

标准模型下可证安全的多身份单密钥解密方案

明 洋¹ 王育民² 庞辽军²

(长安大学信息工程学院 西安 710064)¹

(西安电子科技大学 ISN 国家重点实验室 西安 710071)²

摘 要 多身份单密钥解密方案是基于身份加密方案的一个变体,用户的一个解密密钥可以对应于多个公钥(身份),即单一的密钥可以解密多个不同公钥加密下的密文。在双线性对,提出标准模型下可证安全的多身份单密钥解密方案。在判定性 q -TBDHE 假设下,证明了所提方案在适应性选择密文和身份攻击下是不可区分的。

关键词 多身份单密钥解密,基于身份加密,标准模型,双线性对

中图法分类号 TP918.1

文献标识码 A

Provably Secure Multi-identity Single-key Decryption Scheme in the Standard Model

MING Yang¹ WANG Yu-min² PANG Liao-jun²

(School of Information Engineering, Chang'an University, Xi'an 710064 China)¹

(State Key Lab. of Integrated Service Networks, Xidian University, Xi'an 710071, China)²

Abstract Multi-Identity Single-Key Decryption (MISKD) scheme is a variant of Identity-Based Encryption (IBE) where a private decryption key can map multiple public keys (identities). More exactly, a single private key can be used to decrypt multiple ciphertexts encrypted with different public keys. Based on the bilinear pairings, the MISKD scheme was presented and was provably secure in the standard model. The proposed scheme was proven secure against indistinguishably in adaptively chosen ciphertext and identity under the decision q -TBDHE assumption.

Keywords Multi-identity single-key decryption, Identity-based encryption, Standard model, Bilinear pairings

1 引言

为了简化公钥证书的管理,避免基于目录的公钥认证框架的束缚,1984年 Shamir^[1]提出基于身份公钥密码系统(Identity Based Public Key Cryptosystem-ID-PKC)的概念,同时给出基于身份的签名方案。在这个系统中,直接使用用户的身份信息(如IP地址、电子邮件等等)作为公钥,而私钥由可信第三方——密钥生成器(Private Key Generator-PKG)生成,因此基于身份密码系统可以很自然地解决公钥和实体身份的绑定问题。自提出基于身份密码系统后,直到2001年, Boneh 和 Franklin^[2]两位学者利用双线性对提出实际的基于身份加密(IBE)方案,并在随机预言机模型中证明该方案在适应性选择密文和身份攻击下是不可区分的(IND-ID-CCA2)。自从该方案提出后,又提出了大量基于身份的加密方案^[3-6]。

考虑现实中的情景:一个用户可以成为多个公司(n 个)的顾问,这里每个公司均采用通常 IBE 方案,用户拥有每个公司提供的 Email 地址(公钥)。采用通常 IBE 的方法,用户只有拥有每个公钥相对应的私钥(n 个)时,才能够和每个公司进行保密通信,从而大大地增加了用户的负担。基于此, Guo 等^[7]在 2007 年提出多身份单密钥解密的概念,同时基于

q -BSDH 假设,给出随机预言机(Random Oracle)模型中可证安全的方案。在这个方案中,用户仅仅拥有一个私钥就能够解密不同公司发送来的加密消息。

随机预言机模型中,hash 函数被看作为一个完全随机的理想模型,这是一个很强的要求。在随机预言机模型下是可证安全的方案,但在具体应用中却无法构造出相应的实例。因此 Guo 等^[8]在 DBDH 假设下提出标准模型(不使用随机预言机)中可证安全的多身份单密钥解密方案。但该方案的安全性是基于弱 Selective-ID 模型的,该模型需要攻击者在安全性证明之前先确定挑战目标的身份。同时,为了 CCA 的安全性,使用了 Canetti 等^[9]提出的方法(使用一次不可伪造签名),但这大大增加了系统的复杂性。

本文首次提出标准模型中适应性选择身份(Adaptive-ID)模型下(攻击者可以适应性选取挑战目标的身份)可证安全的多身份单密钥解密方案。基于判定性 q -TBDHE 假设,证明了所提方案在适应性选择密文和身份攻击下是不可区分的(IND-ID-CCA2)。同时所提方案中不需要使用不可伪造的一次签名,而直接取得选择密文攻击下(CCA)的安全性,因此所提方案更加有效。

