一种可证安全的基于身份门限代理签密方案

孙 华[1] 郭 磊[1] 郑雪峰[2] 王爱民[1]
(安阳师范学院计算机与信息工程学院 安阳 455000)[1] (北京科技大学信息工程学院 北京 100083)[2]

摘 要 代理签名可以实现签名权利的委托,具有可认证性和不可否认性,然而却不能提供保密性。签密是一种将加密和签名结合在一起的技术,它同时具有两者的优点。利用双线性对技术,提出了一种在标准模型下有效的基于身份门限代理签密方案,并对方案的安全性进行了分析。最后,通过DBDH问题的困难性证明了方案的语义安全性,同时利用CDH问题的困难性证明了方案的不可伪造性。

关键词 基于身份的密码学,门限代理签密,双线性对,CDH问题,DBDH问题
中图法分类号 TP309 **文献标识码** A

Provable Secure Identity-based Threshold Proxy Signcryption Scheme

SUN Hua[1] GUO Lei[1] ZHENG Xue-feng[2] WANG Ai-min[1]
(School of Computer and Information Engineering, Anyang Normal University, Anyang 455000, China)[1]
(School of Information Engineering, University of Science and Technology Beijing, Beijing 100083, China)[2]

Abstract The proxy signature allows a designated person, called a proxy signer, to sign on behalf of an original signer. It has the properties of authenticity and non-repudiation of message except confidentiality. Signcryption is a technique that can encrypt and sign data together in some way, while it has merits of them. This paper presented an efficient identity-based threshold signcryption scheme in the standard model and gave its security analysis in terms of bilinear pairing technique. At last, we proved its semantic security on the hardness of Decisional Bilinear Diffie-Hellman problem and its unforgeability on the hardness of Computational Diffie-Hellman problem.

Keywords Identity based cryptography, Threshold proxy signcryption, Bilinear pairing, Computational diffie-hellman problem, Decisional bilinear diffie-hellman problem

1984年,Shamir[1]首先提出了基于身份的公钥密码体制,用以解决传统公钥密码体制中的证书管理。在基于身份的密码体制中,用户的公钥为能够标识用户身份的信息,如E-mail地址或IP地址,而其私钥则由可信第三方生成。2001年,Boneh和Franklin[2]利用双线性对技术提出了第一个实用的基于身份的加密方案,随后基于身份的密码学迅速成为人们研究的热点。

1996年,Mambo等人[3]提出了代理签名的概念,以实现数字签名权利的委托。通常在一个代理签名方案中包含原始签名人、代理签名人和验证者,由原始签名人将其签名权委托给代理签名人,代理签名人代表原始签名人生成有效的数字签名。由于代理签名的广泛应用,因此其一提出就一直受到密码学界的广泛关注。

代理签名与基于身份的密码体制相结合,形成了基于身份的代理签名。2003年,Zhang和Kim[4]提出了第一个基于身份的代理签名方案,不过文献中只是对方案做了简单的安全分析。随后,人们又陆续提出了一些基于身份的代理签名方案[5,6]。

消息的保密和认证是密码学中最重要的两个研究内容,如何在消息通信过程中同时实现保密和认证是信息安全研究的主要目标之一。1997年,Zheng[7]首次提出了签密的概念,即能够在一个合理的步骤内同时完成加密和数字签名两项功能,而其通信成本和计算量都低于传统的先签名后加密方法。Dodis[8]等人第一次对签密方案的机密性和不可伪造性进行了形式化的描述,随后一些可证安全的签密方案被相继提出。

2002年,Malone-Lee[9]提出了第一个基于身份的签密方案,该方案具有消息的保密性和签名的不可伪造性。然而Libert[10]等人指出Malone-Lee的方案不是语义安全的,并提出了满足语义安全的基于身份的签密方案。2004年,Duan[11]等人提出了一个基于身份的门限签密方案,可是该方案不满足不可否认性和语义安全性。2008年,Li[12]等人提出了一个可证安全的基于身份的门限签密方案,可是该方案不满足不可伪造性。2009年,Yu[13]等人提出了一个在标准模型下基于身份的签密方案,然而该方案不满足密文的不可区分

到稿日期:2011-11-21 返修日期:2012-01-19 本文受国家自然科学基金资助项目(61170244),河南省科技攻关计划项目(112102210370),河南省教育厅自然科学基础研究计划项目(12A520002)资助。
孙 华(1980-),男,博士,讲师,主要研究方向为密码学与信息安全,E-mail:sh1227@163.com;郭 磊(1976-),男,硕士,讲师,主要研究方向为信息安全理论与技术;郑雪峰(1951-),男,教授,主要研究方向为网络与信息安全;王爱民(1957-),男,教授,主要研究方向为数据挖掘、信息处理。

性和存在不可伪造性。2010年，Sharmila等人[14]对已有的几个门限签密方案进行了分析，指出它们并不是安全的，同时针对每一种方案给出了改进后的方案并进行了安全性分析。2011年，Kushwah等人[15]对已有几个基于身份的签密方案进行了分析，指出它们是不安全的，同时提出了一个在标准模型下基于身份的签密方案。Li等人[16,17]提出了两个基于身份的门限代理签密方案，然而其均是基于随机预言模型的。

