

基于 ECC 的可转换签密及其门限共享验证方案*

彭长根¹, 李 祥², 罗文俊³

(1,2,3 贵州大学计算机软件与理论研究所, 贵阳 550025; 1 贵州大学数学系, 贵阳 550025)

摘 要: 本文首先基于椭圆曲线密码体制, 提出了一个具有可转换功能的签密方案。该方案能抵抗已知明文攻击, 并克服了 H-C 方案和 W-B 方案不满足语义安全的不足。由于方案是基于椭圆曲线密码体制建立的, 因而它的计算代价和通信代价均很小。基于该签密方案, 构建出了一个 (t, n) 门限共享验证签密方案, 其优点在于能防止可信中心的欺诈, 并在共享验证和消息恢复阶段, 提出了一种能防止验证成员提供假秘密份额进行欺诈的方法。

关键词: 认证加密; 签密; 可转换性; 共享验证; 椭圆曲线密码体制

1. 引言

Zheng^[1]在 1997 年提出了一个新的认证加密方案, 称为签密 (Signcryption)。它是指在一个单一的逻辑步骤中, 同时实现数字签名和公钥加密两项功能, 且它的计算代价远比传统的“先签名后加密”的方法低得多^[2]。认证加密法是一种能提供消息恢复的数字签名方案^[3]。传统的方案存在这样的问题: 由于只有指定接收者才能验证签名和恢复消息, 如果出现发送者抵赖, 那么纠纷就无法通过第三方进行仲裁。公开验证方法和可转换方法就是针对这类问题而提出的。这些方法能够实现当发送者抵赖时, 指定接收者就可以将签密转换成普通的签名, 然后由第三方进行公开验证以证明发送者抵赖。1998 年 Petersen 和 Michels^[4]指出, Zheng 的方案存在这样的问题: 要实现不可抵赖性, 必然会失去保密性。之后, 不少文献提出了新的或改进的认证加密方案^[5-10], 以实现公开验证功能。最初的可公开验证方案^[5]需要发送者合作才能将签密转换成普通签名。Wu 等^[6]在 2002 年提出了一个不需要发送方合作的可转换方案。后来 Huang 和 Chang^[7]指出 Wu 的方法存在一个安全弱点: 一旦攻击者得到恢

复的消息, 他就可以将签密转换成普通签名, 从而可以宣称自己是合法的接收者。为此 Huang 和 Chang 提出了一个改进方案 (简称 H-C 方案), 克服了 Wu 方案的不足。但文献[8]和文献[11]都指出了 H-C 方案不能抵抗已知明文攻击, 而且文献[8]和文献[12]还指出 H-C 方案不具备消息的语义安全性, 同时文献[12]还基于离散对数 (DLP) 困难性提出了一个具有语义安全性的认证加密方案。2003 年 Ma 和 Chen^[9]提出了一个有效的具有公开验证功能的认证加密方案, 但紧接着 Wang 和 Bao 等^[10]就指出该方案存在接收方伪造攻击的漏洞和数学推算中的一个错误, 并提出了一个可公开验证的方案 (简称 W-B 方案)。本文的研究将指出 W-B 方案也存在不满足语义安全的弱点。

本文基于椭圆曲线密码体制 (ECC), 建立了一个可转换的签密方案。该方案除了具有可转换 (公开验证) 功能外, 还能抵抗已知明文攻击, 并克服了 H-C 方案和 W-B 方案不满足语义安全的弱点。该方案与目前的一些方案相比, 具有更小的计算代价和通信代价。在此基础上, 我们基于所提出的签密方案, 建立了一个能实现 (t, n) 门限共享验证的签密方案。该门限方案能防止可信中心的欺

