一个多授权中心的属性基签密方案

聂旭云[1,2], 鲍阳阳[1,2], 孙剑飞[1,2], 熊 虎[1,2*], 秦志光[1,2]

[1] 电子科技大学信息与软件工程学院 成都 中国 610054
[2] 网络与数据安全四川省重点实验室(电子科技大学) 成都 中国 610054

摘要 属性基签密体制能同时保证消息的保密性和存在性不可伪造，并能实现一对多的密文数据共享和细粒度访问控制。现有的属性基签密方案均是在单一授权机构下实现，容易产生单点失效和负担过重等问题。本文通过将用户的多个属性交由不同的授权中心分别管理，从而构造出一个适用于个人健康管理系统(PHR)的多授权中心属性基签密方案，并通过性能分析和仿真实验说明本文所提方案具有较短的用户密钥长度和较小的解签密时间开销。方案的安全性在标准模型下被规约到双线性 Diffle-Hellman 假设和计算 Diffle-Hellman 假设。

关键词 多授权中心；属性基密码体制；签密
中图法分类号 TP309.7 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2018.09.02

A Multi-Authority Attribute-based Signcryption Scheme

NIE Xuyun[1,2], BAO Yangyang[1,2], SUN Jianfei[1,2], XIONG Hu[1,2*], QIN Zhiguang[1,2]

[1]School of Information and Software Engineering, University of Electronic Science and Technology of China, Chengdu 610054, China
[2] Network and Data Security Key Laboratory of Sichuan Province (University of Electronic Science and Technology of China), Chengdu 610054, China

Abstract Attribute-based signcryption schemes can not only achieve confidentiality and existential unforgeablity, but also provide one-to-many encryption and fine-grained access control. Unfortunately, all of the existing attribute-based signcryption are constructed with the support of a single authority center, which may suffer from single point failure and become the efficiency bottle-neck. we multiple attributes of associated with users are managed by the single authority. To tackle this challenge, we propose a multi-authority attribute-based signcryption scheme by allowing different authority centers to manage multiple attributes. Furthermore, a secure Personal Health Record (PHR) sharing system is also constructed based on the suggested multi-authority attribute-based signcryption scheme. Performance evaluation and simulation experiment demonstrate that the proposed scheme outperforms the existing work in terms of the length of the private key and the computational cost of unsigncryption algorithm. The security of our scheme is formally proved under the Bilinear Diffie-Hellman assumption and Computational Diffie-Hellman assumption in the standard model.

Key words multi-authority; attribute-based cryptosystem; signcryption

1 引言

基于属性密码体制是近年来密码学领域的研究热点。与传统的基于身份的密码体制相比，基于属性密码体制实现了一对多的细粒度的访问权限控制，提升了发送方的效率。属性基密码体制源于 2005 年 Sahai 等[1]提出的模糊身份基加密体制，该方案中，当用户所持有的属性个数与密文相关的属性个数达到预设的门限值时，才能获取解密权限。基于模糊身份基加密体制及的思想，Goyal 等[2]提出了第一个密钥策略属性基加密(KP-ABE)方案，其中用户私钥关联于访问结构，而密文关联于属性集合，只有密

通讯作者： 熊虎，博士，教授，xionghu.uestc@gmail.com。
本课题得到国家自然科学基金[No.61672135]；广东省科技项目[No.2016A010101002]；四川省科技厅科技支撑计划[No.2016JZ0020]；“十三五”国家密码发展基金密码理论课题[No.MMJJ20170204]；电子科技大学中央高校新进教师科研启动基金[No.ZYGX2015KYQD136]；内江市科技孵化项目[No.170676]；国家自然基金重点国际(地区)合作研究项目[No.61520106007]；国家自然科学基金项目[No.61602097]；四川省科技支撑计划[No.2016GZ0065]资助。
收稿日期: 2017-12-29；修改日期: 2018-04-13；定稿日期: 2018-08-20

文的属性满足密钥的访问结构时, 才能进行解密。相应地, Bethencourt 等[3]提出了密文策略属性基加密(CP-ABE)方案, 密文对应于访问结构, 而密钥对应于属性集合, 当且仅当密钥的属性满足于密文的访问结构时才获得访问权限, CP-ABE 方法中用户可以决定哪些用户可以访问密文, 因此更适用于云计算环境下的应用。Qin 等[4]提出一种支持加解密外包的可撤销存储的密文策略属性基加密方案, 通过定期更新存储在云服务器中的密文, 来实现用户在撤销后无法访问这些密文。Li 等[5]基于个人健康档案系统(PHR)提出了一个适用于多个用户场景的属性基加密方案, 相对于此前的其他类似工作, 该方案有着更高的计算性能和安全性。Yan 等[6]基于格上带误差学习问题提出一种新的属性基加密方案, 并证明了该方案在标准模型下, 能够抵挡自适应选择明文攻击。

近年来, 与属性基加密一样, 属性基签名(ABS)也得到了快速的发展。属性基签名源于 Yang 等[7]提出的基于模糊身份签名方案。Maji 等[8]第一次提出了属性基签名的原语, 同时构造了一个支持有效隐私保护且抗合谋攻击的属性基签名方案。随后, 国内外的学者关于属性基签名做了大量研究[9-11], 并提出了一些功能扩展和安全性提升方面的属性基签名的应用。Shahandashti[12]提出了一个可用于匿名认证的门限属性基签名方案, 并基于计算 Diffie-Hellman 假设证明了其不可伪造性。Liu[13]等提出了一个有效实现云计算环境下细粒度访问控制的 PHR 的密文策略属性基签名方案, 并进一步提出了一个在线/离线属性基签名方案[14], 以较低的本地计算成本实现了数据完整性和签名者身份隐私保护, 更加适用于可携带的健康监测设备。

