一个动态门限的基于属性签密方案

张国印*①　付小晶①②　马春光①②
①(哈尔滨工程大学计算机科学与技术学院　哈尔滨　150001)
②(网络与数据安全四川省重点实验室　成都　611731)

摘　要：签密能同时实现加密与签名，并且代价小于传统的先签名再加密。该文在 Li 等人(2010)签名方案的基础上提出了一个动态门限的基于属性签密方案，除具有一般签密方案的保密性和认证性外，还同时具有签密者属性隐私安全性和多接收者特性。在随机预言机模型下，利用判定双线性 Diffie-Hellman (DBDH)问题和计算 Diffie-Hellman (CDH)问题的困难性，证明了该方案满足在适应性选择密文攻击下的不可区分性及适应性选择消息下的不可伪造性。

关键词：基于属性签密；动态门限；属性隐私；多接收者；随机预言机模型
中图分类号：TP309　　**文献标识码**：A　　**文章编号**：1009-5896(2012)11-2680-07
DOI: 10.3724/SP.J.1146.2012.00342

A Dynamic Threshold Attributes-based Signcryption Scheme

Zhang Guo-yin①　Fu Xiao-jing①②　Ma Chun-guang①②
①(*College of Computer Science and Technology*, *Harbin Engineering University*, *Harbin* 150001, *China*)
②(*Network and Data Security Key Laboratory of Sichuan Province*,
University of Electronic Science and Technology of China, *Chengdu* 611731, *China*)

Abstract: Signcryption combines the functionalities of signature and encryption and costs less than that required by the traditional signature-then-encryption approach. On the basis of Li *et al.* (2010) attribute-based signature, a new attributes-based signcryption is proposed in this paper, in which not only confidentiality and authentication is provided but also attribute-signcryptor privacy and multi-recipient is achieved. This scheme is provable secure in the random oracle model and it satisfies indistinguishability against adaptive chosen ciphertext attack based on Decisional Bilinear Diffie-Hellman (DBDH) assumption and satisfies existential unforgeability against adaptive chosen message attack based on the standard Computational Diffie-Hellman (CDH) assumption.

Key words: Attributes-Based SignCryption (ABSC); Dynamic threshold; Attribute privacy; Multi-recipient; Random oracle model

1　引言

文献[1]最早提出签密(signcryption)概念，签密可以在一个逻辑步骤内同时完成加密与签名，实现信息的保密性和认证性，并且代价小于传统的先签名再加密。基于身份密码学[2,3]解决了传统公钥基础设施中公钥证书的复杂性管理问题，文献[4]首次提出基于身份签密(IBSC)的概念，并且定义了 IBSC 的两个安全性：不可区分性(indistinguishability)和存在不可伪造性(existential unforgeability)。之后，出现了基于身份广播签密方案[5]和基于身份基多接收者签密方案[6]，实现了多用户接收信息的私密性和认证性。但是这两种签密方案要求签密者明确知道接收者群组成员的身份，并且至少需要暴露签密者的身份，不能较好满足一些网络应用的隐私保护需求。文献[7]基于秘密共享理论，提出了基于模糊身份的加密(Fuzzy IBE)概念，用户的生物信息作为其身份，被看作是一个描述属性的集合。文献[8]首次提出了基于属性加密(Attribute-Based Encryption, ABE)的概念，不用暴露用户的身份，任何用户只要它的属性满足指定的访问策略就能够解密消息。基于属性密码学具有天然的“多用户”和“隐藏身份”特性，为隐私保护提供可行的途径。Maji 等人[9,10]提出了支持任何访问结构的基于属性签名(ABS)方案，能够保护签名者的属性隐私，只在一般群模型下证明其安全性。文献[11]提出第 1 个标准 CDH 问题假设下可证安全的(n,n)固定门限的 ABS 方案，

2012-03-29 收到，2012-07-16 改回
国家自然科学基金(61073042, 61170241)，中央高校基本科研业务费专项资金(HEUCF100606)和网络与数据安全四川省重点实验室开放课题基金(201107)资助课题
*通信作者：张国印　zhangguoyin@hrbeu.edu.cn

实现了签名者匿名性和属性隐私安全性。之后出现了其改进方案[12,13]，支持(k,n)动态门限，并提高了效率。Herranz 等人[14]提出一个基于属性短签名方案，支持门限访问结构，但是属性私钥数量和计算代价较大。目前仍缺乏有效的基于属性签密(ABSC)方案。Gagne 等人[15]提出 1 个标准模型下可证安全的(n,n)门限 ABSC 方案，签密者和加密者的门限是固定的。Emura 等人[16]提出一个密文策略 ABSC 方案，支持复杂访问结构和动态属性，但是需要明确知道签密者具体拥有的属性。现有的 ABSC 方案在门限、属性隐私保护等方面存在不足。基于此，本文在文献[13]方案的基础上提出了一个 ABSC 方案，实现了签密者属性隐私安全和多接收者等特性，并在随机预言机模型下证明其安全性。

2　预备知识

定义 1　双线性对：G_1，G_2是阶为素数q的循环群，g是G_1的生成元。双线性对$\hat{e}:G_1\times G_1\to G_2$满足以下条件：

(1)双线性(bilinearity)：对于任意$g_1,g_2\in G_1$，$a,b\in {}_RZ_q^*$，$\hat{e}(g_1^a,g_2^b)=\hat{e}(g_1,g_2)^{ab}$都成立；

(2)非退化性(nondegeneracy)：对于任意$g_1,g_2\in G_1$，存在$\hat{e}(g_1,g_2)\neq 1_{G_2}$，$1_{G_2}$是$G_2$的单位元；

(3)可计算性(computable)：对于任意$g_1,g_2\in G_1$，存在一种有效的算法计算$\hat{e}(g_1,g_2)\in G_2$。

定义 2　计算Diffie-Hellman问题(CDHP)：对于$x,y\in {}_RZ_q^*$，已知$g,g^x,g^y\in G_1$，计算g^{xy}。

定义 3　判定双线性 Diffie-Hellman 问题(DBDHP)：对于$x,y,z\in {}_RZ_q^*$，已知$g^x,g^y,g^z\in G_1$，$h\in G_2$，判断$h=\hat{e}(g,g)^{xyz}$。

3　形式化安全模型

本文借鉴基于身份签密安全模型[4,17]构造了适合基于属性签密方案的安全模型。分别给出了基于属性签密方案的保密性和不可伪造性相关定义和“攻击-挑战”游戏的形式化描述。

定义 4(IND-ASC-CCA)　在概率多项式时间内，如果攻击者$\mathcal{A}$没有以不可忽略的优势在如下游戏中获胜，则称基于属性签密方案在适应性选择密文攻击下具有不可区分性(简称 IND-ASC-CCA)：

初始化：挑战者$\mathcal{C}$运行初始化算法，利用系统安全参数$\mathcal{K}$产生公共参数 params 和系统密钥t。将 params 发布给攻击者$\mathcal{A}$。t保密。

询问阶段 1：$\mathcal{A}$向$\mathcal{C}$执行以下询问：

(1)Hash 询问：$\mathcal{A}$可以询问任意输入的 Hash 值；

(2)私钥生成询问：$\mathcal{A}$选择一个属性集ω_i，根据系统参数 params 和主密钥t，$\mathcal{C}$计算用户私钥S_{ω_i}，并发送给$\mathcal{A}$；

