对一类基于身份的门限代理签名方案的伪造攻击

陈 亮[1,3] 田苗苗[2] 汤学明[1] 崔永泉[1]
(华中科技大学计算机科学技术学院 武汉 430074)[1]
(中国科学技术大学计算机科学技术学院 合肥 230026)[2] (河南科技学院数学系 新乡 453003)[3]

摘 要 近来,于义科等人提出了一系列标准模型下基于身份的门限代理签名方案,并以其中最新的于-郑方案作为攻击目标,设计了3个有效的伪造攻击算法。利用这些算法,攻击者可以在得不到原始签名人和任何代理签名人私钥的情况下,仅通过选取随机参数以及多项式时间内的计算,就可达到以显著的成功概率伪造普通签名或任意代理签名人的部分签名的目的。这些伪造攻击算法对于-郑方案及与其同类的其他几个方案都具有有效性。攻击显示,此类基于身份的门限代理签名方案是不安全的。最后分析了方案遭受攻击的原因,并给出了两种可能的改进措施。

关键词 基于身份签名,门限代理签名,伪造攻击,双线性映射
中图法分类号 TP309 **文献标识码** A

Forgery Attacks on a Series of ID-based Threshold Proxy Signature Schemes

CHEN Liang[1,3] TIAN Miao-miao[2] TANG Xue-ming[1] CUI Yong-quan[1]
(School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan 430074, China)[1]
(School of Computer Science and Technology, University of Science and Technology of China, Hefei 230026, China)[2]
(Department of Mathematics, Henan Institute of Science and Technology, Xinxiang 453003, China)[3]

Abstract Recently, YU Y K et al. proposed a series of ID-based threshold proxy signature in the standard model. This paper constructed three attack algorithms for the latest scheme of YU-ZHENG, with which attacker can forge valid both regular signature on behalf of the original signer and proxy signature of any proxy signer on any message without knowing the signing key of these signers. Our attacking algorithms work well with scheme of YU-ZHENG and the decedent schemes. Attacks show that this series of schemes are unsecure. We analyzed the root cause of attacks and gave some suggestions for modifications in the end.

Keywords Identity based signature, Threshold proxy signature, Forge attack, Bilinear map

1 引言

数字签名是密码学研究领域最为重要的分支之一。在传统的公钥签名方案中,签名者的公钥是某个给定的集合中的随机串。公钥和签名实体之间的绑定通常要借助PKI的证书机制来实现,因此不可避免地带来了证书的管理问题。为了解决此问题,Shamir于1984年首次提出了基于身份的密码体制,并基于整数分解难题给出了第一个基于身份的签名方案[1]。2001年,Boneh等人利用Weil配对提出了第一个安全、实用的基于身份的加密方案。此后,基于身份的密码体制引起了国内外众多学者的广泛关注并得到迅速发展,提出了大量的基于身份的加密和签名方案。

1996年,代理签名的概念首次由Mambo等人[2]提出。在一个代理签名方案中,原始的签名人可通过委托的方式将其签名权暂时或者永久性地委托给代理签名人,由代理签名人代表原始签名人生成有效签名。代理签名在很多电子商务领域中有着广泛的应用背景,比如股票交易、电子投票或电子签章等应用。

把基于身份的密码体制和代理签名相结合,形成了基于身份的代理签名。2003年,Zhang等人[3]构造了第一个基于身份的代理签名方案。该方案只考虑了把权限全权委托给单个代理人的情况,导致权力过于集中。Zhang等人[4]最早提出了门限代理签名方案。另外一些基于身份的门限代理签名方案[5]也相继被提出。然而,这些方案的安全性都是建立在随机预言模型下。2005年,Waters等人创造性地提出了标准模型下的高效IBE方案[6],同时也指出该方法可用来构造标准模型下安全、高效的IBS方案。2006年,Paterson等人在Waters等人基于身份加密方案的基础上提出了一个标准模型下基于身份的签名方案[7],该方案被证明能够归约于计算的Diffie-Hellman问题。同时,文献[7]给出了基于身份的签

到稿日期:2011-12-12 返修日期:2012-04-23 本文受国家自然科学基金资助项目(61100221),中央高校基本科研业务费专项资金(2011QN044)资助。

陈 亮(1983-),男,博士生,主要研究方向为公钥密码和数字签名,E-mail:crypto.liang@gmail.com;田苗苗(1987-),男,博士生,主要研究方向为信息安全、无线传感网络;汤学明(1974-),男,博士,副教授,主要研究方向为密码学、数据库安全、网络安全;崔永泉(1977-),男,讲师,主要研究方向为访问控制和密码协议。

