Journal of Computer Applications
计算机应用,2014,34(11):3291-3294
ISSN 1001-9081
CODEN JYIIDU
2014-11-10
http://www.joca.cn

文章编号:1001-9081(2014)11-3291-04
doi:10.11772/j.issn.1001-9081.2014.11.3291

基于身份的强不可伪造代理重签名方案

冯　婕[1*],蓝才会[1,2],郑伯荣[1]
(1.兰州城市学院 信息工程学院,兰州 730070;　2.西北师范大学 计算机科学与工程学院,兰州 730070)
(*通信作者电子邮箱 lzfenjie@163.com)

摘　要:针对代理重签名方案的存在性不可伪造问题,利用目标抗碰撞杂凑函数和双线性映射,提出了一种基于身份的双向代理重签名方案。在计算 Diffie-Hellman 困难问题的假设下,证明了该方案在适应性选择消息攻击下是强不可伪造的。所提方案的系统参数和重签名的长度短,重签名的计算量小,解决了现有代理重签名方案中存在的密钥管理复杂和安全性低等问题。

关键词:基于身份的代理重签名;强不可伪造性;不可伪造性;双线性对;双向性
中图分类号:TP309.7　　**文献标志码**:A

ID-based proxy re-signature scheme with strong unforgeability

FENG Jie[1*], LAN Caihui[1,2], JIA Borong[1]
(1. *School of Information Science and Engineering, Lanzhou City University, Lanzhou Gansu* 730070, *China*;
2. *College of Computer Science and Engineering, Northwest Normal University, Lanzhou Gansu* 730070, *China*)

Abstract: Concerning the problem that ID-based proxy re-signature schemes are existentially unforgeable, an ID-based bidirectional proxy re-signature scheme was proposed by using target collision-resistant Hash function and bilinear pairing. Under computational Diffie-Hellman assumption, the proposed proxy re-signature scheme is provably secure against strongly forgery under adaptive chosen message attacks. Moreover, the proposed scheme has short system parameters, short re-signature, low re-signing computation cost and high security. The proposed scheme solves the existing proxy re-signature in the presence of low security and complex key management.

Key words: ID-based proxy re-signature; strong unforgeability; unforgeability; bilinear pairing; bidirectionality

0　引言

基于身份的代理重签名方案不仅能实现受托者和委托者之间的签名转换,还能有效解决公钥与实体身份的绑定问题,在跨域身份认证[1]、数据交换系统[2]和构造审查系统[3-4]等方面有广泛的应用前景。Shao 等[5]提出了一个基于身份的双向代理重签名方案(下文简称 Shao 方案),但该方案的系统公开参数太长。为了克服该方案存在的参数过长问题,Hu 等[6]提出了一个较短公开参数的基于身份代理重签名方案(下文简称 Hu 方案),但该方案的安全性基于较强的 q-SDH 困难问题假设[7-8],并且重签名的长度比 Shao 方案多两个群元素。然而,这两个方案均满足强不可伪造性[9-10],攻击者利用已有的消息和相应的签名,可以伪造一个该消息的新签名。强不可伪造性具有更强的安全性[11-12],保证敌手不仅无法伪造新的消息的签名,也不能伪造已经签名的消息的合法签名,可有效防止电子投票、电子现金和数字版权等的篡改。针对这两个方案的安全缺陷,本文利用较弱的基于密钥的目标抗碰撞(Target Collision Resistant,TCR)杂凑函数[13],提出一个新的基于身份的双向代理重签名方案。本文方案满足强不可伪造性,并在系统公开参数长度、重签名长度和计算代价等方面具有较大的优势。

1　预备知识

1.1　双线性映射

设 p 是一个大素数,G_1 和 G_2 均为 p 阶的循环群,g 是 G_1 的生成元,双线性映射 $\hat{e}:G_1\times G_1\rightarrow G_2$ 是满足以下条件的一个映射:

1)双线性性。对任意的 $a,b\in \mathbf{Z}_p$,有 $\hat{e}(g^a,g^b)=\hat{e}(g,g)^{ab}$。

2)非退化性。$\hat{e}(g,g)\neq 1_{G_2}$,其中 1_{G_2} 是 G_2 的单位元。

3)可计算性。对任意的 $g_1,g_2\in G_1$,存在一个有效的算法计算 $\hat{e}(g_1,g_2)$。

1.2　计算 Diffie-Hellman 问题

设 G_1 是阶为素数 p 的循环群,g 是 G_1 的生成元,计算 Diffie-Hellman(Computational Diffie-Hellman,CDH)问题为:给定 $(g,g^a,g^b)\in G_1^3$,计算 $g^{ab}\in G_1$,其中 $a,b\in_R \mathbf{Z}_p$ 未知。

定义 1　CDH 假设。如果不存在一个概率多项式时间算法在时间 t 内以至少 ε 的概率解决群 G_1 上的 CDH 问题,则称群 G_1 上的 (t,ε)-CDH 假设成立[5]。

