

一种新的无证书签密方案^{*}

陈 明¹, 吴开贵², 何 盼²

(1. 重庆医科大学附属第二医院 信息中心, 重庆 400010; 2. 重庆大学 计算机学院, 重庆 400044)

摘 要: 分析王会歌等人提出的一种无证书的签密方案(W-CL-SC)发现,由于公钥设置不合理,W-CL-SC 方案没有实现抗密钥托管属性。提出一种新的无证书签密方案,引入更强的敌手模型证明新方案能达到抗密钥托管、IND-CCA2 安全和 EUF-CMA 安全。分析表明,新机制是安全和有效的。

关键词: 无证书签密; 双线性对; 密钥托管; 标准模型

中图分类号: TP309

文献标志码: A

文章编号: 1001-3695(2011)10-3799-04

doi:10.3969/j.issn.1001-3695.2011.10.053

Analysis and improvement of certificateless signcryption scheme

CHEN Ming¹, WU Kai-gui², HE Pan²

(1. Information Center, Second Affiliated Hospital Chongqing Medical University, Chongqing 400010, China; 2. College of Computer Science, Chongqing University, Chongqing 400044, China)

Abstract: Recently, Wang Hui-ge, et al. proposed a certificateless signcryption scheme(W-CL-SC), but it did not achieve anti-key escrow property due to the irrational public key. This paper presented an improved certificateless signcryption scheme. It introduced a stronger adversary model, and proved that the new scheme could achieve anti-key escrow, IND-CCA2 and EUF-CMA securities. The analyzing shows that the new scheme is secure and efficient.

Key words: certificateless signcryption; bilinear pairings; key escrow; standard model

签密机制将数字签名和公钥加密机制融为一体,不仅实现了通信的机密性,而且达到了签名者身份的认证性和签名事实的不可否认性,并且总的计算和通信开销低于签名和加密两者之和。随着基于身份密码(ID-PKC)系统^[1]的深入研究和广泛应用,基于身份的签密方案也得到了越来越多研究者的关注^[2~4]。但是,ID-PKC 存在一个固有弱点,即密钥托管问题,密钥产生中心(KGC)拥有所有用户私钥,能假冒系统中的所有用户,恶意的 KGC 是 ID-PKC 系统的最大隐患。无证书的公钥加密(CL-PKC)机制^[5]被提出来解决这一问题。

CL-PKC 的基本思想是:为了防止恶意的 KGC,用户依然保有其完全的秘密密钥,即 KGC 产生用户部分私钥,而用户自己产生另一半私钥,防止了密钥托管。近来,一些研究者基于 CL-PKC 的思想,提出了基于无证书的签密方案(CL-SC)^[6,7]。文献[6]方案(下文简称为 W-CL-SC)是基于文献[2]方案的一种改进方案,效率较高,但是由于其用户公钥设置不合理,因而并未能实现抗密钥托管特性。在 W-CL-SC 方案中,KGC 的主密钥为 s ,用户私钥为 $S_i = x_i D_i = x_i s Q_i$,用户公钥为 $PK_i = (X_i, Y_i) = (x_i P, x_i Q_i)$,其中, $x_i \in Z_q^*$ 是用户随机选择的秘密值, $Q_i = H_1(ID_i)$ 是用户基于身份的公钥参数, $H_1: \{0,1\}^* \rightarrow G_1^*$ 是安全单向散列函数。从中可以看出,恶意的 KGC 可以利用用户的公钥和自己的主密钥计算用户私钥 $S_i^* = s Y_i = s x_i Q_i = S_i$ 。因此,W-CL-SC 方案未能真正实现抗密钥托管特性,恶意的 KGC 能够解密相应的密文,伪造用户签名。

1 双线性映射及困难问题假设

本章简要介绍双线性对(bilinear pairings)及其困难问题假设,详细内容可参考相关文献[1~4]。

假设 G_1 和 G_2 分别是素阶为 q 的循环加法群和循环乘法群,定义 $e: G_1 \times G_1 \rightarrow G_2$ 为满足以下性质的双线性映射:

- 双线性性,对于 $\forall (P, Q) \in G_1$ 和 $\forall (a, b) \in Z_q^*$ 有 $e(aP, bQ) = e(P, Q)^{ab}$, $e(aP + bP, Q) = e(aP, Q)e(bP, Q)$;
- 非退化性,存在 $(P, Q) \in G_1$ 满足 $e(P, Q) \neq 1$;
- 可计算性,对于 $\forall (P, Q) \in G_1$,能有效计算 $e(P, Q)$ 。

在给定的双线性对中存在以下主要的困难问题假设:

a) CDH (computational Diffie-Hellman) 假设。对于任意未知的 $a, b \in Z_q^*$,给定生成元 $P \in G_1$ 和 $aP, bP \in G_1$,不存在概率多项式时间(probabilistic polynomial-time, PPT)算法能成功计算 abP 。

b) BDH (bilinear Diffie-Hellman) 假设。对于任意未知的 $a, b, c \in Z_q^*$,给定 $(P, aP, bP, cP) \in G_1$,不存在 PPT 算法能成功计算 $e(P, P)^{abc}$ 。