名方案的可证安全模型。然而，该方案的计算效率不高，需要多次乘法和双线性对计算。随后，谷科等人[8]又对 Paterson 方案进行了改进。

2011 年，于义科等人使用 Waters 方法，在谷科等人工作的基础上，提出了一系列的标准模型下基于身份的(动态)门限代理签名方案[9,10]。虽然他们都声称其方案能够满足普通签名和门限代理签名强不可伪造性等一组安全需求，但是经过分析发现，他们的方案都是不安全的。本文以于-郑方案[11]为例，构造了 3 个攻击算法。利用这些伪造攻击，攻击者可以在不得到原始签名人和任何代理签名人私钥的情况下，仅通过选取随机参数以及多项式时间内的计算，就可达到以显著的成功概率伪造普通签名或任意代理签名人的部分签名的目的。这些伪造攻击算法对于-郑方案及与其同类的其他几个方案[9,10]都具有有效性。攻击显示，此类基于身份的门限代理签名方案是不安全的。最后分析了方案遭受攻击的原因，并给出了两种可能的改进措施。

2 预备知识

2.1 双线性对(Bilinear pairing)

令 G 和 G_T 是两个 p 阶循环群，g 是 G 的生成元，定义 G 和 G_T 上的双线性映射为 $e:G\times G\rightarrow G_T$，且 e 满足下面的性质：

(1) 双映射性：$e(g^a,g^b)=e(g,g)^{ab}$。

(2) 非退化性：$e(g,g)\neq 1$。

(3) 可计算性：存在有效算法来计算 e。

注意：双线性映射运算 e 是可交换的，因为 $e(g^a,g^b)=e(g^b,g^a)=e(g,g)^{ab}$。

2.2 基于身份的门限代理签名

定义 1 设 P_A 是原始签名人，身份为 ID_A。$P_S=\{P_1,P_2,\cdots,P_n\}$ 是 n 个代理签名人组成的集合，相应身份为 ID_i，门限值为 t，则基于身份的动态门限代理签名方案由以下算法组成：

(1) 系统参数产生算法 Setup。输入参数 k'，算法输出系统公开参数 $params$ 和主密钥 mk。

(2) 用户密钥生成算法 Extract。给定身份 ID，该算法输入 $params$、ID、mk，输出 ID 的私钥 ID_d。

(3) 普通签名算法 Sign。该算法输入私钥 ID_d 和消息 m，输出用户 ID 在消息 m 的普通签名 σ。

(4) 普通签名验证算法 verify。算法输入 $params$、ID、m、σ，若 σ 是用户 ID 在 m 上的有效普通签名，输出 1，否则输出 0。

(5) 秘密分享算法 TP。该算法输入门限值 t、签名人集合的规模 n 和代理签名人子秘密 S_i，输出代理签名人的秘密分享 x_i。

(6) 门限代理授权算法(TD,TP)，由一对交互算法组成。它把 P_A 的签名权委托给代理签名人 P_i。

① TD 由 P_A 执行，输入 (ID_A,w,d_{P_A})，其中，w 是授权文件，包括 P_A 的身份 ID_A、代理签名人的规模 n、门限值 t、代理签名人的 ID_i 和代理签名的有效期，TD 与 TP 交互完成代理授权，产生授权 σ_w，输出 (w,σ_w) 给每个代理签名人。

② TP 由 P_i 执行，它输入 $(ID_A,ID_i,w,\sigma_w,x_i,d_{P_i})$，输出 P_i 代表 P_A 签名的私钥 psk_{P_i}。

(7) 部分代理签名产生算法 TPS，它由 P_i 执行。它的输入是 $(ID_A,ID_i,w,\sigma_w,psk_{P_i},m)$，该算法输出代理人 P_i 在消息 m 上的部分代理签名 $p\sigma_{P_i}$。

(8) 部分代理签名验证算法 TPV，由每个门限代理签名人执行。算法输入 $(ID_A,ID_i,w,m,p\sigma_{P_i})$，其中 $p\sigma_{P_i}$ 是 P_i 对消息 m 的签名。若该签名是 P_i 在消息 m 上的有效部分代理签名，输出 1，否则输出 0。

(9) 代理签名产生算法 PS，由任何门限代理签名人执行。算法输入任意 $k(t\leqslant k\leqslant n)$ 个有效部分代理签名，算法输出代理签名 $p\sigma$。

(10) 代理签名验证算法 PV，由任何验证人执行。算法输入 $(ID_A,ID_1,\cdots,ID_k,w,m,p\sigma)$，若 $p\sigma$ 是任意 $k(t\leqslant k\leqslant n)$ 个有效部分代理签名人在消息 m 上的有效代理签名，则输出 1，否则输出 0。

2.3 基于身份签名的安全需求

一个安全的基于身份的门限代理签名至少应满足以下几方面的需求：

(1) 不可伪造性：除 P_A 外，任何人都不能生成 P_A 的普通数字签名。

(2) 强不可伪造性。只有被授权的代理签名人能代表 P_A 产生有效的部分代理签名，而 P_A 和其他没有指定为代理签名人的第三方都不能产生有效的部分代理签名；只有有效的部分代理签名数目不少于 t 才能产生合法的代理签名；P_A 和没有指定为代理人的第三方都不能产生有效的代理签名。

(3) 强可验证性。根据部分代理签名，验证人能确信代理签名人是 P_A 的合法授权人。根据代理签名，验证人能确信所有参与的代理签名人都是 P_A 的合法授权人。

(4)强不可否认性。若代理签名人产生了有效的部分代理签名，他就不能否认他产生的部分代理签名；若代理签名人集合代表原始签名人产生了有效的代理签名，他们就不能否认其所做的代理签名。