1.3　TCR 杂凑函数

假设 M_1 和 M_2 分别为 TCR 杂凑函数的输入和输出消息空

收稿日期:2014-05-16;**修回日期**:2014-07-14。
基金项目:国家自然科学基金资助项目(61262057,61163038,61063041);甘肃省科技计划项目(145RJDA325);国家档案局科技计划项目(2014-X-33);甘肃省自然科学基金资助项目(1308RJYA039);兰州市科技计划项目(2013-4-22)。
作者简介:冯婕(1976-),女,甘肃定西人,讲师,硕士,主要研究方向:信息管理、信息系统;　蓝才会(1977-),男,江西永丰人,副教授,博士,主要研究方向:代理重加密;　郑伯荣(1973-),女,安徽蒙城人,副教授,主要研究方向:网络信息系统。

间,K 为密钥空间,其中 $k \in K$,利用下面的游戏定义一个 TCR 杂凑函数 $H_k: K \times M_1 \to M_2$ 的安全性:敌手首先输出消息 $m_1 \in M_1$;挑战者然后随机选取 $k \in K$,并将 k 发送给敌手;最后敌手输出消息 $m_2 \in M_1$。如果 $H_k(m_1) = H_k(m_2)$ 且 $m_1 \neq m_2$,则敌手赢得游戏。

定义 2 如果敌手在多项式时间 t 内赢得上述游戏的概率 ε 是可忽略的,那么称 TCR 杂凑函数 H_k 是 (t,ε) 安全的[13]。

2 新的基于身份双向代理重签名方案

2.1 方案描述

利用 TCR 杂凑函数,构造一个新的基于身份双向代理重签名方案,具体描述如下:

1) 系统参数生成算法(Setup)。群 (G_1,G_2) 的定义如 1.1 节所示,在 G_1 中随机选取 7 个元素 $g_2, v_{ID}, v_m, ID_0, ID_1, m_0$ 和 m_1;K 为 TCR 杂凑函数的密钥空间,选取两个函数 $H_{k_{ID}}: \{0,1\}^* \to \mathbf{Z}_p$ 和 $H_{k_m}: \{0,1\}^* \to \mathbf{Z}_p$,其中 $k_m, k_{ID} \in K$;任选一个随机数 $\alpha \in \mathbf{Z}_p^*$,计算 $g_1 = g^\alpha$。公开系统参数 $cp = (G_1, G_2, p, \hat{e}, g, g_1, g_2, v_{ID}, v_m, ID_0, ID_1, m_0, m_1, k_m, k_{ID}, H_{k_m}, H_{k_{ID}})$,秘密保存密钥生成中心 PKG 的主密钥 $mk = \alpha$。

2) 密钥提取算法(Extract)。给定一个身份 ID,PKG 随机选取 $r_{ID} \in \mathbf{Z}_p^*$,计算 $d_{ID_1} = g^{r_{ID}}$ 和 $h_{ID} = H_{k_{ID}}(ID \| d_{ID_1}) = H_{k_{ID}}(ID \| g^{r_{ID}})$,并检查 h_{ID} 的最右边比特值 $u_{ID} \in \{0,1\}$,输出 ID 对应的私钥 $d_{ID} = (d_{ID_1}, d_{ID_2}) = (g^{r_{ID}}, g_2^\alpha (ID_{u_{ID}} v_{ID}^{h_{ID}})^{r_{ID}})$。

3) 重签名密钥生成算法(ReKey)。输入受托者的私钥 $d_A = (d_{A_1}, d_{A_2}) = (g^{r_A}, g_2^\alpha (ID_{u_A} v_{ID}^{h_A})^{r_A})$ 和委托者的私钥 $d_B = (d_{B_1}, d_{B_2}) = (g^{r_B}, g_2^\alpha (ID_{u_B} v_{ID}^{h_B})^{r_B})$,输出代理者的重签名密钥 $rk_{A\to B} = (rk_{A\to B}^1, rk_{A\to B}^2) = (d_{B_1}/d_{A_1}, d_{B_2}/d_{A_2}) = (g^{r_B}/g^{r_A}, (ID_{u_B} v_{ID}^{h_B})^{r_B}/(ID_{u_A} v_{ID}^{h_A})^{r_A})$。

4) 签名生成算法(Sign)。对于待签名的消息 M,签名者首先随机选取 $s_1 \in \mathbf{Z}_p^*$,然后计算 $\sigma_3 = g^{s_1}$ 和 $h = H_{k_m}(M \| \sigma_3)$,并检查 h 的最右边比特值 $u \in \{0,1\}$;利用私钥 $d_{ID} = (d_{ID_1}, d_{ID_2}) = (g^{r_{ID}}, g_2^\alpha (ID_{u_{ID}} v_{ID}^{h_{ID}})^{r_{ID}})$ 计算 $\sigma_2 = d_{ID_2} (m_u v_m^h)^{s_1} = g_2^\alpha (ID_{u_{ID}} v_{ID}^{h_{ID}})^{r_{ID}} (m_u v_m^h)^{s_1}$,输出消息 M 的签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3) = (d_{ID_1}, g_2^\alpha (ID_{u_{ID}} v_{ID}^{h_{ID}})^{r_{ID}} (m_u v_m^h)^{s_1}, g^{s_1}) = (g^{r_{ID}}, g_2^\alpha (ID_{u_{ID}} v_{ID}^{h_{ID}})^{r_{ID}} (m_u v_m^h)^{s_1}, g^{s_1})$。