* 本文得到贵州省自然科学基金项目(No.[2005]2107, No.[2005]2110)的资助。

¹ 彭长根, 男, 副教授, 博士研究生; 研究方向: 计算机密码与信息安全。

² 李 祥, 男, 教授, 博士生导师; 研究方向: 计算复杂性, 可计算性理论, 计算机密码与信息安全。

³ 罗文俊, 男, 博士, 教授; 研究方向: 计算机密码与信息安全。

诈，并在共享验证和消息恢复阶段，提出了一种能检测验证成员提供假秘密份额进行欺诈的方法。

2. 基于 ECC 具有公开验证功能的签密方案

本节将基于椭圆曲线离散对数困难问题 (ECDLP) 建立一个具有公开验证功能的签密方案。方案分为四个阶段：系统初始化阶段、签密阶段、消息恢复及验证阶段和公开验证阶段。

2.1 系统初始化阶段

可信中心 CA 在有限域 F_p 上选择一条安全的椭圆曲线 $E(F_p)$ 和一个阶为 q 的基点 P , q 是一个大于 160bit 的大素数；签名者 Alice 和接收者 Bob 分别选择 $x_a \in Z_q^*$, $x_b \in Z_q^*$ 作为私钥，并计算相应的公钥 $Q_a = x_a \cdot P$, $Q_b = x_b \cdot P$ 发送给 CA； $H(\cdot)$ 是 CA 选择的一个单向无碰撞 hash 函数；最后可信中心 CA 公开 $E(F_p)$ 、 P 、 q 、 Q_a 、 Q_b 和 $H(\cdot)$ 。

2.2 签密阶段

Alice 对消息 $m \in Z_p^*$ 进行签密的操作如下：

Step 1: 随机选取整数 $k \in Z_q^*$ ，计算 $k \cdot P = (x_1, y_1)$, $k \cdot Q_b = (x_2, y_2)$ ，如果 $x_1 = 0$ 或 $x_2 = 0$ ，重新选择 k ；

Step 2: 计算 $c = m \cdot x_2 \bmod p$, $r = H(H(m), Q_b, x_1, x_2)$, $s = k - x_a \cdot r \bmod q$ ；

Step 3: 将签密 (c, r, s) 发送给 Bob。

2.3 消息恢复及验证阶段

Bob 收到签密 (c, r, s) 后，通过如下操作实现签密验证和消息的恢复：

Step 1: 计算

$$Y_1 = r \cdot Q_a + s \cdot P = (x'_1, y'_1), Y_2 = x_b \cdot Y_1 = (x'_2, y'_2);$$

Step 2: 恢复消息 $m = c \cdot (x'_2)^{-1} \bmod p$ ；

Step 3: 验证 $r = H(H(m), Q_b, x'_1, x'_2)$ 是否成立。

如果等式成立，则确信签密是 Alice 发送的。

2.4 公开验证阶段

如果后来 Alice 否认她对消息 m 的签密，则可通过以下操作进行公开验证：

Step 1: Bob 首先将签密 (c, r, s) 转换成普通签名 (m, r, s) ，然后将 (m, r, s) 和 x'_2 交给第三方验证；

Step 2: 第三方先求出 $r \cdot Q_a + s \cdot P = (x'_1, y'_1)$ 然后验证等式 $r = H(H(m), Q_b, x'_1, x'_2)$ 是否成立。如果

等式成立，则确信签密是 Alice 发送的。

2.5 方案的完备性证明

定理 1 若签密者 Alice 能严格遵循签密步骤，则接收者 Bob 就能正确恢复消息 m 和进行有效性验证，第三方也能够正确对签密进行公开验证。

证明：若 Alice 能严格遵循签密步骤，则有

$$\begin{aligned} (x'_1, y'_1) &= Y_1 = r \cdot Q_a + s \cdot P \\ &= r \cdot (x_a \cdot P) + (k - x_a \cdot r) \cdot P \\ &= k \cdot P = (x_1, y_1) \end{aligned}$$

$$\begin{aligned} (x'_2, y'_2) &= Y_2 = x_b \cdot Y_1 = x_b \cdot (k \cdot P) \\ &= k \cdot Q_b = (x_2, y_2) \end{aligned}$$