3 方案回顾

设 P_A 是原始签名人，身份为 ID_A。$P_S=\{P_1,P_2,\cdots,P_n\}$ 是 n 个代理签名人组成的集合，相应身份为 ID_i，门限值为 t。选择两个 p 阶的循环群 G 和 G_T，g 为 G 的生成元，定义一个 G 和 G_T 上的双线性映射 $e:G\times G\rightarrow G_T$；选取 3 个安全 Hash 函数：$H_1:\{0,1\}^*\rightarrow\{0,1\}^{n_u}$，$H_2:\{0,1\}^*\rightarrow\{0,1\}^{n_m}$ 和 $H_3:\{0,1\}^*\rightarrow\{0,1\}^{n_w}$，这 3 个 Hash 函数分别用于把身份 ID、消息 m 和授权文件 w 映射成固定长度为 n_u、n_m 和 n_w 的二进制串。于-郑的方案描述如下：

(1) 系统参数产生算法 Setup。PKG 随机选择 $a\in Z_p$，$g_2\in G$，计算 $g_1=g^a$；同时，随机选择 $u'\in Z_p$，$m'\in G$，n_u 维的向量 $U_v=(u_i)$，n_m 维的向量 $M_v=(m_i)$，其中 $u_i\in Z_p$，$m_i\in G$。

令 $z_1=e(g_1,g_2)$，$z_2=e(g,g_2)$，则 PKG 的系统参数为 $params=(p,g,g_1,g_2,u',U_v,m',M_v,z_1,z_2)$，主密钥 $mk=a$。

(2) 用户密钥生成算法 Extract。若用户身份 ID 是长度为 n_u 的二进制串，假定 U 为 u 中 Bit 值为 1 的位置集合。PKG 随机选择 $t\in Z_p$，计算用户的签名私钥：$d_u=(d_0,d_1)=(g_2^{a+t(u'+\sum_{i\in u}u_i)},z_2^t)$，并通过安全信道把密钥传给用户。

(3) 普通签名算法 Sign。用户在取得 d_u 后，先验证 d_u 是否满足：$e(g,d_0)=z_1\cdot d_1^{u'+\sum_{i\in u}u_i}$。若不成立，用户再次向 PKG 询问 d_u。若 d_u 验证通过，则用户相信 d_u 是由 PKG 生成的，可对消息签名。假定消息 m 是长度为 n_m 的二进制串，令 M 为 m 中 Bit 值为 1 的位置集合。用户随机选择 $s\in Z_p$，则对消息 m 的签名为：

$$\sigma=(\sigma_1,\sigma_2,\sigma_3)=(d_0\cdot(m'\prod_{j\in M}m_j)^s,g^s,d_1)$$

(4) 普通签名验证算法 verify。验证者用 PKG 系统参数 $params$ 和身份 u 对消息 m 的签名 σ 进行验证，若等式 $e(g,\sigma_1)=z_1\cdot\sigma_3^{u'+\sum_{i\in U_A}u_i}\cdot e(\sigma_2,m'\prod_{j\in M}m_j)$ 成立，则签名有效，反之签名无效。

(5) 代理签名人秘密分享算法 TP。代理签名人 P_i 随机地选取 (s_i,s_i')，$s_i\in Z_p$，$s_i'\in Z_p$，公开 $r_i=g^{s_i}$ 和 $r_i'=g^{s_i'}$，计算并公开 $R=\prod_{i=1}^{n}r_i$，$R'=\prod_{i=1}^{n}r_i'$。随机选取 2 个 $t-1$ 次多项式 $f_i(z)$ 和 $h_i(z)$，且其系数在 Z_p 中：

$$f_i(z)=a_{i,0}+a_{i,1}z+\cdots+a_{i,t-1}z^{t-1}$$

$$h_i(z)=b_{i,0}+b_{i,1}z+\cdots+b_{i,t-1}z^{t-1}$$

令 $s_i=a_{i,0}$，$s_i'=b_{i,0}$，公开 $C_{i,d}=g^{a_{i,d}}$，$C_{i,d}'=g^{b_{i,d}}$ $(d=0,1,\cdots,t-1)$，计算 $s_{i,j}=f_i(j)$，$s_{i,j}'=h_i(j)$，并把它们通过安全信道传送给 P_j。P_j 从 P_i 那里取得 $s_{i,j}$ 和 $s_{i,j}'$ 后，做如下验证：

$$g^{s_{i,j}}=\prod_{d=0}^{t-1}(C_{i,d})^{i^d};\ g^{s_{i,j}'}=\prod_{d=0}^{t-1}(C_{i,d}')^{i^d}。$$