2 基础知识

2.1 双线性对

到稿日期:2009-04-17 返修日期:2009-06-26 本文受国家自然科学基金(60803151)资助。

明 洋(1979—),男,博士,讲师,主要研究方向为密码学、信息安全, E-mail: yangming@chd.edu.cn; 王育民(1936—),男,教授,博士生导师,主要研究方向为密码学、信息安全; 庞辽军(1979—),男,博士,副教授,主要研究方向为密码学、信息安全。

设 $(G_1, +)$ 是由 g 生成的加法群,其阶数为素数 p ; $(G_2, \cdot)$ 是乘法群,阶数也为 p 。设 $e: G_1 \times G_1 \rightarrow G_2$ 是一个映射,具有下面的性质:

1) 双线性性: 对所有的 $u, v \in G_1, a, b \in Z_p$, 都有 $e(u^a, v^b) = e(u, v)^{ab}$ 。

2) 非退化性: $e(g, g) \neq 1$ 。

3) 可计算性: 对所有的 $u, v \in G_1$, 存在有效的算法计算 $e(u, v)$ 。

那么 e 称为双线性对。

2.2 困难问题

q-TBDHE 问题: 给定 $(g', g, g^a, g^{a^2}, \dots, g^{a^q}) \in G_1^{q+1}$, 这里 $a \in Z_p^*$, 计算 $e(g', g)^{a^{q+1}}$ 。

判定性 q-TBDHE 问题: 给定 $(g', g, g^a, g^{a^2}, \dots, g^{a^q}, Z) \in G_1^{q+1} \times G_2$, 判定 $e(g', g)^{a^{q+1}} = Z$ 是否成立。

3 多身份单密钥解密形式化定义和安全模型

3.1 形式化定义

多身份单密钥解密方案包含以下 4 个多项式时间算法。

系统建立算法: 输入系统参数 1^k , 输出主密钥 Φ 和系统参数 ψ 。

密钥生成算法: 输入主密钥 Φ 和多身份 $I_s = \langle I_1, I_2, \dots, I_l \rangle (1 \leq l \leq n)$, 输出密钥 d_{I_s} 。

加密算法: 输入系统参数 ψ 、消息 m 和身份 $I_i \in I_s$, 输出密文 C 。

解密算法: 输入系统参数 ψ 、 $\langle I_i, C \rangle$ 、密钥 d_{I_i} 和其它身份 $\langle I_1, \dots, I_{i-1}, I_{i+1}, \dots, I_l \rangle$, 输出消息 m 。

3.2 安全模型

为了说明多身份单密钥解密方案在适应性选择密文和身份攻击下的不可区分性(IND-ID-CCA2), 考虑下述攻击者 A 和挑战者 C 之间的交互游戏。

系统建立: 挑战者 C 运行系统建立算法, 将系统参数 ψ 返回给 A, 秘密保存主密钥 Φ 。

阶段 1 攻击者 A 能够适应性进行多项式有界次以下询问:

私钥询问: 当询问身份 $I_s = \langle I_{i+1}, \dots, I_{i+l} \rangle (1 \leq l \leq n)$ 的密钥时, C 运行密钥生成算法, 生成私钥 d_{I_s} , 返回给攻击者 A。

解密询问: 当询问 $\langle I_i, C_i; I_s \rangle$ 时, C 首先运行密钥生成算法得到私钥 d_{I_i} , 然后运行解密算法, 解密 $\langle I_i, C_i \rangle$ 得到相应的明文, 返回给 A。

挑战: 当 A 决定结束阶段 1 后, 返回两个等长的明文 m_0, m_1 给 C。C 选取一个随机比特 $b \in \{0, 1\}$, 定义挑战 $C^* = \text{Encrypt}(\psi, I^*, m_b)$ 并返回给 A。

阶段 2 和阶段 1 相同, A 对 I^* 不能进行私钥询问($I^* \notin I_i$), 对 $\langle I^*, C^* \rangle$ 不能进行解密询问。

猜测: 最后, A 输出猜测 $b' \in \{0, 1\}$ 。如果 $b' = b$, 则 A 赢得游戏。

定义上述的攻击者 A 为 IND-ID-CCA2 攻击者, 则 A 攻破上述游戏的优势为 $\text{Adv} = |\Pr[b' = b] - 1/2|$ 。