2 一种新的 CL-SC 机制

本文提出一种新的无证书签密方案(N-CL-SC),新方案基于前面介绍的双线性映射及困难数学问题,包括系统参数建

收稿日期: 2011-01-19; 修回日期: 2011-04-07 基金项目: 国家自然科学基金资助项目(90818028); 国家科技支撑计划资助项目(2008BAH37B04)

作者简介: 陈明(1978-),男,重庆人,博士,主要研究方向为信息安全、电子商务安全、形式化技术、分布式计算(chenming9824@yahoo.com.cn); 吴开贵(1966-),男,重庆人,副教授,硕导,博士,主要研究方向为信息安全、分布式计算; 何盼(1984-),女,重庆人,博士研究生,主要研究方向为分布式计算、服务计算。

立、部分私钥产生、用户私钥设置、用户公钥设置、签密产生和解签密等六个算法,具体如下:

a) 系统参数建立。算法输入 $q \in \mathbb{Z}_q^*$, 输出 $\text{params} = (G_1, G_2, e, P, P_0, H_1, H_2, H_3, q)$ 。其中: (G_1, G_2) 为素阶为 q 的循环群; P 为 G_1 的生成元; $P_0 = sP$ 为 KGC 的公钥, 对应的主密钥为 $s \in \mathbb{Z}_q^*$; $H_1: \{0, 1\}^* \rightarrow G_1$; $H_2: G_2 \times G_1 \rightarrow \{0, 1\}^k$; $H_3: G_1 \times \{0, 1\}^* \rightarrow \mathbb{Z}_q^*$ 为安全的单向散列函数。

b) 部分私钥产生。算法输入 $(\text{params}, s, \text{ID}_i)$, 输出 $D_i = sQ_i$ 作为实体 i 的部分私钥, 并通过安全信道发送给 i 。这里 $\text{ID}_i \in \{0, 1\}^*$ 是 i 的身份标志, $Q_i = H_1(\text{ID}_i)$ 。

c) 用户私钥设置。算法输入 $(\text{params}, \text{ID}_i, D_i)$, 输出 $X_i = (x_i, D_i)$ 作为 i 的全部私钥, 其中, $x_i \in \mathbb{Z}_q^*$ 是实体 i 选择的私有秘密。

d) 用户公钥设置。算法输入 $(\text{params}, \text{ID}_i, D_i, x_i)$, 输出 $(Q_i, P_i = x_i P)$ 作为 i 的公钥。

e) 签密产生。假设实体 A 拥有身份密钥对 (ID_A, X_A, P_A) , 期望产生对消息 M 的签密, 解签密对象为拥有身份密钥对 (ID_B, X_B, P_B) 的实体 B 。算法输入 $(\text{params}, M, \text{ID}_A, X_A, \text{ID}_B, P_B)$, 随机选择 $r \in \mathbb{Z}_q^*$, 输出 (C, σ, R) 。计算过程如下:

- (a) $R = rP$;
- (b) $u = e(D_A, Q_B), v = x_A P_B$;
- (c) $K = H_2(u, v, R)$;
- (d) $C = K \oplus M$;
- (e) $\alpha = H_3(R, M)$;
- (f) $\sigma = \alpha(x_A P_0 + D_A)$ 。

f) 解签密。算法输入 $(\text{params}, \text{ID}_A, P_A, \text{ID}_B, X_B, C, \sigma, R)$, 输出 $(M, \text{accept/reject})$ 。解签密过程如下:

- (a) $u^* = e(Q_A, D_B), v^* = x_B P_A$;
- (b) $K^* = H_2(u^*, v^*, R)$;
- (c) $M^* = K^* \oplus C$;
- (d) $\alpha^* = H_3(R, M^*)$;
- (e) $e(\sigma, P) \stackrel{?}{=} e(P_A + Q_A, \alpha^* P_0)$ 。

3 N-CL-SC 方案分析

3.1 有效性分析

新的无证书签密方案的有效性和正确性可由下式验证。

$$\begin{aligned} u &= e(D_A, Q_B) = e(Q_A, Q_B)^s = e(Q_A, D_B) = u^* \\ v &= x_A P_B = x_A x_B P = x_B P_A = v^* \\ K &= K^*, M = M^*, a = a^* \end{aligned} \quad (1)$$

$$\begin{aligned} e(\sigma, P) &= e(a(x_A P_0 + D_A), P) = \\ e(ax_A P_0, P) &= e(aD_A, P) = e(x_A P, asP) e(Q_A, asP) = \\ e(P_A, aP_0) &e(Q_A, aP_0) = (P_A + Q_A, aP_0) \end{aligned} \quad (2)$$

3.2 安全性分析

3.2.1 安全模型定义

签密机制最主要的两个安全属性是加密的机密性(选择密文攻击下加密不可区分性, IND-CCA2)和签名不可伪造性(选择消息攻击不可伪造性, EUF-CMA)^[7]。本文采用文献[7]中定义的两类敌手模型(记为 A_I 和 A_{II})以及四类游戏(记为 game I、game II、game III 和 game IV)分析 N-CL-SC 的安全性。