若未通过验证，则 P_j 产生对 P_i 的控告。若验证通过，则 P_j 计算秘密分享 $x_i=\sum_{k=1}^{n}f_k(i)$ 和 $y_i=\sum_{k=1}^{n}h_k(i)$，并公开 $X_i=g^{x_i}$，$Y_i=g^{y_i}$。其他的代理签名者可计算 $X_i=\prod_{j=1}^{n}\prod_{k=0}^{t-1}(C_{i,k})^{i^k}$ 和 $Y_i=\prod_{j=1}^{n}\prod_{k=0}^{t-1}(C_{i,k}')^{i^k}$，得到 X_i 和 Y。若令 $f(z)=\sum_{i=1}^{n}f_i(z)$，$h(z)=\sum_{i=1}^{n}h_i(z)$，则 $x_i=f(i)$，$y_i=h(i)$。

(6) 门限代理授权协议(TD,TP)。

TD：令 W 为授权文件不为零的位置集合。P_A 的普通签名私钥为 $d_A=(d_{A,1},d_{A,2})$，P_A 随机选择 $r_w\in Z_p$，计算：

$$\begin{aligned}\sigma_w&=(d_{A,1}(w'\prod_{j\in W}w_j)^{r_w},d_{A,2},g^{r_w})\\&=(g_2^{a+r_a(u'+\sum_{i\in U_A}u_i)}(w'\prod_{j\in W}w_j)^{r_w},z_2^{r_a},g^{r_w})\\&=(\sigma_{w1},\sigma_{w2},\sigma_{w3})\end{aligned}$$

P_A 发送 (W,σ_w) 给所有代理成员 P_k。

TP：代理签名人 P_k 验证 (W,σ_w) 是否满足：

$$e(g,\sigma_{w1})=z_1\cdot\sigma_{w2}^{u'+\sum_{i\in U_A}u_i}\cdot e(\sigma_{w3},w'\prod_{j\in W}w_j)$$

若成立，P_k 计算 $w_k=\prod_{j=1,j\neq k}^{t}\frac{j}{j-k}$，

$$\begin{aligned}psk_k&=(\sigma_{w1}d_{P_k,1}(w'\prod_{j\in W}w_j)^{x_kw_k},\sigma_{w2},d_{P_k,2},\sigma_{w3},g^{x_kw_k})\\&=(g_2^{2a+r_a(u'+\sum_{i\in U_A}u_i)}+r_k(u'+\sum_{i\in U_{P_k}}u_i)(w'\prod_{j\in W}w_j)^{r_w+x_kw_k},z_2^{r_a},z_2^{r_k},g^{r_w},g^{x_kw_k})\\&=(pk_1,pk_2,pk_3,pk_4,pk_5)\end{aligned}$$

则 psk_k 为代理签名人 P_k 代表 P_A 签名的代理私钥。

(7) 部分代理签名产生算法 TPS。它由 P_k 执行。输入 $(ID,ID_i,w,\sigma_w,psk_{P_k},m)$。算法输出部分代理签名 $p\sigma_k$。设 m 为要签名的消息，令 M 为其不为零的位置的序号的集合。则 P_k 计算：

$$\begin{aligned}p\sigma_k&=(pk_{k,1}(m'\prod_{k\in M}m_k)^{y_kw_k},pk_{k,2},pk_{k,3},pk_{k,4},pk_{k,5},g^{y_kw_k})\\&=(g_2^{2a+r_a(u'+\sum_{i\in U_A}u_i)+r_k(u'+\sum_{i\in U_{P_k}}u_i)}(w'\prod_{j\in W}w_j)^{r_w+x_kw_k}(m'\prod_{k\in M}m_k)^{y_kw_k},z_2^{r_a},z_2^{r_k},g^{r_w},g^{x_kw_k},g^{y_kw_k})\\&=(p\sigma_{k,1},p\sigma_{k,2},p\sigma_{k,3},p\sigma_{k,4},p\sigma_{k,5},p\sigma_{k,6})\end{aligned}$$

式中，$p\sigma_k$ 为 P_k 对消息 m 产生的部分代理签名，输出 $(ID_A,ID_k,W,\sigma_w,p\sigma_k)$。

(8) 部分代理签名验证算法 TPV。若下面的等式成立，则输出 1，否则输出 0。

$$e(g,p\sigma_{k,1})=z_1^2(p\sigma_{k,2})^{u'+\sum_{i\in U_A}u_i}(p\sigma_{k,3})^{u'+\sum_{i\in U_k}u_i}\cdot e(w'\prod_{j\in W}w_j,p\sigma_{k,4}p\sigma_{k,5})e(m'\prod_{k\in M}m_k,p\sigma_{k,6})$$

(9) 代理签名产生算法 PS。若所有的部分代理签名通过验证，则计算：

$$\begin{aligned}p\sigma'&=(\prod_{k=1}^{t}p\sigma_{k,1},\prod_{k=1}^{t}p\sigma_{k,2},p\sigma_{1,3},p\sigma_{2,3},\cdots,p\sigma_{t,3},\prod_{k=1}^{t}p\sigma_{k,4},\prod_{k=1}^{t}p\sigma_{k,5},\prod_{k=1}^{t}p\sigma_{k,6})\\&=(PR_1,PR_2,PR_{3,1},PR_{3,2},\cdots,PR_{3,t},PR_4,PR_5,PR_6)\end{aligned}$$