4 提出的方案

基于文献[10]中的方法, 本节给出标准模型下可证安全

的多身份单密钥解密方案, 具体如下。

系统建立: 随机选取 $g, g_2, g_3, h_1, h_2 \in G_1, a \in Z_p^*$, 抗碰撞哈希函数 $H_1: \{0, 1\}^* \rightarrow Z_p^*, H_2: \{0, 1\}^* \rightarrow Z_p^*$ 。定义 $g_1 = g^a$ 。随机选取 $k_1, k_2, \dots, k_n$ 满足 $k_i = g^{k_i} (1 \leq i \leq n)$ 。选取 $f(x) = ax + b$, 其中 $a, b \in Z_p^*$ 。如果 $g_2 = g_3^{-a}$ 或 $h_1 = g_3^{-b}$, 重新选取 $f(x)$, 则系统参数为 $\psi = (g, g_1, g_2, g_3, h_1, h_2, H_1, H_2, f(x), k_1, k_2, \dots, k_n)$, 主密钥为 $\Phi = a$ 。

密钥生成: 对于身份 $I_s = \langle I_1, \dots, I_l \rangle (1 \leq l \leq n)$ 随机选取 $r', r'' \in Z_p^*$, 计算 $d_{I_s} = (d_1, d_2, d_2) = ((h_1 g_2^{r'} g_3^{f(r')})^a (h_2 k_1^{r'} k_2^{r''} \dots k_l^{r'})^{r'}, g^{r'}, r')$ 。

加密: 在 $I_i \in I_s$ 下对消息 $m \in G_2$ 进行加密, 随机选取 $s \in Z_p^*$, 计算

$$C_1 = (h_2 k_1^{s_i})^s$$

$$C_{2,1} = k_1^s, \dots, C_{2,i-1} = k_{i-1}^s, C_{2,i+1} = k_{i+1}^s, \dots, C_{2,n} = k_n^s$$

$$C_3 = g^s, C_4 = e(g_1, g_2)^s$$

$$C_5 = e(g_1, g_3)^s, C_6 = e(g_1, h_1)^{s+\eta} \cdot M$$

其中, $\eta = H_1(C_1, C_{2,1}, \dots, C_{2,i-1}, C_{2,i+1}, \dots, C_{2,n}, C_3, C_4, C_5, e(g_1, h_1)^s)$,

$$h = H_2(C_1, C_{2,1}, \dots, C_{2,i-1}, C_{2,i+1}, \dots, C_{2,n}, C_3, C_4, C_5, C_6, M, M \cdot e(g_1, h_1)^s),$$

则密文为 $C = (C_1, C_{2,1}, \dots, C_{2,i-1}, C_{2,i+1}, \dots, C_{2,n}, C_3, C_4, C_5, C_6, h)$ 。

解密: 身份 $I_s = \langle I_1, \dots, I_l \rangle (1 \leq l \leq n)$ 下消息 m 的密文 C 解密如下:

1) 计算 $K = C_1 \cdot C_{2,1}^{d_1} C_{2,2}^{d_2} \dots C_{2,i-1}^{d_{i-1}} C_{2,i+1}^{d_{i+1}} \dots C_{2,l}^{d_l} = (h_2 k_1^{s_1} \dots k_l^{s_l})^s$ 。

2) 计算

$$\begin{aligned} & \frac{e(d_1, C_3)}{C_4^s C_5^{f(d_3)} e(K, d_2)} \\ &= \frac{e((h_1 g_2^{r'} g_3^{f(r')})^a (h_2 k_1^{r'} k_2^{r''} \dots k_l^{r'})^{r'}, g^s)}{e(g_1, g_2)^s e(g_1, g_3)^{sf(r')} e((h_2 k_1^{r'} k_2^{r''} \dots k_l^{r'})^s, g^{r'})} \\ &= \frac{e(g^s, h_1^s) e(g^s, g_2^{r'}) e(g^s, g_3^{f(r')}) e(g^s, (h_2 k_1^{r'} k_2^{r''} \dots k_l^{r'})^s)}{e(g^a, g_2)^s e(g^a, g_3)^{sf(r')} e((h_2 k_1^{r'} k_2^{r''} \dots k_l^{r'})^s, g^{r'})} \\ &= e(g_1, h_1)^s, \end{aligned}$$

