可转换的指定证实人签名方案

王晓明[1,2], 符方伟[1]
(1. 南开大学数学科学学院, 天津 300071; 2. 青岛大学电气及自动化工程学院, 山东青岛 266071)

摘 要: 提出了一个新的基于椭圆曲线的可转换的指定证实人签名方案. 该方案不仅能抵抗一切伪造攻击, 而且具有可转换和可收回的特性. 可转换特性就是在需要的时候可以将指定证实人签名变为普通数字签名, 任何人都可以验证它的有效性. 可收回特性是指签名者根据需要可以收回委托给指定证实人的签名验证权. 新方案是基于椭圆曲线构造的, 所以具有安全性高, 速度快, 密钥最小, 简单等优点.

关键词: 指定证实人签名; 伪造攻击; 椭圆曲线
中图分类号: TN918.1 文献标识码: A 文章编号: 0372-2112 (2002) 11-1690-04

Convertible Designated Confirmer Signature Scheme

WANG Xiao-ming[1,2], FU Fang-wei[1]
(1. *School of Mathematics Science, Nankai University, Tianjin 300071, China;*
2. *College of Electric & Automatic Engineering, Qingdao University, Qingdao, Shandong 266071, China*)

Abstract: A new convertible designated confirmer signature based on elliptic curve is presented. The new scheme not only can resist all forgery attacks, but also has the properties of convertibility and retraction. The convertibility is that the designated confirmer signature can be converted into general signature if needed. The retraction is that the original signer can retract the right of the designated confirmer's signature verification if needed. The new scheme is constructed based on elliptic curve, therefore the scheme is possessed of the merits of higher security, higher efficiency, smaller key, and very simplicity etc.

Key words: designated confirmer signature; forgery attacks; elliptic curve

1 引言

指定证实人签名是普通数字签名和不可否认数字签名的折中, 签名者采用不可否认数字签名, 验证必须在签名者或指定证实人配合下才能进行, 从而防止了所签发的消息被复制或散布的可能性. 同时, 指定证实人签名也具有防止签名失效和签名者完全控制签名的实施等特性.

目前, 已有一些指定证实人签名方案被提出[1,2,4,6], 但这些方案都不具有可转换和可收回特性. 本文首先对 Okamoto[1] 的指定证实人签名方案进行分析, 指出了该方案存在着不安全因素, 即指定证实人能伪造签名者的签名. 然后提出了一个基于椭圆曲线的可转换的指定证实人签名方案. 该方案不仅能克服文献[1]的不安全因素, 而且能抵抗一切伪造攻击, 并具有可转换和可收回的特性. 可转换特性就是在需要的时候可以将指定证实人签名变为普通数字签名, 任何人都可以验证它的有效性. 可收回特性是指签名者在需要的时候可以收回委托给指定证实人的签名验证权. 一般的指定证实人签名方案, 一旦签名者将签名验证权委托给指定证实人, 指定证实人就具有对这个签名的永久验证权, 但有时签名者希望指定证实人在某一段时间内具有验证权, 当这段有效期过后, 就收回签名验证权, 这一点在现实生活中是有用的. 新方案是基于椭圆曲线构造的, 所以具有安全性高, 速度快, 密钥量小, 简单等优点.

2 基于 Schnorr 签名的指定证实人签名方案的分析

2.1 基于 Schnorr 签名的指定证实人签名方案

(1)安全参数, 包括以下几个方面:

①选取安全的 Hash 函数 h, h 公开; ②选取两个大素数 p、q, q 是 $p-1$ 的素因子, p、q 公开; ③选取 $g \neq 1$, 满足 $g^q = 1 \bmod p$、g 公开; ④指定证实人选取 u 作为私钥, 计算 $b = g^u \bmod p$ 作为公钥. 签名者选 s 作为私钥, 计算 $a = g^{-s} \bmod p$ 作为公钥.

(2)签名者签名. 设待签的消息为 m, 签名者为 S, 签名接收者为 V, 指定证实人为 C.