随机预言机是一个函数，它的输出是随机和不可预测的。当密码算法中的哈希函数被假设为随机预言机时，这个模型就称为随机预言模型，它是由Bellare等人[18]提出的一种非标准化的计算模型。然而，该模型存在缺陷，不能全面考虑攻击者的实际能力。

本文将门限签密和代理相结合，提出了一个基于身份的门限代理签密方案，并且利用DBDH问题和CDH问题的困难性证明了方案的语义安全性和不可伪造性。由于随机预言模型下可证安全的方案在具体应用中有时无法构造相应的实例，因此，设计在标准模型下高效且可证安全的门限代理签密方案更有实际意义。

1 预备知识

1.1 双线性对

设G、G_T是两个阶为素数q的循环加法群和循环乘法群，g是群G的生成元，双线性对$e:G\times G\to G_T$是具有如下性质的映射：

1. 双线性：对于所有的$P,Q\in G$与$a,b\in Z^*$，都有$e(aP,bQ)=e(P,Q)^{ab}$；

2. 非退化性：$e(g,g)\neq 1$；

3. 可计算性：存在一个有效的算法用于计算$e(P,Q)$，其中$P,Q\in G$。

1.2 困难问题假设

DBDH问题：已知G和G_T是两个阶为素数q的循环群，P是群G的生成元，$e:G\times G\to G_T$为双线性映射，给定$P,P^a,P^b,P^c\in G,h\in G_T,a,b,c\in Z_q^*$，判定是否$h=e(P,P)^{abc}$。

CDH问题：已知G是阶为素数q的循环群，P是群G的生成元，给定$P,aP,bP\in G,a,b\in_R Z_p^*$，计算$abP$。

2 基于身份的门限代理签密

2.1 形式化定义

定义1 设P_A是原始签密者，$PS=\{P_1,P_2,\cdots,P_n\}$是由代理人组成的代理签密组，基于身份的$(t,n)$门限代理签密方案可由以下算法组成，即系统建立、私钥提取、秘密分享、代理授权(TD,TP)、签密和解签密。

1. 系统建立：给定安全参数k，该算法生成系统参数$params$、公钥P_{pub}以及相应的主密钥s。

2. 私钥提取：输入系统参数$params$、主密钥s和用户身份ID，该算法输出身份ID的私钥s_{ID}。

3. 秘密分享：每个代理人$P_i(i=1,\cdots,n)$选择其子秘密s_i以及$t-1$次多项式$f_i(x)$，广播公开参数，然后计算其它各代理人$P_j(j\neq i)$的秘密分享，并将它们秘密发送给其它代理人。各代理人P_j可以通过验证来鉴别其收到的秘密分享是否正确，并最终计算其私有秘密x_i。

4. 代理授权：原始签密者P_A将其签名权委托给代理签密组的各个成员$P_i(i=1,\cdots,n)$，并由各代理签密人生成相应的代理签名私钥ps_i。

5. 签密：输入系统参数$params$、待签密消息m、t个代理成员的代理签名私钥$\{ps_i\}_{i=1,\cdots,t}$以及解签密者的身份ID_B，该算法输出在消息m上的(t,n)门限代理签密c。

6. 解签密：输入系统参数$params$、密文c、原始签密者的身份ID_A、代理人的身份$ID_i(i=1,\cdots,t)$以及解签密者的私钥s_{ID_B}，该算法输出明文m；如果c不是一个有效的门限代理签密，则输出$\perp$，否则，方案需满足一致性检查，即如果$c=Signcrypt(m,\{ps_i\}_{i=1,\cdots,t},ID_B)$，则有$m=Unsigncrypt(c,ID_A,ID_1,\cdots,ID_t,S_{ID_B})$。

2.2 基于身份门限代理签密(IBTPSC)的安全要求

基于身份的门限代理签密方案应满足下面的安全要求。

1)可区分性：任何人都可以区分标准签密方案和门限代理签密方案。

2)可验证性：由门限代理签密，验证者能确信它是由代理者经原始签密者授权而产生的。

3)强可识别性：任何人能够从门限代理签密中识别相应的代理签密者的身份。

4)强不可伪造性：代理签密者能代表原始签密者产生有效的门限代理签密，而原始签密者和其他没有被指定为代理签密者的第三方都不能产生有效的门限代理签密。

5)强不可否认性：如果代理签密者代表原始签密者生成一个有效的门限代理签密，它们不能否认该签密的生成。

6)抗滥用性：代理签密者不能将其代理密钥用于除产生有效门限代理签密以外的其它目的，也就是说，它们不能未经授权而产生签密密文。

7)机密性：对于攻击者而言，由签密密文获取任何有关签密消息信息在计算上是不可行的。

3 标准模型下基于身份的门限代理签密方案

3.1 方案描述

设P_A是原始签密者，身份为ID_A，$PS=\{P_1,\cdots,P_n\}$是一个由代理人组成的代理签密组，相应身份为$ID_i(i=1,\cdots,n)$，P_B是解签密者，身份为ID_B，W是授权文件(包括原始签密人和代理签密人的身份信息、代理权限的有效期等)，t为门限值。设用户的身份ID、授权文件W分别是长度为n_u和n_w的比特串。方案由如下几个算法构成：