A_I 模拟一类外部攻击者, 其被允许替换用户公钥 P_i 和查

询未被替换公钥用户的私有秘密 x_i , 但是不被允许查询用户部分私钥 D_i 。 A_{II} 模拟恶意的 KGC, 其可以根据攻击的需要产生具有秘密门限的主密钥 s 和公钥参数 P_0 , 但不被允许替换目标用户的公钥 P_i 。可见, 文献[7]中 A_{II} 的能力强于文献[5, 6]的 A_{II} 敌手。

GameI 和 gameIII 模拟 A_I 和挑战者 C 之间的游戏, gameII 和 gameIV 模拟 A_{II} 和挑战者 C 之间的游戏。N-CL-SC 的安全性定义为不存在多项式时间敌手 (A_I 和 A_{II}) 赢得 game I ~ game IV。

1) GameI

Initialization。挑战者 C 运行系统参数生成算法, 输入安全参数 k , 输出系统主密钥 msk 和系统参数 params , 并将 params 发送给 A_I 而对 msk 保密。

Phase 1 A_I 适应性地执行多项式有界次的查询。

a) request public key: A_I 请求身份标志为 ID_i 的主体公钥, C 返回相应的公钥 P_{k_i} 。

b) partial key extraction: A_I 请求身份标志为 ID_i 的主体部分私钥, C 返回相应的部分私钥 D_i 。

c) private key extraction: A_I 请求身份标志为 ID_i 的主体私钥, 如果 ID_i 公钥未被替换, 那么 C 返回相应的私钥 x_i 。

d) public key replacement: A_I 请求替换身份标志为 ID_i 的主体公钥, 并输入新的公钥, C 用 P^* 替换 ID_i 的当前公钥。

e) signcrypt: A_I 请求对消息 $(\text{ID}_i, \text{ID}_j, m)$ 的签密(这里, ID_i 是签密发送者的身份, ID_j 是签密接收者的身份), C 执行签密算法并返回 $\sigma = \text{signcrypt}(\text{params}, \text{ID}_j, S_{k_i}, P_{k_j}, m)$ 给 A_I 。如果 ID_i 的公钥已被替换, 而 C 并不知道已替换公钥 P^* 所对应的私钥 x_i^* , 在这种情况下, 要求 A_I 提供相应的替换私有秘密 x_i^* 。此外, 为了不失一般性, C 不允许请求签密的发送者和接收者为同一实体, 即要求 $\text{ID}_i \neq \text{ID}_j$ 。

f) unsigncrypt: A_I 请求解签密消息 $(\text{ID}_i, \text{ID}_j, \sigma, m)$ (这里, ID_i 是签密发送者的身份, ID_j 是签密接收者的身份), C 执行解签密算法并返回解签密结果给 A_I 。同样地, 如果 ID_j 的公钥已被替换, 而 C 并不知道已替换公钥 P_j^* 所对应的私钥 x_j^* , 在这种情况下, 要求 A_I 提供相应的替换私有秘密 x_j^* 。此外, 为了不失一般性, C 不允许请求签密的发送者和接收者为同一实体, 即要求 $\text{ID}_i \neq \text{ID}_j$ 。

Challenge。Phase 1 结束后, A_I 输出两个等长且完全不同的消息 (m_0, m_1) , 以及一个签密发送者身份 ID_i 和一个签密接收者身份 ID_j , 作为对签密算法的挑战。 A_I 将 $(\text{ID}_i, \text{ID}_j, m_0, m_1)$ 发送给 C , C 随机选择 $b \in \{0, 1\}$, 执行对 m_b 的签密 σ^* , 并将 σ^* 返回给 A_I 。这里, 要求 A_I 并未在 Phase 1 阶段执行对 ID_j 的部分私钥查询(partial key extraction)。

Phase 2 A_I 继续请求在 Phase 1 阶段定义的各项查询, 但是不被允许请求对 ID_j 的部分私钥查询和对挑战消息 $(\text{ID}_i, \text{ID}_j, m_0, m_1, \sigma^*)$ 的任何签密和解签密查询。

Guess。最后, A_I 输出对 b 的猜测 b' 。如果 $b' = b$, 那么可认为 A_I 赢得 gameI。定义 A_I 赢得 gameI 的优势为

$$\text{adv}_{A_I}^{\text{IND-CCA2}} = |2\Pr[b' = b] - 1|$$

其中: $\Pr[b' = b]$ 表示 $b' = b$ 的概率。

2) GameII

Initialization。挑战者 C 运行系统参数生成算法, 输入安全

参数 k , 输出系统主密钥 msk 和系统参数 params , 并将 msk 和 params 发送给 A_{II} 。根据定义, A_{II} 模拟恶意的 KGC, 因此其可以计算任何实体的部分私钥。

Phase 1 A_{II} 适应性地执行多项式有界次的查询。各项查询的定义与 gameI 相同。

Challenge。 Phase 1 结束后, A_{II} 输出两个等长且完全不同的消息 (m_0, m_1) 以及一个签密发送者身份 ID_I 和一个签密接收者身份 ID_J , 作为对签密算法的挑战。 A_{II} 将 $(\text{ID}_I, \text{ID}_J, m_0, m_1)$ 发送给 C , C 随机选择 $b \in \{0, 1\}$, 执行对 m_b 的签密 σ^* , 并将 σ^* 返回给 A_{II} 。这里, 要求 A_{II} 并未在 Phase 1 阶段执行对特定实体 ID_J 的公钥替换查询 (public key replacement)。