S 选取随机数 $r, w \in Z_q$, 计算

$$x = g^w \bmod p \tag{1}$$

$$e = (b^r \bmod p) \oplus h(m \| x) \tag{2}$$

收稿日期: 2001-05-25; 修回日期: 2001-12-12
基金项目: 国家自然科学基金(No. 60172060); 教育部跨世纪优秀人才计划基金; 教育部资助高等学校骨干教师计划基金

$$y = w + es \bmod q \tag{3}$$

$$d = g^r \bmod p \tag{4}$$

送(m, d, e, y)给 V. 符号 $\|$ 表示两个数的级连.

(3) 指定证实人与签名接收者对签名的认证, 包括以下几个方面:

①V 送 d 给 C.

②V 计算

$$z = e \oplus h(m \| g^y a^e) \tag{5}$$

③C 选取随机数 $t \in Z_q$, 计算

$$l_1 = g^t \bmod p \tag{6}$$

$$l_2 = d^t \bmod p \tag{7}$$

$$k = t + h(l_1 \| l_2)\, u \bmod q \tag{8}$$

送(l_1, l_2, k)给 V.

④V 验证

$$g^k \stackrel{?}{=} l_1 b^{h(l_1 \| l_2)} \bmod p \tag{9}$$

$$d^k \stackrel{?}{=} l_2 z^{h(l_1 \| l_2)} \bmod p \tag{10}$$

如等式成立, V 确信签名有效, 接收消息 m 及签名.

说明: 式(9), (10a) 成立 $\Leftrightarrow z = b^r \bmod p,\ d = g^r \bmod p \Leftrightarrow$ 签名是 S 的签名.

因为, 如(m, d, e, y)是 S 的签名, 则由式(1) ~ (3)、(5), 得

$$\begin{aligned} z &= e \oplus h(m \| g^y a^e) \\ &= (b^r \bmod p) \oplus h(m \| x) \oplus h(m \| g^y a^e) \\ &= (b^r \bmod p) \oplus h(m \| g^w) \oplus h(m \| g^y a^e) \\ &= (b^r \bmod p) \oplus h(m \| g^y g^{-es}) \oplus h(m \| g^y a^e) \\ &= (b^r \bmod p) \oplus h(m \| g^y a^e) \oplus h(m \| g^y a^e) \\ &= b^r \bmod p \end{aligned} \tag{10a}$$

由式(6)、(8)得 $g^k = g^t g^{uh(l_1 \| l_2)} = l_1 b^{h(l_1 \| l_2)} \bmod p$, 由式(4)、(7)、(8)、(10a) 得 $d^k = d^t d^{uh(l_1 \| l_2)} = l_2 (g^r)^{uh(l_1 \| l_2)} = l_2 b^{rh(l_1 \| l_2)} = l_2 z^{h(l_1 \| l_2)} \bmod p$, 所以, 式(9), (10) 成立 $\Leftrightarrow z = b^r \bmod p,\ d = g^r \bmod p \Leftrightarrow$ 签名是 S 的签名.

2.2 安全性分析

该方案存在不安全因素, 即指定证实人能伪造签名者 S 的签名, 并使 V 相信该签名为 S 的签名.

(1) C 截取 S 的签名(m, d, e, y), 将 m 换为 m', 选取随机数 w', 且 $w' \in Z_q$, 计算.

$$x' = g^{w'} \bmod p \tag{11}$$

$$b^r \bmod p = d^u \bmod p \tag{12}$$

$$e' = (b^r \bmod p) \oplus h(m' \| x') \tag{13}$$

$$y' = w' - e' u \bmod q \tag{14}$$

$$d' = ((b^r \bmod p) \oplus h(m' \| g^{y'} b^{e'}) \oplus h(m' \| g^{y'} a^{e'}))^{u^{-1}} \tag{15}$$

送(m', d', e', y')给 V.

(2) 指定证实人与签名接收者对签名进行认证

①V 送 d' 给 C.

②V 计算

$$z = e' \oplus h(m' \| g^{y'} a^{e'}) \tag{16}$$

③C 选取随机数 $t \in Z_q$, 计算

$$l_1 = g^t \bmod p \tag{17}$$

$$l_2 = d'^t \bmod p \tag{18}$$

$$k = t + h(l_1 \| l_2)\, u \bmod q \tag{19}$$

送(l_1, l_2, k)给 V.