则 Bob 能用 $m = c \cdot (x'_2)^{-1} \bmod p$ 正确恢复消息 m ，并能通过等式 $r = H(H(m), Q_b, x'_1, x'_2)$ 正确地进行有效性验证，第三方也能通过该等式正确地进行公开验证，证毕。

2.6 安全性分析及其与相关方案比较

(1) 能抵抗已知明文攻击

H-C 方案存在一个缺陷^[8,11]：若攻击者获得了明文 m_1 的有效签密 (c_1, r_1, s_1) ，他就可以计算出发送者和接收者的会话钥，之后就能从另外截获的签密 (c_2, r_2, s_2) 中恢复出消息 m_2 ，也就是说 H-C 方案不能抵抗已知明文攻击。我们的方案利用非同态的椭圆曲线密码体制克服了该缺陷。攻击者可以从等式 $c_1 = m_1 \cdot x_2 \bmod p$ 中求出 $x_2 = m_1 \cdot c_1^{-1} \bmod p$ ，但不可能利用等式 $(x_2, y_2) = x_b \cdot Y_1 = r_1 \cdot x_b \cdot Q_a + s_1 \cdot Q_b$ 求出会话钥 $x_b \cdot Q_a$ ，因为 y_2 是未知的，同时也需面对 ECDLP，这样他就不可能从另外截获的签密 (c_2, r_2, s_2) 中求出 $Y_2 = r_2 \cdot x_b \cdot Q_a + s_2 \cdot Q_b$ ，从而恢复消息 m_2 。

(2) 具有语义安全性

文献[8,12]指出了 H-C 方案在不具有语义安全性的弱点：如果攻击者截获了一组签密 (c, r, s) ，他就可以利用验证等式猜测所发送的消息。我们研究发现 W-B 方案也存在不具有语义安全性的弱点：攻击者能够从验证等式 $r = H(m, g^s \cdot y_a^{-r})$ 中猜测消息 m (其中 g 为生成元， y_a 为发送者公钥)^[11]。我们

的方案已克服了 H-C 方案和 W-B 方案不具有语义安全性的不足, 因为攻击者不知道 x_2 , 他就无法从验证等式 $r = H(H(m^*), Q_b, x_1, x_2)$ 中猜测 m^* 是否为发送的真正消息 m 。因为要求出 x_2 , 必须知道 k 或 Bob 的私钥 x_b 。

从以上的分析可以看出, 我们的方案更好地实现了保密性功能。

(3) 具有不可伪造性

由于攻击者没有发送者的私钥 x_a , 因此他要伪造有效签名 (r, s) , 就必须先伪造 (k, r) 或 (k, s) , 然后从等式 $r \cdot Q_a + s \cdot P = k \cdot P$ 中求出 s 或 r , 这都需要面对 ECDLP; 接收者 Bob 要伪造签名 (m, r, s) 欺骗第三方的公开验证也是不可能的, 因为他需要先伪造 (x'_1, y'_1) , 然后再求出 $(x'_2, y'_2) = x_b \cdot (x'_1, y'_1)$ 和 $r = H(H(m), Q_b, x'_1, x'_2)$, 最后伪造 s 满足 $r \cdot Q_a + s \cdot P = (x'_1, y'_1)$, 这时他就必须求解 ECDLP。

(4) 具有不可抵赖性

$r = H(H(m), Q_b, x_1, x_2)$ 包含 Bob 的公钥 Q_b , 所以 Bob 才是合法的接收者, 任何第三方都不能宣称自己是合法的接收者; 同理, 由于签密 (c, r, s) 包含发送者 Alice 的私钥 x_a , Alice 也不能否认她对 m 的签密。

另外, 为了避免消息重放, 可在消息 m 中增加足够的冗余信息, 用于进一步检验消息的有效性。

2.7 方案的效率分析

在我们的方案中, 签密 (c, r, s) 长度为 $|p|+2|q|$; 在公开验证阶段, 普通签名长度为 $2|q|$ 。这些值与 M-C 和 W-B 方案的一样, 但在相同安全强度下, 椭圆曲线密码系统的密钥长度要更短一些, 从而我们的方案具有更小的通信代价。