最后输出代理签名 $p\sigma=(ID_A,ID_1,\cdots,ID_t,W,p\sigma')$。

(10) 代理签名验证算法 PV。若下面等式：

$$e(g,PR_1)=z_1^{2t}(PR_2)^{u'+\sum_{i\in U_A}u_i}(\prod_{k=1}^{t}PR_{3,k})^{u'+\sum_{i\in U_k}u_i}\cdot e(w'\prod_{j\in W}w_j,PR_4\cdot R)e(m'\prod_{k\in M}m_k,PR_4\cdot R')$$

成立，则 $p\sigma$ 是任意 $k(t\leqslant k\leqslant n)$ 个有效部分代理签名人在 m 上的有效代理签名，输出 1，否则输出 0。

4 方案攻击

本节给出于-郑方案的 3 个伪造攻击算法，通过这 3 个算法可以分别成功地对于-郑方案中的普通签名和部分代理签名进行伪造攻击。

为了叙述方便，假定用户身份 u^* 为一个长度为 n_u 的比特串，令 U 为 u^* 中比特值为 1 的位置的集合。消息 m^* 为一个长度为 n_m 的比特串，令 M 为 m^* 中比特值为 1 的位置的集合。授权文件 w^* 为一个长度为 n_w 的比特串，令 W 为 w^* 中比特值为 1 的位置的集合。

4.1 对普通签名的伪造攻击

攻击 1　多项式时间的攻击者可以通过如下步骤对于-郑方案中的普通签名算法进行伪造攻击：

1. Setup 阶段。挑战者运行 Setup 算法，得到系统参数 $params=(p,g,g_1,g_2,u',U_v,m',M_v,z_1,z_2)$ 和主密钥 $mk=a$。挑战者公开系统参数 $params$，但将主密钥保密。

2. Queries 阶段。攻击者不向挑战者做任何询问。

3. Forgery 阶段。攻击者进行如下操作：

(1) 任意选择 $\sigma_1^* \in G, s \in Z_p$，令 $\sigma_2^* = g^s$。

(2) 令 $id=u'+\sum_{i\in U_A} u_i^* \in Z_p$，$msg=e(\sigma_2^*, m'\prod_{j\in W} m_j^*) \in G_T$。

(3) 令 $\Sigma_3^* = e(g,\sigma_2^*) \cdot z_1^{-1} \cdot msg^{-1}$，$\Sigma_3^* \in G_T$。

(4) 计算 $\sigma_3^* = (\Sigma_3^*)^{id^{-1}}$。

(5) 令 $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*)$，输出 (u^*, m^*, σ^*)。

若 (u^*, m^*, σ^*) 满足以下 3 个条件，则攻击成功：

(1) $\mathrm{Verify}(params, u^*, m^*, \sigma^*) = Accept$。

(2) 攻击者未对身份 u^* 做密钥询问。

(3) 攻击者未对 u^*, m^* 做签名询问。

由于在 Queries 阶段攻击者未向挑战者作任何询问，因此条件(2)、(3)显然成立，下面验证条件(1)是否成立，即验证等式 $e(g,\sigma_1^*) = z_1 \cdot (\sigma_3^*)^{u'+\sum_{i\in U} u_i^*} \cdot e(\sigma_2^*, m'\prod_{j\in W} m_j^*)$ 是否成立，验证如下：

$$
\begin{aligned}
\text{右边} &= z_1 \cdot (\sigma_3^*)^{u'+\sum_{i\in U} u_i^*} \cdot e(\sigma_2^*, m'\prod_{j\in W} m_j^*) \\
&= z_1 \cdot (\sigma_3^*)^{id} \cdot msg \\
&= z_1 \cdot ((\Sigma_3^*)^{id^{-1}})^{id} \cdot msg \\
&= z_1 \cdot ((e(g,\sigma_2^*) \cdot z_1^{-1} \cdot msg^{-1})^{id^{-1}})^{id} \cdot msg \\
&= z_1 \cdot e(g,\sigma_2^*) \cdot z_1^{-1} \cdot msg^{-1} \cdot msg \\
&= z_1 \cdot e(g,\sigma_2^*) \cdot z_1^{-1} \\
&= e(g,\sigma_2^*) \cdot z_1 \cdot z_1^{-1} \\
&= e(g,\sigma_2^*) \\
&= \text{左边}
\end{aligned}
$$

经验证，攻击 1 中攻击者的输出 (u^*, m^*, σ^*) 是于-郑方案中普通签名的一组有效签名。因此，攻击 1 是有效的。由于仿真攻击过程中不存在失败的情况，故于-郑方案是不安全的。