5) 重签名生成算法(ReKey)。输入一个重签名密钥 $rk_{A\to B} = (rk_{A\to B}^1, rk_{A\to B}^2)$,一个消息 M,一个身份 ID_A 和一个签名 $\sigma_A = (\sigma_{A_1}, \sigma_{A_2}, \sigma_{A_3})$,如果 $\text{Verify}(ID_A, M, \sigma_A) = 0$,输出 $\perp$;否则,选取 $s_2 \in \mathbf{Z}_p^*$,计算 $\sigma_{B_4} = g^{s_2}$ 和 $h_2 = H_{k_m}(M \| \sigma_{B_4})$,并检查 h_2 的最右边比特值 $u_2 \in \{0,1\}$,输出对应于身份 ID_B 的消息 M 的重签名:

$$\sigma_B = (\sigma_{B_1}, \sigma_{B_2}, \sigma_{B_3}, \sigma_{B_4}) = (rk_{A\to B}^1 \cdot \sigma_{A_1}, rk_{A\to B}^2 \cdot \sigma_{A2} \cdot (m_{u_2} v_m^{h_2})^{s_2}, \sigma_{A_3}, g^{s_2})$$

6) 签名验证算法(Verify):该算法分签名和重签名两种情形:

① 对于身份 ID,消息 M 和签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3)$,首先计算 $h_{ID} = H_{k_{ID}}(ID \| \sigma_1)$ 和 $h = H_{k_m}(M \| \sigma_3)$,分别检查 h_{ID} 和 h 的最右边比特值 $u_{ID}, u \in \{0,1\}$。然后验证 $\hat{e}(\sigma_2, g) = \hat{e}(g_1, g_2)\hat{e}(\sigma_1, ID_{u_{ID}} v_{ID}^{h_{ID}})\hat{e}(\sigma_3, m_u v_m^h)$ 是否成立,如果成立,则输出 1;否则输出 0。

② 对于身份 ID 和消息 M 的重签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4)$,首先计算 $h_{ID} = H_{k_{ID}}(ID \| \sigma_1)$,$h = H_{k_m}(M \| \sigma_3)$ 和 $h_2 = H_{k_m}(M \| \sigma_4)$,分别检查 h_{ID}, h 和 h_2 的最右边比特值 $u_{ID}, u, u_2 \in \{0,1\}$。然后验证 $\hat{e}(\sigma_2, g) = \hat{e}(g_1, g_2)\hat{e}(\sigma_1, ID_{u_{ID}} v_{ID}^{h_{ID}})\hat{e}(\sigma_3, m_u v_m^h)\hat{e}(\sigma_4, m_{u_2} v_m^{h_2})$ 是否成立,如果成立,输出 1;否则输出 0。

2.2 正确性分析

假定受托者的身份 ID_A 对应的私钥 $d_A = (d_{A_1}, d_{A_2}) = (g^{r_A}, g_2^\alpha (ID_{u_A} v_{ID}^{h_A})^{r_A})$,委托者的身份 ID_B 对应的私钥 $d_B = (d_{B_1}, d_{B_2}) = (g^{r_B}, g_2^\alpha (ID_{u_B} v_{ID}^{h_B})^{r_B})$,重签名密钥 $rk_{A\to B} = (rk_{A\to B}^1, rk_{A\to B}^2) = (d_{B_1}/d_{A_1}, d_{B_2}/d_{A_2})$,消息 M 的签名 $\sigma_A = (\sigma_{A_1}, \sigma_{A_2}, \sigma_{A_3})$ 和重签名 $\sigma_B = (\sigma_{B_1}, \sigma_{B_2}, \sigma_{B_3}, \sigma_{B_4})$,则 σ_B 的正确性验证过程如下:

$$\sigma_{B1} = rk_{A\to B}^1 \cdot \sigma_{A_1} = d_{B_1}/d_{A_1} \cdot \sigma_{A_1} = g^{r_B}/g^{r_A} \cdot g^{r_A} = g^{r_B}$$