(3)签密询问：$\mathcal{A}$选择属性集ω_i,ω_j和明文m，ω_i用于签名，ω_j用于加密。$\mathcal{C}$对ω_i进行私钥生成询问，$\mathcal{C}$计算$\sigma=\mathrm{Signcrypt}(\omega_i,\omega_j,S_{\omega_i},m)$，将密文$\sigma$发送给$\mathcal{A}$。

(4)验证解密询问：$\mathcal{A}$选择属性集ω_i,ω_j和密文σ，ω_i用于签名，ω_j用于加密。$\mathcal{C}$对ω_j进行私钥生成询问，计算$m=\mathrm{Unsigncrypt}(\omega_i,\omega_j,S_{\omega_j},\sigma)$，返回明文$m$或者终止符号$\perp$。

在询问阶段 1，$\mathcal{A}$可以根据以前的询问结果进行自适应询问。最后，$\mathcal{A}$选择两个等长的明文m_0,m_1和两个挑战的属性集$\omega_A^*,\omega_B^*,\omega_A^*$用于签名，$\omega_B^*$用于加密，且$\omega_B^*$没有被执行过私钥生成询问。

挑战阶段：$\mathcal{C}$随机选择$b\in\{0,1\}$，计算$\sigma_b^*=\mathrm{Signcrypt}(\omega_A^*,\omega_B^*,S_{\omega_A}^*,m_b^*)$。返回密文$\sigma_b^*$给$\mathcal{A}$；

询问阶段 2：$\mathcal{A}$执行和阶段 1 相同的询问。但有一定限制：不允许对ω_B^*进行私钥生成询问，不允许询问$\omega_A^*,\omega_B^*,\sigma_b^*$的明文。

猜测阶段：游戏最后，$\mathcal{A}$输出$b'\in\{0,1\}$，如果$b'=b$，则$\mathcal{A}$在游戏中获胜。定义攻击者$\mathcal{A}$在游戏中获胜的优势为$\mathrm{Adv}(\mathcal{A})=|2\Pr(b'=b)-1|$。

定义 5 (EF-ASC-CMA 安全)　在概率多项式时间内，如果攻击者$\mathcal{A}$没有以不可忽略的优势在如下游戏中获胜，则称基于属性签密方案在适应性选择消息攻击下具有存在不可伪造性(简称 EF-ASC-CMA)：

初始化：同定义 4 中的“初始化”；

询问阶段：同定义 4 中的“询问阶段 1”；

伪造阶段：游戏最后，$\mathcal{A}$输出一个新的三元组$(\omega_A^*,\omega_B^*,\sigma^*)$，且$\omega_A^*$在询问阶段没有被执行过私钥生成询问。如果$\mathrm{Unsigncrypt}(\omega_A^*,\omega_B^*,S_{\omega_B^*}^*,\sigma^*)$没有返回终止符号$\perp$，则$\mathcal{A}$在游戏中获胜。定义攻击者$\mathcal{A}$在游戏中获胜的优势为$\mathrm{Adv}(\mathcal{A})=\Pr[\mathrm{Win}]$。

定义 6　签密者属性隐私安全性：设属性集为$U\subset {}_RZ_q^*$，断言Υ为U上的单调布尔函数，如果属性集$\omega\subset U$，则$\Upsilon(\omega)=1$。如果给定消息m，签名属性集合ω_1,ω_2和签名断言Υ上的密文σ，且$\Upsilon(\omega_1)=\Upsilon(\omega_2)=1$，攻击者$\mathcal{A}$无法区分$\omega_1$和$\omega_2$中哪个集合用于产生$\sigma$，则称基于属性签密方案满足签密者属性隐私(attribute-signcryptor privacy)安全性。

4　新方案描述

本文所提基于属性签密方案支持包含门限的断

言 $\Upsilon_{k,\omega^*}(\cdot)$，$\omega^*$ 是用于签名或加密的属性集，k,1 $\le k \le d$ 为门限值。$\Upsilon_{k,\omega^*}(\omega') = \begin{cases} 1, & \left|\omega' \cap \omega^*\right| \ge k \\ 0, & \text{其他} \end{cases}$，即当属性集 ω' 包含属性集 ω^* 中至少 k 个元素时，称 ω' 满足断言 $\Upsilon_{k,\omega^*}(\cdot)$。

(1)参数建立：密钥生成中心(PKG)选择系统安全参数 $\mathcal{K}$, $d \in {}_RZ_q^*$，设拉格朗日插值系数 $\Delta_{j,S}(i) = \prod_{k\in S,k\ne j} \frac{i-k}{j-k}$，属性集 $U \subset {}_RZ_q^*$。设由 $d-1$ 个属性构成的缺省属性集为 $\Omega = \{\Omega_1, \Omega_2, \cdots, \Omega_{d-1}\}$，$\Omega_i \in {}_RZ_q^*$，$1 \le i \le d-1$。选择一个双线性对 $\hat{e}: G_1 \times G_1 \to G_2$，随机选取 $g, g_2 \in G_1$，$x \in {}_RZ_q^*$，计算 $g_1 = g^x$，$Z = \hat{e}(g_1, g_2)$。选择哈希函数 $H_1: \{0,1\}^* \to G_1$，$H_2: \{0,1\}^* \times \{G_1\}^* \to G_1$。选择一个对称密码算法的加、解密算法 $E_k(\cdot)$ 和 $D_k(\cdot)$。保密系统主密钥为 x，公开参数 params=$(\mathcal{K}, d, q, G_1, G_2, \hat{e}, g, g_1, g_2, Z, H_1, H_2, E_k(\cdot), D_k(\cdot))$。

(2)私钥生成：给定用户 ID，其属性集为 $\omega_{\mathrm{ID}} \subset U$。PKG随机选择 $d-1$ 次多项式 $q(y)$，满足 $q(0) = x$。产生一个新的属性集 $\hat{\omega}_{\mathrm{ID}} = \omega_{\mathrm{ID}} \cup \Omega$，对于任一 $i \in \hat{\omega}_{\mathrm{ID}}$，随机选择 $r_i \in {}_RZ_q^*$，计算 $d_{i0} = g_2^{q(i)} H_1(i)^{r_i}$，$d_{i1} = g^{r_i}$。用户的私钥为 $D_i = (d_{i0}, d_{i1})$，$i \in \hat{\omega}_{\mathrm{ID}}$。