(1)系统建立

令G、G_T是阶为素数p的循环群，生成元$g\in G$，双线性映射为$e:G\times G\to G_T$，PKG随机选取$\alpha\in Z_p$，计算$g_1=g^\alpha$。随机选取$g_2,u',w',m'\in G$，n_u维向量$U_v=(u_i)$，n_w维向量$W_v=(w_i)$，n_m维向量$M_v=(m_i)$，其中$u_i,w_i,m_i\in_R G$，两个密码学意义上的Hash函数$H_1:G_T\to\{0,1\}^{n_m}$，$H_2:\{0,1\}^*\to\{0,1\}^{n_u}$，则系统参数为$param=(G,G_T,e,g,g_1,g_2,u',U_v,w',W_v,m',M_v,H_1,H_2)$，主密钥为$msk=g_2^\alpha$。

(2)私钥提取

给定用户身份ID，令u为代表身份ID的长度为n_u的位串，$u[i]$表示该位串中的第i位，$\Phi_u\subseteq\{1,2,\cdots,n_u\}$为$u[i]=1$的序号$i$的集合，PKG任选$r_u\in Z_p$，则身份$ID$的私钥为：

$$d_{ID}=(d_1,d_2)=(g_2^\alpha(u'\prod_{i\in\Phi_u}u_i)^{r_u},g^{r_u})$$

(3)秘密分享

①每个代理人 P_i 随机选取 $s_i \in Z_p$ 为其子秘密，公开 $r_i = g^{s_i}$，选取系数为 Z_p、次数为 $t-1$ 的多项式 $f_i(x)$：

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

令 $s_i = a_{i,0}$，P_i 广播 $C_{i,d} = g^{a_{i,d}}$ $(d=0,1,\cdots,t-1)$，并计算分享 $s_{i,j} = f_i(j)$，然后把它们秘密发送给其它成员 P_j $(j=1,2,\cdots,n; j\neq i)$，自己保留 $s_{i,i} = f_i(i)$。

②成员 P_j 从 P_i 那里得到分享 $s_{i,j}$ 后，用如下等式验证其有效性：$g^{s_{i,j}} = \prod_{d=0}^{t-1}(c_{i,d})^{j^d}$，如果没有通过验证，则 P_j 发出对 P_i 的控告。

③每个成员 P_i 计算其私有密钥 $x_i = \sum_{j=1}^{n} s_{j,i}$ 以及 $R = \prod_{i=1}^{n} r_i$。

(4)代理授权(TD,TP)

TD:对于授权文件 W，令 w 是长度为 n_w 的位串，$w[i]$ 表示该位串中的第 i 位，$\mathcal{W} \subseteq \{1,2,\cdots,n_w\}$ 为 $w[i]=1$ 的序号 i 的集合。原始签密者 ID_A 的私钥为 $(d_{A,1}, d_{A,2})$，随机选取 $r_w \in Z_p$，并计算

$$\sigma_w = (d_{A,1}(w'\prod_{i\in\mathcal{W}} w_i)^{r_w}, d_{A,2}, g^{r_w}) = (g_2^{\alpha}(u'\prod_{i\in\Phi_A} u_i)^{r_A}(w'\prod_{i\in\mathcal{W}} w_i)^{r_w}, g^{r_A}, g^{r_w}) = (\sigma_{w1}, \sigma_{w2}, \sigma_{w3})$$

然后原始签密人 ID_A 发送 (W,σ_w) 给每个代理成员 P_i $(i=1,\cdots,n)$，其中 σ_w 是原始签密人产生的授权证书。

TP:代理签名人 P_i 通过验证下面等式判断 (W,σ_w) 是否有效：

$$e(\sigma_{w1}, g) = e(g_1, g_2)e(u'\prod_{i\in\Phi_A} u_i, \sigma_{w2})e(w'\prod_{i\in\mathcal{W}} w_i, \sigma_{w3})$$

如果成立，代理签名人 P_i 计算

$$ps_i = (\sigma_{w1}\cdot d_{i,1}, \sigma_{w2}, d_{i,2}, \sigma_{w3}) = (ps_{i,1}, ps_{i,2}, ps_{i,3}, ps_{i,4})$$

式中，ps_i 为代理签密人 P_i 生成的代理签名私钥。

(5)签密

令 $m \in G_T$ 为待签密消息，为发送消息 m 给签密接收者 ID_B，各代理签密人 P_i 随机选取 $y_i \in Z_p$ 并执行以下步骤：

①计算 $\sigma_{1i} = e(g_1, g_2)^{y_i}$

②计算 $\sigma_{2i} = g^{y_i}$

③计算 $\sigma_{3i} = (u'\prod_{i\in\Phi_B} u_i)^{y_i}$

④计算 $M = H_1(m)$，令 $\mathcal{M} \subseteq \{1,2,\cdots,n_m\}$ 表示该位串中 $M[i]=1$ 的序号 i 的集合，计算 $\sigma_{4i} = \sigma_{w1}\cdot d_{i,1}(m'\prod_{i\in\mathcal{M}} m_i)^{x_i\eta_i}$，其中 $\eta_i = \prod_{j=1,j\neq i}^{t} \frac{j}{j-i} \bmod p$ 为拉格朗日系数。