$$h_{ID} = H_{k_{ID}}(ID \| \sigma_{B_1}) = H_{k_{ID}}(ID \| g^{r_B})$$

$$\sigma_{B_3} = g^{s_1}$$

$$\sigma_{B_4} = g^{s_2}$$

$$h = H_{k_m}(M \| \sigma_{B_3}) = H_{k_m}(M \| g^{s_1})$$

$$h_2 = H_{k_m}(M \| \sigma_4) = H_{k_m}(M \| g^{s_2})$$

$$\sigma_{B2} = rk_{A\to B}^2 \cdot \sigma_{A2} \cdot (m_{u_2} v_m^{h_2})^{s_2} = (ID_{u_B} v_{ID}^{h_B})^{r_B}/(ID_{u_A} v_{ID}^{h_A})^{r_A} g_2^\alpha (ID_{u_A} v_{ID}^{h_A})^{r_A} (m_u v_m^h)^{s_1} (m_{u_2} v_m^{h_2})^{s_2} = g_2^\alpha (ID_{u_B} v_{ID}^{h_B})^{r_B} (m_u v_m^h)^{s_1} (m_{u_2} v_m^{h_2})^{s_2}$$

$$\hat{e}(\sigma_{B2}, g) = \hat{e}(g_2^\alpha (ID_{u_B} v_{ID}^{h_B})^{r_B} (m_u v_m^h)^{s_1} (m_{u_2} v_m^{h_2})^{s_2}, g) = \hat{e}(g_2^\alpha, g) e((ID_{u_B} v_{ID}^{h_B})^{r_B}, g)\hat{e}((m_u v_m^h)^{s_1}, g)\hat{e}((m_{u_2} v_m^{h_2})^{s_2}, g) = \hat{e}(g^\alpha, g_2)\hat{e}(g^{r_B}, ID_{u_B} v_{ID}^{h_B})\hat{e}(g^{s_1}, m_u v_m^h)\hat{e}(g^{s_2}, m_{u_2} v_m^{h_2}) = \hat{e}(g_1, g_2)\hat{e}(\sigma_{B_1}, ID_{u_B} v_{ID}^{h_B})\hat{e}(\sigma_{B_3}, m_u v_m^h)\hat{e}(\sigma_{B_4}, m_{u_2} v_m^{h_2})$$

因为 $rk_{A\to B} = (rk_{A\to B}^1, rk_{A\to B}^2) = (d_{B_1}/d_{A_1}, d_{B_2}/d_{A_2}) = (d_{A_1}/d_{B_1}, d_{A_2}/d_{B_2})^{-1} = 1/rk_{B\to A}$,所以新方案满足双向性。

对于消息 M 的签名 $\sigma = (\sigma_1, \sigma_2, \sigma_3) = (g^{r_{ID}}, g_2^\alpha (ID_{u_{ID}} v_{ID}^{h_{ID}})^{r_{ID}} (m_u v_m^h)^{s_1}, g^{s_1})$,其中 $h_{ID} = H_{k_{ID}}(ID \| g^{r_B})$ 和 $h = H_{k_m}(M \| g^{s_1})$。如果敌手选择参数 $r'_{ID}, s'_1 \in \mathbf{Z}_p^*$,利用 $\sigma_1 = g^{r_{ID}}$ 和 $\sigma_3 = g^{s_1}$ 分别计算新的 $\sigma'_1 = \sigma_1 g^{r'_{ID}} = g^{r_{ID}+r'_{ID}}$ 和 $\sigma'_3 = \sigma_3 g^{s'_1} = g^{s_1+s'_1}$,但 σ_2 中的 h_{ID} 和 h 无法改变,因此新构造的签名无法通过验证,从而保证了新方案中签名的强不可伪造性。同理,消息 M 的重签名中所 σ_2 包含的 h_{ID}, h 和 h_2 也无法改变,使得伪造的重签名无法通过验证,从而保证了新方案中重签名的强不可伪造性。

2.3 安全性分析

定理 1 若 TCR 杂凑函数 H_k 是 $(t,\varepsilon/2)$ 安全的或 G_1 上的 $(t,\varepsilon/16)$-CDH 假设成立,则本文提出的基于身份双向代理重签名方案是 (t,ε) 强不可伪造的。

证明 假设敌手 A 在多项式时间 t 内最多查询了 q_E 次用户密钥提取预言机、q_S 次签名预言机、q_{RK} 次重签名密钥生成预言机和 q_{RS} 次重签名预言机,能以一个不可忽略的概率 ε 攻破新方案的强不可伪造性,下面证明将存在一个敌手 F 能解决 G_1 上的 CDH 问题或找到 TCR 杂凑函数的一个碰撞。

假设 (ID_i, M_i) 是 A 第 i 次询问签名和重签名预言机的输入,预言机返回身份 ID_i 关于 M_i 的签名 $\sigma_i = (\sigma_{i1}, \sigma_{i2}, \sigma_{i3})$ 和