(3)签密：设签名断言为 $\Upsilon_{k,\omega_1^*}(\cdot)$，$|\omega_1^*| = n_1$，加密断言为 $\Upsilon_{k',\omega_2^*}(\cdot)$，$|\omega_2^*| = n_2$。签密者 A 的属性集为 $\omega_A = \{i_1, i_2, \cdots, i_{n_A}\}$，且 $\Upsilon_{k,\omega_1^*}(\omega_A) = 1$。$A$ 用属性集 ω_A 在断言 $\Upsilon_{k,\omega_1^*}(\cdot)$ 和 $\Upsilon_{k',\omega_2^*}(\cdot)$ 下对消息 m 签密。A 选择属性子集 $\omega_A' \subseteq \omega_1^* \cap \omega_A$。从属性集 Ω 选取 $d-k'$ 个缺省属性构成缺省属性集 $\Omega_1' = \{i_{k+1}, i_{k+2}, \cdots, i_d\} \subseteq \Omega$，从属性集 Ω 选取 $d-k'$ 个缺省属性构成缺省属性集 $\Omega_2' = \{i_{k'+1}, i_{k'+2}, \cdots, i_d\} \subseteq \Omega$。选择随机数 $s \in {}_RZ_q^*$，计算 $\sigma_0 = g^s$，$\{\sigma_i = H_1(i)^s\}_{i\in\omega_2^*\cup\Omega_2'}$，$k_e = Z^s$，$c = E_{k_e}(m)$。对于 $r_i \in \omega_1^* \cup \Omega_1'$。选择 $n_1 + d - k$ 个随机数 $r_i' \in {}_RZ_q^*$。计算 $\sigma_0' = \left[\prod_{i\in\omega_A'\cup\Omega_1'} d_{i,0}^{\Delta_{i,S}(0)}\right]\left[\prod_{i\in\omega_1^*\cup\Omega_1'} H_1(i)^{r_i'}\right] \cdot H_2\left(c, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}\right)^s$，$\left\{\sigma_i' = d_{i1}^{\Delta_{i,S}(0)} g^{r_i'}\right\}_{i\in\omega_A'\cup\Omega_1'}$，$\{\sigma_i' = g^{r_i'}\}_{i\in\omega_1^*/\omega_A'}$，密文为 $\sigma = \left\{\sigma_0, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}, \sigma_0', \{\sigma_i'\}_{i\in\omega_1^*\cup\Omega_1'}, c\right\}$。

(4)验证解密：用户 B 的属性集 $\omega_B = \{i_1, i_2, \cdots, i_{n_B}\}$，且 $\Upsilon_{k,\omega_2^*}(\omega_B) = 1$，可以验证消息 m 的密文 $\sigma = \{\sigma_0, \{\sigma_i\}_{i\in\omega_1^*\cup\Omega_1'}, \sigma_0', \{\sigma_i'\}_{i\in\omega_2^*\cup\Omega_2'}, c\}$ 的签名者是否满足签名断言 $\Upsilon_{k,\omega_1^*}(\cdot)$，并解密获得密文。$B$ 计算 $H_2(c, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'})$，判断式(1)是否成立，如果成立则接受密文 σ，否则拒绝。B 选择属性集 $\omega_B' \subseteq \omega_2^* \cap \omega_B$。令 $\{d_{i0}' = d_{i0}\}_{i\in\omega_B'\cup\Omega_2'}$，$\{d_{i0}' = H(i)\}_{i\in\omega_2^*/\omega_B'}$，$\{d_{i1}' = d_{i1}\}_{i\in\omega_B'\cup\Omega_2'}$，$\{d_{i1}' = g\}_{i\in\omega_2^*/\omega_B'}$。计算

$$k_e = \prod_{i\in\omega_2^*\cup\Omega_2'} \left(\frac{\hat{e}\left(d_{i0}', \sigma_0\right)}{\hat{e}\left(\sigma_i, d_{i1}'\right)}\right)^{\Delta_{i,S}(0)}, \quad m = D_{k_e}(c)$$

得到消息明文 m。

$$\frac{\hat{e}\left(g, \sigma_0'\right)}{\left[\prod_{i\in\omega_1^*\cup\Omega_1'} \hat{e}\left(H_1(i), \sigma_i'\right)\right] \hat{e}\left(H_2\left(c, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}\right), \sigma_0\right)} = Z \tag{1}$$

正确性证明：

$$\frac{\hat{e}\left(g, \sigma_0'\right)}{\left[\prod_{i\in\omega_1^*\cup\Omega_1'} \hat{e}\left(H_1(i), \sigma_i'\right)\right] \hat{e}\left(H_2\left(c, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}\right), \sigma_0\right)}$$

$$= \frac{\hat{e}\left(g, \left[\prod_{i\in\omega_A'\cup\Omega_1'} \left(g_2^{q(i)} H_1(i)^{r_i}\right)^{\Delta_{i,S}(0)}\right]\left[\prod_{i\in\omega_1^*\cup\Omega_1'} H_1(i)^{r_i'}\right] H_2\left(c, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}\right)^s\right)}{\left[\prod_{i\in\omega_A'\cup\Omega_1'} \hat{e}\left(H_1(i), g^{r_i\Delta_{i,S}(0)} g^{r_i'}\right) \prod_{i\in\omega_1^*/\omega_A'} \hat{e}\left(H_1(i), g^{r_i'}\right)\right]\left(H_2\left(c, \{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}\right), g^s\right)} = \prod_{i\in\omega_A'\cup\Omega_1'} \left(g, g_2^{q(i)}\right)^{\Delta_{i,S}(0)} = Z$$

$$k_e = \prod_{i\in\omega_2^*\cup\Omega_2'} \left(\frac{\hat{e}\left(d_{i0}', \sigma_0\right)}{\hat{e}\left(\sigma_i, d_{i1}'\right)}\right)^{\Delta_{i,S}(0)} = \prod_{i\in\omega_B'\cup\Omega_2'} \left(\frac{\hat{e}\left(g_2^{q(i)} H_1(i)^{r_i}, g^s\right)}{\hat{e}\left(H_1(i)^s, g^{r_i}\right)}\right)^{\Delta_{i,S}(0)} \prod_{i\in\omega_2^*/\omega_B'} \left(\frac{\hat{e}\left(H_1(i), g^s\right)}{\hat{e}\left(H_1(i)^s, g\right)}\right)^{\Delta_{i,S}(0)}$$

$$= \prod_{i\in\omega_B'\cup\Omega_2'} \left(g_2^{q(i)}, g^s\right)^{\Delta_{i,S}(0)} = Z^s$$

5 方案分析

5.1 安全性证明

定理 1 如果 G_1 上的DBDH困难问题成立，则本文所提签密方案满足IND-ASC-CCA安全，即不存在一个IND-ASC-CCA攻击者以不可忽略的优势攻破所提方案。

证明　假设攻击者 $\mathcal{A}$ 能够在概率多项式时间内以 ε 的优势在定义4中的游戏中获胜，并且 $\mathcal{A}$ 最多进行 q_{H_i} 次 H_i 询问，$i=1,2$，q_K 次私钥生成询问，q_S 次签密询问和 q_{US} 次验证解密询问。构造算法 $\mathcal{C}$，利用 $\mathcal{A}$ 解决DBDH问题。即给定 (g,g^x,g^y,g^z,h)，判断 $h=\hat{e}(g,g)^{xyz}$ 是否成立。设置系统参数 $\mathcal{K}$, $d\in {}_RZ_q^*$，缺省属性集 $\Omega=\{\Omega_1,\Omega_2,\cdots,\Omega_{d-1}\}$，$\mathcal{A}$ 输出预挑战的用于签名的属性集 ω_1^* 和门限 $1\le k\le d$，用于加密的属性集 ω_2^* 和门限 $1\le k'\le d$，设签名断言为 $\Upsilon_{k,\omega_1^*}(\cdot)$，加密断言为 $\Upsilon_{k',\omega_2^*}(\cdot)$。$\mathcal{C}$ 随机选择缺省属性集 $\Omega_1'^*\subseteq\Omega$，$|\Omega_1'^*|=d-k$，$\Omega_2'^*\subseteq\Omega$，$|\Omega_2'^*|=d-k'$。$\mathcal{C}$ 仿真如下：

