软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(11):3528−3543 [doi: 10.13328/j.cnki.jos.005293]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

分布式无中心授权的属性基可变门限环签名*

刘旭东[1,2], 张文芳[1,2], 王小敏[1]

[1](西南交通大学 信息科学与技术学院,四川 成都 610031)

[2](信息安全与国家计算网格四川省重点实验室(西南交通大学),四川 成都 610031)

通讯作者: 张文芳, E-mail: wfzhang@swjtu.edu.cn

摘 要: 基于属性的环签名具有表达能力强、使用灵活、便于隐匿签名者身份等优点,因此逐渐成为相关领域的研究热点.分析结果表明,现有方案大多无法同时具备无条件强匿名性和抗合谋攻击性,并且存在属性密钥托管、签名门限固定、验证效率低下等问题.针对上述不足,首先给出分布式属性基门限环签名方案的形式化定义和安全模型,然后提出一个分布式无中心授权的属性基可变门限环签名方案.该方案采用分布式密钥生成协议,分散了属性授权机构权限,解决了属性密钥托管问题;通过在属性密钥中嵌入用户身份标识,在签名中引入用户身份模糊因子的方式,使该方案同时具备无条件强匿名性和抗合谋攻击性.另外,提出了一种适用于该方案的批验证算法,能够将验证计算量由 $nO(\cdot)$降为 $O(\cdot)+n$(其中,n 为待验证签名的数量),有效提高了验证效率.在随机预言机模型和 CDH 困难问题假设下,该方案被证明在适应性选择消息和断言攻击下是存在性不可伪造的,并且能够抵抗由拥有互补属性集合的恶意成员发动合谋攻击.

关键词: 基于属性的环签名;无条件强匿名性;抗合谋攻击;无中心授权;批验证

中图法分类号: TP309

中文引用格式: 刘旭东,张文芳,王小敏.分布式无中心授权的属性基可变门限环签名.软件学报,2018,29(11):3528−3543. http://www.jos.org.cn/1000-9825/5293.htm

英文引用格式: Liu XD, Zhang WF, Wang XM. Multi-Authority attribute-based alterable threshold ring signature without central authority. Ruan Jian Xue Bao/Journal of Software, 2018,29(11):3528−3543 (in Chinese). http://www.jos.org.cn/1000-9825/5293.htm

Multi-Authority Attribute-Based Alterable Threshold Ring Signature without Central Authority

LIU Xu-Dong[1,2], ZHANG Wen-Fang[1,2], WANG Xiao-Min[1]

[1](School of Information Science and Technology, Southwest Jiaotong University, Chengdu 610031, China)

[2](Key Laboratory of Information Science and National Computing Grid (Southwest Jiaotong University), Chengdu 610031, China)

Abstract: Attribute based ring signature has gradually become a hot topic in the related field, owing to its priorities including strong in expressive power, flexible in use, and easy to hide the identity of signer. By analyzing existing attribute-based ring signature schemes, it can be found that the majority of earlier schemes cannot resist the collusion attack with the premise of unconditional strong anonymity, and there are many issues such as attribute key escrow, fixed threshold and inefficient verification. To address the above defects, this paper firstly introduces the formal definitions and security model for the multi-authority attribute-based threshold ring signature scheme.

* 基金项目: 四川省科技计划(2017GZDZX0002, 2018GZ0195, 2017SZYZF0002); 国家自然科学基金(61872302, 61371098); 国家铁路智能运输系统工程技术中心开放课题(RITS2018KF02)

Foundation item: Sichuan Science and Technology Program (2017GZDZX0002, 2018GZ0195, 2017SZYZF0002); National Natural Science Foundation of China (61872302, 61371098); Project Fund for the Center of National Railway Intelligent Transportation System Engineering and Technology (RITS2018KF02)

收稿时间: 2017-01-10; 修改时间: 2017-03-13; 采用时间: 2017-04-17; jos 在线出版时间: 2018-04-16

CNKI 网络优先出版: 2018-04-16 10:37:43, http://kns.cnki.net/kcms/detail/11.2560.TP.20180416.1037.002.html

Then a multi-authority attribute-based variable threshold ring signature scheme is presented. This scheme uses distributed key generation protocol to constrain the rights of attribute authority, and to overcome the problem of attribute key escrow. Through embedding a random identity factor in each user's attribute key, and introducing a random fuzzy parameter in each signature, the scheme can provides both unconditional strong anonymity and collusion resistance. In addition, a batch verification algorithm is proposed to reduce the computation complexity of verification from $nO(\cdot)$ to $O(\cdot)+n$. Under random oracle model and computational Diffie–Hellman assumption, the proposal can be proven to be existentially unforgeable and can resist collusion attacks launched by the malicious users with the complementary attributes in chosen message and predicate attack.