④V 验证

$$g^k \stackrel{?}{=} l_1 b^{h(l_1 \| l_2)} \bmod p \tag{20}$$

$$d'^k \stackrel{?}{=} l_2 z^{h(l_1 \| l_2)} \bmod p \tag{21}$$

如等式(20)、(21)成立, V 确信签名有效, 接收消息 m' 及签名. 而其原因为: 由式(11)、(13) ~ (16), 得

$$\begin{aligned} z &= e' \oplus h(m' \| g^{y'} a^{e'}) \\ &= (b^r \bmod p) \oplus h(m' \| x') \oplus h(m' \| g^{y'} a^{e'}) \\ &= (b^r \bmod p) \oplus h(m' \| g^w) \oplus h(m' \| g^{y'} a^{e'}) \\ &= (b^r \bmod p) \oplus h(m' \| g^{y'} g^{-e'u}) \oplus h(m' \| g^{y'} a^{e'}) \\ &= (b^r \bmod p) \oplus h(m' \| g^{y'} b^{e'}) \oplus h(m' \| g^{y'} a^{e'}) \end{aligned} \tag{21a}$$

由式(17)、(19)得 $g^k = g^t g^{uh(l_1 \| l_2)} = l_1 b^{h(l_1 \| l_2)} \bmod p$, 由式(15)、(18)、(19)、(21a)得

$$\begin{aligned} d'^k &= d'^t d'^{uh(l_1 \| l_2)} = l_2 (((b^r \bmod p) \oplus h(m' \| g^{y'} b^{e'}) \\ &\quad \oplus h(m' \| g^{y'} a^{e'}))^{u^{-1}})^{uh(l_1 \| l_2)} \\ &= l_2 ((b^r \bmod p) \oplus h(m' \| g^{y'} b^{e'}) \oplus h(m' \| g^{y'} a^{e'}))^{h(l_1 \| l_2)} \\ &= l_2 z^{h(l_1 \| l_2)} \bmod p \end{aligned}$$

所以, 伪造的签名(m', e', d', y')是可以通过 C 与 V 对签名的认证的, 因此, 文献[1]存在不安全的因素.

3 可转换的指定证实人签名方案

3.1 安全参数

(1)选取安全的 Hash 函数 h, h 公开.

(2)选取有限域 F_q 上一条安全的椭圆曲线 $E(F_q)$, 保证椭圆曲线群上的离散对数问题是难解的.

(3)在椭圆曲线 $E(F_q)$ 上选一点 P, P 的阶为 n(n 为一个大素数), P 公开.

(4) 签名者选 $k_{as} \in \{1, 2, \cdots, n-1\}$ 作为私钥, 计算 $k_{ap} = k_{as} P \in E(F_q)$ 作为公钥; 指定证实人选 $k_{cs} \in \{1, 2, \cdots, n-1\}$ 作为私钥, 计算 $k_{cp} = k_{cs} P \in E(F_q)$ 作为公钥. 其中, $k_{as} k_{as}^{-1} = 1 \bmod n$, $k_{cs} k_{cs}^{-1} = 1 \bmod n$.

3.2 签名者签名

设待签名的消息为 m, 签名者为 S, 签名接收者为 V, 指定证实人为 C.

(1) S 选取随机数 γ, 且 $\gamma \in \{1, 2, \cdots, n-1\}$. 计算

$$a = \gamma k_{cp} \tag{22}$$

$$(x, y) = k_{as} k_{cp} \tag{23}$$

$$b = x k_{as} + \gamma h(m) \tag{24}$$

送(b, m)给 V, (m, a)给 C, 并在 S 的公共文件夹中公布 a.

3.3 签名者与签名接收者对签名的认证

(1) V 选取随机数 r, 且 $r \in \{1, 2, \cdots, n-1\}$, 计算

$$d_1 = rh(m) P \tag{25}$$

$$d_2 = rP \tag{26}$$

送(d_1, d_2)给S.

(2) S 选取随机数q, 且$q \in \{1, 2, \cdots, n-1\}$, 计算

$$e_1 = qP \tag{27}$$

$$e_2 = k_{as}(xd_2 + e_1) + \gamma d_1 \tag{28}$$

送(e_1, e_2)给 V.

