ 并且 $\beta \in Z_n$ 且满足等式 $\gamma P - \beta P_A = (x, y)$, $\varepsilon = xm \bmod n$. 接着计算在两种分布中, 该三维组分别出现的概率:

$$\Pr_{\delta}[(r, e, s) = (\varepsilon, \beta, \gamma)] = \Pr_{k \neq 0, e} [hP = (x, y), \varepsilon = xm \bmod n, e = \beta, k + ek_1 = \gamma] = \frac{1}{n(n-1)};$$

$$\Pr_{\delta'}[(r, e, s) = (\varepsilon, \beta, \gamma)] = \Pr_{k \neq 0, e} [e = \beta, s = k = \gamma, \gamma P - \beta P_A = hP = (x, y), \varepsilon = xm \bmod n] = \frac{1}{n(n-1)}.$$

可以看出模拟者 S 与签名者以相同的分布产生三维组 (r, e, s) . 为了对消息 m 进行模拟签名, S 随机选取 $k \in Z_n^*, e \in Z_n$, 令 $s = k$ 计算 $sP - eP_A = (x, y)$, $r = x \bmod n$, 这样 S 就模拟得到签名 (m, r, e, s) .

2 基于椭圆曲线的指定验证人代理签名方案

2.1 代理签名过程

文献 [11] 给出了一种基于椭圆曲线的代理签名方案, 该方案分为 4 个阶段, 本文将这个方案移植到上述改进的 ECDSA 方案中 (这样, 在代理签名的产生与验证阶段避免了模逆运算), 具体描述如下:

2.1.1 系统初始化阶段

假设 E 是定义在有限域 F 上的一条椭圆曲线, $\#(E)$ 表示 E 中元素的个数, 大素数 $n \mid \#(E)$, $P \in E$ 是 E 的一个阶为 n 的点, 将 (F, E, n, P, h) 作为系统公开参数. 并假设: A 为原始签名人, A 的公钥为 P_A , 私钥为 k_A ($0 < k_A < n$), 且有关系式 $P_A = k_A P$; B 为代理签名人, B 的公钥为 P_B , 私钥为 k_B ($0 < k_B < n$), 且有关系式 $P_B = k_B P$.

2.1.2 委托阶段

在这个阶段, 原始签名人 A 将签名的权力委托给代理签名人 B .

(1) A 得到 B 的公钥 P_B 后, 选取随机数 k_0 ($0 < k_0 < n$), 计算 $Q_0 = k_0 P = (x_0, y_0)$, $Q_B = k_0 P_B = (x_B, y_B)$.

(2) 计算 $r_0 = x_0 \bmod n$, $\lambda = (k_A + k_0 r_0) \bmod n$ 和 $\lambda' = \lambda \cdot x_B$.

(3) A 将 (λ', Q_0) 公开地发送给 B . 这里 (λ', Q_0) 即为 A 给 B 的委托信息.

作为代理签名人 B , 收到委托信息 (λ', Q_0) 后, 需要判断 (λ', Q_0) 是否确实来自合法的原始签名人 A , 并用自己的私钥生成代理签名密钥. B 需做以下事情:

(4) 计算 $k_B Q_0 = (x_B, y_B)$, $\lambda = \lambda' \cdot x_B^{-1}$.

(5) 验证等式: $\lambda P = P_A + r_0 Q_0$ 是否成立 (其中 r_0 可通过 Q_0 得到, $Q_0 = (x_0, y_0)$, $r_0 = x_0 \bmod n$). 如果等式成立, 则说明 (λ', Q_0) 确是来自合法的原始签名人 A , 则 B 接受委托信息; 反之, 则 B 拒绝接受.

(6) 生成代理签名密钥 s_B : $s_B = \lambda + k_B \bmod n$, s_B, Q_0 即可作为代理签名密钥对.

2.1.3 代理签名的产生阶段

对任何消息 m ($0 < m < n$), 代理签名人 B 首先选取随机数 k_1 ($0 < k_1 < n$), 然后计算 $k_1 P = (x_1, y_1)$, 接着计算 $r_1 = x_1 \bmod n$, $e = h(m, r_1)$, $s_1 = k_1 + e s_B \bmod n$, 则 B 产生的对消息 m 的代理签名为 (r_1, e, s_1, Q_0, P_B) .

2.1.4 代理签名的验证阶段

对于系统中的任意验证人 C , 得到系统参数、签名者 A 的公钥 P_A 以及代理签名 $(m, r_1, e, s_1, Q_0, P_B)$ 后, 判断 $0 < r_1, s_1 < n$ 是否成立. 若成立则计算下列等式: $e = h(m, r_1)$, $s_1 P - e(P_A + r_0 Q_0 + P_B) = (x', y')$, $r' = x' \bmod n$. 当且仅当 $r' = r_1$ 时, 确定 $(m, r_1, e, s_1, Q_0, P_B)$ 为有效代理签名. 反之, 则签名无效.