⑤计算 $\sigma_{5i} = d_{i,2} = g^{r_i}$

⑥计算 $\sigma_{6i} = \sigma_{w2} = g^{r_A}$

⑦计算 $\sigma_{7i} = \sigma_{w3} = g^{r_w}$

⑧计算 $\sigma_{8i} = g^{x_i\eta_i}$

然后把 $(\sigma_{1i}, \sigma_{2i}, \sigma_{3i}, \sigma_{4i}, \sigma_{5i}, \sigma_{6i}, \sigma_{7i}, \sigma_{8i})$ 发送给门限代理签密生成者 C，其计算 $\sigma_1 = \prod_{i=1}^{t}\sigma_{1i}m$，$\sigma_2 = \prod_{i=1}^{t}\sigma_{2i}$，$\sigma_3 = \prod_{i=1}^{t}\sigma_{3i}$，$\sigma_4 = \prod_{i=1}^{t}\sigma_{4i}$，$\sigma_6 = \prod_{i=1}^{t}\sigma_{6i}$，$\sigma_7 = \prod_{i=1}^{t}\sigma_{7i}$，$\sigma_8 = \prod_{i=1}^{t}\sigma_{8i}$，则最终的门限代理签密为 $\sigma = (\sigma_1, \sigma_2, \sigma_3, \sigma_4, \sigma_{5,1}, \sigma_{5,2}, \cdots, \sigma_{5,t}, \sigma_6, \sigma_7, \sigma_8)$。

(6)解签密

当收到门限代理签密 σ 后，解签密者 ID_B 进行如下计算：

①计算 $m = \sigma_1 \cdot e(d_{B,2}, \sigma_3)e(d_{B,1}, \sigma_2)^{-1}$

②计算 $M = H_1(m)$，并令 $\mathcal{M} \subseteq \{1,2,\cdots,n_m\}$ 表示该位串中 $M[i]=1$ 的序号 i 集合。

③当且仅当等式

$$e(\sigma_4, g) = e(g_1, g_2)^{2t}\cdot e(u'\prod_{i\in\Phi_A} u_i, \sigma_6)\cdot e(w'\prod_{i\in\mathcal{W}} w_i, \sigma_7)\cdot \prod_{i=1}^{t} e(u'\prod_{i\in\Phi_i} u_i, \sigma_{5i})\cdot e(m'\prod_{i\in\mathcal{M}} m_i, R)$$

3.2 方案正确性

根据秘密共享技术，有：

$\sum_{i=1}^{t} x_i\eta_i = f(0) = \sum_{i=1}^{n} f_i(0) = \sum_{i=1}^{n} s_i$，对签密 σ，有：

$$\sigma_1 = \prod_{i=1}^{t}\sigma_{1i}m = e(g_1, g_2)^{\sum_{i=1}^{t} y_i}m, \text{令 } Y = \sum_{i=1}^{t} y_i$$

$$\sigma_2 = \prod_{i=1}^{t}\sigma_{2i} = g^Y, \sigma_3 = \prod_{i=1}^{t}\sigma_{3i} = (u'\prod_{i\in\Phi_B} u_i)^Y$$

$$\sigma_4 = \prod_{i=1}^{t}\sigma_{4i} = g_2^{2\alpha}(u'\prod_{i\in\Phi_A} u_i)^{r_A}(w'\prod_{i\in\mathcal{W}} w_i)^{r_w}\cdot \prod_{i\in 1}^{t}(u'\prod_{i\in\Phi_i} u_i)^{r_i}(m'\prod_{i\in\mathcal{M}} m_i)^{x_i\eta_i}$$

$$\sigma_6 = \prod_{i=1}^{t}\sigma_{6i} = g^{r_A}, \sigma_7 = \prod_{i=1}^{t}\sigma_{7i} = g^{r_w}$$

$$\sigma_8 = \prod_{i=1}^{t}\sigma_{8i} = R$$

对 σ 进行验证可得：

$$\sigma_1 \cdot e(d_{B,2}, \sigma_3)e(d_{B,1}, \sigma_2)^{-1} = m$$

$$e(\sigma_4, g) = e(g_1, g_2)^{2t}\cdot e(u'\prod_{i\in\Phi_A} u_i, \sigma_6)\cdot e(w'\prod_{i\in\mathcal{W}} w_i, \sigma_7)\cdot \prod_{i=1}^{t} e(u'\prod_{i\in\Phi_i} u_i, \sigma_{5i})\cdot e(m'\prod_{i\in\mathcal{M}} m_i, R)$$

3.3 方案安全性

由于在一个有效的门限代理签密中包含授权文件、原始签密人身份、代理签密人身份和解签密人身份，而在签密的验证等式中授权文件、原始签密人身份、代理签密人身份和解签密人身份需要同时出现，因此很容易看出本门限代理签密方案满足可区分性、可验证性、强可识别行、强不可否认性和抗滥用性等安全性要求。