为了分析计算效率, 我们以 T_h 、 T_p 、 T_e 、 T_m 、 T_i 和 T_s 分别表示 hash 函数、点乘、幂模、模乘、模逆和对称加密或解密等计算。三个操作阶段中, 我们方案的总计算量为 $3T_h+7T_p+3T_m+T_i$, H-C 方案为 $3T_h+7T_e+5T_m$, W-B 方案为 $5T_h+7T_e+3T_m+2T_s$ 。当 $|p|=1024\text{bit}$, $|q|=160\text{bit}$ 时, 点乘运算速度比幂模运算速度快近八倍^[13], 因此我们方案的计算效率更高。

3. 基于 ECC 的(t, n)门限共享验证签密方案

为了分散验证权力, 常采取门限共享验证方式。本节将基于第 2 节的签密方案, 建立一个基于 ECC 和 Shamir 秘密共享^[14]的 (t, n) 门限共享验证签密方案。门限共享签名方案较好地实现了防止签名成员提供假部分签名的欺诈, 但对于门限共享验证方案, 验证成员提供假秘密份额欺骗的验证问题却不好解决。文献[15]提出了一种验证方法, 但该方法需要发送者合作。本文提出了一种检测方法, 在验证和消息恢复阶段不需要发送者合作, 在注册阶段, 方案运用 Pedersen-VSS 可验证方法^[16]可实现对可信中心的欺诈行为的检测。

方案由注册阶段、签密阶段、共享验证及消息恢复阶段和公开验证阶段组成。

3.1 注册阶段

设签密者仍为 Alice, 但接收者是一个组, 记为 $G = \{B_1, B_2, \dots, B_n\}$, 在组 G 中设立一名组执行员 B_c , 负责收集部分验证和恢复消息。首先可信中心 CA 随机选择 $x_G \in Z_q^*$ 作为组 G 的私钥, 则相应的公钥为 $Q_G = x_G \cdot P$ 。然后 CA 在 Z_q 上随机选择次数为 $t-1$ 的多项式:

$$f(x) = a_0 + a_1x + \Lambda + a_{t-1}x^{t-1} \pmod{q}$$

其中 $a_0=f(0)=x_G$, 并计算 $d_i=f(i)$ 和 $Q_i = d_i \cdot P$ 分别作为接收组成员 B_i 的私钥和公钥, 其中 $i=1, 2, \dots, n$ 。最后 CA 将私钥 d_i 通过安全信道传送给 B_i , 把 $a_j \cdot P (j=1, 2, \dots, t-1)$ 广播给组 G 的所有成员, 并公开 $Q_G, Q_i (i=1, 2, \dots, n)$ 。

$h(?)$ 是 CA 选择的另一个单向无碰撞 hash 函数。本方案的其它参数与 2.1 节的相同。

3.2 签密阶段

Alice 对消息 m 签密操作如下:

Step 1: 随机选取整数 $k \in Z_q^*$, 计算 $k \cdot P = (x_1, y_1)$, $k \cdot Q_G = (x_2, y_2)$ 。如果 $x_1=0$ 或 $x_2=0$, 重新选择 k ;

Step 2: 计算 $c = m \cdot x_2 \pmod{p}$, $r = H(H(m), Q_G, x_1, x_2)$, $s = k - x_a \cdot r \pmod{q}$;

Step 3: 计算 $k \cdot Q_i = (\tilde{x}_i, \tilde{y}_i)$, $h_i = h(\tilde{x}_i \parallel \tilde{y}_i)$, 其中 $i=1, 2, \dots, n$, “ \parallel ”为连接运算;

Step 4: 将签密 (c, r, s) 和 (h_1, h_2, \dots, h_n) 发送给接收组 G 的组执行员 B_c 。

3.3 (t, n) 门限共享验证及消息恢复阶段

接收组 G 收到签密 (c, r, s) 后, 由 t 个成员共享验证并进行消息恢复。假设这 t 个成员记为 $B = \{B_i\}_{i \in \Phi}$, 这里 $\Phi \subset \{1, 2, \dots, n\}$ 且 $|\Phi| = t$ 。具体操作步骤如下:

Step 1: B_c 计算 $Y_1 = r \cdot Q_a + s \cdot P = (x'_1, y'_1)$, 并向 B 中成员广播;

Step 2: 每个成员 $B_i \in B$ 用自己的私钥 d_i 计算 $V_i = d_i \cdot Y_1 = (\tilde{x}'_i, \tilde{y}'_i)$, 然后将 V_i 交给组执行员 B_c ;

Step 3: B_c 收到 V_i 后, 验证等式 $h_i = h(\tilde{x}'_i \parallel \tilde{y}'_i)$ 是否成立。如果等式成立, 则证明成员 B_i 没有提供假的秘密份额; 如果 G 的所有成员都没有欺诈行为, 则 B_c 通过如下计算实现消息恢复:

$$l_i = \prod_{j \in \Phi, j \neq i} \frac{-j}{i-j} \bmod q$$

$$Y_2 = \sum_{i \in \Phi} l_i \cdot V_i = (x'_2, y'_2)$$

$$m = c \cdot (x'_2)^{-1} \bmod p$$

Step 4: B_c 验证 $r = H(H(m), Q_G, x'_1, x'_2)$ 是否成立。如果等式成立, 则确信签密是 Alice 发送的。

3.4 公开验证阶段

如果后来 Alice 否认她对消息 m 的签密, 则组执行员 B_c 可将签密 (c, r, s) 转换成普通签名 (m, r, s) , 并将该普通签名及 x'_2 交给第三方验证。第三方首先求出 $r \cdot Q_a + s \cdot P = (x'_1, y'_1)$, 然后再验证等式 $r = H(H(m), Q_G, x'_1, x'_2)$ 是否成立, 如果等式成立, 则确信签密是 Alice 发送的。

3.5 门限方案的完备性证明

定理 2 在验证及消息恢复阶段, 组成员 B_i 的欺诈一定可通过等式 $h_i = h(\tilde{x}'_i \parallel \tilde{y}'_i)$ 得以验证。

证明: 若 B_i 没有欺诈行为, 则有

$$\begin{aligned} (\tilde{x}'_i, \tilde{y}'_i) = V_i &= d_i \cdot Y_1 = d_i \cdot (r \cdot Q_a + s \cdot P) \\ &= d_i \cdot (r \cdot x_a \cdot P + s \cdot P) \\ &= (x_a \cdot r + s) \cdot (d_i \cdot P) \\ &= k \cdot Q_i = (\mathcal{X}_i, \mathcal{Y}_i) \end{aligned}$$

这样就有 $h_i = h(\tilde{x}'_i \parallel \tilde{y}'_i) = h(\mathcal{X}'_i \parallel \mathcal{Y}'_i)$ 。

证毕。

定理 3 若签密者 Alice 能严格遵循签密步骤, 则指定接收组 G 的 t 个诚实成员就能正确恢复消息 m 并进行有效性验证; 第三方也能正确地对接密进行公开验证。

证明: 若 Alice 能严格遵循签密步骤, 就有

$$\begin{aligned} (x'_1, y'_1) = Y_1 &= r \cdot Q_a + s \cdot P \\ &= r \cdot (x_a \cdot P) + (k - x_a \cdot r) \cdot P \\ &= k \cdot P = (x_1, y_1) \end{aligned}$$

$$\begin{aligned} (x'_2, y'_2) = Y_2 &= \sum_{i \in \Phi} l_i \cdot V_i = \sum_{i \in \Phi} l_i \cdot (d_i \cdot Y_1) \\ &= \left(\left(\sum_{i \in \Phi} d_i \cdot l_i \right) \bmod q \right) \cdot Y_1 \end{aligned}$$