Phase 2 A_{II} 继续请求在 Phase 1 阶段定义的各项查询, 但是不被允许请求对 ID_J 的公钥替换查询和对挑战消息 $(\text{ID}_I, \text{ID}_J, m_0, m_1, \sigma^*)$ 的任何签密和解签密查询。

Guess。 最后, A_{II} 输出对 b 的猜测 b' 。如果 $b' = b$, 那么可认为 A_{II} 赢得 gameII 。定义 A_{II} 赢得 gameII 的优势为

$$\text{adv}_{A_{\text{II}}}^{\text{IND-CCA2}} = |2\Pr[b' = b] - 1|$$

定义 1 如果不存在 t -time 敌手 $A \in \{A_I, A_{\text{II}}\}$ (A 至多执行 q_{pk} 次公钥查询、 q_{pr} 次公钥替换查询、 q_{pp} 次部分私钥查询、 q_{ps} 次私钥查询、 q_s 次签密查询和 q_u 次解签密查询), 以 $\geq \epsilon$ 的优势分别赢得 gameI 和 gameII , 那么 CL-SC 机制被认为满足 $(\epsilon, t, q_{\text{pk}}, q_{\text{pr}}, q_{\text{pp}}, q_{\text{ps}}, q_s, q_u)$ -IND-CCA2 安全性。

3) GameIII

Initialization。 挑战者 C 运行系统参数生成算法, 输入安全参数 k , 输出系统主密钥 msk 和系统参数 params , 并将 params 发送给 A_I 而对 msk 保密。

Queries。 A_I 适应性地执行多项式有界次的查询。各项查询的定义与 GameI 相同。

Output。 最后, A_I 产生一个新的元组 $(\text{ID}_I, \text{ID}_J, m, \sigma^*)$ 。这里, 要求 A_I 在 Phase 1 阶段未执行过对 $(\text{ID}_I, \text{ID}_J, m)$ 的签密查询和对 ID_J 的部分私钥查询。

如果 σ^* 是对 $(\text{ID}_I, \text{ID}_J, m)$ 的一个有效签密, 那么 A_I 赢得 gameIII 。定义 A_I 赢得 gameIII 的优势为

$$\text{adv}_{A_I}^{\text{EUF-CMA}} = \Pr[A_I \text{ wins}]$$

4) GameIV

Initialization。 挑战者 C 运行系统参数生成算法, 输入安全参数 k , 输出系统主密钥 msk 和系统参数 params , 并将 msk 和 params 发送给 A_{II} 。根据定义, A_{II} 模拟恶意的 KGC, 因此其可以计算任何实体的部分私钥。

Queries。 A_{II} 适应性地执行多项式有界次的查询。各项查询的定义与 gameI 相同。

Output。 最后, A_{II} 产生一个新的元组 $(\text{ID}_I, \text{ID}_J, m, \sigma^*)$ 。这里, 要求 A_{II} 在 Phase 1 阶段未执行过对 $(\text{ID}_I, \text{ID}_J, m)$ 的签密查询和对 ID_J 的部分私钥查询。

如果通过解签密验证, σ^* 是对 $(\text{ID}_I, \text{ID}_J, m)$ 的一个有效签密, 那么 A_{II} 赢得 gameIV 。定义 A_{II} 赢得 gameIV 的优势为

$$\text{adv}_{A_{\text{II}}}^{\text{EUF-CMA}} = \Pr[A_{\text{II}} \text{ wins}]$$

定义 2 如果不存在 t -time 敌手 $A \in \{A_I, A_{\text{II}}\}$ (A 至多执行了 q_{pk} 次公钥查询、 q_{pr} 次公钥替换查询、 q_{pp} 次部分私钥查询、 q_{ps} 次私钥查询、 q_s 次签密查询和 q_u 次解签密查询), 以 $\geq \epsilon$ 的优势分别赢得 gameIII 和 gameIV , 那么 CL-SC 机制被认为满足

$(\epsilon, t, q_{\text{pk}}, q_{\text{pr}}, q_{\text{pp}}, q_{\text{ps}}, q_s, q_u)$ -EUF-CMA 安全性。

3.2.2 无证书签密安全性分析

定理 1 如果 CDH 假设和 BDH 假设成立, 在存在敌手 $A \in \{A_I, A_{\text{II}}\}$ 的情况下, N-CL-SC 机制实现了 IND-CCA2 安全。

证明 定理 1 由引理 1 和 2 直接证明。

引理 1 假设 (ϵ', t') -BDH 不可求解假设成立, 在存在敌手 A_I 的情况下, N-CL-SC 机制实现了 IND-CCA2 安全。特定地, 若存在一个 IND-CCA2 敌手 A_I 能够在多项式有界时间 t 内, 以 ϵ 的优势赢得 gameI , 并且, A_I 最多进行 q_i 次 H_i 查询 ($i = 1, 2, 3$)、 q_{pk} 次公钥查询、 q_{pr} 次公钥替换查询、 q_{pp} 次部分私钥查询、 q_{ps} 次私钥查询、 q_s 次签密查询和 q_u 次解签密查询, 则必然存在一个挑战者 C , 能够在多项式有界时间 $t' = t + O((q_1 + q_2 + q_3)t_H + (q_{\text{pk}} + q_{\text{pr}} + 4q_s + 2q_u)t_M + (q_s + 3q_u)t_P)$ 内以 $\epsilon' \geq \frac{1}{2q_1^2 q_2 q_3 q_s q_u} (1 - \frac{1}{q_{\text{pp}}}) \epsilon$ 的优势解决 BDH 问题。这里, (t_H, t_M, t_P) 分别表示哈希函数、 G_1 中乘和对运算时间。