下面证明方案满足强不可伪造性和机密性。

定理 1 在 CDH 困难问题的假设下，我们的方案在自适应选择消息攻击下满足密文的存在不可伪造性。

证明：假设伪造者 A 能以不可忽略的优势攻击上面的方案，则能够构造算法 B，B 可以利用 A 解决 CDH 问题。

给定 B 一个 CDH 问题的实例 (g, g^a, g^b)，为了计算 g^{ab}，B 模仿 A 的挑战者，具体过程如下。

系统初始化：B 设定 $l_u = 2(q_e + q_s)$、$l_m = 2q_s$，其中 q_e 是 A 私钥询问的次数，q_s 是 A 签密询问的次数。选择 k_u、k_w 和 k_m，满足 $0 \leqslant k_u \leqslant n_u$、$0 \leqslant k_w \leqslant n_w$ 和 $0 \leqslant k_m \leqslant n_m$，并假定 $l_u(n_u+1) < p$、$l_w(n_w+1) < p$ 和 $l_m(n_m+1) < p$。B 选择 $x' \in_R Z_{l_u}$ 及长度为 n_u 的向量 $X = (x_i)$，其中 $x_i \in_R Z_{l_u}$；选择 $y' \in_R Z_{l_w}$ 及长度为 n_w 的向量 $Y = (y_j)$，其中 $y_j \in_R Z_{l_w}$；选择 $z' \in_R Z_{l_m}$ 及长度为 n_m 的向量 $Z = (z_k)$，其中 $z_k \in_R Z_{l_m}$。最后 B 选择 a'，b'，$c' \in_R Z_p$，长度为 n_u 的向量 $A = (a_i)$，长度为 n_w 的向量 $B = (b_j)$，长度为 n_m 的向量 $C = (c_k)$，其中 $a_i, b_j, c_k \in_R Z_p$。

对于身份 ID、授权文件 W 和消息 m，定义以下几个函数：

$$F(ID) = x' + \sum_{i\in\Phi} x_i - l_u k_u, J(ID) = a' + \sum_{i\in\Phi} a_i$$

$$Q(W) = y' + \sum_{j\in\mathcal{W}} y_j - l_w k_w, R(W) = b' + \sum_{j\in\mathcal{W}} b_j$$

$$K(M) = z' + \sum_{k\in\mathcal{M}} z_k - l_m k_m, L(M) = c' + \sum_{k\in\mathcal{M}} c_k$$

算法 B 构造上面方案中的公开参数如下：

$g_1=g^a, g_2=g^b$

$u'=g_2^{-l_u k_u+x'} g^{a'}, u_i=g_2^{x_i} g^{a_i}, 1\leqslant i\leqslant n_u$

$w'=g_2^{-l_w k_w+y'} g^{b'}, w_j=g_2^{y_j} g^{b_j}, 1\leqslant j\leqslant n_w$

$m'=g_2^{-l_m k_m+z'} g^{c'}, m_k=g_2^{z_k} g^{c_k}, 1\leqslant k\leqslant n_m$

可以看出这些参数的分布与一个真正的挑战者产生的公开参数的分布是一样的。这样主密钥为 $g_2^a=g^{ab}$，同时有下面的等式：

$$u'\prod_{i\in\Phi_u}u_i=g_2^{F(ID)}g^{J(ID)}, w'\prod_{j\in W}w_j=g_2^{Q(W)}g^{R(W)}$$

$$m'\prod_{k\in M}m_k=g_2^{K(m)}g^{L(m)}$$

然后算法 B 将公开参数发送给敌手 A。

询问：当敌手 A 发起如下询问时，算法 B 进行如下响应：

①私钥询问：当敌手 A 询问身份 ID_u 的私钥时，虽然算法 B 不知道主密钥，但假定 $F(ID_u)\neq 0 \bmod p$，B 也能够构造其私钥 d_{ID_u}。B 任选 $r_u\in Z_p$ 并计算：

$$d_{ID_u}=(d_{u1},d_{u2})=(g_1^{-J(ID)/F(ID)}(u'\prod_{i\in\Phi_u}u_i)^{r_u}, g_1^{-1/F(ID)}g^{r_u})$$

令 $\tilde{r}_u=r_u-a/F(ID)$，可以验证 d_{ID_u} 是 ID_u 的有效私钥。

$$\begin{aligned}d_{u1}&=g_1^{-J(ID)/F(ID)}(u'\prod_{i\in\Phi_u}u_i)^{r_u}\\&=g_2^a(g_2^{F(ID)}g^{J(ID)})^{-a/F(ID)}(g_2^{F(ID)}g^{J(ID)})^{r_u}\\&=g_2^a(g_2^{F(ID)}g^{J(ID)})^{r_u-a/F(ID)}\\&=g_2^a(u'\prod_{i\in\Phi_u}u_i)^{\tilde{r}_u}\end{aligned}$$

$$d_{u2}=g_1^{-1/F(ID)}g^{r_u}=g^{r_u-a/F(ID)}=g^{\tilde{r}_u}$$

如果 $F(u)=0 \bmod p$，上面的计算将无法进行，B 将失败退出。

②门限代理私钥询问Ⅰ：敌手 A 提交原始签密人身份 ID_A 和门限代理签密人身份 $ID_i(i=1,\cdots,n)$，A 扮演原始签密人角色 P_A，首先运行 TD 算法产生授权证书

$$\sigma_w=(g_2^a(u'\prod_{i\in\Phi_A}u_i)^{r_a}(w'\prod_{j\in W}w_j)^{r_w}, g^{r_a}, g^{r_w})$$