由 Lagrange 插值多项式性质有:

$$\begin{aligned} \left(\sum_{i \in \Phi} d_i \cdot l_i \right) \bmod q &= \left(\sum_{i \in \Phi} f(i) \cdot \prod_{j \in \Phi, j \neq i} \frac{-j}{i-j} \right) \bmod q \\ &= f(0) = x_G \end{aligned}$$

则 $(x'_2, y'_2) = x_G \cdot Y_1 = x_G \cdot (k \cdot P) = k \cdot Q_G = (x_2, y_2)$, 这样就有 $m = c \cdot (x'_2)^{-1} \bmod p = c \cdot x_2^{-1} \bmod p$ 。所以指定接收组 G 的 t 个诚实成员能正确恢复消息 m , 且验证等式 $r = H(H(m), Q_G, x'_1, x'_2)$ 是否成立, 第三方也能正确地通过该验证等式进行公开验证。

证毕。

3.6 门限方案的安全性分析

本文所提出的门限方案除了具有 2.6 节所述安全性外, 还具如下的安全性:

在注册阶段, 接收组的成员能够通过下式验证自己私钥 d_i 的正确性:

$$d_i \cdot P = \sum_{j=0}^{t-1} i^j \cdot (a_j \cdot P)$$

若等式成立, 则 B_i 收到的私钥 d_i 正确, 否则可信中心有欺诈行为。攻击者要伪造 d_i 使验证等式成立, 等同于求解 ECDLP 问题。

在共享验证及消息恢复阶段, 组执行员想获取 B_i 的私钥 d_i 是不可能的, 因为要从 $V_i = d_i \cdot Y_1$ 中求解 d_i 等同求解 ECDLP 问题。

在共享验证及消息恢复阶段, 组执行员不需发送方合作就能够检测验证成员 B_i 是否提供假

秘密份额进行欺骗。由于 hash 函数 $h(\cdot)$ 的安全性, 成员 B_i 不可能伪造 h_i 并使其通过等式 $h_i = h(\tilde{x}_i' \parallel \tilde{y}_i')$ 的验证, 攻击者也不可能从 h_i 中求出 kQ_i , 从而求出 kQ_G 。

方案具有 Shamir 门限方案的安全性, 任意少于 t 个合法验证者无法合谋通过签密验证和恢复消息。

3.7 方案效率

为了实现验证组成员是否提供了假的秘密份额, 签密者需要发送 (h_1, h_2, \dots, h_n) 给组执行员 B_c , 这样本文方案的效率会有所降低, 但能够防止门限共享验证体制中假秘密份额的欺诈, 牺牲一定的效率也是可以接受的。由于椭圆曲线密码体制的密钥长度相对较短, 这可使通信复杂度得到一定程度的降低。另外还可以采取对椭圆曲线上的点进行压缩处理的办法^[17]来进一步降低通信量。

4. 结 论

保密性和认证性是密码学中研究的重要课题, 其中保密性通过加密方法实现, 认证性通过数字签名实现, 签密方法将加密操作和签名操作融合在一起实现, 因而效率有所提高。本文基于椭圆曲线密码体制, 提出并建立了可转换签密方案, 解决了目前一些方案存在的问题。它除了具有保密性、认证性外, 还具有发送方的不可抵赖性, 并具有更小的计算量和通信量。基于本文所提出的签密方案而建立的 (t, n) 门限共享验证签密方案, 在共享验证和消息恢复阶段, 解决了验证成员提供假秘密份额进行欺诈的问题。

参考文献:

[1] Y. Zheng, *Signcryption and Its Application in Efficient Public Key Solutions*, Information Security Workshop (ISW '97), LNCS 1396, Springer-Verlag, 1997: pp. 291-312.

[2] Y. Zheng, *Digital Signcryption or How to Achieve Cost (signature & encryption) << cost (signature) + cost (encryption)*, CRYPTO'97, LNCS 1294, Springer-Verlag, 1997: pp. 165-179.

[3] K Nyberg, R A Rueppel, *Message Recovery for Signature Scheme Based on the Discrete Logarithm Problem*, Designs Codes and Cryptography, 1996: pp. 61-81.