证明 假设存在 A_I 敌手, 显示 C 怎样利用算法 A_I 求解 BDH 问题。给定一个 BDH 问题挑战 $(P, aP, bP, cP) \in G_1$, 为了求解 BDH 问题, C 模拟成为一个挑战者, 响应 A_I 的每一次查询。

Initialization。 挑战者 C 运行系统参数生成算法, 输入安全参数 k , 输出系统主密钥 msk 和系统参数 params , 并将 params 发送给 A_I 而对 msk 保密。

Phase 1 挑战者 C 响应 A_I 的以下查询。

a) H_1 : 当收到第 i 次 H_1 查询, C 首先查询初始为空的列表 L_1 , 如果存在相应元组, 那么返回相应的 Q_i ; 否则, 如果 $i = J$, C 随机选择 b 并设置 $Q_i = bP$, 将 $(\text{ID}_I, Q_i, \perp)$ 插入 L_1 ; 否则, 随机选择 d_i 并设置 $Q_i = d_i P$, 将 $(\text{ID}_I, Q_i, \text{ad}_i P)$ 插入 L_1 。最后, 返回 Q_i 。这里 a 表示 KGC 主密钥。

b) H_2 : 当收到针对 $(M, \text{ID}_I, \text{ID}_J, u, v, R)$ 的 H_2 查询, C 首先查询初始为空的列表 L_2 , 如果存在相应元组 $(M, \text{ID}_I, \text{ID}_J, u, v, R, K, C, \alpha, \sigma)$, 那么返回相应的 K ; 否则, C 随机选择 $K \in \{0, 1\}^k$, 并更新列表 L_2 。

c) H_3 : 当收到针对 (M, R) 的 H_3 查询, C 首先查询初始为空的列表 L_2 , 如果存在相应元组 $(M, \text{ID}_I, \text{ID}_J, u, v, R, K, C, \alpha, \sigma)$, 那么返回相应的 α ; 否则, C 随机选择 $\alpha \in Z_q^*$, 并更新列表 L_2 。

d) request public key: 当收到对 ID_i 的公钥查询, C 查询初始为空的列表 L_{PK} , 若存在相应项, 返回相应的公钥 P_i ; 否则, C 执行用户私钥设置算法和用户公钥设置算法, 获得 ID_i 的密钥对 (x_i, P_i) 并将 (ID_i, x_i, P_i) 插入列表 L_{PK} 。然后返回用户公钥 P_i 。

e) partial key extraction: 当收到对 ID_i 的部分私钥查询, 如果 $i = J$, C 终止查询并返回失败; 否则, 如果 $i = I$, C 随机选择 $c \in Z_q^*$, 返回 acP ; 否则, C 请求 H_1 查询, 返回相应的部分私钥 $\text{ad}_i P$ 。

f) private key extraction: 当收到对 ID_i 的私钥查询, 如果 $i = J$, C 终止查询并返回失败; 否则, 如果 ID_i 的公钥未被替换, C 查询列表 L_{PK} , 返回相应的私钥 x_i ; 否则, 返回 $\perp$ 。

g) public key replacement: 当收到 $\langle \text{ID}_i, P_i^* \rangle$ 的公钥替换查询, C 查询列表 L_{PK} , 如果 (ID_i, x_i, P_i) 存在, 则用 $(\text{ID}_i, \perp, P_i^*)$ 替换原有值; 否则插入新元组 $(\text{ID}_i, \perp, P_i^*)$ 。

h) signcrypt: 当收到 $\langle \text{ID}_i, \text{ID}_j, M \rangle$ 的签密查询 ($i, j \in \{1, 2, \dots, q_1\}$), 如果 $\text{ID}_I = \text{ID}_I$ 且 $\text{ID}_J = \text{ID}_J$, 则终止查询; 否则 C 按

如下规则执行:

(a) 如果 $ID_i \neq ID_j$, 那么, C 首先查询列表 L_2 , 如果存在相应元组 $(M, ID_i, ID_j, u, v, R, K, C, \alpha, \sigma)$, 且 (C, R, σ) 不为空, 那么返回相应的 (C, R, σ) ; 否则, C 按照签密算法计算并返回相应签密结果 (C, R, σ) , 同时, 将 $(M, ID_i, ID_j, u, v, R, K, C, \alpha, \sigma)$ 插入列表 L_2 。