(1)初始化：$\mathcal{C}$ 设置 $g_1=g^x$，$g_2=g^y$。

(2)随机预言机：$\mathcal{A}$ 保存列表 $\mathcal{L}_1$ 和 $\mathcal{L}_2$ 用来存储 H_1-预言机和 H_2-预言机的答案。$\mathcal{C}$ 选择2个随机数 $\delta_0,\delta_1\in[1,q_{H_2}]$。

H_1-预言机：如果对 i 进行 H_1-预言机询问，$\mathcal{C}$ 检查 $\mathcal{L}_1$，仿真如下：

(a)如果能在 $\mathcal{L}_1$ 中找到 i，返回其对应的值；

(b)否则，如果 $i\in\omega_2^*\cup\Omega_2'^*$，选择随机数 $\beta_i\in {}_RZ_q^*$，返回 $H_1(i)=g^{\beta_i}$，并记录于 $\mathcal{L}_1$；

(c)否则，如果 $i\notin\omega_2^*\cup\Omega_2'^*$，选择随机数 $\beta_i,\gamma_i\in {}_RZ_q^*$，返回 $H_1(i)=g_1^{-\beta_i}g^{\gamma_i}$，并记录于 $\mathcal{L}_1$。

H_2-预言机：如果对 $c_i,\{\sigma_j\}_{j\in U},\sigma_j\in G_1$ 进行 H_2-预言机询问。$\mathcal{C}$ 检查列表 $\mathcal{L}_2$，仿真如下：

(a)如果能在 $\mathcal{L}_1$ 中找到 i，返回其对应的值；

(b)否则，如果 $i\ne\delta_0,i\ne\delta_1$，选择随机数 $\alpha_i,\beta_i\in {}_RZ_q^*$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g_1^{\alpha_i}g^{\beta_i}$，并记录于 $\mathcal{L}_2$；

(c)如果 $i=\delta_0$，选择随机数 $\beta_{\delta_0}\in {}_RZ_q^*$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g^{\beta_{\delta_0}}$，并记录于 $\mathcal{L}_2$；

(d)如果 $i=\delta_1$，选择随机数 $\beta_{\delta_1}\in {}_RZ_q^*$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g^{\beta_{\delta_1}}$，并记录于 $\mathcal{L}_2$。

(3)私钥生成预言机：

(a)如果对属性集 ω_i，且满足 $|\omega_i\cap\omega_2^*|<k'$，进行私钥生成询问。定义3个集合 Γ,Γ',S，满足：$\Gamma=(\omega_i\cap\omega_2^*)\cup\Omega_i'$，$\Gamma\subseteq\Gamma'\subseteq S$，$|\Gamma'|=d-1$，$S=\Gamma'\cup\{0\}$。$\mathcal{C}$ 仿真如下：

对于 $i\in\Gamma'$，令 $D_i=(g_2^{t_i}H_1(i)^{r_i},g^{r_i})$，其中 $t_i,r_i\in {}_RZ_q^*$。相当于隐式选择了一个 $d-1$ 次多项式 $q(x)$，且 $q(i)=t_i$，并且 $q(0)=x$。对于 $i\notin\Gamma'$，设 $r_i=\dfrac{\Delta_{0,S}(i)}{\beta_i}y+r_i'$，$q(i)=\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)$,

$$D_i=\left(g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)\Sigma}\left(g_1^{-\beta_i}g^{\gamma_i}\right)^{r_i'},g_2^{\frac{\Delta_{0,S}(i)}{\beta_i}}g^{r_i'}\right)_{i\in\omega_i}$$

因为

$$g_2^{q(i)}H_1(i)^{r_i}=g_2^{\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)+\Delta_{0,S}(i)q(0)}\left(g_1^{-\beta_i}g^{\gamma_i}\right)^{\frac{\Delta_{0,S}(i)}{\beta_i}y+r_i'}$$

$$=g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)}\left(g_1^{-\beta_i}g^{\gamma_i}\right)^{r_i'}$$

$$g^{r_i}=g^{\frac{\Delta_{0,S}(i)}{\beta_i}y+r'}=g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}}g^{r_i'}$$

所以对 $\mathcal{A}$ 来说，D_i 是一个合法的私钥；

(b)如果 $|\omega_i\cap\omega_2^*|\ge k'$，则 $\mathcal{C}$ 仿真失败。

(4)签密预言机：$\mathcal{A}$ 请求在属性集 ω_A 和断言 $\Upsilon_{k,\omega_1^*}(\cdot),\Upsilon_{k,\omega_2^*}(\cdot)$ 下的消息 m 的签密询问。$\mathcal{C}$ 仿真如下：

(a)如果 $|\omega_A\cap\omega_2^*|<k'$。则 $\mathcal{C}$ 利用私钥生成预言机产生 ω_A 的私钥 $D_{Ai}=(d_{i0},d_{i1})$，并且按照正常的签名算法产生密文并返回给 $\mathcal{A}$；

(b)否则，$\mathcal{C}$ 从缺省属性集 Ω 随机选择由 $d-k$ 个元素构成的子集 Ω_1'。从属性集 Ω 随机选取 $d-k'$ 个缺省属性构成缺省属性集 Ω_2'，设 $\omega_A\cup\Omega_1'=\{i_1,i_2,\cdots,i_d\}$，$\mathcal{C}$ 随机选择 k_e，计算 $c_i=E_{k_e}(m_i)$。随机选择 $r_i,s',\in {}_RZ_q^*$。设 $s=\dfrac{-1}{\alpha_{i_d}}y+s'$。设置 $\sigma_0=g^s=g_2^{\frac{-1}{\alpha_{i_d}}}g^{s'}$，$\left\{\sigma_i=g^{\beta_i s}=g_2^{\frac{-\beta_i}{\alpha_{i_d}}}g^{\beta_i s'}\right\}_{i\in\omega_2^*\cup\Omega_2'}$，$H_2(c_i,\{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'})=g_1^{\alpha_{i_d}}g^{\beta_i}$，$\sigma_0'=g_2^x\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i}H_2\left(c_i,\{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'}\right)^s=\left(g_1^{\alpha_{i_d}}g^{\beta_i}\right)^{s'}\prod_{i\in\omega_1^*\cup\Omega_1'}H_1(i)^{r_i}g_2^{\frac{-\beta_i}{\alpha_{i_d}}}$，$\left\{\sigma_i'=g^{r_i'}\right\}_{i\in\omega_1^*\cup\Omega_1'}$。因为 $\mathcal{A}$ 不能对 ω_B，$|\omega_B\cap\omega_2^*|\ge k'$ 进行私钥生成询问，不能计算 $k_e\in {}_RZ_q^*$，因此无法判断随机数 k_e 不合法。从攻击者 $\mathcal{A}$ 角度看签名 $\sigma=\left\{\sigma_0,\{\sigma_i\}_{i\in\omega_2^*\cup\Omega_2'},\sigma_0',\{\sigma_i'\}_{i\in\omega_1^*\cup\Omega_1'},c_i\right\}$ 是一个合法的密文。