Key words: attribute-based ring signature; unconditional strong anonymity; anti-collusion attack; without central authority; batch verification

为了对人群进行细粒度划分,Sahai 等人[1]将身份的概念泛化,于 2005 年提出了属性的概念.在其方案中,用户身份被描述为一系列属性的集合,每个属性对应唯一的密钥,只要用户属性满足解密策略,他就可以通过解密获得相应的信息,从而实现多对多的加解密过程.目前,基于属性的加密方案(attribute-based encryption,简称 ABE)可以分为两类:一类是密钥策略的属性基加密方案(key-policy attribute-based encryption,简称 KP-ABE)[2−4],即将解密策略与用户密钥绑定;另一类是密文策略的属性基加密方案(ciphertext-policy attribute-based encryption,简称 CP-ABE)[5−7],即将解密策略与密文绑定.

属性的概念同样可以应用于数字签名,形成基于属性的签名体制(attribute-based signature,简称 ABS).在该体制中,属性授权机构(attribute of authority,简称 AA)负责用户属性密钥的分发和管理,只有满足签名策略的用户才能对相应的消息进行签名,任何人均可利用公开参数验证签名的合法性.由于基于属性的签名体制具有表达能力强、使用灵活、便于隐匿签名者身份等优点,因此逐渐成为相关领域的研究热点.2005 年,Burnett 等人[8]提出了基于模糊身份的签名方案,该方案被认为是首个广义 ABS 方案.随后,Guo 等人[9]和 Maji 等人[10]于 2008 年分别提出了真正意义的 ABS 方案.文献[9]的方案采用自底向上(bottom-up)构造访问控制树的方式,允许签名者使用自身拥有的属性进行签名.然而该方案并未对签名者的隐私进行保护,且缺乏完整的形式化定义和安全性证明.文献[10]中的方案虽然具备签名者隐私保护功能且支持任意访问结构,但其安全性只能在一般群模型(generic group model)下得到证明.随后,为了更好地保护签名者的隐私,环签名[11]的思想被引入到属性基签名体制中,形成了基于属性的环签名方案(attribute-based ring signature,简称 ABRS).由于环签名具备无条件匿名性、自发性和群特性等优点,因此 ABRS 方案在签名过程中没有组织过程,无需群管理员参与,可以很好地保护签名者的隐私.首个基于属性的环签名方案由 Li 等人[12]于 2008 年提出,但该方案只能实现(n,n)门限签名(其中,n 为签名策略声明属性集合中元素的个数),并且在签名过程中,针对每个属性需要计算 3 个子签名,验证过程需要进行 $3n$ 次双线性对运算,因此效率很低,实用性较差.随后,一系列改进 ABRS 方案[13−21]相继被提出.

由于基于属性的环签名方案通常被应用于对匿名性要求较高的环境,因此,匿名性的强弱是评判一个 ABRS 方案优劣的重要依据.匿名性通常可以分为两类:计算匿名性(computational anonymity)和无条件匿名性(unconditional anonymity).针对 ABRS 方案,Shahandashti 等人[14]为了更好地区分方案匿名性强弱,又将无条件匿名性细分为无条件弱匿名性(unconditional weak anonymity)和无条件强匿名性(unconditional strong anonymity),匿名性分类及定义如下.

(1) 计算匿名性:将方案的匿名性规约为求解某一数学难题(如离散对数问题、大整数分解问题、Diffi-Hellman 问题等)的困难性.如果存在某一敌手能够在多项式时间内有效求解这一困难问题,则该方案的匿名性将会被攻破.