(b) 如果 $ID_i = ID_j$, 那么, 显然有 $ID_i \neq ID_j$, C 可查询 ID_j 的部分私钥 ad_jP 和私钥 x_j , 随机选择 $r \in Z_q^*$ 计算 $R = rP, u = e(bP, ad_jP), v = x_jP$, 并请求 H_2 查询和 H_3 查询。然后, C 计算 $C = K \oplus M, \sigma = \alpha(x_i^* P_0 + abP)$, 返回签密结果 (C, R, σ) , 同时将 $(M, ID_i, ID_j, u, v, R, K, C, \alpha, \sigma)$ 插入列表 L_2 。

i) **unsigncrypt**: 当收到 $\langle ID_i, ID_j, C, R, \sigma \rangle$ 的解签密查询 $(i, j \in \{1, 2, \dots, q_1\})$, 如果 $ID_i = ID_j$ 且 $ID_j = ID_j$, 则终止查询。否则, C 按如下规则执行: 如果 $ID_j = ID_j$, 那么, 显然有 $ID_i \neq ID_j$, C 可查询 ID_j 的部分私钥 ad_jP 和私钥 x_j , 计算 $u = e(ad_jP, bP), v = x_jP$, 并请求 H_2 查询和 H_3 查询。然后, C 计算 $M = K(\oplus C)$ 。

Phase 1 结束后, A_1 输出两个等长且完全不同的消息 (m_0, m_1) 以及一个签密发送者身份 ID_i 和一个签密接收者身份 ID_j , 作为对签密算法的挑战。 C 随机选择 $b \in \{0, 1\}$, 执行对 m_b 的签密 σ^* , 并将 σ^* 返回给 A_1 。最后, A_1 输出对 b 的猜测 b' 。

在上述过程中, 定义以下事件:

$E1$: A_1 未选择 ID_i 和 ID_j 作为挑战实例。

$E2$: A_1 执行了对 ID_j 的部分私钥查询。

$E3$: C 终止了签密查询。

$E4$: C 终止了解签密查询。

显然, 有 $\Pr[\neg E1] = 1/q_1, \Pr[E2] = 1/q_{pp}, \Pr[\neg E3] \geq 1/(2q_1q_2q_3q_s), \Pr[\neg E4] \geq 1/q_u$ 。

$$\Pr[\neg E1 \wedge \neg E2 \wedge \neg E3 \wedge \neg E4] \geq \frac{1}{2q_1^2q_2q_3q_sq_u} (1 - \frac{1}{q_{pq}})$$

证毕。

引理 2 假设 (ϵ', t') -CDH 不可求解假设成立, 在存在敌手 A_{II} 的情况下, N-CL-SC 机制实现了 IND-CCA2 安全。特定地, 若存在一个 IND-CCA2 敌手 A_{II} 能够在多项式有界时间 t 内, 以 ϵ 的优势赢得 gameII, 并且, A_{II} 最多进行 q_i 次 H_i 查询 $(i = 1, 2, 3)$ 、 q_{pk} 次公钥查询、 q_{pr} 次公钥替换查询、 q_{pp} 次部分私钥查询、 q_{ps} 次私钥查询、 q_s 次签密查询和 q_u 次解签密查询, 则必然存在一个挑战者 C 能够在多项式有界时间 $t' = t + O((q_1 + q_2 + q_3)t_H + (q_{pk} + q_{pp} + 4q_s + 2q_u)t_M + (q_s + 3q_u)t_P)$ 内以 $\epsilon' \geq \frac{1}{2q_1q_2q_3q_sq_u} (1 - \frac{1}{q_{pq}})\epsilon$ 的优势解决 CDH 问题。这里, (t_H, t_M, t_P) 分别表示哈希函数、 G_1 中乘和对运算时间。

证明 引理 2 的证明过程与引理 1 类似。

定理 2 如果 CDH 假设和 BDH 假设成立, 在存在敌手 $A \in \{A_I, A_{II}\}$ 的情况下, N-CL-SC 机制实现了 EUF-CMA 安全。

证明 定理 2 的由引理 3 和 4 直接证明。

引理 3 假设 (ϵ', t') -BDH 不可求解假设成立, 在存在敌手 A_I 的情况下, N-CL-SC 机制实现了 EUF-CMA 安全。特定地, 若存在一个 EUF-CMA 敌手 A_I 能够在多项式有界时间 t 内, 以 ϵ 的优势赢得 gameI, 并且 A_I 最多进行 q_i 次 H_i 查询 $(i = 1, 2, 3)$ 、 q_{pk} 次公钥查询、 q_{pr} 次公钥替换查询、 q_{pp} 次部分私钥查询、 q_{ps} 次私钥查询、 q_s 次签密查询和 q_u 次解签密查询, 则必然存在一个挑战者 C , 能够在多项式有界时间 $t' = t + O((q_1 + q_2 + q_3)$

$t_H + (q_{pk} + q_{pp} + 4q_s + 2q_u)t_M + (q_s + 3q_u)t_P)$ 内以 $\epsilon' \geq \frac{1}{12q_u(q_s + q_u)} (1 - \frac{1}{q_{pq}})\epsilon$ 的优势解决 BDH 问题。这里, (t_H, t_M, t_P) 分别表示哈希函数、 G_1 中乘和对运算时间。