$\eta = H_1(C_1, C_{2,1}, \dots, C_{2,i-1}, C_{2,i+1}, \dots, C_{2,n}, C_3, C_4, C_5, e(g_1, h_1)^s)$ 。

3) 计算 $\frac{C_6}{e(g_1, h_1)^{\eta} e(g_1, h_1)^s} = M$ 。

4) 计算 $h' = H_2(C_1, C_{2,1}, \dots, C_{2,i-1}, C_{2,i+1}, \dots, C_{2,n}, C_3, C_4, C_5, C_6, M, \frac{C_6}{e(g_1, h_1)^{\eta}})$, 检验 $h' = h$ 是否成立。如果成立, 密文是有效的; 否则解密者返回错误信息。

5 所提方案的分析

定理 1 如果攻击者 A 在时间 t' 内进行 q_k 次密钥询问、 q_d 次解密询问后, 能够以不可忽略的概率 ϵ' 攻破方案的不可区分性, 那么存在一个算法 B, 以 $t = t' + O(t_e q_l) + O(t_p q)$, $\epsilon \geq \epsilon' - \frac{1}{p-1}$ 解判定性 q-TBDHE 问题, 这里 t_e 表示群 G_1 中计算一个指数时间, t_p 表示计算一个对的时间。

证明: 算法 B 把 A 作为子程序来解决一个随机的判定性 q-TBDHE 问题的实例, 即给定 $(g', g, g^a, g^{a^2}, \dots, g^{a^q}, Z)$ 下判定 $e(g', g)^{a^{q+1}} = Z$ 是否成立。

算法 B 模拟不可区分性游戏中的挑战者 C 和攻击者 A 交互如下。

系统建立: B 随机选取 $\gamma, \beta_1, \beta_2, \dots, \beta_n \in Z_p^*$, q 次多项式 $f_1(x), f_2(x), f_3(x) \in Z_p[x]$, 这里 $f_1(x) = \sum_{i=0}^q a_i x^i, f_2(x) = \sum_{i=0}^q b_i x^i, f_3(x) = \sum_{i=0}^q c_i x^i$ 。令 $g_1 = g^a, h_1 = g^{f_1(a)}, g_2 = g^{f_2(a)}, g_3 = g^{f_3(a)}, h_2 = g^\gamma, f(x) = -\frac{b_q}{c_q}x - \frac{a_q}{c_q}, k_i = g^{\beta_i} (i=1, \dots, n)$ 。B 返回系统参数 $\psi = (g, g_1, g_2, g_3, h_1, h_2, f(x), k_1, k_2, \dots, k_n)$ 给 A。

阶段 1 攻击者 A 适应性进行多项式有界次以下询问:

密钥询问: 当 A 询问 $I_s = \langle I_1, \dots, I_l \rangle (1 \leq l \leq n)$ 的私钥时, B 执行以下操作:

- 1) 如果 $I = \alpha$, B 直接使用 α 解判定性 q-TBDHE 问题。
- 2) 如果 $I \neq \alpha$, B 随机选取 $r', r'' \in Z_p^*$, 计算

$$d_1 = (g_{i=0}^{q-1} (a_i + r'b_i + f(r')c_i) a^{i+1}) \cdot (h_2 k_1^{I_1} k_2^{I_2} \dots k_l^{I_l})^{r'}$$

$$d_2 = g^{r'}, d_3 = r'$$

如果 $h_1 g_2^{r'} g_3^{f(r')} = 1$, B 重新选取 $r' \in Z_p^*$ 。

正确性: 由 $f(r') = -\frac{b_q}{c_q}r' - \frac{a_q}{c_q}$ 可知 $a_q + b_q r' + c_q f(r') = 0$ 。