上述的属性基加密或属性基签名设计, 均只单独提供了对消息的保密性或是不可伪造性的保证。但是在实际应用中, 消息的接收者通常不仅需要对密文解密, 还要确定该密文确实是否由发送者本人发出的。传统的“先签名后加密”方法虽然可以达到这一要求, 但是这种方法使得系统的计算开销和通信成本都会大幅增加。对此, Zheng 在文献[15]中第一次提出签密的概念并给出了一个具体的方案, 用于同时保证消息的机密性和存在性不可伪造。随后, Malone 等[16]首次利用椭圆曲线上的双线性对设计了一种基于身份的签密方案。Shi 等[17]和 Chen 等[18]分别提出了两种不同的属性基签密方案, 但他们的方案的效率较低。近年来, 国内外学者又对属性基签密进行了大量研究, 在计算效率上有了一定的提升, 并扩展了很多新的应用: Yang 等[19]提出了一种高效的模糊身份基签密方案, 该方案同时满足可公开验证性和短密文性, 且具有较小的运算量。Gagne 等[20]提出了一种标准模型下的阈值属性基签密方案。在该方案中, 发送方可以选择性地公开自己的隐私属性。Emura 等[21]第一次提出了一种前向安全的属性基签密方案, 实现了在不需要重新发布用户私钥的前提下, 签密者的访问结构能够动态地更新。Han 等[22]提出一个非单调访问结构的属性基签密方案, 具有固定密文长度, 且同时满足可公开验证性。Hu 等[23]设计了一种可用于体域网(BAN)的模糊基于属性签密方案, 在保护病人隐私的同时, 支持在紧急情况下急救人员对存储在 BAN 中的信息进行灵活访问, 具有很强的实用价值。Guo 等[24]将环签名的思想引入到属性基签密中, 使用属性环来保护签密用户身份隐私。Rao 等[25]于 2014 年第一次提出了一个固定密文长度的属性基签密方案, 并在随机预言机模型下证明了其具有机密性和不可伪造性。Zhang 等[26]提出了一种模糊生物特性签密方案, 当与用户私钥相关的生物特性字符串相比与密文相关的特性字符串的误差小于某个值时, 用户可以使用其私钥进行解密, 从而说明该方案具有容错性。Yu 等[27]提出了一个同时支持密钥策略签名和密文策略加密的混合访问结构属性基签密方案(KCP-ABSC), 且实现了签密密文长度固定。Wei 等[28]提出一种高效的可追踪属性基签密方案, 其权威机构可以在必要时打破签密的匿名性。Hu 等[29]分析了密文策略属性基签密(CP-ABSC)的计算量和安全性, 并将其应用到保护智能电网中的组播通信。Zheng 等[30]为了克服传统 PKI 在证书管理上的缺陷, 设计了一个门限属性基签密方案, 方案具有高效安全的特点, 具有较高的实用价值。Pei 等[31]提出了一种云环境下增强安全性的属性基签密方案, 并给出了一个在医疗保健系统下的应用, 通过将用户身份融合到属性基签密中, 从而防止患者的隐私遭受合谋攻击。Hong 等[32]提出了一个密钥策略的属性基签密方法, 具有授权计算和高效密钥更新的功能。当发生访问权限改变或密钥泄露时, 系统将自动进入下一个时间片, 从而保证前向安全性。Zhao[33]等提出了一种强制定验证者环签密体制, 保证只有指定的验证者才能进行有效验证。Rao 等[34]第一次提出了一种基于 LSSS 的属性基签密方法, 该方案具有固定密文长度, 且具有可公开验证性, 即允许任何第三方检验密文的有效性和完整性。随后, Rao 等[35]又提出了一种适用于个人健康管理系统(PHR)的密文策略属性基签密

(CP-ABSC)方案, 该方案可同时实现细粒度访问控制、机密性、隐私保护和可公开验证性。

上述方案都是在单个授权中心模式下提出的, 在结合如针对安全 PHR 共享的属性基签密应用实例后, 单一授权中心模式暴露出了两个问题。一是 PHR 是一个社会公益系统, 用户规模非常庞大, 给授权中心带来了沉重的用户密钥生成和管理负担, 影响了系统的效率。二是当该唯一的授权中心受到攻击时, 所有的用户私钥都有可能泄露, 从而产生极大地安全隐患。我们尝试通过利用多授权中心的方式来有效解决这一问题。多授权中心公钥密码体制于 2010 年由 Chase[36]提出了, 并同时提出了相应的多授权中心属性基加密方案。随后, Sun 等[37]和 Cao 等[38]基于 Chase 的工作, 分别提出了不同的多授权中心签名方案。

为了解决例如 PHR 等云计算环境下的应用在数据保密和认证方面的问题, 克服实际应用中单一授权中心系统效率和安全性方面的弊端, 我们在 Chase[36]的基础上, 构造一种适合于 PHR 应用的多授权中心属性基签密方案, 据我们所知, 截至目前, 并没有人做过上述工作。

具体来说, 本文的贡献如下:

1. 我们定义了一个多授权中心属性基签密方法的架构, 架构造由系统建立算法、密钥生成算法、签密算法和解签密算法等四个部分组成;

2. 在上述多授权中心属性基签密方法的架构的基础上, 我们提出了一个具体的构造方案, 并对方案做了安全性分析;

3. 我们讨论了本方案在例如PHR系统等应用实例上的实用性, 并对方案做了性能分析和实验仿真, 证明了我们的方案在密钥长度和解签密时间上存在优势。

2 预备知识

2.1 双线性映射

G, G_T 为素数 p 阶循环群, g 为 G 的生成元, 双线性映射 $e: G\times G\to G_T$ 存在以下性质:

(1) 双线性性 $e(g_1^u, g_2^v)=e(g_1,g_2)^{uv}$, 其中 $g_1,g_2\in G$, $u,v\in Z_p$;

(2) 非退化性: 存在 $g_1,g_2\in G$, 使得 $e(g_1,g_2)\neq 1$;

(3)可计算性: 对任意的 $g_1,g_2\in G$, 都可以计算 $e(g_1,g_2)$。

2.2 困难性假设

定义 1 双线性 Diffle-Hellman 难题(BDH): 在素数阶 p 的循环群 G 中, g 是 G 的生成元, 随机选取 $a,b,c\in Z_p$, 已知 (g,g^a,g^b,g^c), 以及一个双线性映射 e, 任选 $R\in Z_p$, 分辨 $e(g,g)^{abc}$ 与 $e(g,g)^R$ 是困难的。

定义 2 计算性 Diffle-Hellman 难题(CDH):随机选择 $a,b\in Z_p$, g 为 G 的生成元, 已知 (g,g^a,g^b), 计算 g^{ab} 被认为是困难的。

2.3 拉格朗日插值定理

Shamir[39]提出使用多项式插值来实现秘密分享。其思想是将密钥分为 n 个部分并分别发放给 n 个用户, 当持有秘密份额的用户达到一定数量 d 时就可以恢复密钥, 当持有秘密份额的用户数量不足 d 时, 不能获得关于多项式的任何信息。

设 $f(x)$ 是一个 $d-1$ 阶多项式: $f(x)=\alpha+\alpha_1 x+\alpha_2 x^2+\ldots+\alpha_{d-1}x^{d-1}$, 已知该多项式上 d 个不同点 $(x_i,f(x_i))$ 的集 S, 可通过 $f(x)=\sum_{i=1}^{d} f(x_i)\Delta_{i,S(x)}$ 恢复出秘密分享值, 其中 $\Delta_{i,S(x)}=\prod_{i\in S,j\neq i}\frac{x-j}{i-j}$。