(5)验证解密预言机：$\mathcal{A}$ 请求密文 σ 的解密询问。$\mathcal{C}$ 仿真如下：

(a)如果 $|\omega_A\cap\omega_2^*|<k'$，$|\omega_B\cap\omega_2^*|<k'$，则 $\mathcal{C}$ 利用私钥生成预言机产生 ω_A 和 ω_B 的私钥，并且按照正常的验证解密算法，验证解密得到明文 m_i 并返回或者放回终止符号 $\perp$；

(b)否则，$\mathcal{C}$ 返回无效的签名。如果之前 $\mathcal{A}$ 已经对 $(\omega_1^*,k,\omega_2^*,k',\omega_A,m)$ 进行了签密询问。那么从 $\mathcal{A}$ 角度看 σ 是一个合法的密文，则 $\mathcal{C}$ 仿真失败。

在询问阶段1，$\mathcal{A}$ 可以根据以前的询问结果进行自适应询问。最后，$\mathcal{A}$ 选择两个等长的明文 m_0,m_1 和两个挑战的属性集 ω_1^*,ω_2^* 和缺省属性集 $\Omega_1'^*,\Omega_2'^*$，且 ω_2^* 没有被执行过私钥生成询问，如果 $\mathcal{A}$ 没有选择 ω_1^*,ω_2^* 和 $\Omega_1'^*,\Omega_2'^*$，则 $\mathcal{C}$ 仿真失败。

(6)挑战阶段：$\mathcal{C}$ 随机选择 $b\in\{0,1\}$，$\mathcal{C}$ 仿真如下：

选取 k 个属性构成的属性集 $\omega_A'^{*}\subseteq\omega_1^{*}$，$\mathcal{C}$ 询问私钥生成预言机，获得 $\omega_A'^{*}$ 的私钥 $d_{i,0},d_{i,1}$，且按照正常的签名算法计算 $k_e^{*}=h^{s^{*}}$，$c_b^{*}=E_{k_e}(m_b)$，$\sigma_0^{*}=g^{zs^{*}}$，$\left\{\sigma_i^{*}=H_1(i)^{zs^{*}}=g^{z\beta_i s^{*}}\right\}_{i\in\omega_2^{*}\cup\Omega_2'^{*}}$ $\sigma_0'^{*}=\left[\prod_{i\in\omega_A'^{*}\cup\Omega_1'^{*}}d_{i,0}^{\Delta_{i,S}(0)}\right]\cdot\left[\prod_{i\in\omega_1^{*}\cup\Omega_1'^{*}}H_1(i)^{r_i'}\right]$，$H_2\left(c_b^{*},\left\{\sigma_i^{*}\right\}_{i\in\omega_2^{*}\cup\Omega_2'^{*}}\right)^{zs^{*}}=\left[\prod_{i\in\omega_A'^{*}\cup\Omega_1'^{*}}d_{i,0}^{\Delta_{i,S}(0)}\right]\left[\prod_{i\in\omega_1^{*}\cup\Omega_1'^{*}}\left(g_1^{-\beta_i}g^{\gamma_i}\right)^{r_i'}\right]g^{z\beta_{\delta_b}s^{*}}$，$\left\{\sigma_1'^{*}=d_{i1}^{\Delta_{i,S}(0)}\cdot g^{r_i'}\right\}_{i\in\omega_A'^{*}\cup\Omega_1'^{*}}$，$\left\{\sigma_i'^{*}=g^{r_i'}\right\}_{i\in\omega_1^{*}/\omega_A'^{*}}$，$\mathcal{C}$ 输出 $\sigma^{*}=\left\{\sigma_0^{*},\{\sigma_i^{*}\}_{i\in\omega_2^{*}\cup\Omega_2'^{*}},\sigma_0'^{*},\{\sigma_i'^{*}\}_{i\in\omega_1^{*}\cup\Omega_1'^{*}},c_b^{*}\right\}$ 作为挑战结果给 $\mathcal{A}$。如果 $H_2\left(c_b,\{\sigma_i^{*}\}_{i\in\omega_2^{*}\cup\Omega_2'^{*}}\right)\neq g^{\beta_{\delta_b}}$，则 $\mathcal{C}$ 仿真失败。如果 $h=\hat{e}(g,g)^{xyz}$，从攻击者 $\mathcal{A}$ 角度看 σ^{*} 是一个合法密文。假设解密者的属性集为 $\omega_B=\{i_1,i_2,\cdots,i_{n_B}\}$，且 $\Upsilon_{k,\omega_2^{*}}(\omega_B)=1$，令 $\omega_B'\subseteq\omega_2^{*}\cap\omega_B$，则

$$
\begin{aligned}
k_e^{*}&=\prod_{i\in\omega_2^{*}\cup\Omega_2'}\left(\frac{\hat{e}\left(d_{i0}',\sigma_0\right)}{\hat{e}\left(\sigma_i,d_{i1}'\right)}\right)^{\Delta_{i,S}(0)}\\
&=\prod_{i\in\omega_B'\cup\Omega_2'}\left(\frac{\hat{e}\left(g_2^{q(i)}g^{\beta_i r_i},g^{zs^{*}}\right)}{\hat{e}\left(g^{z\beta_i s^{*}},g^{r_i}\right)}\right)^{\Delta_{i,S}(0)}\\
&\quad\cdot\prod_{i\in\omega_2^{*}/\omega_B'}\left(\frac{\hat{e}\left(g^{\beta_i r_i},g^{zs^{*}}\right)}{\hat{e}\left(g^{z\beta_i s^{*}},g^{r_i}\right)}\right)^{\Delta_{i,S}(0)}\\
&=\prod_{i\in\omega_B'\cup\Omega_2'}\left(g_2^{q(i)},g^{zs^{*}}\right)^{\Delta_{i,S}(0)}=\hat{e}\left(g_1,g_2\right)^{zs^{*}}=Z^{s^{*}}
\end{aligned}
$$

挑战阶段之后，$\mathcal{A}$ 执行上述询问。但不允许对 ω_2^{*} 进行私钥生成询问，不允许询问 σ^{*} 的明文，但可以询问 σ^{*} 是否合法，即判断式(1)是否成立。猜测阶段，如果攻击者 $\mathcal{A}$ 输出 b'，且 $b'=b$，则攻击者 $\mathcal{A}$ 赢得游戏，则 $\mathcal{C}$ 可判断 $h=\hat{e}(g,g)^{xyz}$，解决 DBDH 问题。根据文献[17]的概率分析方法分析 $\mathcal{C}$ 解决 DBDH 问题的优势：$\mathcal{A}$ 不对 ω_2^{*} 进行私钥生成询问的概率至少为 $1/q_{H_1}$，$\mathcal{A}$ 拒绝有效的密文的概率最多为 $q_{US}/2^{\mathcal{K}}$，$\mathcal{A}$ 选择挑战 $\omega_1^{*},\omega_2^{*}$ 的概率至少为 $1\Big/\binom{2}{q_{H_1}}$，$\mathcal{A}$ 选择缺省属性 $\Omega_1'^{*},\Omega_2'^{*}$ 的概率至少为 $1\Big/\binom{d-k}{d-1}\cdot\binom{d-k'}{d-1}$，$H_2\left(c_b,\{\sigma_i^{*}\}_{i\in\omega_2^{*}\cup\Omega_2'^{*}}\right)=g^{\beta_{\delta_b}}$，$b\in\{0,1\}$ 的概率至少为 $1/q_{H_2}^2$，可得 $\mathcal{C}$ 解决 DBDH 问题的优势为