$$\begin{aligned} & g_{i=0}^{q-1} (a_i + r'b_i + f(r')c_i) a^{i+1} \\ &= g^{(a_0 a + a_1 a^2 + \dots + a_{q-1} a^q) + (b_0 a + b_1 a^2 + \dots + b_{q-1} a^q) r'} \cdot \\ & g^{(c_0 a + c_1 a^2 + \dots + c_{q-1} a^q) f(r') + (a_q + b_q r' + c_q f(r')) a^{q+1}} \\ &= g^{(a_0 a + a_1 a^2 + \dots + a_{q-1} a^q + a_q a^{q+1}) + (b_0 a + b_1 a^2 + \dots + b_{q-1} a^q + b_q a^{q+1}) r'} \cdot \\ & g^{(c_0 a + c_1 a^2 + \dots + c_{q-1} a^q + c_q a^{q+1}) f(r')} \\ &= g^{(a_0 + a_1 a + \dots + a_{q-1} a^{q-1} + a_q a^q) a + (b_0 + b_1 a + \dots + b_{q-1} a^{q-1} + b_q a^q) r'} \cdot \\ & g^{(c_0 + c_1 a + \dots + c_{q-1} a^{q-1} + c_q a^q) f(r')} \\ &= (g^{f_1(x)} g^{f_2(x) r'} g^{f_3(x) f(r')})^a \\ &= (h_1 g_2^{r'} g_3^{f(r')})^a \end{aligned}$$

$$\begin{aligned} d_1 &= (g_{i=0}^{q-1} (a_i + r'b_i + f(r')c_i) a^{i+1}) \cdot (h_2 k_1^{I_1} k_2^{I_2} \dots k_l^{I_l})^{r'} \\ &= (h_1 g_2^{r'} g_3^{f(r')})^a \cdot (h_2 k_1^{I_1} k_2^{I_2} \dots k_l^{I_l})^{r'} \end{aligned}$$

解密询问: 攻击者 A 对 (C, I_s) 进行解密询问, B 执行以下操作: B 首先对 I_s 运行密钥生成算法, 得到 d_{I_s} , 然后运行解密算法。如果通过验证, B 返回 A 相应的明文, 否则输出错误信息。

挑战: 当 A 决定结束阶段 1 后, 发送 $(I_s^* = \langle I_1^*, I_2^*, \dots, I_l^* \rangle, m_0, m_1)$ 给 B, B 随机选取 $b \in \{0, 1\}$ 计算 $C_1^* = (g')^\gamma \prod_{i=1}^l (g')^{\beta_i I_i^*}, C_{2,1}^* = (g')^{\beta_1}, \dots, C_{2,i-1}^* = (g')^{\beta_{i-1}}, C_{2,i+1}^* = (g')^{\beta_{i+1}}, \dots, C_{2,n}^* = (g')^{\beta_n}, C_3^* = g', C_4^* = Z^{b_q} \cdot e(g', g)^{\sum_{i=0}^{q-1} b_i a^{i+1}}, C_5^* = Z^{c_q} \cdot e(g', g)^{\sum_{i=0}^{q-1} c_i a^{i+1}}, C_6^* = m_b$ 。

$$\frac{e(d_1^*, C_3^*)}{(C_1^*)^{d_3^*} (C_5^*)^{f(d_3^*)} e(C_1^*, d_2^*)} \cdot e(g_1, h_1)^{\eta^*},$$

$$\eta^* = H_1(C_1^*, C_{2,1}^*, \dots, C_{2,i-1}^*, C_{2,i+1}^*, \dots, C_{2,n}^*, C_3^*, C_4^*, C_5^*,$$

$$\frac{e(d_1^*, C_3^*)}{(C_1^*)^{d_3^*} (C_5^*)^{f(d_3^*)} e(C_1^*, d_2^*)})$$

$$h^* = H_2(C_1^*, C_{2,1}^*, \dots, C_{2,i-1}^*, C_{2,i+1}^*, \dots, C_{2,n}^*, C_3^*, C_4^*, C_5^*, C_6^*, m_b, m_b \cdot \frac{e(d_1^*, C_3^*)}{(C_1^*)^{d_3^*} (C_5^*)^{f(d_3^*)} e(C_1^*, d_2^*)})$$

B 返回 $C^* = (C_1^*, C_{2,1}^*, \dots, C_{2,i-1}^*, C_{2,i+1}^*, \dots, C_{2,n}^*, C_3^*, C_4^*,$