重签名 $\sigma_i=(\sigma_{i1},\sigma_{i2},\sigma_{i3},\sigma_{i4})$,令 $q=q_S+q_{RS}$,$q\geqslant q_E$,$h_{ID_i}=H_{k_{ID}}(ID_i\|\sigma_{i1})$,$h_i=H_{k_m}(M_i\|\sigma_{i3})$,$h_{i2}=H_{k_m}(M_i\|\sigma_{i4})$,$i=1,2,\cdots,q$。$A$ 输出消息 $M^*(\notin\{M_i\}_{i=1}^q)$ 的伪造为 $(M^*,\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*))$,令 $h_{ID}^*=H_{k_{ID}}(ID^*\|\sigma_1^*)$,$h^*=H_{k_m}(M^*\|\sigma_3^*)$ 和 $h_2^*=H_{k_m}(M^*\|\sigma_4^*)$。将 A 的伪造分成两类:

类型 1　$h_{ID}^*\neq h_{ID_i},i=1,2,\cdots,q$;

类型 2　$h_{ID}^*=h_{ID_i}$,存在 $i\in\{1,2,\cdots,q\}$。

如果 A 能成功伪造一个合法签名,则 A 的输出必然是以上某种类型。下面证明类型 1 的伪造可解决一个 CDH 问题实例,类型 2 的伪造可找到 H_k 的一对碰撞。

类型 1　假设 A 是类型 1 的敌手,将存在一个敌手 F 能解决 G_1 上的 CDH 问题。给定一个 CDH 问题实例 $(g,g^\alpha,g^\beta)\in G_1^3$,$F$ 的任务是计算 $g^{\alpha\beta}\in G_1$。敌手 F 执行如下的模拟操作:

建立　令 $g_1=g^\alpha$,$g_2=g^\beta$,随机选取 8 个元素 $x_1,y_1,z_1,t_1,x_2,y_2,z_2,t_2\in\mathbf{Z}_p^*$,计算 $ID_0=g^{x_1}$,$ID_1=g_2^{t_1}g^{y_1}$,$m_0=g^{x_2}$,$m_1=g_2^{t_2}g^{y_2}$,$v_{ID}=g^{z_1}$ 和 $v_m=g^{z_2}$,运行 Setup 算法得到系统其他参数,并将 $cp=(G_1,G_2,p,\hat{e},g,g_1,g_2,v_{ID},v_m,ID_0,ID_1,m_0,m_1,k_m,k_{ID},H_{k_m},H_{k_{ID}})$ 发送给敌手 A。

查询　F 建立如下的预言机。

1) 密钥提取预言机 O_{Extract}:A 输入一个身份 ID_i,F 选取一个随机数 $r_{ID_i}\in\mathbf{Z}_p$,计算 $d_{ID_i,1}=g_1^{-1/t_1}g^{r_{ID_i}}=g^{r_{ID_i}-\alpha/t_1}$ 和 $h_{ID_i}=H_{k_{ID}}(ID_i\|d_{ID_i,1})$;然后检查 h_{ID_i} 的最右边比特值 $u_{ID_i}\in\{0,1\}$,若 $u_{ID_i}\neq1$,则重新选择 r_{ID_i} 使得 $u_{ID_i}=1$;最后计算 $d_{ID_i,2}=g_1^{-(y_1+z_1h_{ID_i})/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}$,并返回 ID_i 对应的密钥 $d_{ID_i}=(d_{ID_i,1},d_{ID_i,2})$ 给 A。

2) 签名预言机 O_{Sign}:攻击者 A 输入一个身份 ID_i 和一个消息 M_j,F 首先询问预言机 O_{Extract} 获得私钥 d_{ID_i},然后随机选取 $s_{j,1}\in\mathbf{Z}_p^*$ 运行 Sign 算法生成 M_j 的签名 $\sigma_j=(\sigma_{j1},\sigma_{j2},\sigma_{j3})$,并将 σ_j 返回给 A。

假定密钥提取预言机返回的私钥 $d_{ID_i}=(d_{ID_i,1},d_{ID_i,2})=(g^{r_{ID_i}-\alpha/t_1},g_1^{-(y_1+z_1h_{ID_i})/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}})$,则消息 M_j 的签名 $\sigma_j=(\sigma_{j1},\sigma_{j2},\sigma_{j3})$ 的正确性验证过程如下:

$\sigma_{j1}=d_{ID_i,1}$,$\sigma_{j3}=g^{s_{j,1}}$,$h_{ID_i}=H_{k_{ID}}(ID_i\|\sigma_{j1})$,$h_i=H_{k_m}(M_i\|\sigma_{i3})$,$h_{ID_i}$ 和 h_i 的最右边比特值 $u_{ID_i},u_i\in\{0,1\}$

$$\begin{aligned}\sigma_{j2}&=d_{ID_i,2}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&g_1^{-(y_1+z_1h_{ID_i})/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&(g_2^\alpha g_2^{-\alpha})g_1^{-(y_1+z_1h_{ID_i})/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&g_2^\alpha(g_2^{t_1}g_1^{(y_1+z_1h_{ID_i})/\alpha})^{-\alpha/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&g_2^\alpha(g_2^{t_1}(g^\alpha)^{(y_1+z_1h_{ID_i})/\alpha})^{-\alpha/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&g_2^\alpha((g_2^{t_1}g^{y_1})(g^{z_1})^{h_{ID_i}})^{-\alpha/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&g_2^\alpha(ID_1v_{ID}^{h_{ID_i}})^{-\alpha/t_1}(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}}(m_{u_j}v_m^{h_j})^{s_{j,1}}=\\&g_2^\alpha(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}-\alpha/t_1}(m_{u_j}v_m^{h_j})^{s_{j,1}}\end{aligned}$$