3 多授权中心属性基签密结构与安全模型

3.1 多授权中心属性基签密结构

多授权中心属性基签密由以下四个算法构成:

系统建立算法(Setup): 输入安全参数 λ, 产生系统主公钥 MPK, 主私钥 MSK, 以及每个属性授权中心的公钥 APK 和私钥 ASK;

密钥生成算法(Extract): 用户的私钥由两部分构成, 一部分由属性授权中心生成: 输入属性授权中心的私钥 ASK, 用户身份以及相关的属性集合, 生成用户的部分私钥 $D_{k,i}$; 另一部分由中心授权方生成:输入系统主私钥 MSK 和用户的身份信息, 输出用户另一部分私钥;

签密算法(Signcrypt): 签密者输入消息, 签名私钥, 系统公钥, 签密者私钥和一个签密属性集 w_A, 输出密文;

解签密算法(Unsigncrypt): 输入密文, 系统公钥 MPK 和解签密者私钥, 若解签密者的属性集合

w_B 满足 $|w_A \cap w_B| \geq d$，即满足要求的属性达到一定数量，就进行解密和验证操作。如果验证合法，则说明消息是可信的。

多授权中心属性基签密方案的正确性定义，对于任意的 Setup(λ) $\rightarrow$ (MPK, MSK, APK, ASK), Extract(ASK, u, A_C, MSK) $\rightarrow$ ($D_{k,i}, D_{ca}, D'_{ca}$), Signcrypt($m, A_C, MPK, MSK, APK, D_{k,i}, D_{ca}, D'_{ca}$) $\rightarrow \sigma$，方案的正确性要求 Unsigncrypt($\sigma, A_u, D_{k,i}, D_{ca}$) $\rightarrow (m, e(g, g^{y_0'}))$成立。

3.2 安全性定义

由于涉及同一个逻辑步骤内的签名和加密，因此多授权中心属性基签密方案的安全性要同时保证机密性和不可伪造性。以下两个游戏反映了该签密方案的安全模型，游戏双方为攻击者 $\mathcal{A}$ 和挑战者。

3.2.1 游戏 1: 选择明文攻击下不可区分性(IND-CPA)游戏

初始化: 攻击者 A 选择其要攻击的属性集合 w'，并分配到各个相关的属性授权中心;

参数建立: 挑战者 C 建立系统产生系统，并将系统公钥和各属性授权中心公钥传递给攻击者 A;

阶段 1&阶段 2: 攻击者 A 向挑战者 C 询问相关访问结构的私钥，该私钥不能直接用于解密 w' 下签密的密文，且对于某一个属性授权中心，不可以重复询问某一用户的密钥;

挑战: 攻击者 A 选择两个明文消息 m_0, m_1，再从挑战者 C 获得消息 m_γ 的密文 c_γ，其中 $\gamma \in \{0,1\}$；阶段 2: 攻击者 A 继续向挑战者做密钥询问，具体同阶段 1;

猜测: 攻击者 A 输出 γ'，如果 $\gamma' = \gamma$，则攻击者成功。攻击者在游戏中的优势为:

$$Adv_A = Pr[\gamma' = \gamma] - \frac{1}{2}。$$

定义 1 不存在多项式有界的攻击者 $\mathcal{A}$ 能以不可忽略的优势赢得游戏，则可以说多授权中心属性基签密方案对于选择属性集在选择密文攻击下满足机密性。

3.2.2 游戏 2: 选择消息攻击下不可伪造性(EUF-CMA)游戏

初始化: 攻击者 $\mathcal{A}$ 公开将要攻击的属性集合 w'，并分配到各个相关的属性授权中心;

参数建立: 挑战者 C 建立系统产生系统，并将系统公钥和各属性授权中心公钥一并传递给攻击者 $\mathcal{A}$;

阶段 1&阶段 2: 攻击者 $\mathcal{A}$ 向挑战者提交明文消息 m，挑战者 C 返回相应签密密文，该询问可以做多项式有界次，且不能直接询问关于 w' 的签密密文;

伪造: 攻击者 $\mathcal{A}$ 计算基于属性集合 w' 对消息 m' 的签密密文 σ'，如果 σ' 可以被正确地解密和验证，且攻击者 $\mathcal{A}$ 没有询问过，就可以认为赢得了游戏 2。攻击者 $\mathcal{A}$ 赢得游戏 2 的优势为 $AdvA = Pr[\mathcal{A}$ 赢得游戏 2$]$。

定义 2 不存在多项式有界的攻击者 $\mathcal{A}$ 能以不可忽略的优势赢得游戏 2，则可以认为多授权中心属性基签密方案对于选择属性集在选择消息攻击下满足不可伪造性。

4 多授权中心属性基签密方案的具体构造

本文提出的多授权中心属性基签密方案，建立在 Chase[35]提出的多授权中心模型之上。用户的多个属性由不同的多个属性授权中心管理，属性授权中心根据用户持有的属性为用户生成部分密钥。中心授权机构负责管理用户身份信息，生成系统公私钥对，并根据每个属性授权中心产生的属性私钥为用户产生另一部分密钥。为保证授权中心给用户生成的私钥有随机性，方案中使用了伪随机函数(PRF)。具体构造如下:

系统建立算法(Setup): 选取素数阶群 G, G_T，双线性映射 $e: G \times G \rightarrow G_T$，生成元 $g \in G$，随机选择 $g_1 \in G$，假设系统中存在 n 个属性，n 个属性的集合为 $U = \{1, 2, \cdots, n\}$，$i \in U$，d 为属性门限值。选择一个 Hash 函数 $H: G_T \rightarrow Z_p$。将属性域分为 K 个不相邻的的属性集合，分属 K 个属性授权中心管理。选择 K 个属性授权中心的伪随机数种子 $s_1, s_2, \cdots, s_K$，任取 $y_0, y_0' \in Z_p$，$g_2 = g^{y_0'}$，从 Z_p 中随机选取 $\{t_{k,i}\}$，其中，$i = 1, \cdots, n$, $k = 1, \cdots, K$，$T_{k,i} = g^{t_{k,i}}$。中心授权机构生成的系统主公钥: $MPK = \{g, g_1, g_2, G, G_T, Y_0 = e(g,g)^{y_0}\}$，系统主私钥 $MSK = \{y_0, y_0'\}$；每个属性授权中心的公钥 $APK = \{T_{k,1}, T_{k,2}, \cdots, T_{k,n}\}$ 和私钥 $ASK = \{sk, t_{k,1}, t_{k,2}, \cdots, t_{k,n}\}$。