证明 引理 3 的证明过程与引理 1 类似。

引理 4 假设 (ϵ', t') -CDH 不可求解假设成立, 在存在敌手 A_{II} 的情况下, N-CL-SC 机制实现了 EUF-CMA 安全。特定地, 若存在一个 EUF-CMA 敌手 A_{II} 能够在多项式有界时间 t 内, 以 ϵ 的优势赢得 gameI, 并且, A_{II} 最多进行 q_i 次 H_i 查询 $(i = 1, 2, 3)$ 、 q_{pk} 次公钥查询、 q_{pr} 次公钥替换查询、 q_{pp} 次部分私钥查询、 q_{ps} 次私钥查询、 q_s 次签密查询和 q_u 次解签密查询, 则必然存在一个挑战者 C , 能够在多项式有界时间 $t' = t + O((q_1 + q_2 + q_3)t_H + (q_{pk} + q_{pp} + 4q_s + 2q_u)t_M + (q_s + 3q_u)t_P)$ 内以 $\epsilon' \geq \frac{1}{12q_u(q_s + q_u)} (1 - \frac{1}{q_{ps}})\epsilon$ 的优势解决 CDH 问题。这里, (t_H, t_M, t_P) 分别表示哈希函数、 G_1 中乘和对运算时间。

证明 引理 4 的证明过程与引理 1 类似。

另外, 除了机密性和不可伪造性以外, N-CL-SC 机制还需要实现认证性和不可否认性等性质, 这些性质可以从机密性和不可伪造性直接推出。

3.3 效率分析

表 1 对比了本文 N-CL-SC 方案与文献[6,7]中方案的计算开销。表中数值为通信双方的总的计算次数。

表 1 计算开销比较

	乘运算	指数运算	对运算
W-CL-SC ^[6]	3	1	4
Z-CL-SC ^[7]	n	4	5
N-CL-SC	6	0	4

从表 1 可以看出, 在计算开销上, 本文的方案多了 3 次 G_1 上的乘运算, 而文献[6]方案多了一次 G_2 上的指数运算。 G_2 上的指数运算的运算量远高于 G_1 上乘的运算量^[8]。因此, 本文方案的计算开销略低于文献[6]方案。但是, 本文方案优于文献[6]方案主要表现在实现了真正的抗密钥托管特性。

与文献[7]方案比较, 该方案中 G_1 和 G_2 都为乘法群, 且采用了更加复杂的计算方式, 很难进行确切的量化比较。初略统计, 该方案需要进行 5 次对运算、4 次指数运算, 因此, 本文方案的计算开销相对较小。

4 结束语

由于无证书的签密 (CL-SC) 方案解决了基于身份签密方案的密钥托管问题, 本文提出了改进的 CL-SC 机制, 在更强的敌手模型下, 证明了新方案能达到抗密钥托管、IND-CCA2 安全和 EUF-CMA 安全, 且效率更高。

参考文献:

[1] BONEH D, FRANKLIN M K. Identity-based encryption from the weil pairing[C]//Proc of CRYPTO. Berlin: Springer-Verlag, 2001: 213-229.

[2] MALONE-LEE J. Identity-based signcryption, Cryptology ePrint Archive, 2002/098[R/OL]. (2002-07-19). <http://eprint.iacr.org/2002/098>.

[3] BOYEN X. Multipurpose identity-based signcryption: a swiss army knife for identity-based cryptography[C]//Proc of CRYPTO. Berlin: Springer-Verlag, 2003: 383-399. (下转第 3822 页)

函数的性质可知,如果 $H''_n = H'_n$,则嵌入水印后的数据没有经过任何篡改,也意味着 $P'_n = P_n$,即原始数据得到了准确无误的恢复;否则,即便是 P'_n 经历了很微小的改动,也会导致提取的哈希值不匹配,即 $H''_n \neq H'_n$ 。

2 实验结果

在 Windows XP 平台上用 Visual C++ .NET 实现了本文算法。实验中采用了 MD5 哈希算法计算数字摘要,对任意长度的输入比特流产生固定长度为 128 bit 的数字摘要,用 LZW 编码方法进行数据的无损压缩。实验所用矢量图形是 shapefile 格式的河流图,含有 2 438 个坐标点,每个组至少含 500 个坐标点。图 1 为实验结果,其中,(a) 为原始矢量图形,(b) 为对应的嵌入水印后的矢量图形,两幅图之间的差异被严格控制在误差容限以内。只要含水印图形没有经过任何篡改,那么原始图形数据能够被准确无误地恢复出来。为了检验算法的检测及定位篡改位置的能力,对含水印图形的特定区域进行人为的改动(更改一些坐标点的坐标值、增加一些坐标点、删除一些坐标点),图 1(c) 显示了检测结果,对于没有改动的数据,原始数据仍被准确恢复,对于存在任何改动的数据,算法能够准确地检测出来,并用虚线标志出可能被修改的部分。

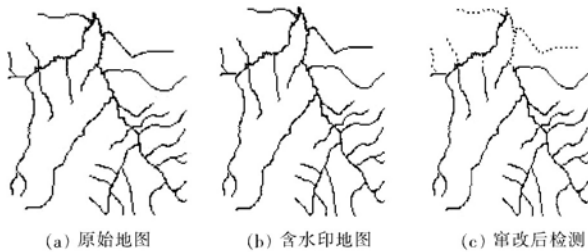


图 1 水印嵌入与检测实验结果

3 结束语

数字水印技术是近几年发展起来的新兴研究领域,针对矢量图形数据的数字水印技术研究相对较少。本文针对线状实体组成的矢量图形,提出将矢量图形中的线状实体分成不同的组,以组为计算单位将水印信息嵌入在矢量图形中,不仅能验证矢量图形的完整性,还能将篡改的定位能力精确到相应的分组,有效地克服了传统密码学认证方法的缺点。另外,水印信息的嵌入考虑了图形的误差容限,嵌入了水印信息的矢量图形仍有使用价值,在对数据精度要求极高的情况下,可以通过数据完整性验证提取出原始矢量图形数据,更好地满足了一些特殊应用的需求。

参考文献:

[1] 邵承永,王孝通. 矢量地图的安全问题与一种可逆数字水印认证方案[C]//全国博士学术论坛论文集. 2005:326-331.