验证过程的正确性证明如下:

$$\begin{aligned} s_1 P - e(P_A + r_0 Q_0 + P_B) &= s_1 P - e(k_A P + r_0 k_0 P + k_B P) = s_1 P - e(k_A + r_0 k_0 + k_B) P = \\ &= s_1 P - e s_B P = (s_1 - e s_B) P = k_1 P = (x_1, y_1). \end{aligned}$$

所以, 有 $r' = x' \bmod n = x_1 \bmod n = r_1$.

2.2 指定验证人代理签名过程

系统参数同 2.1 同样, A 为原始签名人, B 为代理签名人, 假设 C 为指定的验证人, C 的公钥为 P_C , 私钥为 k_C ($0 < k_C < n$), 且有关系式 $P_C = k_C P$. 方案过程如下:

(1) 代理签名人 B 得到代理签名密钥对 (s_B, Q_0) 的过程如 2.1 所述.

(2) B 的代理签名过程: 对于消息 m ($0 < m < n$), 代理签名人 B 首先选取随机数 k_1 ($0 < k_1 < n$), 然后计算 $P_1 = k_1 P = (x_1, y_1)$. 接着计算 $r_1 = x_1 \bmod n$, $e = h(m, r_1)$, $s = (k_1 + e s_B) \bmod n$, $P_s = s P_C$, 则 B 对指定的验证人 C 产生的对消息 m 的代理签名为 (Q_0, P_1, P_s, P_B) .

(3) C 的验证过程: 指定验证人 C 得到系统参数、签名者 A 的公钥 P_A 以及签名消息 (m, Q_0, P_1, P_s, P_B)

后, 计算 $e = h(m, r_1)$, 并利用自己的私钥 k_C 验证等式 $P_s = k_C P_1 + e k_C (P_A + r_0 Q_0 + P_B)$ 是否成立. 若成立, 则接受; 否则, 拒绝.

(4) 对于任何消息 $m' (0 < m' < n)$, C 随机选取 E 上一点 $P_1' = (x_1, y_1)$, 计算 $r_1 = x_1 \bmod n$, 都能够产生一个伪造签名 $(m', Q_0, P_1', P_s', P_B)$, 使得 $P_s' = k_C P_1' + e' k_C (P_A + r_0 Q_0 + P_B) = s' P_C$, 其中 $e' = h(m', r_1)$. 而且这样产生的签名与 B 产生的代理签名是不可区分的.

定理 3 对于这个指定验证人的代理签名方案, 若方案中的每一参与者都严格遵循协议, 则其签名验证等式成立.

证明 $e = h(m, r)$,

$$\begin{aligned} P_s &= P_C = (k_1 + e s_B) P_C = k_1 P_C + e (k_A + r_0 k_0 + k_B) P_C \\ &= k_1 k_C P + e (k_A + r_0 k_0 + k_B) k_C P = k_C P_1 + e k_C (P_A + r_0 Q_0 + P_B). \end{aligned}$$

3 本方案的复杂性与安全性分析

3.1 方案的复杂性

方案的复杂性主要依据时间复杂度. 为了方便, 定义以下符号用于计算复杂性分析: E , 有限域上的指数运算; M_p , 点的数乘; A_p , 点的加法; I , 模逆运算; M : 模乘运算; H , hash函数运算. 具体分析比较如表 1所示.

表 1 方案复杂性分析比较表
Table 1 Complexity analysis of the schemes

	代理密钥产生过程	指定验证人的代理签名过程	验证过程	总计
文献 [4] 的方案	$6E + 5M + 4I$	$2E + M + H$	$4E + 3M + 2I$	$12E + 9M + 7H$
本文的方案	$3M_p + A_p + I + M$	$2M_p + M + H$	$3M_p + 3A_p + M + H$	$8M_p + 4A_p + I + 3M + 2H$

本方案需要多次运用椭圆曲线上点的数乘以及加法运算, 看上去比较复杂, 但是与文献 [3] 中方案 (或者其它非基于椭圆曲线的方案) 相比, 本文的方案不需要进行有限域上的指数运算 (而且, 这个指数往往都很大), 相对而言, 本文的方案比 [3] 中方案要快很多, 时间开销要小很多. 并且在点的数乘与加法运算过程中, 可以采用一些现成的快速运算方法^[8-9], 从而进一步提高整个方案的效率.

3.2 方案的安全性

该方案是基于 ECDLP 的困难性, 在整个方案中, 总假设 ECDLP 是难解的. 为了叙述简便, 用 ECDVPS 表示本文所给出的基于椭圆曲线的指定验证人代理签名方案.

定理 4 ECDVPS 具有可验证性.

证明 可验证性是指任意验证人可以根据一个有效的代理签名确认原始签名人的授权信息. 本方案中授权信息含有代理签名人 B 的身份信息 P_B , 原始签名人和验证人都可以用 P_B 来验证, 在验证的同时, 证实了代理签名人的身份.

定理 5 ECDVPS 具有可鉴别性.

证明 由代理签名的验证等式可知, 验证人必须得到原始签名人和代理签名人的公钥, 故通过验证等式可以直接找到原始签名人和代理签名人.

定理 6 ECDVPS 具有代理签名的强不可伪造性.