(2) 无条件弱匿名性:指即便存在某一敌手(包括属性授权机构)计算能力不受限,也无法在多项式时间内从拥有"签名属性集合"的群体成员中揭露签名者的真实身份.

(3) 无条件强匿名性:除满足无条件弱匿名性之外,任何敌手(包括属性授权机构)甚至无法在多项式时间内从"声明属性集合"中揭露"签名属性集合"的信息.

目前,仅有部分 ABRS 方案[14,17,19,21]可以实现无条件强匿名性,大多数方案由于在签名验证阶段需要使用实际签名属性集合,因此只能实现无条件弱匿名性,而文献[20]中的方案仅能实现计算匿名性.

除匿名性之外,抗合谋攻击性对于衡量 ABRS 方案的优劣同样重要.合谋攻击是指拥有互补属性集合的恶意用户相互勾结,通过组合密钥的方式,伪造他们各自无法单独产生的签名.目前,仅有少数 ABRS 方案[20,21]可以抵抗这种攻击.文献[20]中的方案通过将用户身份信息直接嵌入属性密钥的方式,虽然能够确保签名不能由多个用户合谋产生,但是由于引入了身份信息,导致方案匿名性退化,只能实现计算匿名性.

此外,现有的 ABRS 方案大多只包含一个属性授权机构(AA),该 AA 负责系统中所有属性密钥的分发和管理,一旦 AA 被敌手控制,整个系统就会被攻破.利用分布式的方式,将属性密钥分发和管理权限交由不同的 AA 分别管理,可以克服上述安全瓶颈.2007 年,Chase[22]首先将这一思想应用于属性基加密体制.随后,Maji 等人[10]于 2008 年提出了分布式属性基签名的概念,但其并未给出具体的实现方案.首个多属性授权机构的 ABRS 方案由 Li 等人[17]于 2010 年提出,该方案包含一个系统中心(central authority)、多个 AA 和终端用户这 3 种类型的实体.其中,系统中心负责生成并分发各 AA 的私钥,而各 AA 则负责用户不同属性密钥的分发和管理.该方案虽然通过分布式的方式分散了 AA 的权限,但仍然要求系统中心绝对可信,因此并未完全克服属性密钥托管这一缺陷.随后,Li 等人[21]借鉴 Chase 等人[23]提出的密钥匿名分发协议对文献[17]中的方案进行完善,提出一个改进的 ABRS 方案,但是密钥匿名分发协议的引入,导致该方案在密钥分发阶段,AA 除了需要为用户生成属性密钥之外,还需额外产生 t^2 个密钥来克服属性密钥托管问题,其中,t 为属性授权机构集合中 AA 的数量.这无疑在降低 AA 工作效率的同时增加了 AA 与用户之间的通信代价.此外,该方案签名门限固定,且只能在单属性授权机构条件下,被证明具备匿名性和不可伪造性,并未给出抗合谋攻击的形式化安全证明.综上可以看出:如何设计形式化可证明安全且同时具备无条件强匿名性和抗合谋攻击性的无可信中心分布式 ABRS 方案,是一个亟待解决的问题.

本文针对现有 ABRS 方案无法同时具备无条件强匿名性和抗合谋性,并且存在密钥托管、签名门限固定、验证效率低下等问题,提出一个分布式无中心授权的属性基可变门限环签名方案,并给出该方案在随机预言机模型及多属性授权机构条件下的形式化定义和安全模型.本方案利用 DKG(distributed key generation)协议[24,25]将可信的系统中心移除,把属性密钥的分发和管理权限交由不同的 AA,在解决效率瓶颈的同时,克服了属性密钥托管这一缺陷.在密钥生成过程中,将属性密钥与用户身份标识绑定,保证签名只能由满足签名策略的用户独立产生,在签名过程中,引入用户身份模糊因子保护签名者的隐私,确保方案在抵抗合谋攻击的前提下还具备无条件强匿名性.另外,通过借鉴 Ferrara 等人[26]的思想,提出了一种适用于本方案的批验证算法.该算法能够将验证计算复杂度由 $nO(\cdot)$降为 $O(\cdot)+n$,其中,n 为待验证签名(可以由多个用户在不同的签名策略下产生)的数量,$O(\cdot)$为验证单个签名的计算复杂度,有效提高了验证效率.在随机预言机模型(random oracle model,简称 ROM)和 CDH(computational Diffie–Hellman)困难问题假设下,本文方案能够被证明在适应性选择消息和断言攻击下是存在性不可伪造的,并能抵抗由拥有互补属性集合的恶意用户发动合谋攻击.