$C_5^*, C_6^*, h^*)$ 给攻击者 A。

正确性: 令 $s^* = \log_{g'} g', Z = e(g, g')^{a^{q+1}}$, 则

$$\begin{aligned} & \frac{e(d_1^*, C_3^*)}{(C_1^*)^{d_3^*} (C_5^*)^{f(d_3^*)} e(C_1^*, d_2^*)} \\ &= \frac{e((h_1 g_2^{r'} g_3^{f(r')})^a)}{(Z^{b_q} \cdot e(g', g)^{\sum_{i=0}^{q-1} b_i a^{i+1}})^{r'} (Z^{c_q} \cdot e(g', g)^{\sum_{i=0}^{q-1} c_i a^{i+1}})^{f(r')}} \cdot \\ & \frac{(h_2 k_1^{I_1^*} k_2^{I_2^*} \dots k_l^{I_l^*})^{r'}}{e((g')^\gamma \prod_{i=1}^l (g')^{\beta_i I_i^*}, g^{r'})} \\ &= \frac{e(h_1, g')^a \cdot e(g_2^{r'}, g')^a \cdot e(g_3^{f(r')}, g')^a}{Z^{b_q r'} \cdot e(g', g)^{r'(b_0 + b_1 a + \dots + b_{q-1} a^{q-1})} \cdot e(g', g)^{-b_q a^{q+1} r'} \cdot Z^{c_q f(r')}} \cdot \\ & \frac{e((h_2 k_1^{I_1^*} k_2^{I_2^*} \dots k_l^{I_l^*})^{r'}, g')}{e(g', g)^{f(r')(c_0 + c_1 a + \dots + c_{q-1} a^{q-1})} \cdot e((h_2 k_1^{I_1^*} k_2^{I_2^*} \dots k_l^{I_l^*})^s, g')} \\ &= \frac{1}{e(g', g)^{-c_q a^{q+1} f(r')}} \cdot \frac{e(h_1, g')^a \cdot e(g_2^{r'}, g')^a \cdot e(g_3^{f(r')}, g')^a}{Z^{b_q r'} \cdot e(g', g)^{r' f_2(a) a} \cdot e(g', g)^{-b_q a^{q+1} r'} \cdot Z^{c_q f(r')}} \cdot \\ & \frac{1}{e(g', g)^{f(r') f_3(a) a} \cdot e(g', g)^{-c_q a^{q+1} f(r')}} \\ &= \frac{e(h_1, g')^a}{Z^{b_q r'} \cdot e(g', g)^{-b_q a^{q+1} r'} \cdot Z^{c_q f(r')} \cdot e(g', g)^{-c_q a^{q+1} f(r')}} \\ &= Z^{b_q} \cdot \frac{e(g, g')^{a(a_0 + a_1 a + \dots + a_q a^q)}}{e(g', g)^{-b_q a^{q+1} r'} \cdot e(g', g)^{-c_q a^{q+1} f(r')}} \\ &= Z^{b_q} \cdot e(g, g')^{\sum_{i=0}^{q-1} a_i a^{i+1}} \end{aligned}$$

阶段 2 和阶段 1 相同。A 对 I_s^* 不能进行私钥询问, 对 $\langle I_s^*, C^* \rangle$ 不能进行解密询问。

猜测: A 输出 b' 。如果 $b' = b$, B 输出 1; 否则输出 0。

概率分析: 如果 $Z = e(g, g')^{a^{q+1}}$, B 模拟的挑战密文和真实密文具有相同的分布, 因此 A 正确猜测比特 b 的概率为 $1/2 + \epsilon'$, 即 $\Pr[B(g', g, g^a, \dots, g^{a^q}, e(g, g')^{a^{q+1}}) = 0] \geq 1/2 + \epsilon'$; 如果 Z 是群 G_1 中的随机元素, 则 $(C_1^*, C_{2,1}^*, \dots, C_{2,i-1}^*, C_{2,i+1}^*, \dots, C_{2,n}^*, C_3^*, C_4^*, C_5^*, C_6^*, h^*)$ 均是随机元素, 因为 $s^* = \log_{g'} g'$ 是随机元素, η^* 是均匀随机的, 所以 $s^* + \eta^* = 0$ 的概率为 $\frac{1}{p-1}$ 。

假设没有等于 α 的身份进行询问, 则 $\Pr[B(g', g, g^a, \dots, g^{a^q}, Z) = 0] \geq \frac{1}{2} + \frac{1}{p-1}$ 。