4.2 对门限代理签名的伪造攻击

攻击 2　多项式时间的攻击者可以通过如下步骤对于-郑方案中的部分代理签名算法进行伪造攻击：

1. Setup 阶段。挑战者运行 Setup 算法，得到系统参数 $params=(p,g,g_1,g_2,u',U_v,m',M_v,z_1,z_2)$ 和主密钥 $mk=a$。挑战者公开系统参数 $params$，但将主密钥保密。

2. Queries 阶段。攻击者不向挑战者做任何询问。

3. Forgery 阶段。攻击者进行如下操作：

(1) 任意选择 $p\sigma_{k,1}^* \in G, r_k, r_w, w_k, x_k, y_k \in Z_p$，则有：

$p\sigma_{k,3}^* = z_2^{r_k} \in G$，$p\sigma_{k,4}^* = g^{r_w} \in G$

$p\sigma_{k,5}^* = g^{r_k w_k} \in G$，$p\sigma_{k,6}^* = g^{y_k w_k} \in G$

(2) 令 $id_A = u' + \sum_{i\in U_A} u_i \in Z_p$，$id_k = u' + \sum_{i\in U_k} u_i^* \in Z_p$

$msg = e(p\sigma_{k,6}^*, m'\prod_{j\in W} m_j^*) \in G_T$

$warr = e(p\sigma_{k,4}^* p\sigma_{k,5}^*, w'\prod_{j\in W} w_j^*) \in G_T$

(3) 计算：

$P\Sigma_{k,2}^* = e(g, p\sigma_{k,1}^*)(z_1^2)^{-1}(p\sigma_{k,3}^*)^{(id_k)^{-1}} \cdot msg^{-1} \cdot warr^{-1}$，且 $P\Sigma_{k,2}^* \in G_T$。

(4) 计算 $P\sigma_{k,2}^* = (P\Sigma_{k,2}^*)^{id_A^{-1}}$。

(5) 令：$P\sigma_k^* = (p\sigma_{k,1}^*, p\sigma_{k,2}^*, p\sigma_{k,3}^*, p\sigma_{k,4}^*, p\sigma_{k,5}^*, p\sigma_{k,6}^*)$，输出 $(u_A, w^*, u_k^*, m^*, P\sigma_k^*)$。

若 $(u_A, w^*, u_k^*, m^*, P\sigma_k^*)$ 满足以下 4 个条件，则攻击成功：

(1) $P\sigma_k^*$ 可以通过部分代理签名验证算法 TPV。

(2) 攻击者未对身份 u_k^* 做密钥询问。

(3) 原始签名人未对 u_k^* 做代理签名授权。

(4) 攻击者未对 (u_k^*, m^*) 做部分代理签名询问。

由于在 Queries 阶段攻击者未向挑战者作任何询问，因此条件(2)－(4)显然成立，下面验证条件(1)是否成立。即验证等式：

$$
e(g, p\sigma_{k,1}^*) = z_1^2 (p\sigma_{k,2}^*)^{u'+\sum_{i\in U_A} u_i} (p\sigma_{k,3}^*)^{u'+\sum_{i\in U_k} u_i^*} \cdot e(w'\prod_{j\in W} w_j^*, p\sigma_{k,4}^* p\sigma_{k,5}^*) e(m'\prod_{k\in M} m_k^*, p\sigma_{k,6}^*)
$$

是否成立，验证如下：

$$
\begin{aligned}
\text{右边} &= z_1^2 (p\sigma_{k,2}^*)^{u'+\sum_{i\in U_A} u_i} (P\sigma_{k,3}^*)^{u'+\sum_{i\in U_k} u_i^*} \cdot e(w'\prod_{j\in W} w_j^*, p\sigma_{k,4}^* p\sigma_{k,5}^*) e(m'\prod_{k\in W} m_k^*, p\sigma_{k,6}^*) \\
&= z_1^2 ((P\sigma_{k,2}^*)^{u'+\sum_{i\in U_A} u_i} (P\sigma_{k,3}^*)^{id_k} \cdot warr \cdot msg \\
&= z_1^2 ((P\Sigma_{k,2}^*)^{id_A^{-1}})^{u'+\sum_{i\in U_A} u_i} (p\sigma_{k,3}^*)^{id_k} \cdot warr \cdot msg \\
&= z_1^2 ((P\Sigma_{k,2}^*)^{id_A^{-1}})^{id_A} (p\sigma_{k,3}^*)^{id_k} \cdot warr \cdot msg \\
&= z_1^2 (P\Sigma_{k,2}^*)(p\sigma_{k,3}^*)^{id_k} \cdot warr \cdot msg \\
&= z_1^2 (e(g, p\sigma_{k,1}^*)(z_1^2)^{-1}(p\sigma_{k,3}^*)^{(id_k)^{-1}} \cdot msg^{-1} \cdot warr^{-1})(p\sigma_{k,3}^*)^{id_k} \cdot warr \cdot msg \\
&= z_1^2 (e(g, p\sigma_{k,1}^*)(z_1^2)^{-1}(p\sigma_{k,3}^*)^{(id_k)^{-1}} \cdot msg^{-1})(p\sigma_{k,3}^*)^{id_k} \cdot msg \\
&= z_1^2 (e(g, p\sigma_{k,1}^*)(z_1^2)^{-1}(p\sigma_{k,3}^*)^{(id_k)^{-1}})(p\sigma_{k,3}^*)^{id_k} \\
&= z_1^2 (e(g, p\sigma_{k,1}^*)(z_1^2)^{-1}) \\
&= e(g, p\sigma_{k,1}^*) \\
&= \text{左边}
\end{aligned}
$$