本文第 1 节回顾相关的预备知识.第 2 节给出分布式属性基门限环签名方案的形式化定义和安全模型.第 3 节提出一个分布式无中心授权的属性基可变门限环签名方案.第 4 节从匿名性、不可伪造性和抗合谋攻击这 3 个方面对所提出的方案进行安全性证明.第 5 节通过效率比较和性能分析对所提出的方案进行综合评价.最后对全文进行总结.

1 预备知识

1.1 双线性对

定义 1. 假设 G_1,G_2 是阶为素数 p 的循环群,g 是群 G_1 的生成元,映射 $e:G_1\times G_1\to G_2$ 是一个双线性对,如果 e 满足以下性质.

1) 双线性性:对于任意群元素 $g_1,g_2\in G_1$ 和随机数 $a,b\in Z_p$,满足 $e(g_1^a,g_2^b)=e(g_1,g_2)^{ab}$;
2) 非退化性:存在群元素 $g_1,g_2\in G_1$,满足 $e(g_1,g_2)\neq 1$,其中,1 是 G_2 的单位元;
3) 可计算性:存在有效算法可以在多项式时间内计算 $e(g_1,g_2)$的值.

1.2 CDH困难问题假设

定义 2. 假设 G_1,G_2 是阶为素数 p 的循环群,g 是群 G_1 的生成元,对于任意 $a,b\in Z_p$,给定元组$\langle g,g^x,g^y\rangle$,若不存在有效算法能够在多项式时间内以不可忽略的优势计算 g^{xy},则假设成立.

1.3 批验证假设

定义 3. 给定算法 $Psetup(1^\tau)\rightarrow(q,g_1,g_2,G_1,G_2,G_T,e)$,对于任意 $j\in[1,n]$,其中,q 为大素数,τ为安全参数,$n\in poly(\tau)$,任意选取群中固定元素 A 和 Z_q 上的随机向量$\mu=(\mu_1,\ldots,\mu_n)$,若等式 $\prod_{j=1}^{n}A^{\mu_j}=\prod_{j=1}^{n}Y^{(j)\mu_j}$ 成立,则等式 $A=Y^{(j)}$成立.

1.4 拉格朗日插值定理

定义 4. 假设 $f(x)$为 x 的 d–1 次多项式函数,任意给定多项式上 d 个不同的点$(x_i,f(x_i))$,则通过下式可以唯一确定任意 x 所对应的多项式 $f(x)$的值:

$$f(x)=\sum_{i=1}^{d}f(x_i)\left(\prod_{j=1,j\neq i}^{d}\frac{x-x_j}{x_i-x_j}\right).$$

通过上式定义拉格朗日系数 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-x_j}{x_i-x_j}$,其中,$S$ 为这 d 个元素的集合.

2 形式化定义与安全模型

2.1 形式化定义

本文使用门限断言 $\Upsilon_{t,\omega^*}(\cdot)$ 表示签名策略,其中,ω^*为断言声明属性集合;t 为动态签名门限,满足 $1\leqslant t\leqslant d$,d 为 AA 预设门限值.假设签名者拥有属性集合ω,若$|\omega\cap\omega^*|\geqslant t$,则 $\Upsilon_{t,\omega^*}(\omega)=1$,表示签名者可以产生合法签名;否则 $\Upsilon_{t,\omega^*}(\omega)=0$,表示签名者无法产生合法签名.