于是有

$$\begin{aligned}&\hat{e}(\sigma_{j2},g)=\hat{e}(g_2^\alpha(ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}-\alpha/t_1}(m_{u_j}v_m^{h_j})^{s_{j,1}},g)=\\&\hat{e}(g_2^\alpha,g)e((ID_1v_{ID}^{h_{ID_i}})^{r_{ID_i}-\alpha/t_1},g)\hat{e}((m_{u_j}v_m^{h_j})^{s_{j,1}},g)=\\&\hat{e}(g_2,g^\alpha)\hat{e}(g^{r_{ID_i}-\alpha/t_1},ID_1v_{ID}^{h_{ID_i}})\hat{e}(g^{s_{j,1}},m_{u_j}v_m^{h_j})=\\&\hat{e}(g_2,g_1)\hat{e}(\sigma_{j1},ID_1v_{ID}^{h_{ID_i}})\hat{e}(\sigma_{j3},m_{u_j}v_m^{h_j})\end{aligned}$$

3) 重签名密钥生成预言机 O_{ReKey}:攻击者 A 输入两个不同的身份 ID_i 和 ID_j,F 首先询问预言机 O_{Extract} 获得身份 (ID_i,ID_j) 对应的私钥 (d_i,d_j),然后运行 ReKey 算法生成重签名密钥 $rk_{i\to j}$,并将 $rk_{i\to j}$ 返回给 A。

4) O_{ReSign} 是重签名生成预言机:攻击者 A 输入两个身份 (ID_i,ID_j),一个消息 M_i 和一个签名 σ_i,F 首先验证 σ_i 的合法性,如果 $\text{Verify}(ID_i,M_i,\sigma_i)=0$,输出 $\perp$;否则,F 首先询问预言机 O_{Extract} 获得身份 (ID_i,ID_j) 对应的私钥 (d_{ID_i},d_{ID_j}),如果 ID_i 和 ID_j 中有一个已被攻陷,F 返回一个重签名 $\sigma_j=O_{\text{Sign}}(ID_j,M_i)$;如果 ID_i 和 ID_j 均已被攻陷或均未被攻陷,F 运行重签名生成算法和查询重签名密钥生成预言机,然后返回一个重签名 $\sigma_j=\text{ReSign}(O_{\text{ReKey}}(ID_i,ID_j),ID_i,M_i,\sigma_i)$。

伪造　敌手 A 输出类型 1 的伪造 $(M^*,\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*))$,其中 $h_{ID}^*=H_{k_{ID}}(ID^*\|\sigma_1^*)$,$h^*=H_{k_m}(M^*\|\sigma_3^*)$ 和 $h_2^*=H_{k_m}(M^*\|\sigma_4^*)$。若 h_{ID}^*,h^* 和 h_2^* 的最右边比特值都不是 0,则敌手 F 宣告模拟失败;否则,由于 $ID_0=g^{x_1}$ 和 $m_0=g^{x_2}$,该伪造必须满足:

$$\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*)=(g^{r_{ID}^*},g_2^\alpha(ID_0v_{ID}^{h_{ID}^*})^{r_{ID}^*}(m_0v_m^{h^*})^{s_1^*}(m_0v_m^{h_2^*})^{s_2^*},g^{s_1^*},g^{s_2^*})$$

为了解决 CDH 实例 $(g,g^\alpha,g^\beta)\in G_1^3$,$F$ 计算

$$\begin{aligned}&\frac{\sigma_2^*}{(\sigma_1^*)^{x_1+z_1h_{ID}^*}(\sigma_3^*)^{x_2+z_2h^*}(\sigma_4^*)^{x_2+z_2h_2^*}}=\\&\frac{g_2^\alpha(ID_0v_{ID}^{h_{ID}^*})^{r_{ID}^*}(m_0v_m^{h^*})^{s_1^*}(m_0v_m^{h_2^*})^{s_2^*}}{(g^{r_{ID}^*})^{x_1+z_1h_{ID}^*}(g^{s_1^*})^{x_2+z_2h^*}(g^{s_2^*})^{x_2+z_2h_2^*}}=\\&\frac{g_2^\alpha(ID_0v_{ID}^{h_{ID}^*})^{r_{ID}^*}(m_0v_m^{h^*})^{s_1^*}(m_0v_m^{h_2^*})^{s_2^*}}{(g^{x_1}g^{z_1h_{ID}^*})^{r_{ID}^*}(g^{x_2}g^{z_2h^*})^{s_1^*}(g^{x_2}g^{z_2h_2^*})^{s_2^*}}=\\&\frac{g_2^\alpha(ID_0v_{ID}^{h_{ID}^*})^{r_{ID}^*}(m_0v_m^{h^*})^{s_1^*}(m_0v_m^{h_2^*})^{s_2^*}}{(ID_0v_{ID}^{h_{ID}^*})^{r_{ID}^*}(m_0v_m^{h^*})^{s_1^*}(m_0v_m^{h_2^*})^{s_2^*}}=g_2^\alpha=g^{\alpha\beta}\end{aligned}$$