$$
\begin{aligned}
\varepsilon'&=\frac{\left((\varepsilon+1)/2-1/2\right)\left(1-q_{US}/2^{\mathcal{K}}\right)}{q_{H_1}q_{H_2}^2\binom{2}{q_{H_1}}\binom{d-k}{d-1}\binom{d-k'}{d-1}}\\
&>\frac{\varepsilon/2-q_{US}/2^{\mathcal{K}}}{q_{H_1}q_{H_2}^2\left(q_{H_1}^2/2\right)\dfrac{(d-1)^{d-k}}{d-k}\dfrac{(d-1)^{d-k'}}{d-k'}}\\
&=\frac{(d-k)(d-k')\left(\varepsilon-q_{US}/2^{\mathcal{K}-1}\right)}{q_{H_2}^2q_{H_1}^3(d-1)^{2d-k-k'}}
\end{aligned}
$$

定理 2 假定 G_1 上的CDH困难问题成立，则本文所提签密方案满足EF-ASC-CMA安全，即不存在一个IND-ASC-CMA攻击者以不可忽略的优势攻破所提方案。

证明 假设攻击者 $\mathcal{A}$ 能够在概率多项式时间内以 ε 的优势在定义5中的游戏中获胜，并且攻击者 $\mathcal{A}$ 最多进行 q_{H_i} 次 H_i 询问，$i=1,2$，q_K 次私钥生成询问，q_S 次签密询问和 q_{US} 次验证解密询问。构造算法 $\mathcal{C}$，利用 $\mathcal{C}$ 解决CDH问题，即给定 (g,g^x,g^y)，计算 g^{xy}。其他设置同定理1证明部分。$\mathcal{C}$ 仿真如下：

(1)初始化：$\mathcal{C}$ 设置 $g_1=g^x$，$g_2=g^y$。

(2)随机预言机：$\mathcal{A}$ 保存列表 $\mathcal{L}_1$ 和 $\mathcal{L}_2$ 用来存储 H_1-预言机和 H_2-预言机的答案。$\mathcal{C}$ 选择1个随机数 $\delta\in[1,q_{H_2}]$。

H_1-预言机：仿真过程同定理1证明中的 H_1-预言机。

H_2-预言机：如果对 $c_i,\{\sigma_j\}_{j\in U},\sigma_j\in G_1$ 进行 H_2-预言机询问。$\mathcal{C}$ 检查列表 $\mathcal{L}_2$，仿真如下：

(a)如果能在 $\mathcal{L}_1$ 中找到 i，返回其对应的值；

(b)否则，如果 $i\neq\delta$，选择随机数 $\alpha_i,\beta_i\in{}_RZ_q^{*}$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g_1^{\alpha_i}g^{\beta_i}$，并记录于 $\mathcal{L}_2$；

(c)如果 $i=\delta$，选择随机数 $\beta_\delta\in{}_RZ_q^{*}$，返回 $H_2(c_i,\{\sigma_j\}_{j\in U})=g^{\beta_\delta}$，并记录于 $\mathcal{L}_2$。

(3)私钥生成预言机：

(a)如果对属性集 ω_i，且满足 $|\omega_i\cap\omega_1^{*}|<k$，进行私钥生成询问。仿按照定理1私钥生成预言机步骤(a)的仿真过程生成 ω_i 的私钥

$$
D_i=\left(g_2^{\frac{\Delta_{0,S}(i)\gamma_i}{\beta_i}+\sum_{j\in\Gamma'}\Delta_{j,S}(i)q(j)}\left(g_1^{-\beta_i}g^{\gamma_i}\right)^{r_i'},g_2^{\frac{\Delta_{0,S}(i)}{\beta_i}}g^{r_i'}\right)
$$

(b)如果 $|\omega_i\cap\omega_1^{*}|\geq k$，则 $\mathcal{C}$ 仿真失败。

(4)签密预言机：$\mathcal{A}$ 请求在属性集 ω_A 和断言 $\Upsilon_{k,\omega_1^{*}}(\cdot),\Upsilon_{k,\omega_2^{*}}(\cdot)$ 下的消息 m 的签密询问。$\mathcal{C}$ 仿真如下：

(a)如果 $|\omega_A\cap\omega_1^{*}|<k$。则 $\mathcal{C}$ 利用私钥生成预言机产生 ω_A 的私钥 $D_{Ai}=(d_{i0},d_{i1})$，并且按照正常的签名算法产生密文并返回给 $\mathcal{A}$；

(b)否则，如果 $|\omega_A\cap\omega_1^{*}|>k$，$|\omega_B\cap\omega_1^{*}|<k$，$\mathcal{C}$ 从

缺省属性集 Ω 随机选择由 $d-k$ 个元素构成的子集 Ω_A'。假设 $\omega_A \cup \Omega_A' = \{i_1, i_2, \cdots, i_d\}, \omega_B = \{i_1, i_2, \cdots, i_{k'}\}$。$\mathcal{C}$ 随机选择 $r_i, s' \in {}_R Z_q^*$，设 $s = \frac{-1}{\alpha_{i_d}} y + s'$，设置 $\sigma_0 = g^s = g_2^{\frac{-1}{\alpha_{i_d}}} g^{s'}$，$\left\{\sigma_i = g^{\beta_i s} = g_2^{\frac{-\beta}{\alpha_{i_d}}} g^{\beta s'}\right\}_{i \in \omega_2^* \cup \Omega_2'}$，$\mathcal{C}$ 利用私钥生成预言机产生 ω_B 的私钥 $D_{Bi} = (d_{i,0}, d_{i,1})$，计算 $k_e = \prod_{i \in \omega_B^* \cup \Omega_2'} \left(\frac{\hat{e}\left(d_{i0}', \sigma_0'\right)}{\hat{e}\left(\sigma_i', d_{i1}'\right)}\right)^{\Delta_{i,S}(0)}$，$c_i = E_{k_e}(m_i)$。设置 $H_2\left(c_i, \{\sigma_i\}_{i \in \omega_2^* \cup \Omega_2'}\right) = g_1^{\alpha_{i_d}} g^{\beta_i}$，$\sigma_0' = \left(g_2^x\right) \prod_{i \in \omega_1^* \cup \Omega_1'} \cdot H_1(i)^{r_i} \cdot H_2\left(c_i, \{\sigma_i\}_{i \in \omega_2^* \cup \Omega_2'}\right)^s = \left(g_1^{\alpha_{i_d}} g^{\beta_i}\right)^{s'} \prod_{i \in \omega_1^* \cup \Omega_1'} H_1(i)^{r_i} \cdot g_2^{\frac{-\beta_i}{\alpha_{i_d}}}$，$\left\{\sigma_i' = g^{r_i'}\right\}_{i \in \omega_1^* \cup \Omega_1'}$。返回密文 $\sigma = \left\{\sigma_0, \{\sigma_i\}_{i \in \omega_2^* \cup \Omega_2'}, \sigma_0', \{\sigma_i'\}_{i \in \omega_1^* \cup \Omega_1'}, c_i\right\}$。$\sigma$ 是一个有效的密文；