密钥生成算法(Extract): 属性授权中心首先为用户生成部分密钥，输入用户身份 u 和属性集合，构造 $d-1$ 次多项式 $f(x)$，使得 $f(0) = y_{k,u}$，其中 $y_{k,u} = F_{sk}(u)$，计算用户的一部分私钥 $D_{k,i} = g^{\frac{f(i)}{t_{k,i}}}$；另一方面，输入系统主私钥 MSK 和身份 u，中心授

权机构计算用户的另一部分私钥 $D_{ca}=g^{y_0-\sum_{k=1}^{K}y_{k,u}}$，$D'_{ca}=g^{y'_0-\sum_{k=1}^{K}y_{k,u}}$。

签密算法(Signcrypt):签密者选取随机数 $r\in Z_p$，$r'\in Z_p$，输入消息 m，签密者的属性集合 A_C，属性公钥 APK，系统公私钥对 MPK,MSK，以及用户密钥 $D_{k,i},D_{ca},D'_{ca}$。随后，该算法计算消息 m 的签名为 $\sigma=\{C_1,C_2,C_3,C_4,C_5,E,\{E_{k,i}\}\}_{i\in A_C}$；其中，$C_1=D_{k,i}{}^{r'}$，$C_2=D'_{ca}\cdot(g_1{}^{H(m)})^{r'}$，$C_3=T_{k,i}{}^{\frac{1}{r'}}$，$C_4=g^{r}$，$C_5=g^{r'}$，$E=Y_0{}^{r}m$，$\{E_{k,i}=T_{k,i}{}^{r}\}_{i\in A_C{}^{k}}$。

解签密算法(Unsigncrypt): 设解签密者的属性集合为 A_u，进行以下操作:

若存在 $|A_u\cap A_C|\geqslant d$，则进行以下解密过程:计算 $e(E_{k,i},D_{k,i})=e(g,g)^{f(i)r}$，通过拉格朗日插值最终得 $Y_{k,u}{}^{r}=e(g,g)^{f(0)r}=e(g,g)^{y_{k,u}r}$，计算 $Y_{ca}{}^{r}=e(C_4,\ D_{ca})$，结合以上信息，计算 $Y_0{}^{r}=Y_{ca}{}^{r}\times\prod_{k=1}^{K}Y_{k,u}{}^{r}$，最后通过计算 $m=E/Y_0{}^{r}$，获取明文消息 m。

选取 $S\subseteq A_C$，且 $|S|=d$，验证:

$$\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}\prod_{k=1}^{K}(\prod_{i\in S}e(C_1,C_3)^{\Delta_{i,S}(0)})=e(g,g_2),$$

其中 $\Delta_{i,S}(0)=\prod_{j\in S,j\neq i}\frac{j}{j-i}$。

如果上式成立，说明明文消息有效，具体的解签密推导过程如下:

解签密者使用其私钥 $D_{k,i}$，D_{ca} 进行如下解密:

$$\frac{e(g,g)^{y_0r}m}{Y_{ca}{}^{r}\times\prod_{k=1}^{K}Y_{k,u}{}^{r}}=\frac{e(g,g)^{y_0r}m}{e(C_4,D_{ca})\times\prod_{k=1}^{K}Y_{k,u}{}^{r}}$$

$$=\frac{e(g,g)^{y_0{}^{r}}m}{e(g^{r},g^{y_0-\sum_{k=1}^{K}y_{k,u}})\times e(g,g)^{r\cdot\sum_{k=1}^{K}y_{k,u}}}$$

$$=\frac{e(g,g)^{y_0{}^{r}}m}{e(g,g^{r(y_0-\sum_{k=1}^{K}y_{k,u})})\times e(g,g)^{r\cdot\sum_{k=1}^{K}y_{k,u}}}$$

$$=\frac{e(g,g)^{y_0r}m}{e(g,g)^{y_0r}}=m$$

如果消息m没有被修改或伪造，则有:

$$\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}\prod_{k=1}^{K}(\prod_{i\in S}e(C_1,C_3)^{\Delta_{i,S}(0)})$$

$$=\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}\prod_{k=1}^{K}(\prod_{i\in S}e(g^{\frac{f(i)}{t_{k,i}}r'},g^{\frac{t_{k,i}}{r'}})^{\Delta_{i,S}(0)})$$

$$=\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}\prod_{k=1}^{K}(\prod_{i\in S}e(g,g)^{\sum_{i\in S}f(i)\Delta_{i,S}(0)})$$

$$=\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}\prod_{k=1}^{K}e(g,g)^{f(0)}$$

$$=\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}\prod_{k=1}^{K}e(g,g)^{y_{k,u}}$$

$$=\frac{e(C_2,g)}{e(g_1{}^{H(m)},C_5)}e(g,g)^{\sum_{k=1}^{K}y_{k,u}}$$

$$=\frac{e(g^{y'_0-\prod_{k=1}^{K}y_{k,u}}\cdot(g_1{}^{H(m)})^{r'},g)}{e(g_1{}^{H(m)},g^{r})}e(g,g)^{\sum_{k=1}^{K}y_{k,u}}$$

$$=e(g^{y_0{}'-\sum_{k=1}^{K}y_{k,u}},g)e(g,g)^{\sum_{k=1}^{K}y_{k,u}}$$

$$=e(g,g^{y_0{}'})$$

$$=e(g,g_2)$$

5 安全性分析

5.1 机密性

定理 1 如果 BDH 问题在群 G 中是困难的，则本方案在选择属性集 ω' 和选择密文攻击下满足机密性。

证明: 假设存在一个多项式时间的攻击者 $\mathcal{A}$ 能以不可忽略的优势 ε 赢得游戏 1，那么我们将能利用该攻击者以不可忽略的优势解决群 G 中的 BDH 问题。

首先假设对于每个可信的授权中心 k，即使用普通的随机函数取代伪随机函数 F_{s_k}，攻击者 $\mathcal{A}$ 仍然能以不变的优势获得成功。设用户持有的属性集为 A_u，解密密文所要求的属性集 A_C。攻击者 $\mathcal{A}$ 选择要攻击用户属性集合 ω'，并发送给挑战者 C, 属性集 A_C 和被攻破的属性授权中心列表 $Corr$。