因此, 算法 B 解判定性 q-TBDHE 问题的优势 Adv_B 为

$$Adv_B = |\Pr[B(g', g, g^a, \dots, g^{a^q}, e(g, g')^{a^{q+1}}) = 0] -$$

$$\Pr[B(g', g, g^a, \dots, g^{a^q}, Z) = 0]|$$

$$\geq |\frac{1}{2} + \epsilon' - \frac{1}{2} - \frac{1}{p-1}| \geq \epsilon' - \frac{1}{p-1}$$

在上述模拟中, B 的运行时间为解困难问题时间以及回答密钥和解密询问的时间。每次密钥询问需要群 G_1 中 $O(l)$ 次指数运算, 每次解密询问需要群 G_1 中 $O(l)$ 次指数运算和 $O(1)$ 次对运算。因为 A 最多进行 $q-1$ 次询问, 所以 $t = t' + O(\epsilon_q l) + O(\epsilon_p q)$ 。

结束语 多身份单密钥解密方案在现实中具有广泛的应用。用户仅仅使用单一的密钥便可解密在多个不同身份(公钥)加密下的密文。本文基于双线性对提出标准模型下可证

(下转第 85 页)

(f_u)).

3) $P_{NCC} \rightarrow P_{Ui}$: P_{NCC} 收到 ($sid, r_{ui} \parallel v_2, v_4 \oplus f_u, v_4 \oplus H(f_u)$), 利用 r_{ui} 查找数据库获得相应的秘密信息 (ID_{ui}, r_{ui}, k_i), 然后计算: $V^* \leftarrow F(k_i, r_{NCC} \parallel r_{ui})$; 如果查找不到相应的信息, 那么根据数据库中记录的所有更新前的三元组中的密钥 k_i' 逐个计算 $V^* \leftarrow F(k_i', r_{NCC} \parallel r_{ui})$ 。将 V^* 分离为 $V^* = v_1^* \parallel v_2^* \parallel v_3^* \parallel v_4^*$, 假如 $v_2 = v_2^*$, 则 P_{NCC} 对 P_{Ui} 的认证成功并更改记录 (ID_{ui}, r_{ui}) 为 (ID_{ui}, v_1^*)。然后, P_{NCC} 计算: $f_u = v_4^* \oplus (v_4 \oplus f_u)$, $H(f_u) = v_4^* \oplus (v_4 \oplus H(f_u))$ 。接着, P_{NCC} 检查计算出的 $H(f_u)$ 是否正确。如果正确, P_{NCC} 开始计算: $f_c = g^b \bmod p$, 新的会话密钥 $k_i^* = f_u^a \bmod p = g^{ab} \bmod p$, 并计算 $v_4^* \oplus f_c, H(f_u \parallel k_i^* \parallel v_1^*)$ 。这里, v_1^* 是一个 P_{Ui} 新的临时身份。然后, P_{NCC} 把 (ID_{ui}, r_{ui}, k_i) 更新成 (ID_{ui}, v_1^*, k_i^*)。 P_{NCC} 向 P_{Ui} 发送 ($v_4^* \oplus f_c, H(f_u \parallel k_i^* \parallel v_1^*), v_3^*$)。

4) P_{Ui} 收到消息 ($v_4^* \oplus f_c, H(f_u \parallel k_i^* \parallel v_1^*), v_3^*$) 后, 计算 $f_c = v_4 \oplus (v_4^* \oplus f_c)$, $k_i^* = f_c^a \bmod p = g^{ab} \bmod p$ 。然后, P_{Ui} 检查是否 $H(f_u \parallel k_i^* \parallel v_1^*) = H(f_u \parallel k_i^* \parallel v_1)$, $v_3^* = v_3$ 。如果相等, P_{Ui} 相信 P_{NCC} 是合法的, 并且 k_i^* 是有效的。然后 P_{Ui} 更改记录 (ID_{ui}, r_{ui}, k_i) 为 (ID_{ui}, v_1, k_i^*)。

可以证明, 修改后的协议是 UC 安全的, 证明过程与文献 [10] 中的相同。

结束语 在认证协议设计过程中, 认证双方数据同步问题难于把握, 往往被忽视。对近来证明是 UC 安全的几个认证协议进行了分析, 指出了安全证明中存在的问题以及这些协议在数据同步方面的缺陷, 并给出了相应的修改, 以弥补存在的安全隐患。修改后的协议可以证明是 UC 安全的。