综上所述,如果敌手 A 能攻破新方案的强不可造性,那么 F 能解决 G_1 上的 CDH 问题。由于 A 成功伪造签名的概率是 ε,模拟不中断的概率是 1/8,选择类型 1 的概率都是 1/2,所以 F 成功计算出 CDH 困难问题实例的概率是 $\varepsilon/16$。

类型 2　假设存在类型 2 的敌手 A,它能攻破新方案的 (t,ε) 强不可伪造性,将存在一个敌手 F 能以 $\varepsilon/2$ 的概率找到 TCR 杂凑函数 $H_{k_{ID}}$ 的一对碰撞。F 首先获得杂凑函数密钥 $k^*\in K$,它的目标是找到一对消息 (m_1^*,m_2^*),满足 $m_1^*\neq m_2^*$ 且 $H_{k^*}(m_1^*)=H_{k^*}(m_2^*)$。敌手 F 执行如下的模拟操作:

建立　令 $k_{ID}=k^*$,运行 Setup 算法得到系统其他参数,将 $(g,g_1,g_2,v_{ID},v_m,ID_0,ID_1,m_0,m_1,k_m,k_{ID})$ 发送给敌手 A。

询问　敌手 A 可以自适应性地向 F 询问用户的公钥/私钥、重签名密钥、消息的签名和重签名,F 通过运行相应的算法(Extract、ReKey、Sign 和 ReSign)回答 A 所发起的各种询问请求,并将询问结果返回给 A。

伪造　敌手 A 输出类型 2 的伪造 $(M^*,\sigma^*=(\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*))$,令 $h_{ID}^*=H_{k_{ID}}(ID^*\|\sigma_1^*)$,并且存在某个 $i\in\{1,2,\cdots,q\}$,使得 $h_{ID}^*=h_{ID_i}$,即 $H_{k_{ID}}(ID^*\|\sigma_1^*)=H_{k_{ID}}(ID_i\|\sigma_{i1})$。$F$ 设置 $m_1^*=ID^*\|\sigma_1^*$ 和 $m_2^*=ID_i\|\sigma_{i1}$;由于 $m_1^*\neq m_2^*$ 且 $H_{k^*}(m_1^*)=H_{k^*}(m_2^*)$,所以 F 找到杂凑函数 $H_{k_{ID}}$ 的一对碰撞 (m_1^*,m_2^*)。如果敌手 A 成功伪造签名的概率是 ε,由于整个模拟没有中断且选择类型 1 的概率是 1/2,因此 F 能以 $\varepsilon/2$ 的概率找到 $H_{k_{ID}}$ 的一对碰撞。

2.4 有效性分析

下面将已有基于身份的双向代理重签名方案和本文方案进行效率和安全属性比较，其结果见表 2。假定所有方案选择相同长度的大素数 p，表中：$|\cdot|$ 表示元素长度，E 表示指数运算，P 表示双线性对运算，n 表示 Waters 签名[14] 方案中的签名消息长度，Y 表示具有此种属性，N 表示不具有此种属性。

表 1 效率和安全属性比较

签名方案	系统公开参数长度	重签名长度	私钥长度	重签名生成代价	强不可伪造性	困难问题假设
Shao 方案[5]	$(2n+3)\|G_1\|$	$3\|G_1\|$	$2\|G_1\|$	$2E+3P$	否	CDH 问题
Hu 方案[6]	$4\|G_1\|$	$5\|G_1\|$	$\|G_1\|+\|p\|$	$4E+3P$	否	q-SDH 问题
本文方案	$10\|G_1\|$	$3\|G_1\|$	$2\|G_1\|$	$2E+3P$	是	CDH 问题

从表 1 可看出：本文提出的双向代理重签名方案比 Shao 方案[5] 的系统参数小很多，比 Hu 方案[6] 的系统参数多；但新方案比 Hu 方案的重签名长度和重签名生成代价都要小，且新方案基于的困难问题假设更弱。本文方案满足强不可伪造性，但其余两个方案只满足存在不可伪造性。

3 结语

本文提出了一个基于身份的双向代理重签名方案，并证明了新方案满足强不可伪造性。与已有的双向代理重签名方案比较，新方案在系统公开参数长度、重签名长度、安全属性等方面具有较大的优势。下一步的工作是设计基于身份的强不可伪造单向代理重签名方案。

参考文献：

[1] HAO S G, LI Z, GHULAM M. A union authentication protocol of cross-domain based on bilinear pairing [J]. Journal of Software, 2013, 8(5): 1094 – 1100.