本方案由属性授权机构和用户两种类型的实体构成,包含初始化、密钥分发、签名、验证这 4 个阶段,各阶段具体过程如下:

1) 初始化算法 $Setup(1^\lambda)$:由各属性授权机构 AA_k 运行的概率性随机算法,输入安全参数λ,输出系统公开参数 *params* 和系统秘密参数 *privates*.
2) 密钥生成算法 $KeyGen(\omega_{ID})$:由各属性授权机构运行的概率性随机算法,输入 *params*、*privates*、用户的身份 *ID* 及其属性集合ω_{ID},输出用户相应的属性密钥 *SK*.
3) 签名算法 $Sign(\Upsilon,params,m,SK)$:由签名者运行的概率性随机算法,输入 *params*、消息 *m* 及用户相应的属性密钥 *SK*,输出签名σ.
4) 验证算法 $Verify(\Upsilon,params,m,\sigma)$:由验证者运行的确定性算法,输入 *params*、消息 *m* 及签名σ,若可以判定 $\Upsilon_{t,\omega^*}(\omega_{ID})=1$, 则签名$\sigma$有效,输出 true;否则,输出 false.

2.2 安全模型

本节给出分布式属性基门限环签名方案的安全模型.分布式属性基门限环签名方案除了应该满足不可伪造性和匿名性之外,还应该能够抵抗拥有互补属性集合的恶意成员通过组合密钥的方式发动合谋攻击.其中,无条件强匿名性是指给定某断言下的合法签名,任何攻击者(包括各属性授权机构 AA_k)即便其计算能力不受限,且可以获得系统所有用户的任意属性密钥,也无法在多项式时间内从满足该断言的用户集合中揭露签名者的实际身份.不可伪造性是指任何不满足门限断言的用户均无法在多项式时间内单独伪造该断言下的合法签名.抗合谋攻击是指任何拥有互补属性集合的恶意用户无法通过组合密钥的方式在多项式时间内伪造他们各自无法独立产生的合法签名.

2.2.1 无条件匿名性

定义 5. 基于属性的环签名方案具备无条件匿名性,如果不存在攻击者 A(即便其计算能力不受限)能够在多项式时间内以一个不可忽略的优势在以下游戏中获胜.

1) 初始化:A 声明挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$.挑战者 C 运行初始化算法,将生成的系统公开参数 *params* 和系统秘密参数 *privates* 全部发送给 A,因此,A 可以生成系统中所有用户的任意属性密钥.
2) 挑战:A 随机选取消息 m 和用户 ID_1(属性集合为 ω_1),ID_2(属性集合为 ω_2),满足 $\Upsilon_{t_k,\omega_k^*}(\omega_1)=\Upsilon_{t_k,\omega_k^*}(\omega_2)=1$,并将 m,(ID_1,ω_1),(ID_2,ω_2)发送给 C.C 首先运行密钥生成算法生成(ID_1,ω_1),(ID_2,ω_2)对应的密钥集合 SK_1,SK_2,然后抛掷一枚公平硬币 $b\in\{1,2\}$,调用签名算法,使用 SK_b 为 m 生成签名 σ_b,最后,将 σ_b 发送给 A.
3) 猜测:A 输出对 b 的猜测 b',若 $b=b'$,则 A 赢得游戏.

2.2.2 不可伪造性

定义 6. 基于属性的环签名方案在适应性选择消息和断言攻击下,是存在性不可伪造的,如果不存在攻击者 A 能够在多项式时间内以一个不可忽略的优势在以下游戏中获胜.

1) 初始化:假设攻击者 A 已经攻破的 l–1 个属性授权机构组成集合 Ψ,其余未被攻破的属性授权机构组成集合 T,A 声明挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\Psi\cup\bar{I}}$,其中,$AA_{\bar{I}}\in T$.挑战者 C 运行初始化算法生成系统公开参数 *params* 和系统秘密参数 *privates*,并将 *params* 和集合 Ψ中成员的秘密参数发送给 A.
2) 询问阶段:A 可以适应性地进行多项式次散列询问、密钥解析询问、签名询问.C 将相应的仿真结果发送给 A.
3) 伪造阶段:游戏最后,A 输出消息 m^*的签名 σ^*.如果满足以下条件,则 A 赢得游戏.
   - $Verify(\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\Psi\cup\bar{I}},params,m^*,\sigma^*)=\text{true}$.
   - 任何属性集合 ω,满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega)=1$,未进行密钥解析询问.
   - (ω,m^*)未进行签名询问.

2.2.3 抗合谋攻击性

定义 7. 基于属性的环签名方案在适应性选择消息和断言攻击下是抗合谋攻击的,如果不存在攻击者 A 能够在多项式时间内以一个不可忽略的优势在以下游戏中获胜.