(上接第 3802 页)

[4] YU Yong, YANG Bo, SUN Ying, et al. Identity based signcryption scheme without random oracles [J]. Computer Standard & Interfaces, 2009, 31(1): 56-62.
[5] AL-RIYAMI S S, PATERSON K G. Certificateless public key cryptography[C]//Advances in Cryptology, vol 2894. Berlin: Springer-Verlag, 2003:452-473.

[2] OHBUCHI R, UEDA H, ENDOH S. Robust watermarking of vector digital maps[C]//Proc of IEEE International Conference on Multimedia and Expo. 2002:577-580.
[3] SONNET H, ISENBERG T, DITTMANN J, et al. Illustration watermarks for vector graphic[C]//Proc of the 11th Pacific Conference on Computer Graphics and Applications. 2003:73-82.
[4] VOIGT M, BUSCH C. Watermarking 2D-vector data for geographical information system[C]//Proc of IS&T/SPIE Electron Imaging. 2002: 621-628.
[5] VOIGT M, BUSCH C. Feature-based watermarking of 2D-vector data [C]//Proc of SPIE. 2003:359-366.
[6] SCHULZ G, VOIGT M. A high capacity watermarking system for digital maps[C]//Proc of ACM Multimedia and Security Workshop. New York: ACM Press, 2004:180-186.
[7] 闵连权. 矢量地图数据的数字水印技术[J]. 测绘通报, 2007(1): 43-46.
[8] 李媛媛, 许录平. 用于矢量地图版权保护的数字水印[J]. 西安电子科技大学学报, 2004, 31(5): 719-723.
[9] 马桃林, 顾翀, 张良培, 等. 基于二维矢量数字地图的水印算法研究[J]. 武汉大学学报, 2006, 31(9): 792-794.
[10] 王勋, 林海, 鲍虎军. 一种鲁棒的矢量地图数字水印算法[J]. 计算机辅助设计与图形学学报, 2004, 16(10): 1377-1381.
[11] 朱长青, 杨成松. 一种抗数据压缩的矢量地图数据数字水印算法[J]. 测绘科学技术学报, 2006, 23(4): 281-283.
[12] SOLACHIDIS V, NIKOLAIDIS N, PITAS I. Fourier descriptors watermarking of vector graphics images[C]//Proc of International Conference on Image Processing. 2000:9-12.
[13] KITAMURA I, KANAI S, KISHINAMI T. Copyright protection of vector map using digital watermarking method based on discrete fourier transform[C]//Proc of IEEE International Geoscience and Remote Sensing. 2001:191-193.
[14] VOIGT M, YANG B, BUSCH C. Reversible watermarking of 2D-vector data[C]//Proc of ACM Multimedia and Security Workshop. New York: ACM Press, 2004:160-165.
[15] VOIGT M, YANG B, BUSCH C. High-capacity reversible watermarking for 2D-vector data[C]//Proc of the SPIE. 2005:409-417.
[16] 钟尚平, 高庆狮. 矢量地图水印归一化相关检测的可行性分析与改进[J]. 中国图象图形学报, 2006, 11(3): 401-409.
[17] 杨成松, 朱长青. 基于小波变换的矢量地理空间数据数字水印算法[J]. 测绘科学技术学报, 2007, 24(1): 37-39.
[18] 李媛媛, 许录平. 矢量图形中基于小波变换的盲水印算法[J]. 光子学报, 2004, 33(1): 97-100.
[19] KITAMURA I, KANAI S, KISHINAMI T. Watermarking vector digital map using wavelet transformation[C]//Proc of Annual Conference of Geographical Information Systems Association. 2000:417-421.
[20] 闵连权, 喻其宏. 基于离散余弦变换的数字地图水印算法[J]. 计算机应用与软件, 2007, 24(1): 146-148.
[21] 梅蕊蕊. 数字地图版权保护[D]. 西安: 西安电子科技大学, 2002.
[22] 邵承永, 王孝通, 徐晓刚, 等. 矢量地图的无损数据隐藏算法研究[J]. 中国图象图形学报, 2007, 12(2): 206-211.

[6] 王会歌, 王彩芬, 易玮, 等. 高效的无证书可公开验证签密方案[J]. 计算机工程, 2009, 35(5): 147-149.
[7] LIU Zhen-hua, HU Yu-pu, ZHANG Xiang-son, et al. Certificateless signcryption scheme in the standard model [J]. Information Sciences, 2010, 180(1): 452-464.
[8] SHACHAM H. New paradigms in signature schemes [D]. Stanford: Stanford University, 2005.