并将 (W,σ_W) 发送给 B。B 验证 σ_W 的有效性，如果 σ_W 有效，则 B 以下面的方法构造门限代理私钥。首先判断是否有 $F(ID_i)\neq 0 \bmod l_u$，如是，则 B 先构造 ID_i 的私钥，然后运行 TP 算法产生门限代理私钥；否则，由假设 $l_w(n_w+1)<p$ 下蕴含 $Q(W)\neq 0 \bmod p$，则 B 随机选择 $r_i\in Z_p$，计算门限代理私钥：

$$\begin{aligned}ps_i&=(g_2^a(u'\prod_{i\in\Phi_A}u_i)^{r_a}(u'\prod_{i\in\Phi_i}u_i)^{r_i}g_1^{-R(W)/Q(W)}(w'\prod_{j\in W}w_j)^{r_w}, g^{r_a}, g^{r_i}, g_1^{-1/Q(W)}g^{r_w})\\&=(g_2^{2a}(u'\prod_{i\in\Phi_A}u_i)^{r_a}(u'\prod_{i\in\Phi_i}u_i)^{r_i}(w'\prod_{j\in W}w_j)^{\tilde{r}_w}, g^{r_a}, g^{r_i}, g^{\tilde{r}_w})\end{aligned}$$

式中，$\tilde{r}_w=r_w-a/Q(W)$。如果 $Q(W)=0 \bmod p$，上面的计算将无法进行，B 将失败退出。

②门限代理私钥询问Ⅱ：敌手 A 提交原始签密人身份 ID_A 和门限代理签密人身份 $ID_i(i=1,\cdots,n)$，A 扮演门限代理签密人 ID_i，如果 $F(ID_A)\neq 0 \bmod l_u$，则 B 先构造 ID_A 的私钥，然后运行 TD 算法产生授权证书 σ_W；否则，如果 $Q(W)\neq 0 \bmod l_w$，则 B 随机选择 $r_a, r_w\in Z_p$，计算

$$\begin{aligned}\sigma_W&=(g_1^{\frac{-R(W)}{Q(W)}}(u'\prod_{i\in\Phi_A}u_i)^{r_a}(w'\prod_{j\in W}w_j)^{r_w}, g^{r_a}, g_1^{-1/Q(W)}g^{r_w})\\&=(g_2^a(u'\prod_{i\in\Phi_A}u_i)^{r_a}(w'\prod_{j\in W}w_j)^{r_w'}, g^{r_a}, g^{r'_w})\end{aligned}$$

式中，$r_w'=r_w-a/Q(W)$。如果 $Q(W)=0 \bmod p$，上面的计算将无法进行，B 将失败退出。

③签密询问：敌手 A 发起一个在原始签密人 ID_A、代理签密人 $ID_i(i=1,\cdots,n)$、解签密者 ID_B 和授权文件 W 下对消息 m 的门限代理签密询问，其中 A 扮演原始签密人角色 ID_A。A 运行 TD 算法产生授权证书：

$$\sigma_w=(g_2^a(u'\prod_{i\in\Phi_A}u_i)^{r_a}(w'\prod_{j\in W}w_j)^{r_w}, g^{r_a}, g^{r_w})$$

并将 (W,σ_W) 发送给 B。B 验证 σ_W 的有效性，如果 σ_W 有效，则 B 以下面的方法构造门限代理私钥。首先判断是否有 $F(ID_i)\neq 0 \bmod l_u$，如是，则 B 构造 ID_i 的门限代理私钥，然后运行签密算法生成部分代理签密；否则，如果 $K(M)\neq 0 \bmod l_m$，则 B 随机选择 $r_i, y_i, x_i\eta_i\in Z_p$，计算：

$$\sigma_{1i}=e(g_1,g_2)^{y_i}, \sigma_{2i}=g^{y_i}, \sigma_{3i}=(u'\prod_{i\in\Phi_B}u_i)^{y_i}$$

$$\begin{aligned}\sigma_{4i}&=g_2^a(u'\prod_{i\in\Phi_A}u_i)^{r_a}(u'\prod_{i\in\Phi_i}u_i)^{r_i}(w'\prod_{j\in W}w_j)^{r_w}g_1^{-L(M)/K(M)}\\&\quad(m'\prod_{k\in M}m_k)^{x_i\eta_i}=g_2^{2a}(u'\prod_{i\in\Phi_A}u_i)^{r_a}(u'\prod_{i\in\Phi_i}u_i)^{r_i}(w'\prod_{j\in W}w_j)^{r_w}(m'\prod_{k\in M}m_k)^{\tilde{r}_m}\end{aligned}$$

$$\sigma_{5i}=g^{r_i}, \sigma_{6i}=g^{r_a}, \sigma_{7i}=g^{r_w}$$

$$\sigma_{8i}=g_1^{\frac{-1}{K(M)}}g^{x_i\eta_i}=g^{\tilde{r}_m}$$

式中，$\tilde{r}_m=x_i\eta_i-\dfrac{a}{K(M)}$，可见 σ_i 是一个有效的部分签密。如果 $K(M)=0 \bmod p$，上面的计算将无法进行，B 将失败退出。

解签密询问：敌手 A 可以发起一个在原始签密人 ID_A、代理签密人 $ID_i(i=1,\cdots,n)$、解签密者 ID_B 和授权文件 W 下对密文 σ 的解签密询问。如果 $F(ID_B)\neq 0 \bmod p$，B 首先运行前面的私钥提取算法计算 ID_B 的私钥，然后运行解密签算法生成明文 m 作为对 A 的响应；否则，B 将失败退出。