[2] ZHANG L, ZHANG J, XIA A, *et al.* Domain authentication protocol based on certificate signcryption in IPv6 network [C]// Proceedings of the International Conference on Information Engineering and Applications, LNCS 218. Berlin: Springer-Verlag, 2013: 213 – 220.

[3] HONG X, LONG Y. A novel unidirectional proxy re-signature scheme and its application for MANETs [J]. Journal of Computers, 2012, 7(7): 1796 – 1800.

[4] ATENIESE G, HOHENBERGER S. Proxy re-signatures: new definitions, algorithms, and applications [C]// Proceedings of the 12th ACM Conference on Computer and Communications Security. New York: ACM Press, 2005: 310 – 319.

[5] SHAO J, CAO Z, WANG L, *et al.* Proxy re-signature schemes without random oracles [C]// Proceedings of the 8th International Conference on Cryptology, LNCS 4859. Berlin: Springer-Verlag, 2007: 197 – 209.

[6] HU X, ZHANG Z, YANG Y. Identity based proxy re-signature schemes without random oracle [C]// Proceedings of the 2009 International Conference on Computational Intelligence and Security. Piscataway: IEEE Press, 2009: 256 – 259.

[7] YANG X, WANG C, ZHANG L, *et al.* On-line/off-line threshold proxy re-signatures [J]. Chinese Journal of Electronics, 2014, 23(2): 248 – 253.

[8] DENG Y, DU M, YOU Z, *et al.* A blind proxy re - signatures scheme based on standard model [J]. Journal of Electronics and Information Technology, 2010, 32(5): 1119 – 1223.

[9] HE D. A novel blind proxy re-signature scheme [J]. Computer Applications and Software, 2012, 29(3): 294 – 296. (贺得飞. 一种新的盲代理重签名方案[J]. 计算机应用与软件, 2012, 29(3): 294 – 296.)

[10] MENON T. An identity based proxy re-signature scheme[J]. IACSIT International Journal of Engineering and Technology, 2012, 4(3): 303 – 306.

[11] RAWAT S S, SHRIVASTAVA G K. Improved ID-based proxy re-signcryption scheme [C]// Proceedings of the 2012 IEEE CICN. Berlin: Springer-Verlag, 2012: 730 – 733.

[12] BUCHMANN J, DAHMEN E, ERETH S, *et al.* On the security of the Winternitz one-time signature scheme [J]. International Journal of Applied Cryptography, 2013, 3(1): 84 – 96.

[13] LIU Z, HU Y, ZHANG X. Efficient and strongly unforgeable short signature scheme in standard model [J]. Journal of Jiangsu University: Natural Science, 2013, 34(3): 309 – 313. (刘振华, 胡予濮, 张襄松. 标准模型下高效的强不可伪造短签名方案[J]. 江苏大学学报: 自然科学版, 2013, 34(3): 309 – 313.)

[14] WATERS B. Efficient identity-based encryption without random oracles [C]// Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005: 114 – 127.

(上接第 3233 页)

[10] SHU W, ZHENG S, WANG X. A load balanced method for VOD cluster based on linear transformation genetic algorithm[J]. Geomatics and Information Science of Wuhan University, 2006, 31(9): 839 – 841. (舒万能, 郑世珏, 王雄. 一种基于线性变换遗传算法的 VOD 集群负载均衡方法[J]. 武汉大学学报: 信息科学版, 2006, 31(9): 839 – 841.)

[11] XU H, FU J. Research on model and simulation of load balance for server cluster[J]. Computer Simulation, 2012, 29(3): 180 – 183. (许海成, 傅锦伟. 服务器集群负载均衡的建模与仿真研究[J]. 计算机仿真, 2012, 29(3): 180 – 183.)

[12] CALHEIROS R N, RANJAN R, de ROSE C A F, *et al.* Cloudsim: a novel framework for modeling and simulation of cloud computing infrastructures and services, GRIDS-TR-2009-1[R]. Melbourne: University of Melbourne, 2009.

[13] YANG X, MA Z, SUN L. Research on extended ant colony optimization based virtual machine deployment in infrastructure clouds [J]. Computer Science, 2012, 39(9): 33 – 37. (杨星, 马自堂, 孙磊. 云环境下基于改进蚁群算法的虚拟机批量部署研究[J]. 计算机科学, 2012, 39: (9): 33 – 37.)

[14] WANG Q. Research and implementation of smart TV cloud VOD system based on HDFS[D]. Mianyang: Southwest University of Science and Technology, 2014. (王庆凤. 基于 HDFS 的智能电视云点播系统的研究与实现[D]. 绵阳: 西南科技大学, 2014.)