初始化: 攻击者 $\mathcal{A}$ 选取并发送给挑战者 C 一个挑战属性集合 A_C 和被攻破的属性授权中心列表 $Corr$。

系统建立: 输入参数 $A=g^{a},B=g^{b},C=g^{c}$，攻击者的目标是区分 $Z=e(g,g)^{abc}$ 或者 $Z=e(g,g)^{R}$，其中 R 表示从 Z_p 中任意取的随机数; 挑战者 C 随机选取 $v,y'\in Z_p$ 以及一个哈希函数 $H:G\rightarrow Z_p$，计算 $g_1=g^{v}$，$g_2=g^{y'}$ $Y_0=e(A,B)=e(g,g)^{ab}$。在这里意味着 $y_0=ab$。此外，对于属性 $i\in A_u\cap A_C{}^{k}$，挑战者 C 随机选取若干个 $\beta_{k,i}$，并计算 $T_{k,i}=g^{\beta_{k,i}}$；对于属性 $i\in A_u-A_C{}^{k}$，计算 $T_{k,i}=(g^{b})^{\beta_{k,i}}=B^{\beta_{k,i}}$。

输出公钥 $MPK=\{g,g_1,g_2,G,G_T,H,Y_0=e(A,B)\}$。

输出可信授权中心的公钥: $\{T_{k,i}=g^{\beta_{k,i}}\}_{i\in A_u\cap A_C{}^k}$, $\{T_{k,i}=B^{\beta_{k,i}}\}_{i\in A_u-A_C{}^k}$。被攻破授权中心的私钥: 任选 $t_{k,i}\in Z_p$ 和伪随机函数种子 s_k, 私钥为: $\{s_k,\{t_{k,i}\}\}$。

阶段 1&阶段 2: 令 $k(u)$ 为第一个被查询到属性不能满足访问结构的授权中心, 即 $|A_u{}^k\cap A_C{}^k|<d$。

对可信属性授权中心 $k\neq k(u)$ 关于用户 u 的询问: 设 $f(0)=F_{s_k}(u)=z_{k,u}b$。挑战者 C 随机选择 $z_{k,u}$ 和多项式 φ 使得 $\varphi(0)=z_{k,u}$, 设 $f(i)=b\varphi(i)$。因此, 当 $i\in A_C{}^k$, $t_{k,i}=\beta_{k,i}$, 就有 $D_{k,i}=g^{\frac{f(i)}{t_{k,i}}}=g^{\frac{b\varphi(i)}{\beta_{k,i}}}=B^{\frac{\varphi(i)}{\beta_{k,i}}}$; 当 $i\notin A_C{}^k$, $t_{k,i}=b\beta_{k,i}$, 就有 $D_{k,i}=g^{\frac{f(i)}{t_{k,i}}}=g^{\frac{b\varphi(i)}{b\beta_{k,i}}}=g^{\frac{\varphi(i)}{\beta_{k,i}}}$。所以, 获得私钥 $\{D_{k,i}=B^{\frac{\varphi(i)}{\beta_{k,i}}}\}_{i\in A_u{}^k\cap A_C{}^k}$, $\{D_{k,i}=g^{\frac{\varphi(i)}{\beta_{k,i}}}\}_{i\in A_u{}^k\cap A_C{}^k}$。

对可信属性授权中心 $k=k(u)$ 关于用户 u 的询问: 对于用户 u 对应的属性授权中心, 随机选取 $r_{k,u}$, 设 $f(0)=F_{s_k}(u)=ab+z_{k,u}b$。选取 $d-1$ 个随机的点 v_i, 对于其中的 $i\in A_C{}^k$, 设 $f(i)=v_ib$。对于这些属性, $t_{k,i}=\beta_{k,i}$, 即 $D_{k,i}=g^{\frac{f(i)}{t_{k,i}}}=g^{\frac{v_ib}{\beta_{k,i}}}=B^{\frac{v_i}{\beta_{k,i}}}$。根据这些点, 通过插值, 对于任何其他属性 i, 定义 $\Delta_0(i)(ab+z_{k,u}b)+\sum\Delta_j(i)v_jb$。对于这些属性, $t_{k,i}=b\beta_{k,i}$, 因此有

$$D_{k,i}=g^{\frac{f(i)}{t_{k,i}}}=g^{\frac{\Delta_0(i)(ab+z_{k,u}b)+\sum\Delta_j(i)v_jb}{b\beta_{k,i}}}$$
$$=g^{\Delta_0(i)a}\cdot g^{\frac{\Delta_0(i)z_{k,u}+\sum\Delta_j(i)v_j}{\beta_{k,i}}}$$
$$=A^{\Delta_0(i)}\cdot g^{\frac{\Delta_0(i)z_{k,u}+\sum\Delta_j(i)v_j}{\beta_{k,i}}}$$

所以, 获得私钥 $\{D_{k,i}=B^{\frac{v_i}{\beta_{k,i}}}\}_{i\in A_u{}^k\cap A_C{}^k}$,

$$\{D_{k,i}=A^{\Delta0(i)}\cdot g^{\frac{\Delta0(i)z_{k,u}+\sum\Delta_j(i)v_j}{\beta_{k,i}}}\}_{i\in A_u{}^k-A_C{}^k}。$$

对中心授权机构关于用户 u 的询问:

$$D_{ca}=g^{(\sum_{k\notin Corr}z_{k,u}-\sum_{k\in Corr}F_{s_k}(u))};$$

同理, 挑战者 C 随机选择 $z'_{k,u}$, 计算得到:

$$D'_{ca}=g^{(\sum_{k\notin Corr}z'_{k,u}-\sum_{k\in Corr}F_{s_k}(u))}。$$

挑战者 C 将以上生成的签名私钥和解密私钥一并发送给攻击者 $\mathcal{A}$。

挑战阶段: 攻击者 $\mathcal{A}$ 结束询问, 选择两个等长的明文消息 m_0,m_1 发送给挑战者 C, 挑战者选择任意 $\mu\in\{0,1\}$, 对 m_μ 签密, 随机选择 ,计算如下: $C_1=D_{k,i}{}^{r'}$, $C_2=D'_{ca}\cdot(g_1)^{H(m)r'}$, $C_3=T_{k,i}{}^{r'}$, $C_4=g^r=g^c$, $C_5=g^{r'}$, $E=Z\cdot m$, $\{E_{k,i}=g^{r\beta_{k,i}}=C^{\beta_{k,i}}\}_{i\in A_C}$。最后, 输出签密密文。

猜测: 攻击者 $\mathcal{A}$ 输出对 μ 的猜测 μ', 如果 $\mu=\mu'$, 则挑战者判定 $Z=e(g,g)^{abc}$; 若 $\mu\neq\mu'$, 则判定 $Z=e(g,g)^R$。

在 $Z=e(g,g)^R$ 的情况下, 攻击者 $\mathcal{A}$ 不能获取任何有关于 μ 的消息。因此, 当 $Z=e(g,g)^R$ 时, 判断 $\mu=\mu'$ 的概率为 $\frac{1}{2}$, 即 $P[\mu'=\mu|Z=e(g,g)^R]=\frac{1}{2}$。当 $\mu\neq\mu'$ 时, 挑战者 C 随机猜测 $Z'=e(g,g)^R$ 的概率为 $\frac{1}{2}$, $P[Z'\neq Z|Z=e(g,g)^R]=\frac{1}{2}$。