伪造：如果 B 能够回答 A 的所有询问，即 B 没有失败退出，那么 A 可以输出一个在原始签密人 ID_A^*、代理签密人 $ID_i^*(i=1,\cdots,n)$、解签密者 ID_B^* 和授权文件 W^* 下对消息 m^* 的有效部分伪造签密 $\sigma_i^*=(\sigma_{1i}^*,\sigma_{2i}^*,\sigma_{3i}^*,\sigma_{4i}^*,\sigma_{5i}^*,\sigma_{6i}^*,\sigma_{7i}^*,\sigma_{8i}^*)$。

如果 $F(ID_A^*)=0 \bmod p$、$Q(W^*)=0 \bmod p$ 且 $K(M^*)=0 \bmod p$，则 B 可计算

$$\begin{aligned}&\frac{\sigma_{4i}^*}{(\sigma_{6i}^*)^{J(ID_A^*)}(\sigma_{7i}^*)^{R(W^*)}d_{i1}(\sigma_{8i}^*)^{L(M^*)}}\\&=\frac{g_2^{2a}(u'\prod_{i\in\Phi_A}u_i)^{r_A}(u'\prod_{i\in\Phi_i}u_i)^{r_i}(w'\prod_{j\in W}w_j)^{r_w}(m'\prod_{k\in M}m_j)^{x_i\eta_i}}{g_2^a(u'\prod_{i\in\Phi_i}u_i)^{r_i}g^{J(ID_A^*)r_A}g^{R(W^*)r_w}g^{L(M^*)x_i\eta_i}}\\&=g_2^a=g^{ab}\end{aligned}$$

这就是 CDH 问题的解，否则算法 B 将失败退出。

因此，如果存在一个敌手，其可以不可忽略的概率伪造一个有效的门限代理签密，那么就存在一个算法，它可以不可忽略的概率解决 CDH 问题，而这与 CDH 问题是一个困难问题相矛盾，故方案满足自适应选择消息攻击下的密文存在不可伪造性。

定理 2 在 DBDH 困难问题的假设下，我们的方案在自适应选择密文攻击下具有密文不可区分性。

证明：假设敌手 A 能以不可忽略的优势攻击上面的方案，则 A 就能够构造算法 B，B 可以利用 A 解决 DBDH 问题。

给定 B 一个 DBDH 问题的实例 (g,g^a,g^b,g^c,h)，它的目标是判定是否 $h=e(g,g)^{abc}$。为此，B 模仿 A 的挑战者，具体过程如下：

系统初始化：本阶段运用和前面证明中相同的方法去设

定系统的公共参数，并把这些参数发送给 A。

阶段 1：本阶段敌手 A 可以像前面那样，发起一定数量的询问。

挑战：在发起一定数量的询问以后，A 任意选取两个相同长度的消息 m_0, m_1，以及要挑战的原始签密人 ID_A^*、代理签密人 ID_i^* $(i=1,\cdots,n)$、解签密者 ID_B^* 和授权文件 W^*，并将它们发送给 B。如果 A 在第一阶段询问了 ID_B^* 的私钥，那么 B 将失败退出。如果 $F(ID_B^*)\neq 0 \bmod p$，那么 B 将失败退出。否则，B 任选一位 $b\in\{0,1\}$，随机选择 $r_A, r_i (i=1,\cdots,t)$，$r_w, r_k \in Z_p$。如果 $Q(W^*)\neq 0 \bmod p$ 且 $K(m_b)\neq 0 \bmod p$，那么 B 将失败退出，否则，B 可以构造 $\sigma^* = (\sigma_1^*, \sigma_2^*, \sigma_3^*, \sigma_4^*, \sigma_{5,1}^*, \cdots, \sigma_{5,t}^*, \sigma_6^*, \sigma_7^*, \sigma_8^*)$。

如果给定 B 一个 DBDH 问题的实例，并且 $h=e(g,g)^{abc}$，由 $F(ID_B^*)=0 \bmod p$，$Q(W^*)=0 \bmod p$，$K(m_b)=0 \bmod p$，以及 $u'\prod_{i\in\Phi_u} u_i = g_2^{F(U_u)} g^{J(U_u)}$，$w'\prod_{j\in\mathcal{W}} w_j = g_2^{Q(W)} g^{R(W)}$，$m'\prod_{j\in\Omega} m_j = g_2^{K(m)} g^{L(m)}$ 可得：

$$\sigma_1^* = hm_b = e(g,g)^{abc} m_b = e(g_1, g_2)^c m_b$$

$$\sigma_2^* = g^c$$

$$\sigma_3^* = g^{cJ(ID_B^*)} = (u'\prod_{i\in\Phi_B} u_i)^c$$

$$\sigma_4^* = g_1^{\frac{-tJ(ID_A^*)}{F(ID_A^*)}} (g_2^{F(ID_A^*)} g^{J(ID_A^*)})^{r_A} \cdot g^{tR(W^*) r_w} \cdot \prod_{i=1}^{t} g_1^{\frac{-J(ID_i^*)}{F(ID_i^*)}} (g_2^{F(ID_i^*)} g^{J(ID_i^*)})^{r_i} \cdot g^{r_k L(m_b)}$$

$$= g_2^{2ta} \cdot (u'\prod_{i\in\Phi_A} u_i)^{\tilde{r}_A} (w'\prod_{j\in\mathcal{W}} w_j)^{r_w} \prod_{i=1}^{t} (u'\prod_{i\in\Phi_A} u_i)^{\tilde{r}_i} \cdot (m'\prod_{k\in\mathcal{M}} m_k)^{r_k}$$