(c)否则，按照定理 1 签密预言机步骤(b)的构造方法，生成密文 σ。

(5)验证解密预言机：$\mathcal{A}$ 请求密文 σ 的解密询问。$\mathcal{C}$ 仿真如下：

(a)如果 $|\omega_B \cap \omega_1^*| < k$。则 $\mathcal{C}$ 利用私钥生成预言机产生 ω_B 的私钥，并且按照正常的验证解密算法，验证解密得到明文 m_i 并返回或者放回终止符号 $\perp$；

(b)否则，$\mathcal{C}$ 返回无效的签名。如果之前 $\mathcal{A}$ 已经对 $(\omega_1^*, k, \omega_2^*, k', \omega_A, m)$ 进行了签密询问。那么从 $\mathcal{A}$ 角度看 σ 是一个合法的密文，则 $\mathcal{C}$ 仿真失败，该概率最多为 $q_{US}/2^{\mathcal{K}}$。

(6)伪造签名：$\mathcal{A}$ 选择挑战的属性集 ω_1^*, ω_2^* 和缺省属性集 $\Omega_1'^*, \Omega_2'^*$，输出一个消息 m_δ 的密文 $\sigma^* = \left\{\sigma_0^*, \{\sigma_i^*\}_{i \in \omega_2^* \cup \Omega_2'}, \sigma_0'^*, \{\sigma_i'^*\}_{i \in \omega_1^* \cup \Omega_1'}, c_\delta^*\right\}$。如果 $\mathcal{A}$ 没有选择 ω_1^*, ω_2^* 和 $\Omega_1'^*, \Omega_2'^*$ 或者 $H_2\left(c_\delta, \{\sigma_i^*\}_{i \in \omega_2^* \cup \Omega_2'}\right) \neq g^{\beta_\delta}$，则 $\mathcal{C}$ 仿真失败。如果 σ^* 合法，则满足式(1)，那么 $\mathcal{A}$ 赢得游戏。由于 $H_1(i) = g^{\gamma_i}$，$H_2\left(c_\delta, \{\sigma_i^*\}_{i \in \omega_2^* \cup \Omega_2'}\right) = g^{\beta_\delta}$，则 $\frac{\hat{e}\left(g, \sigma_0'^*\right)}{\left[\prod_{i \in \omega_1^* \cup \Omega_1'} \hat{e}\left(H_1(i), \sigma_i'^*\right)\right] \hat{e}\left(H_2\left(c_\delta, \{\sigma_i^*\}_{i \in \omega_2^* \cup \Omega_2'}\right), \sigma_0^*\right)} = \hat{e}\left(g, \sigma_0'^* \Big/ \prod_{i \in \omega_1^* \cup \Omega_1'} \sigma_i'^{*\gamma_i} \sigma_0^{*\beta_\delta}\right) = \hat{e}\left(g, g^{xy}\right)$。所以 $g^{xy} = \sigma_0'^* \Big/ \prod_{i \in \omega_1^* \cup \Omega_A'} \sigma_i'^{*\gamma_i} \sigma_0^{*\beta_\delta}$，$\mathcal{C}$ 解决了CDH问题。

根据文献[17]的概率分析方法分析 $\mathcal{C}$ 解决CDH问题的优势：$\mathcal{A}$ 不对 ω_1^* 进行私钥生成询问的概率至少为 $1/q_{H_1}$，$\mathcal{A}$ 拒绝有效的密文的概率最多为 $q_{US}/2^{\mathcal{K}}$，$\mathcal{A}$ 选择挑战 ω_1^*, ω_2^* 的概率至少为 $1\Big/\binom{2}{q_{H_1}}$，$\mathcal{A}$ 选择缺省属性 $\Omega_1'^*, \Omega_2'^*$ 的概率至少为 $1\Big/\binom{d-k}{d-1}\binom{d-k'}{d-1}$，$H_2\left(c_\delta, \{\sigma_i^*\}_{i \in \omega_2^* \cup \Omega_2'}\right) = g^{\beta_\delta}$ 的概率至少为 $1/q_{H_2}$，可得 $\mathcal{C}$ 解决CDH问题的优势为

$$\varepsilon' = \frac{\varepsilon\left(1 - q_{US}/2^{\mathcal{K}}\right)}{q_{H_1} q_{H_2} \binom{2}{q_{H_1}} \binom{d-k}{d-1} \binom{d-k'}{d-1}} > \frac{(d-k)(d-k')\left(2\varepsilon - q_{US}/2^{\mathcal{K}-1}\right)}{q_{H_2} q_{H_1}^3 (d-1)^{2d-k-k'}}$$

定理 3　本文所提签密方案满足签密者属性隐私安全性

证明　$\mathcal{C}$ 设置主密钥为 $x \in {}_R Z_q^*$ 和系统参数 param，攻击者 $\mathcal{A}$ 输出2个属性集 $\omega_{A1}^*, \omega_{A2}^*$，$\overline{\omega}^* = \omega_{A1}^* \cap \omega_{A2}^*$。选择缺省属性集 Ω。设置 $\hat{\omega}_{Ab}^* = \omega_{Ab}^* \cup \Omega$，$b \in \{0,1\}$。$\mathcal{C}$ 产生属性私钥 $sk_{\hat{\omega}_{A1}^*} = \left(d_{i0}^1, d_{i1}^1\right)_{i \in \hat{\omega}_{A1}^*}$，$sk_{\hat{\omega}_{A2}^*} = \left(d_{i0}^2, d_{i1}^2\right)_{i \in \hat{\omega}_{A2}^*}$，设置 $\left\{d_{i0}^\theta = g_2^{q_\theta(i)} H(i)^{r_i^\theta}, g^{r_i^\theta}\right\}_{i \in \hat{\omega}_\theta^*}$，$\theta \in \{0,1\}$，$r_i^\theta \in {}_R Z_q^*$，$q_\theta(i)$ 为 $d-1$ 次多项式，$q_\theta(0) = x$。$\mathcal{A}$ 输出一个消息 m^* 和属性子集 $\omega_1^* = \{i_1, \cdots, i_k\} \subseteq \overline{\omega}^*$，$|\omega_1^*| \le d$，请求 $\mathcal{C}$ 利用 $sk_{\hat{\omega}_{A1}^*}$ 或 $sk_{\hat{\omega}_{A2}^*}$，在 ω_1^*, ω_2^* 下对消息 m^* 进行签密。$\mathcal{C}$ 随机选择 $b \in \{0,1\}$，输出密文 $\sigma_0 = g^s$，$\left\{\sigma_i = H_1(i)^s\right\}_{i \in \omega_2^* \cup \Omega_2'}$，$\sigma_0' = g_2^x \prod_{i \in \omega_1^* \cup \Omega_1'} H_1(i)^{r_i} H_2\left(c_i, \{\sigma_i\}_{i \in \omega_2^* \cup \Omega_2'}\right)^s$，$\left\{\sigma_i' = g^{r_i'}\right\}_{i \in \omega_1^* \cup \Omega_1'}$，$c_i = E_{k_e}(m_i)$。由拉格朗日插值定理可知，该密文可由 $sk_{\hat{\omega}_{A1}^*}$ 或 $sk_{\hat{\omega}_{A2}^*}$ 产生。$\mathcal{A}$ 无法区分 $\hat{\omega}_{A1}^*$ 和 $\hat{\omega}_{A2}^*$ 中哪个集合用于产生 σ。因此，定理 3 成立。