(3) V 送r 给S.

(4) S 验证 $d_1 \stackrel{?}{=} rh(m)P$

$d_2 \stackrel{?}{=} rP$

如等式成立, 送 q 给 V.

(5) V 验证 $e_1 \stackrel{?}{=} qP$

$e_2 \stackrel{?}{=} rbP + qk_{ap}$ (29)

如等式成立, V 确信签名为S 的签名, 接收消息及签名.

3.4 指定证实人与签名接收者对签名的认证

(1) V 从S 的公共文件夹中取出 a.

(2) V 选取随机数t, 且$t \in \{1, 2, \cdots, n-1\}$, 计算

$$u_1 = th(m)a \tag{30}$$

$$u_2 = tk_{ap} \tag{31}$$

送(u_1, u_2)给 C.

(3) C 选取随机数β, 且$\beta \in \{1, 2, \cdots, n-1\}$, 计算

$$z = \beta P \tag{32}$$

$$(x, y) = k_{cs}k_{ap} \tag{33}$$

$$s = xu_2 + k_{cs}^{-1}u_1 + k_{cs}z \tag{34}$$

送(z, s)给 V.

(4) V 送t 经C.

(5) C 验证 $u_1 \stackrel{?}{=} th(m)a$

$u_2 \stackrel{?}{=} tk_{ap}$

如等式成立, 送 β 给 V.

(6) V 验证 $z \stackrel{?}{=} \beta P$

$s \stackrel{?}{=} tbP + \beta k_{cp}$ (35)

如等式成立, V 确信签名是S 的签名, 接收消息及签名.

3.5 方案性能分析

(1) 证明式(29)的正确性. 由式(24)~(28)得

$$e_2 = k_{as}(xd_2 + e_1) + \gamma d_1 = k_{as}xrP + k_{as}qP + \gamma rh(m)P$$
$$= r(xk_{as}P + h(m)\gamma P) + qk_{ap} = rbP + qk_{ap}$$

证明式(35)的正确性. 由式(22)~(24)、式(30)~(34)得

$$(x, y) = k_{cs}k_{ap} = k_{as}k_{ap}$$
$$s = xu_2 + k_{cs}^{-1}u_1 + k_{cs}z = xtk_{ap} + k_{cs}^{-1}th(m)\gamma k_{cp} + k_{cs}\beta P$$
$$= t(xk_{as}P + h(m)\gamma P) + \beta k_{ap} = tbP + \beta k_{cp}$$

(2) 签名者公开秘密参数$(x, \gamma P)$, 指定证实人签名就变成了普通数字签名. 由式(24)得普通数字签名的验证方程为

$$bP = xk_{ap} + h(m)\gamma P$$

因为知道了$(x, \gamma P)$, 任何人都可以用上式验证该数字签名的有效性, 从而实现了指定证实人签名向普通数字签名的转换.

(3) 如签名者想收回验证权, 只需删除他的公共文件中的 a, 签名接收者没有 a, 无法构造验证过程中的 u_1, 从而也就无法与指定证实人进行签名的验证. 但签名接收者仍然可以与签名者进行对签名的验证, 因为该验证过程中没有用到 a, 因此签名者实现了对验证权的收回.

(4) 从签名方程 $y = xk_{as} + \gamma h(m)$ 知, 签名接收者不知道 x, γP, 无法验证签名的有效性, 只有在签名者或指定证实人的配合下, 才能验证签名的合法性, 满足指定证实人签名的思想.

(5) 指定证实人试图伪造签名者的签名, C 截取S 的签名 (a, b, m), 将 m 替换为m', 选取随机数 γ', 计算

$$a' = \gamma' k_{ap}$$
$$(x, y) = k_{cs}k_{ap}$$
$$b' = xk_{cs} + \gamma' h(m')$$

送(b', m')给 V, 并更改 S 公共文件夹中的 a 为 a'.