当 $Z=e(g,g)^{abc}$ 时, 设攻击者 $\mathcal{A}$ 的优势为 ε, 可以得到 $P[\mu'=\mu|Z=e(g,g)^{abc}]=\frac{1}{2}+\varepsilon$, 当 $\mu'=\mu$ 时, 挑战者 C 随机猜测 $Z'=e(g,g)^{abc}$ 的概率为 $P[Z'=Z|Z\ e(g,g)^{abc}]=\frac{1}{2}+\varepsilon$。

挑战者 C 在整个游戏中的优势计算如下:

$$Adv=|P[Z'=Z]-\frac{1}{2}|$$
$$=|\frac{1}{2}P[Z'=Z|Z=e(g,g)^{abc}]+\frac{1}{2}P[Z'=Z|Z=e(g,g)^R-\frac{1}{2}]|$$
$$=|\frac{1}{2}(\frac{1}{2}+\varepsilon)+\frac{1}{2}\cdot\frac{1}{2}-\frac{1}{2}|$$
$$=\frac{1}{2}\varepsilon$$

推导得出, 挑战者 C 能够以 $\frac{1}{2}\varepsilon$ 的优势赢得游戏的胜利, 说明本方案是选择明文安全的。

5.2 不可伪造性

定理 2 如果 BDH 问题在群 G 中是困难的, 则本方案在选择属性集 ω' 下的自适应选择消息攻击下满足不可伪造性。

证明: 设 (g,g^a,g^b), 挑战者 C 目标为计算 g^{ab}。如果攻击者 $\mathcal{A}$ 要伪造签密密文, 必须拥有签密者密钥。签密者密钥为:

$$\{D_{k,i},D_{ca},D'_{ca}\}=\{g^{\frac{f(i)}{t_{k,i}}},g^{y_0-\sum_{k=1}^{K}y_{k,u}},g^{y'_0-\sum_{k=1}^{K}y_{k,u}}\}$$

由于 y_0, y_0' 为系统主密钥, $t_{k,i}$ 为随机选取的值, $f(i)$ 为 $d-1$ 阶多项式, 只有通过 d 次插值才能获得, 因此攻击不能获得密钥。如果攻击者 A 能伪造密钥, 说明攻击者 A 攻破了该方案, 解决了 CDH 问题。即使攻击者改变签密密文, 解签密者也能用 Unsigncrypt 过程验证密文是否合法。综上, 该方案具有选择消息攻击下的不可伪造性。

6 性能分析

签密方法相比传统的签名和加密算法, 一定程度上减小了运算量和通信开销。而本文所提出的多授权中心属性基签密方案, 与其他属性基签密[18,19,26, 32,35]相比, 不仅完成了在多授权中心体系下新的签密方案的实现, 在某些方面的效率也有了一定程度的提升。

设 $|G|$ 表示群 G 的大小, $|G_T|$ 表示群 G_T 的大小, n 为属性数量, k 为属性授权中心的个数, p 表示一次双线性对运算, e 表示一次指数运算, m 表示一次乘法运算。

6.1 密钥和密文长度分析

如表 1 所示, 在本文所提出的多授权中心属性基签密方案中, 用户密钥长度为 $(n+1)|G|$, 密文长度为。与所列举其他方案相比, 本方案拥有最小的用户密钥长度和尚可接受的密文长度。

6.2 计算量分析

如表 2 所示, 本方案的签密计算量为 $(3n+3)e$, 解签密过程计算量为 $(n+4)p+(n+k+1)e$。与所列举的其他属性基签密方案相比, 本方案虽然在签密过程中的表现并不优异, 但在解签密过程中具有很高的效率, 且随着属性个数的增长, 本方案在解签密过程中的高效性将更加突出。

表 1 方案效率比较

Table 1 Efficiency comparison of relevant schemes

方案	用户密钥长度	密文长度
Chen[18]	$(n+3)\|G\|$	$(2n+5)\|G\|+\|G_T\|$
Yang[19]	$(n+2)\|G\|$	$(n+2)\|G\|+\|G_T\|$
Zhang[26]	$2n\|G\|$	$(2n+2)\|G\|+\|G_T\|$
Hong[32]	$3n\|G\|$	$(4n+1)\|G\|+\|G_T\|$
Rao[35]	$(3n+4)\|G\|$	$(4n+3)\|G\|+\|G_T\|$
本方案	$(n+2)\|G\|$	$(3n+2)\|G\|+\|G_T\|$

表 2 方案计算量比较

Table 2 Computation comparison of relevant schemes

方案	签密计算量	解签密计算量
Chen[18]	$p+(2n+6)e$	$(2n+3)p+(n+3)e$
Yang[19]	$(n+3)e$	$(n+4)p+ne$
Zhang[26]	$(2n+2)e$	$5np+ne$
Hong[32]	$(4n+2)e$	$(4n+1)p+(n+3)e$
Rao[35]	n^2m	$2np+3ne$
本方案	$(3n+3)e$	$(n+4)p+(n+k+1)e$

6.3 签名属性分析

如表 3 所示, 本文所提出的多授权中心属性基签密方案在标准模型下满足机密性和不可伪造性, 同时具有抵抗合谋攻击的性质。Yang 等[16]的方案虽然密钥、密文长度均较短, 且计算量较小, 但却是以牺牲一定的安全性为代价的。与其他方案产生最鲜明对比的是, 本方案引入了多授权中心的结构模型, 具有独特的优势。

表 3 方案属性比较

Table 3 Property comparison of relevant schemes

方案	机密性	不可伪造性	前向安全性	公开验证性	模型	多授权中心	抗合谋
Chen[18]	Y	Y	N	N	随机预言机	N	Y
Yang[19]	Y	Y	N	Y	标准	N	N
Zhang[26]	Y	Y	N	N	标准	N	N
Hong[32]	Y	Y	Y	N	标准	N	N
Rao[35]	Y	Y	N	N	随机预言机	N	Y
本方案	Y	Y	N	N	标准	Y	Y

6.4 仿真实验

本小节对属性基签密方案进行实验仿真, 在一台 Intel Core i5-4660 3.20GHZ, 内存为 8GB RAM, Win7 64 位操作系统的微型计算机上进行操作; 通