$$\sigma_{5,i}^* = g_1^{-1/F(ID_i^*)} g^{r_i} (i=1,\cdots,t) = g^{\tilde{r}_i} (i=1,\cdots,t)$$

$$\sigma_6^* = g_1^{-t/F(ID_A^*)} g^{r_A} = g^{\tilde{r}_A}$$

$$\sigma_7^* = g^{r_w}$$

$$\sigma_8^* = g^{r_k}$$

可知 σ^* 是一个有效的门限代理签密。

阶段 2：敌手 A 可以像阶段 1 那样，重复发出一定数量的询问，但是 A 必须不能询问 ID_B^* 的私钥以及对 σ^* 的解签密询问。

猜测：最后，A 输出对 b 的猜测 b'。如果 $b=b'$，则 B 输出 1，将 $h=e(g,g)^{abc}$ 作为 DBDH 问题的解；否则，B 输出 0。

因此，如果存在一个敌手，其可以不可忽略的概率成功进行攻击，那么就存在一个有效的算法，它可以不可忽略的概率解决 DBDH 问题，而这与 DBDH 问题是一个困难问题相矛盾，故方案在自适应选择密文攻击下具有密文不可区分性。

结束语 门限代理签密是一种重要的具有特殊性质的签密形式，现有基于身份的门限代理签密方案的安全性都是在随机模型下证明的。本文在标准模型下设计了一个基于身份的 (t,n) 门限代理签密方案，通过对方案的安全性进行分析，指出方案在 CDH 困难问题的假设下满足自适应选择消息攻击下的密文存在不可伪造性以及在 DBDH 困难问题的假设下满足自适应选择密文攻击下的不可区分性。因此，相对于随机预言模型下可证安全的方案来说，本文方案具有更高的安全性。

参 考 文 献

[1] Shamir A. Identity-based cryptosystems and signature schemes [C]// Proceedings of Crypto 1984, volume 196 of LNCS. Springer-Verlag, 1984: 47-53

[2] Boneh D, Franklin M. Identity-based encryption from the Weil pairing [C] // Proceedings of Crypto 2001, volume 2139 of LNCS. Springer-Verlag: 213-229

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

[4] Zhang Fang-guo, Kim K. Efficient ID-based blind signature and proxy signature from bilinear pairings [C] // Proceedings of the 8th Australasian Conference on Information Security and Privacy, volume 2727 of LNCS. Springer-Verlag, 2003: 312-323

[5] 李继国，姜平进. 标准模型下可证安全的基于身份的高效签名方案[J]. 计算机学报，2009，32(11)：2130-2136

[6] 李明祥，韩伯涛，朱建勇，等. 在标准模型下安全的基于身份的代理签名方案[J]. 华南理工大学学报：自然科学版，2009，37(5)：118-122

[7] Zheng Yuliang. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature) + cost(encryption) [C] // Advances in Cryptology-Crypto 1997. volume 1294 of LNCS. Springer-Verlag, 1997: 165-179

[8] An J H, Dodis Y, Rabin T. On the security of joint signature and encryption [C] // Advances in Cryptology-Eurocrypt 2002. volume 2332 of LNCS. Springer-Verlag, 2002: 83-107

[9] Malone-Lee J. Identity-based signcryption [EB/OL]. (2002-07-19) [2002-07-20]. http://eprint.iacr.org/2002/098

[10] Libert B, Quisquater J-J. New identity based signcryption schemes from pairings [EB/OL]. (2003-02-04) [2003-02-24]. http://eprint.iacr.org/2003/023

[11] Duan Shan-shan, Cao Zhen-fu, Lu Rong-xing. Robust id-based threshold signcryption scheme from pairings [C] // Proceedings of the 3rd international conference on information security. volume 85, ACM, 2004: 33-37

[12] Li Fa-gen, Yu Yong. An efficient and provably secure id-Based threshold signcryption scheme [C] // Proceedings of ICCCAS 2008. 2008: 488-492

[13] Yu Y, Yang B, Sun Y, et al. Identity based signcryption scheme without random oracles [J]. Computer Standards & Interfaces, 2009, 31(1): 56-62

[14] Selvi S S D, Vivek S S, Nayak S, et al. Breaking and building of threshold signcryption schemes [C] // Proceedings of the 5th international conference on information security and cryptology, volume 6151 of LNCS. Springer-Verlag, 2010: 108-123

[15] Kushwah P, Lal S. Identity based signcryption schemes without random oracles [EB/OL]. http://eprint.iacr.org/2011/372, 2011-07-10

[16] Li Fa-gen, Hu Yu-pu, Liu Shuang-gen. ID-based(t, n) threshold proxy signcryption for multi-agent systems [C] // Proceedings of International Conference on Computational Intelligence and Security, volume 4456 of LNCS. Springer-Verlag, 2007: 406-416

[17] Li Fa-gen, Xin Xiang-jun, Hu Yu-pu. ID-based threshold proxy signcryption scheme from bilinear pairings [J]. International Journal of Security and Networks, 2008, 3(3): 206-215

[18] Bellare M, Rogaway P. Random oracles are practical: a paradigm for designing efficient protocols [C] // Proceedings of the 1st ACM conference on computer and communications security. 1993: 62-73