参考文献

[1] 邓森磊, 邱盟, 周利华. 基于串空间和状态转换的认证协议分析

方法[J]. 计算机科学, 2007, 34(10): 96-98

- [2] Lee S M, Hwang Y J, Lee D H. Efficient authentication for low-cost RFID systems[C]// International Conference on Computational Science and its Applications. IEEE Computer Society, 2005: 619-627
- [3] Henrici D, Muller P. Hash-based enhancement of location privacy for radio-frequency identification devices using varying identifiers [C]// 2nd IEEE Annual Conference on Pervasive Computing and Communications Workshops. IEEE Computer Society, 2005: 149-153
- [4] Osaka K, Takagi T, Yamazaki K, et al. An efficient and secure RFID security method with ownership transfer[C]// CIS. 2006: 778-787
- [5] Seo Y, Lee H, Kim K. A scalable and untraceable authentication protocol for RFID[C]// EUC Workshops. 2006: 252-261
- [6] Ha J, Moon S, Nieto J M G, et al. Low-cost and strong-security RFID authentication protocol[C]// EUC Workshops. 2007: 795-807
- [7] Deursen T, Radomirovic S. Attacks on RFID protocols [EB/OL]. <http://eprint.iacr.org/2008/310.pdf>
- [8] Canetti R. Universally composable security: A new paradigm for cryptographic protocols[C]// 42th IEEE Annual Symposium on Foundations of Computer Science. IEEE Computer Society, 2001: 136-145
- [9] Le T, Burmester M, Medeiros B. Universally composable and forward secure RFID authentication and authenticated key exchange[C]// 2nd ACM Symposium on Information, Computer and Communications Security. ACM Press, 2007: 242-252
- [10] 冯涛, 马建峰. UC 安全的移动卫星通信系统认证密钥交换协议[J]. 宇航学报, 2008, 29(6): 1959-1964

(上接第 75 页)

安全的多身份单密钥解密方案。在判定性 q-TBDHE 假设下, 证明了所提方案在适应性选择密文和身份攻击下是不可区分的。同时直接获得 CCA 的安全性, 因此方案更加有效。

参考文献

- [5] Waters B. Efficient identity-based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt'05. Aarhus, Denmark, LNCS 3494, Berlin: Springer-Verlag, 2005: 114-127
- [6] Gentry C. Practical Identity-based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt'06. Saint Petersburg, Russia, LNCS 4004, Berlin: Springer-Verlag, 2006: 445-464
- [7] Guo Fuchun, Mu Yi, Chen Zhide. Identity-based encryption: how to decrypt multiple ciphertexts using a single decryption key[C]// Pairing-based Cryptography-Pairing'07. Dublin, Ireland, LNCS 4575, Berlin: Springer-Verlag, 2007: 392-406
- [8] Guo Fuchun, Mu Yi, Chen Zhide, et al. Multi-identity single-key decryption without random oracles[C]// Inscrypt'07. Xining, China, LNCS 4990, Berlin: Springer-Verlag, 2007: 384-398
- [9] Canetti R, Halevi S, Kate J. A forward-secure public key encryption scheme[C]// Advances in Cryptology-Eurocrypt'03. Warsaw, Poland, LNCS 2656, Berlin: Springer-Verlag, 2003: 255-271
- [10] Ren Yanli, Gu Dawu. Secure Hierarchical Identity Based Encryption Scheme in the Standard Model[C]// INDOCRYPT 2008. Kharagpur, India, LNCS 5365, Berlin: Springer-Verlag, 2008: 104-115

- [1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Advances in Cryptology-Crypto'84. Santa Barbara, California, USA, LNCS 0196, Berlin: Springer-Verlag, 1984: 47-53
- [2] Boneh D, Franklin M. Identity-based encryption from the weil pairing [C]// Advances in Cryptology-Crypto'01. Santa Barbara, California, USA, LNCS 2139, Berlin: Springer-Verlag, 2001: 213-229
- [3] Boneh D, Boyen X. Efficient selective-ID secure identity based encryption without random oracles[C]// Advances in Cryptology-Eurocrypt'04. Interlaken, Switzerland, LNCS 3027, Berlin: Springer-Verlag, 2004: 223-238
- [4] Boneh D, Boyen X. Secure identity based encryption without random oracles[C]// Advances in Cryptology-Crypto'04. Santa Barbara, California, USA, LNCS 3152, Berlin: Springer-Verlag, 2004: 443-459