证明 不管是任意第四方, 还是原始签名人本身, 要想进行伪造攻击, 必须伪造出适当的 $k + s_B$, 使得 $s = (k + e s_B) \bmod n$. 当且仅当以下两种情形有一种成立时, 才能伪造成功: ① 该攻击者能够解决 ECDLP 问题, 这是不可能的; ② 或者通过随机选取来得到, 这样得到正确的 $s = (k + e s_B) \bmod n$ 的可能性小于 $1/2^{n-1}$, 这是个可忽略概率.

同样对于指定验证人而言, 在 ECDLP 困难性前提下, 伪造出代理签名密钥概率是可忽略概率 $1/2^n$.

由定理 4 定理 5 以及定理 6 可得:

推论 1 ECDVPS 具有强不可否认性.

推论 2 ECDVPS 具有可区分性.

推论 3 ECDVPS 满足防止代理滥用性.

定理 7 ECDVPS 具有可注销性.

对于可注销性, 原始签名人只需要在整个系统中广播代理签名人的公钥不再继续有效即可.

定理 8 ECDVPS 具有指定的可验证性.

证明 只有代理签名人指定的验证人才能够验证代理签名有效性. 因为从 ECDVPS 可以看出, 验证等式 $P_s = k_C P_1 + e_{k_C} (P_A + r_0 Q_0 + P_B)$ 包含了指定验证人的私钥信息 k_C , 所以, 只有拥有该私钥信息的人才能够验证签名的有效性.

定理 9 ECDVPS 具有指定的不可否认性.

证明 代理签名人一旦确定了指定验证人, 这种指定就不可否认. 因为在 ECDVPS 中, 指定代理人 B 根据原始签名人 A 的委托信息 (λ', Q_0) 产生了代理签名信息 (m, r_b, s_b, Q_0, P_B) , 其中包含了代理签名人的私钥 k_B 以及指定验证人的公钥信息 P_C , 因此, 签名一旦产生, B 所产生的指定验证人签名就具有不可否认性.

4 结论

椭圆曲线的数字签名算法是密码学中一个较新的思想, 在实际中有着很多重要的应用. 本文给出了一种更加快速的改进的椭圆曲线数字签名算法, 并且将指定验证人代理签名的思想应用于该算法, 提出了基于椭圆曲线的指定验证人代理签名方案, 同时对该方案的计算复杂性和安全性进行了分析, 分析结果表明该方案是安全的、更快速的.

[参考文献] (References)

- [1] Diffie W, Hellman M. New directions in cryptography[J]. IEEE Transaction on Information Theory, 1976, 22(6): 644-654
- [2] Mambo M, Usuda K, Okamoto E. Proxy signatures for delegating signing operation[C] // Proceedings of the 3rd ACM Conference on Computer and Communications Security. New York: ACM Press, 1996: 48-57.
- [3] Guilin Wang. Designated-verifier proxy signatures for E-commerce[C] // 2004 IEEE CME. Taipei [s.n.], 2004: 1731-1734
- [4] Jakobsson M, Sako K, Impagliazzo R. Designated verifier proofs and their applications[C] // Advances in Cryptology-Eurocrypt'96. LNCS 1070. Berlin: Springer-Verlag, 1996: 143-154.
- [5] Johnson D, Menezes A. The elliptic curve digital signature algorithm [R]. Canada: Dept of Combinatorics and Optimization, University of Waterloo, 1999.
- [6] Blake I F, Seroussi G, Smart N P. Elliptic Curves in Cryptography[M]. Cambridge: Cambridge University Press, 1999: 29-55.
- [7] Menezes Alfred J, Paul C Van Oorschot, Scott A Vanstone. Handbook of Applied Cryptography[M]. New York: CRC Press, 1997: 425-488.
- [8] Julio Lopez Ricardo Dahab. Improved algorithms for elliptic curve arithmetic in $GF(2^n)$ [C] // Selected Areas in Cryptography'98, SAC'98. LNCS1556. Canada: Ontario [s.n.], 1999: 201-212.
- [9] 沈丽敏, 陈恭亮, 游永兴. 特征为 3 的域上的椭圆曲线点的快速计算 [J]. 数学杂志, 2004, 24(5): 557-560.
Shen L i m i n, Chen Gongliang, You Yongxing. Fast elliptic curve arithmetic over fields of characteristic three [J]. Journal of Mathematics, 2004, 24(5): 557-560. (in Chinese)
- [10] Pointcheval Stem. Security arguments for digital signatures and blind signatures[J]. Journal of Cryptology, 2000, 13(3): 361-396.
- [11] 张宁, 傅晓彤, 肖国镇. 对基于椭圆曲线的代理签名的研究与改进 [J]. 西安电子科技大学学报: 自然科学版, 2005, 32(2): 280-283.
Zhang Ning, Fu Xiaotong, Xiao Guozhen. Study and improvement of proxy signature based on elliptic curve [J]. Journal of Xidian University: Natural Science Edition, 2005, 32(2): 280-283. (in Chinese)

[责任编辑: 严海琳]