过 Visual Studio 2010 和 PBC 0.5.14 代码库进行实验，实验对象为随机选取的一组字符串文件。

从签密和解签密两方面对多授权中心的属性基签密方案做出分析。图 1 为本方案与 Chen[18]方案、Yang[19]方案、Zhang[26]方案、Hong[32]方案和 Rao[35]方案在签密开销方面对比测试的结果。图 2 为本方案与上述方案在解签密开销方面的比较测试结果。从图 1 中可以得出，随着属性个数的增长，我们的方案的签密时间开销成线性增长，与其上述的其他签密方案对比，虽然在签密方面的性能上仅优于 Hong[32]的方案，但我们的方案实现了多授权中心的功能。图 2 反映了解签密的时间开销随属性个数的增长而成线性增长，我们的方案在解签密方面相比 Chen[18]、Zhang[26]、Hong[32]和 Rao[35]的方案都有着明显的优势。

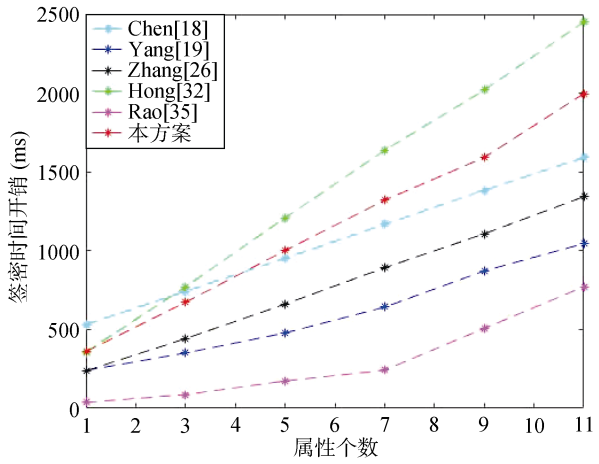

图 1　各方案签密操作开销对比

Figure 1　Signcryption cost comparison of relevant schemes

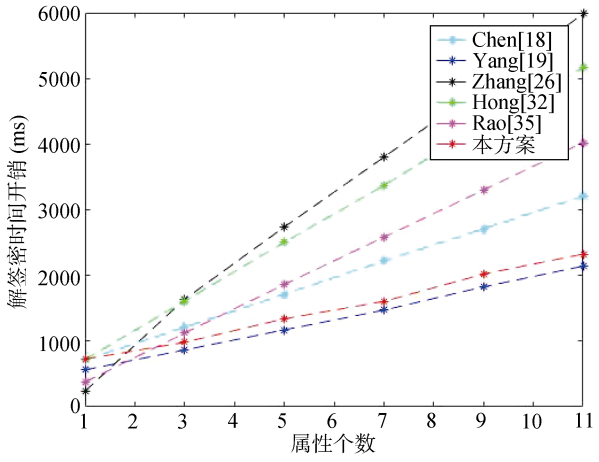

图 2　各方案解签密操作开销对比

Figure 2　Signcryption cost comparison of relevant schemes

7　结论

文章在文献[36]的基础上提出了一种多授权中心的属性基签密方案，并给出了相应的安全性分析。相比于传统的属性基签密方案，我们所提出的多授权中心属性基签密方案将用户的多个属性分别由不同的授权中心管理，提升了系统的安全性和效率。此外，该方案实现了在一个的逻辑步骤内同时保证了消息的保密性和签名身份的不可伪造性，提高了效率，且具有抗合谋攻击的性质。并证明了其在选择密文攻击下的保密性和在选择消息攻击下的不可伪造性，具有一定的应用价值。下一步的工作重点在于进一步提高算法的效率和完善安全性证明。

参考文献

[1] Sahai A, Waters B, “Fuzzy identity-based encryptions,” *Advances in Cryptology-EUROCRYPT 2005. LNCS 3494, Aarhus: Springer-Verlag Press*, pp. 457-473, 2005.

[2] Goyal V, Pandey O, Sahai A,et al. “Attribute-based encryption for fine-grained access control of the encrypted data,” *Proc of CCS. New York:ACM Press*, pp. 89-98, 2006.

[3] Bethencourt J, Sahai A, Waters B. “Ciphertext-policy attribute-based encryption,” *Security and Privacy, 2007. SP'07. IEEE Symposium on. IEEE*, pp. 321-334, 2017.

[4] Qin Y, Sun W, Xiong H, et al. “Outsourcing Encryption and Decryption CP-ABE Scheme with Revocation Storage in Cloud *Computing,” Netinfo Security*, vol. 6, pp. 6-13, 2017.
(卿勇, 孙伟, 熊虎,等. “云计算中可撤销存储的外包加解密 CP-ABE 方案,” *信息网络安全*, 2017(6):6-13.)

[5] Li M, Yu S, Zheng Y, et al. “Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption,” *IEEE transactions on parallel and distributed systems*, vol. 24, no.1, pp. 131-143, 2013.

[6] Yan X, Liu Y, Hu M, et al. “LWE-based Multi-authority Attribute-based Encryption Scheme in Cloud Environment,” *Netinfo Security*, vol. 9, pp. 128-133, 2017.
(闫玺玺, 刘媛, 胡明星,等. “云环境下基于 LWE 的多机构属性基加密方案,” *信息网络安全*, 2017(9):128-133.)

[7] Yang P, Cao F, and Dong X. “Fuzzy Identity Based Signature.” *IACR Cryptology EPrint Archive* 2008 pp. 2, 2008.

[8] Maji H K, Prabhakaran M, Rosulek M. “Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion- Resistance,” *IACR Cryptology ePrint Archive*, pp. 328, 2008.

[9] Li J, Jiang P. “An Efficient and Provably Secure Identity-Based Signature Scheme in the Standard Model” *Chinese Journal of Computers*, vol. 32, no. 11, pp. 2130-2136, 2009.
(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," *计算机学报*, 2009, 32(11): 2130-2136.）

[10] Li J, Jiang P. "An Efficient and Provably Secure Identity-Based Signature Scheme in the Standard Model," *Chinese Journal of Computers*, vol. 32, no. 11, pp. 2130-2136, 2009.

[11] Li J, Au M H, Susilo W, et al. "Attribute-based signature and its applications," *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. ACM*, pp. 60-69, 2010.

[12] Shahandashti S F, Safavi-Naini R. "Threshold attribute-based signatures and their application to anonymous credential systems," *International Conference on Cryptology in Africa. Springer, Berlin, Heidelberg*, pp. 198-216, 2009.

[13] Liu J, Huang X, Liu J K. "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption," *Future Generation Computer Systems*, vol. 52, pp. 67-76, 2015.

[14] Liu J, Ma J, Wu W, et al. "Protecting Mobile Health Records in Cloud Computing: A Secure, Efficient, and Anonymous Design," *ACM Transactions on Embedded Computing Systems*, vol. 16, no. 2, pp. 57, 2017.