5.2 性能分析

由于目前还缺乏有效的支持动态门限、签密者属性隐私安全的 ABSC 方案，因此表 1 中给出了本文方案与“ABS+ABE”方案的性能比较。其中，文献[13]方案是目前高效的支持动态门限和匿名性的 ABS 方案，由于缺乏动态门限 ABE 方案，所以选择 FIBE[7]方案与文献[13]方案相结合。表 1 中分别列出了加密阶段和解密阶段的计算代价。S 表示 G_1 上的幂运算，E 表示 G_2 上的幂运算，P 表示双线性对运算，N_1 表示签名属性集包含的属性数量，N_2 表示加密属性集包含的属性数量，N_{ID} 表示用户 ID 的属性集包含的属性数量。从表 1 中可以看出，本文方案实现了签名和解密属性动态门限，在签密阶段由签密者确定，而文献[13]+FIBE[7]方案的门限是固定的，在初始化阶段确定。本文方案具有较小的

表 1 本文方案与其它方案性能比较

方案	计算代价	通信代价	存储代价	门限
文献[13]+FIBE[7]	$(3(N_1+d-k)+d+3+N_2)S$ $+E[N_1+d-k+2N_2]P+N_2E$	$(N_1+N_2+d-k+3)$ $\cdot\lvert G_1\rvert+\lvert G_2\rvert$	$(4N_{\mathrm{ID}}+2d-2)\lvert G_1\rvert$	(d,n)
本文方案	$(3(N_1+d-k)+d+2+N_2+d-k')S+E[N_1$ $+d-k+2(N_2+d-k')]P+(N_2+d-k')E$	$(N_1+N_2+2d-k$ $-k'+2)\lvert G_1\rvert+\lvert G_2\rvert$	$2(N_{\mathrm{ID}}+d-1)\lvert G_1\rvert$	(k,n) $1\le k\le d$

存储代价，由于加密采用动态门限，增加了一定的计算代价和通信代价。当 $k'=d$ 时，本文方案退化为文献[13]+FIBE[7]方案，但具有较小的计算代价和通信代价。此外，本文方案中，验证解密过程中先验证签名，如果签名不合法，直接拒绝密文，不用解密，降低了验证解密者的计算代价。

6 结论

本文提出的基于属性签密方案具有动态门限、匿名性和多接收者特点，实现了签密者属性隐私安全性。密文不会暴露签密者或者加密者全部的属性，也无法判断其明确拥有哪些属性。并且利用 CDH 问题和 DBDH 问题的困难性，在随机预言机模型下证明了方案的安全性。该方案与“签名+加密”方案相比具有灵活的门限结构和较低的代价。特别适合具有复杂访问控制需求和隐私保护的面向群组通信的网络应用。

参 考 文 献

[1] Zheng Y and Imaih H. Efficient and unforgeable multicast conference key establishment without relying on a key distribution center[C]. Proceedings of the 20th Symposium on Information Theory and Its Applications, Matsuyama, Japan, Dec. 2–5, 1997: 365–368.

[2] Shamir A. Identity-based cryptosystems and signatures schemes[C]. Proceedings of the 4th Annual International Cryptology Conference, Santa Barbara, CA, USA, Aug. 19–22, 1984, LNCS 196: 47–53.

[3] Boneh D and Franklin M K. Identity based encryption from the weil pairing[C]. Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, Santa Barbara, California, USA, Aug. 19–23, 2001: 213–229.

[4] Malone-Lee J. Identity based signcryption[R]. IACR Cryptology ePrint Archive, Report, 2002, 098, 2002.

[5] Mu Y, Susilo W, and Lin Y X. Identity-based authenticated broadcast encryption and distributed authenticated encryption[C]. Proceedings of the 9th Asian Computing Science Conference, Thailand, Dec. 8–10, 2004, LNCS 3321: 169–181.

[6] Yu Y, Yang B, Huang X Y, *et al*.. Efficient identity-based signcryption scheme for multiple receivers[C]. Proceedings of the 4th International Conference on Autonomic and Trusted Computing, Hong Kong, China, July 11–13, 2007, LNCS 4610: 13–21.

[7] Sahai A and Waters B. Fuzzy identity-based encryption[C]. Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques: Advances in Cryptology, Aarhus, Denmark, May 22–26, 2005, LNCS 3494: 457–473.

[8] Goyal V, Pandey O, Sahai A, *et al*.. Attribute-based encryption for fine-grained access control of encrypted data[C]. Proceedings of the 13th ACM Conference on Computer and Communications Security, Alexandria, VA, USA, Oct. 30–Nov. 3, 2006: 221–238.

[9] Maji H K, Prabhakaren M, and Rosulek M. Attribute-based signatures: achieving attribute-privacy and collusion-resistance[R]. IACR Cryptology ePrint Archive, Report, 2008/328, 2008.

[10] Maji H K, Prabhakaren M, and Rosulek M. Attribute-based signatures[R]. Cryptology ePrint Archive, Report, 2010, 595, 2010.

[11] Li J and Kim K. Attribute-based ring signatures[R]. IACR Cryptology ePrint Archive, Report, 2008/394, 2008.

[12] Shahandashti S F and Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems[C]. Proceedings of the 2nd International Conference on Cryptology in Africa, Gammarth, Tunisia, June 21–25, 2009: 198–216.

[13] Li J and Man H A. Attribute-based signature and its applications[C]. Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, Beijing, China, Apr. 13–16, 2010: 60–69.

[14] Herranz J, Laguillaumie F, Libert B, *et al*.. Short attribute-based signatures for threshold predicates[C]. Proceedings of the 12th International Conference on Topics in Cryptology, San Francisco, CA, USA, Feb. 27–Mar. 2, 2012, LNCS 7178: 51–67.

[15] Gagne M, Narayan S, and Safavi-Naini R. Threshold attribute-based signcryption[C]. Proceedings of the 7th International Conference on Security and Cryptography for Networks, Amalfi, Italy, Sep. 13–15, 2010, LNCS 6280: 154–171.

[16] Emura K, Miyaji A, and Rahman M S. Toward dynamic attribute-based signcryption(Poster)[C]. Proceedings of the 16th Australasian Conference on Information Security and Privacy, Melbourne, Australia, July 11–13, 2011, LNCS 6812: 439–443.

[17] Libert B and Quisquater J J. New identity based signcryption schemes from pairings[C]. Proceedings of IEEE Information Theory Workshop, Paris, France, Mar. 31–Apr. 4, 2003: 155–158.

张国印： 男，1962年生，教授，博士生导师，研究方向为网络与信息安全、嵌入式系统.

付小晶： 女，1980 年生，博士生，研究方向为网络与信息安全、密码学.

马春光： 男，1974年生，教授，博士生导师，研究方向为密码学与信息安全、Ad hoc与传感网络安全.