经验证，攻击 2 中攻击者的输出 $(u_A, w^*, u_k^*, m^*, P\sigma_k^*)$ 是于-郑签名方案中一组有效的部分代理签名。因此，攻击 2 是有效的。由于在仿真攻击过程中不存在失败的情况，故于-郑方案是不安全的。

下面给出对于-郑方案中部分代理签名的另一个伪造攻击算法。

攻击 3　多项式时间的攻击者可以通过如下步骤对于-郑方案中的部分代理签名算法进行伪造攻击：

1. Setup 阶段。挑战者运行 Setup 算法，得到系统参数 $params=(p,g,g_1,g_2,u',U_v,m',M_v,z_1,z_2)$ 和主密钥 $mk=a$。挑战者公开系统参数 $params$，但将主密钥保密。

2. Queries 阶段。攻击者不向挑战者做任何询问。

3. Forgery 阶段。攻击者进行如下操作：

(1) 任意选择 $p\sigma_{k,1}^* \in G, r_a, r_w, w_k, x_k, y_k \in Z_p$，则有：

$p\sigma_{k,2}^{*}=z_2{}^{r_a}\in G, p\sigma_{k,4}^{*}=g^{r_w}\in G$

$p\sigma_{k,5}^{*}=g^{r_k w_k}\in G, p\sigma_{k,6}^{*}=g^{y_k w_k}\in G$

(2) 令 $id_A=u'+\sum_{i\in U_A}u_i\in Z_p, id_k=u'+\sum_{i\in U_A}u_i^{*}\in Z_p$

$msg=e(p\sigma_{k,6}^{*}, m'\prod_{j\in W}m_j^{*})\in G_T$

$warr=e(p\sigma_{k,4}^{*}p\sigma_{k,5}^{*}, w'\prod_{j\in W}w_j^{*})\in G_T$

(3) 计算：

$P\Sigma_{k,3}^{*}=e(g, p\sigma_{k,1}^{*})(z_1^2)^{-1}(p\sigma_{k,2}^{*})^{(id_A)^{-1}}\cdot msg^{-1}\cdot warr^{-1}$，且 $P\Sigma_{k,3}^{*}\in G_T$。

(4) 计算 $P\sigma_{k,3}^{*}=(P\Sigma_{k,3}^{*})^{id_k{}^{-1}}$。

(5) 令：$P\sigma_k^{*}=(p\sigma_{k,1}^{*}, p\sigma_{k,2}^{*}, p\sigma_{k,3}^{*}, p\sigma_{k,4}^{*}, p\sigma_{k,5}^{*}, p\sigma_{k,6}^{*})$，输出$(u_A, w^{*}, u_k^{*}, m^{*}, P\sigma_k^{*})$。若$(u_A, w^{*}, u_k^{*}, m^{*}, P\sigma_k^{*})$满足与攻击 2 中列出的 4 个条件，则攻击成功。

由于在 Queries 阶段攻击者未向挑战者做任何询问，因此条件(2)—(4)显然成立，下面验证条件(1)是否成立。即验证：

$$e(g, p\sigma_{k,1}^{*})=z_1^2(p\sigma_{k,2}^{*})^{u'+\sum_{i\in U_A}u_i}(p\sigma_{k,3}^{*})^{u'+\sum_{i\in U_k}u_i{}^{*}}\cdot e(w'\prod_{j\in W}w_j^{*}, p\sigma_{k,4}^{*}p\sigma_{k,5}^{*})e(m'\prod_{k\in W}m_k^{*}, p\sigma_{k,6}^{*})$$

是否成立，验证如下：

$$\begin{aligned}
\text{右边}&=z_1^2(p\sigma_{k,2}^{*})^{u'+\sum_{i\in U_A}u_i^{*}}p\sigma_{k,3}^{*}{}^{u'+\sum_{i\in U_k}u_i^{*}}\cdot e(w'\prod_{j\in W}w_j^{*}, p\sigma_{k,4}^{*}p\sigma_{k,5}^{*})e(m'\prod_{k\in W}m_k^{*}, p\sigma_{k,6}^{*})\\
&=z_1^2(p\sigma_{k,2}^{*})^{u'+\sum_{i\in U_A}u_i}(P\sigma_{k,3}^{*})^{id_k}\cdot warr\cdot msg\\
&=z_1^2(p\sigma_{k,2}^{*})^{id_A}((P\Sigma_{k,3}^{*})^{id_k^{-1}})^{id_k}\cdot warr\cdot msg\\
&=z_1^2(p\sigma_{k,2}^{*})^{id_A}(P\Sigma_{k,3}^{*})\cdot warr\cdot msg\\
&=z_1^2(p\sigma_{k,2}^{*})^{id_A}(e(g, p\sigma_{k,1}^{*})(z_1^2)^{-1}(p\sigma_{k,2}^{*})^{(id_A)^{-1}}\cdot msg^{-1})\cdot msg\\
&=z_1^2(p\sigma_{k,2}^{*})^{id_A}(e(g, p\sigma_{k,1}^{*})(z_1^2)^{-1}(p\sigma_{k,2}^{*})^{(id_A)^{-1}})\\
&=z_1^2(e(g, p\sigma_{k,1}^{*})(z_1^2)^{-1})\\
&=z_1^2(z_1^2)^{-1}e(g, p\sigma_{k,1}^{*})\\
&=e(g, p\sigma_{k,1}^{*})\\
&=\text{左边}
\end{aligned}$$