[15] Zheng Y. "Digital signcryption or how to achieve cost (signature & encryption) < cost (signature) + cost (encryption)," *Annual International Cryptology Conference. Springer, Berlin, Heidelberg*, pp. 165-179, 1997.

[16] Malone-Lee J. "Identity-Based Signcryption," *In Proceedings of Public Key Cryptography* - PKC 2005, LNCS 3386, pp. 362-379, 2002.

[17] Shi Y, Pan W, Zhong S. "Attribute-based Signcryption Scheme," *Information Security and Communication Privacy*, vol. 9, pp. 129-131, 2009.
(史妍, 潘伟, 钟绍春. "基于属性的签密方案," 信息安全与通信保密, 2009(9):129-131.)

[18] Chen S, Wang H. "Efficient Attribute-Based Signcryption Scheme," *Journal of Information Engineering University*, vol. 12, no. 5, pp. 526-531, 2011.
(陈少真, 王海斌. "高效的基于属性的签密方案," *信息工程大学学报*, 2011, 12(5):526-531.)

[19] Yang X, Lin Z, Han Y. "Efficient fuzzy attribute-based signcryption scheme," *Journal on Communications*, vol. s1, pp. 8-13, 2013.
(杨晓元, 林志强, 韩益亮. "高效的模糊属性基签密方案," *通信学报*, 2013(s1): 8-13.)

[20] Gagné M, Narayan S, Safavi-Naini R. "Threshold attribute-based signcryption," *International Conference on Security and Cryptography for Networks. Springer, Berlin, Heidelberg*, pp. 154-171, 2010.

[21] Emura K, Miyaji A, Rahman M S. "Toward dynamic attribute-based signcryption (poster)," *Australasian Conference on Information Security and Privacy. Springer, Berlin, Heidelberg*, pp. 439-443, 2011.

[22] Han Y, Lu W, Yang X. "Attribute-Based Signcryption Scheme with Non-monotonic Access Structure," *International Conference on Intelligent NETWORKING and Collaborative Systems. IEEE*, pp. 796-802, 2013.

[23] Hu C, Zhang N, Li H, et al. "Body Area Network Security: A Fuzzy Attribute-Based Signcryption Scheme," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 9, pp. 37-46, 2013.

[24] Guo Z, Li M, Fan X. "Attribute‐based ring signcryption scheme," *Security & Communication Networks*, vol. 6, no. 6, pp. 790-796, 2013.

[25] Rao Y S, Dutta R. "Expressive attribute based signcryption with constant-size ciphertext," *International Conference on Cryptology in Africa. Springer, Cham*, pp. 398-419, 2014.

[26] Zhang M, Yang B, Takagi T, et al. "Fuzzy biometric signcryption scheme with bilinear pairings in the standard model," *Pacific-Asia Workshop on Intelligence and Security Informatics. Springer, Berlin, Heidelberg*, pp. 77-87, 2010.

[27] Yu G, Cao Z. "Attribute-based signcryption with hybrid access policy," *Peer-to-Peer Networking and Applications*, vol. 10, no. 1, pp. 253-261, 2017.

[28] Wei J, Hu X, Liu W. "Traceable attribute‐based signcryption," *Security & Communication Networks*, vol. 7, no. 12, pp. 2302-2317, 2015.

[29] Hu C, Cheng X, Tian Z, et al. "An attribute-based signcryption scheme to secure attribute-defined multicast communications," *International Conference on Security and Privacy in Communication Systems. Springer, Cham*, pp. 418-437, 2015.

[30] Zheng H, Qin J, Hu J, et al. "Threshold Attribute-Based Signcryption in Standard Model," *2015 IEEE 2nd International Conference on Cyber Security and Cloud Computing (CSCloud). IEEE*, pp. 187-193, 2015.

[31] Pei X, Wang Y, Yao W, et al. "Security Enhanced Attribute Based Signcryption for Private Data Sharing in Cloud," *Trustcom/BigDataSE/I SPA, 2016 IEEE.* pp. 737-743, 2016.

[32] Hong H, Xia Y, Sun Z. "Provably secure attribute based signcryption with delegated computation and efficient key updating," *KSII Transactions on Internet and Information Systems*, vol. 11, no. 5, pp. 2646-2659, 2017.

[33] Zhao Y, Yue F, Xiong H, et al. "A Strong Designated Verifier Ring Signature and Signcryption Scheme," *Netinfo Security*, vol. 10, pp. 8-13, 2015.
(赵洋, 岳峰, 熊虎,等. "一种强指定验证者环签名和签密体制," *信息网络安全*, 2015(10):8-13.)

[34] Rao Y S, Dutta R. "Efficient attribute-based signature and signcryption realizing expressive access structures," *International*

Journal of Information Security, vol. 15, no. 1, pp. 1-29, 2015.

[35] Rao Y S. "A secure and efficient Ciphertext-Policy Attribute-Based Signcryption for Personal Health Records sharing in cloud computing," *Future Generation Computer Systems*, vol. 67, pp. 133-151, 2017.

[36] Chase, M. "Multi-authority attribute based encryption," *In: Vadhan, S.P. (ed.) TCC 2007.Springer, Heidelberg 2007*, LNCS 4392, pp. 515-534, 2007.

[37] Sun C, Ma W, Chen H. "Multi-authority Attribute-based Signature," *Advanced Engineering Science*, vol. 43, no. 1, pp. 83-86, 2011.
(孙昌霞, 马文平, 陈和风. "多授权中心的基于属性的签名," *工程科学与技术*, 2011, 43(1):83-86.)

[38] Cao D, Zhao B, Wang X. "Multi-authority Attribute-Based Signature," *Journal of Sichuan University*, vol. 43, no. 1, pp. 83-86, 2011.

[39] Shamir A. "How to share a secret," *Communications of the ACM*, vol. 22, no. 11, pp. 612-613, 1979.

聂旭云, 博士, 电子科技大学信息与软件工程学院副教授。研究领域为网络安全, 密码学。Email: xynie@uestc.edu.cn

孙剑飞, 现在电子科技大学软件工程专业攻读博士学位。研究领域为网络安全, 密码学。

秦志光, 博士, 教授, 网络与数据安全四川省重点实验室主任。研究领域为网络安全、移动互联网应用。Email: qinzg@uestc.edu.cn

鲍阳阳, 现在电子科技大学软件工程专业攻读硕士学位。研究领域为网络安全, 密码学。

熊虎, 博士, 电子科技大学信息与软件工程学院教授。研究领域为网络安全技术与应用、公钥密码学。Email: xionghu.uestc@gmail.com