当签名接收者和指定证实人对签名验证时, 伪造的签名无法通过第 3.4 节中第(6)步的验证, 因为 $b' = xk_{cs} + \gamma' h(m')$, $b'P = xk_{ap} + h(m')\gamma' P$, 所以 $s = xu_2 + k_{cs}^{-1}u_1 + k_{cs}z = xtk_{ap} + k_{cs}^{-1}th(m')\gamma' k_{cp} + k_{cs}\beta P = t(xk_{ap} + h(m')\gamma' P) + \beta k_{cp} \neq tb'P + \beta k_{ap}$, 指定证实人无法将 k_{ap} 替换为 k_{ap}, 因为他不知道用户随机选的 t. 而正确猜测 t 的概率为 $1/(n-1)$. 所以, 指定证实人无法伪造签名者的签名.

(6) 攻击者截取(b, m), 试图进行中间攻击. 同样会遇到同(5)一样的情况, 因此, 无法实现攻击.

(7) 攻击者无法进行消息替换攻击, 因为签名者是对消息的 Hash 函数值签名的, 安全的 Hash 函数具有单向, 无碰撞的特性, 所以找不到两个数 w_1, w_2 使 $h(w_1) = h(w_2)$.

(8) 攻击者试图假冒指定证实人, 对签名进行验证, 但攻击者不知道指定证实人的私钥及秘密参数 x, 所以, 无法实现攻击.

(9) 攻击者截取(b, m), 送出假消息及假签名, 并假冒签名者与 V 对签名进行验证, 同样, 因不知道 t, 无法替换 k_{ap} 为自己的公钥. 因此, 无法通过式(29)的验证.

(10) 攻击者试图从签名者或指定证实人的公钥求出他们的私钥, 这是求解椭圆曲线上的离散对数的问题.

(11) 本方案是基于椭圆曲线的指定证实人签名方案, 因此, 具有安全性高、速度快、密钥量小等优点.

4 结束语

本文分析了文献[1]中指定证实人签名方案的安全性, 指出存在着不安全因素. 提出了基于椭圆曲线的可转换的指定证实人签名方案, 并对该方案的特性进行了分析, 得出该方案是一个安全性高, 速度快, 有实用价值的可行方案.

参考文献:

[1] T Okamoto. Designated confirmer signatures and public key encryption are equivalent [A]. Advances in cryptology-crypto' 94 [C]. New York: Springer-Verlag, 1994. 61-74.

[2] D Chaum. Designated confirmer signatures [A]. Advances in cryptolo-

gy-eurocrypto' 90 Proc. [C]. Berlin: Springer-Verlag, 1995. 86- 91.
[3] D Chaum, H van Antwerpen. Undeniable signatures [A]. Advances in cryptology-crypto' 89 [C]. Berlin: Springer-Verlag, 1990. 212- 216.
[4] K Nguyer, Y Mu, V Varadharajan. Undeniable confirmer signature [A]. Proc. Inform. Security Workshop' 99 [C]. Tokyo: Springer-Verlag, 1999. 62- 73.
[5] D Chaum. Zero-knowledge undeniable signatures [A]. Advances in cryptology-eurocrypto' 90 [C]. Berlin: Spinger-Verlag, 1990. 458- 464.
[6] M Jakobsson, K Sako, R Impagliazzo. Designated verfier proofs and their applications [A]. Advances in Cryptology-Eurocrypto' 98 Proc. [C]. Finland: Springer-Verlag, 1998. 210- 226.
[7] Y Desmedt, M Yung. Weaknesses with undeniable signatures schemes [A]. Advances in cryptology-eurocrypto' 91 Proc. [C]. England: Springer-Verlag, 1991. 205- 220.
[8] J Boyar, D Chaum, I Damgård. Convertible undeniable signatures [A]. Advances in cryptology-crypto' 90 Proc. [C]. Berlin: Springer-Verlag, 1991. 189- 205.

作者简介:

王晓明　女, 1960 年 10 月出生于重庆, 副教授, 现为南开大学博士生, 在国内外各种刊物发表论文多篇, 研究领域为现代密码学, 计算机网络安全.

符方伟　男, 1963 年 10 月出生于湘潭市, 南开大学教授, 博士生导师, 在国内外重要学术刊物发表论文多篇, 长期从事信息论, 计算机网络安全, 现代密码学, 编码理论的科研和教学.