经验证，攻击 3 中攻击者的输出$(u_A, w^{*}, u_k^{*}, m^{*}, P\sigma_k{}^{*})$是于-郑签名方案中一组有效的部分代理签名。因此，攻击 3 是有效的。由于在仿真攻击过程中不存在失败的情况，故于-郑方案是不安全的。

5 被攻击原因分析

于-郑的基于身份的门限代理签名方案之所以受到攻击，其原因分析如下：

(1) 其直接原因是在于-郑的签名方案中：普通签名 $\sigma=(\sigma_1, \sigma_2, \sigma_3)$或者部分门限代理签名 $p\sigma_k=(p\sigma_{k,1}, p\sigma_{k,2}, p\sigma_{k,3}, p\sigma_{k,4}, p\sigma_{k,5}, p\sigma_{k,6})$在其验证算法的等式中存在多项式时间可解的部分。以普通签名为例：已知 σ_1, σ_2可以从验证算法中分离出(解出)σ_3。得到的 $\sigma=(\sigma_1, \sigma_2, \sigma_3)$将恒满足验证算法中的验证等式。

(2) 其根本原因是方案设计者为了减少双线性映射的运算次数，提高计算效率，结果以不安全的方式使用了用户标识或者消息的比特串。以普通方案为例：用户的密钥抽取过程中，用户私钥的计算使用了 $g_2^{a+r(u'+\sum_{i\in U_A}u_i)}$ 的加法形式。并且在验证过程中未对该部分做双线性映射运算，产生了安全隐患。

针对上面分析的原因，以方案中的普通签名为例，提出如下两种可能的改进措施：

(1)可以将公开签名私钥的第二部分，即 $d_u=(d_0, d_1)$中的 d_1，作为公钥，以防止由原因 (1)导致的攻击。但从 d_1 的产生过程发现，这一部分是与用户的身份独立的。因此，要把 d_1 作为用户的公钥，必须要对其做出认证(确认 d_1 与用户的绑定关系)，这将导致原方案变得复杂。(2) 改变使用用户身份 u 和消息 m 的方式，即使用 $g_2^{a}\cdot(u'\prod_{j\in U}u_j)^{t}$ 和$(m'\prod_{j\in M}m_j)^{s}$的乘法形式，而不是 $g_2^{a+r(u'+\sum_{j\in U}u_j)}$和$(g_2^{s})^{(m'+\sum_{j\in M}m_j)}$的形式，让它们在验证过程中参与双线性映射计算，以防止由原因(2)导致的攻击。

结束语 本文针对于-郑的基于身份的门限代理签名方案设计了 3 个有效的伪造攻击算法。利用这些算法，攻击者可以在不得到原始签名人和任何代理签名人私钥的情况下，仅通过选取随机参数以及多项式时间内的计算，就可成功地伪造普通签名或任意代理签名人的部分签名。本文还分析了原方案遭受攻击的原因，并给出了两种可能的改进措施。

参 考 文 献

[1] Shamir A. Identity-Based Cryptosystems and Signature Schemes [J]. Advances in Cryptology. Springer Berlin/Heidelberg, 1985, 196: 47-53

[2] Mambo M, Usuda K, Okamoto E. Proxy signature for delegating signing operation [C] // Proc of the 3rd ACM Conference on Computer and Communications Security. ACM Press, 1996: 48-57

[3] Zhang F G, Kim K. Efficient ID-based blind signature and proxy signature from bilinear pairings [J]. Information Security and Privacy. Springer Berlin/Heidelberg, 2003, 2727: 218-219

[4] Zhang K. Threshold proxy signature schemes [J]. Information Security, 1998, 1396: 282-290

[5] 鲁荣波，何大可，王常吉. 对一种基于身份的已知签名人的门限代理签名方案的分析[J]. 电子与信息学报，2008，30(1)：100-103

[6] Waters B. Efficient Identity-Based Encryption Without Random Oracles [J]. Advances in Cryptology-EUROCRYPT, 2005, 3494: 557-557

[7] Paterson K, Schuldt J, Efficient Identity-Based Signatures Secure in the Standard Model[J]. Information Security and Privacy, 2006, 4058: 207-222

[8] 谷科，贾维嘉，姜春林. 高效安全的基于身份的签名方案[J]. 软件学报，2011，22(6)：1350-1360

[9] 于义科，郑雪峰，韩晓光. 一种标准模型下基于身份的高效门限代理签名方案[J]. 计算机应用研究，2011(3)：1136-1141

[10] 于义科，郑雪峰，韩晓光. 一个标准模型下基于身份的高效代理签名方案[J]. 计算机科学，2011(6)：133-139

[11] 于义科，郑雪峰. 标准模型下基于身份的高效动态门限代理签名方案[J]. 通信学报，2011(08)：55-63