[4] H. Petersen, M. Michels, *Cryptanalysis and Improvement of Signcryption Schemes*, IEE Computers and Digital Communications, 1998, 145(2): pp. 149-151.

[5] S. Araki, S. Uehara, K. Imamura, *The Limited Verifier Signature and Its Application*, IEICE Transactions on Fundamentals, 1999, E82-A(1): pp. 63-68.

[6] T. Wu, C. Hsu, *Convertible Authenticated Encryption Scheme*, The Journal of Systems and Software, 2002, 62(6): pp. 205-209.

[7] H. Huang, C. Chang, *An Efficient Convertible Authenticated Encryption Scheme and Its Variant*, Proc. of ICICS2003-Fifth International Conference on Information and Communications Security, LNCS 2836, Springer-Verlag, 2003: pp. 382-392.

[8] Jiqiang Lv, Xinmei Wang, Kwangjo Kim, *Practical Convertible Authenticated Encryption Schemes Using Self-certified Public Keys*, Journal of Applied Mathematics and Computation, Elsevier Science, 2004, http://caislab.icu.ac.kr/pub/pub_sci.html.

[9] C. Ma, K. Chen, *Publicly Verifiable Authenticated Encryption*, Electronics Letters, 2003, 39(3): pp. 281-282.

[10] Guilin Wang, Feng Bao, Changshe Ma, Kefei Chen, *Efficient Authenticated Encryption Schemes with Public Verifiability*, Proc. of the 60th IEEE Vehicular Technology Conference (VTC 2004-Fall)-Wireless Technologies for Global Security. IEEE Computer Society, 2004, <http://www.ieeevtc.org/vtc2004fall/>.

[11] Guilin Wang, R. H. Deng, D. Kwak, S. Moon, *Security Analysis of Two Signcryption Schemes*, Information Security (ISC 2004), LNCS 3225, Springer-Verlag, 2004: pp. 123-133.

[12] 李旭宏, 吕继强, 刘培玉, 王宝安, 两个具有语义安全的可转换认证加密方案, 计算机工程与应用, 2004, 40(34): pp. 165-167.

[13] N. Kobitz, A. Menezes, S. Vanstone, *The State of Elliptic Curve Cryptography, Designs, Codes, and Cryptography*, 2000, 19(2-3): pp. 173-193.

[14] Shamir, *How to Share a Secret*, Communications of the ACM, 1979, 22(11): pp. 612-613.

[15] 李继国, 曹珍富, 李建中, 具有指定接收组 (t, n) 门限共享验证签名加密方案, 电子学报, 2003, 31(7): pp. 1086-1088.

[16] T. P. Pedersen, *Distributed Provers with Applications to Undeniable Signatures*, In: Proc. of Eurocrypt'91, LNCS 547, Springer-Verlag, 1991: pp. 221-242.

[17] IEEE P1363, *Standard Specifications for Public Key Cryptography*, <http://grouper.ieee.org/groups/1363/>.

A Convertible Signcryption and Threshold Shared Verification Scheme Based on ECC

Changgen Peng¹, Xiang Li², Wenjun Luo³

(1,2,3 Institute of Computer Science, Guizhou University, Guiyang 550025, China;

1 Department of Mathematics, Guizhou University, Guiyang 550025, China)

Abstract: Firstly, this paper presents a convertible signcryption scheme based on elliptic curve cryptosystem. Our scheme can stand against the known-plaintext attack, and overcome the weaknesses that the semantic security of the message cannot be provided in H-C and W-B schemes. Because our scheme is built based on ECC, its computational cost and communication cost are lower. Based on the proposed signcryption scheme, we design a threshold signcryption scheme with (t, n) shared verification. This threshold scheme can prevent the cheating of trusted center. In the shared verification and message recovery phase, we propose a method to prevent the cheating that the verification member forges secret share.

Key words: Authenticated Encryption; Signcryption; Convertible; Threshold Shared Verification; Elliptic Curve Cryptosystem

(责任编辑 : Susan , 肖星 , Nory)