1) 初始化:同定义 6 的初始化过程.
2) 询问阶段:同定义 6 的询问过程.
3) 挑战阶段:A 随机选择用户 ID_1(属性集合为 ω_1),ID_2(属性集合为 ω_2),满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega_{1,\bar{I}})\neq 1,\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega_{2,\bar{I}})\neq 1$,且存在属性子集 $\omega'_{1,\bar{I}}\subseteq\omega_{1,\bar{I}},\omega'_{2,\bar{I}}\subseteq\omega_{2,\bar{I}}$,构成属性集合 $\omega'_{\bar{I}}=\omega'_{1,\bar{I}}\cup\omega'_{2,\bar{I}}$,满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega'_{\bar{I}})=1$.分别对$(ID_1,\omega'_{1,\bar{I}})$,$(ID_2,\omega'_{2,\bar{I}})$进行密钥解析询问,获得相应的属性密钥集合 $SK'_{1,\bar{I}},SK'_{2,\bar{I}}$,组成新的属性密钥集合.
$$SK'_{\bar{I}}=SK'_{1,\bar{I}}\cup SK'_{2,\bar{I}}.$$
4) 伪造阶段:游戏最后,A 输出消息 m^*的签名 σ^*.如果满足以下条件,则 A 赢得游戏.
   - $Verify(\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\Psi\cup\bar{I}},params,m^*,\sigma^*)=\text{true}$.
   - 任何属性集合 ω,满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega)=1$,未进行密钥解析询问.
   - (ω,m^*)未进行签名询问.

3 分布式无中心授权的基于属性可变门限环签名方案

本方案包括初始化、密钥分发、签名、验证这 4 个阶段,各阶段具体执行过程如下.

3.1 初始化*Setup*(*d*)

随机选取两个阶为大素数 q 的循环群 G_1,G_2,满足双线性映射 $e:G_1\times G_1\to G_2$,生成元 $g\in G_1$.属性集合为 $\omega=\{\omega_1,\omega_2,\ldots,\omega_l\}$, $\omega_k=\{j_{1,k},j_{2,k},\ldots,j_{|\omega_k|,k}\}$ 为 ω 的子集, $j_{m,k}\in {}_RZ_q^*$ 为 ω_k 中的属性元素,其中,$1\leqslant k\leqslant l$,$1\leqslant m\leqslant|\omega_k|$;缺省属性集合为 $\Omega=\{\Omega_1,\Omega_2,\ldots,\Omega_l\}$, $\Omega_k=\{\xi_{1,k},\xi_{2,k},\ldots,\xi_{|\Omega_k|,k}\}$ 为 Ω 的子集, $\xi_{n,k}\in {}_RZ_q^*$ 为 Ω_k 中的缺省属性元素,其中,$|\Omega|=d-1$,$|\Omega_k|=d_k-1$,$1\leqslant n\leqslant|\Omega_k|$.散列函数 $H_1:\{0,1\}^*\to Z_q^*$,$H_2,H_3:\{0,1\}^*\to G_1$.

本方案共包含 n 个属性授权机构 AA_k,$1\leqslant k\leqslant n$,所有 AA_k 预共享一个伪随机函数 PRF,并拥有对任一属性子集 ω_k 和缺省属性子集 Ω_k 的密钥分发和管理权限.初始化阶段,所有 AA_k 首先执行(n,l)门限的 DKG 协议,生成系统主密钥 a_0 和 b_0(执行过程中,每个 AA_k 随机选取 $l-1$ 次多项式 $f_k(x)$),计算 $g_1=g^{a_0}$,$g_2=g^{b_0}$,$Z=e(g_1,g_2)$,各 AA_k 分别拥有系统主密钥 a_0 的部分秘密信息 $a_{k,0}=\sum_{i=1}^{n}f_i(k)$.然后,随机选取秘密参数 $x_k\in Z_q^*$,公布 $P_k=g_1^{x_k}$ 作为自己的公钥.最后,随机选取 $t_{j,k}\in Z_q^*$,计算属性 $j\in\omega_k\cup\Omega_k$ 的公钥 $T_{j,k}=g^{t_{j,k}}$.

- 公开参数: $params=\langle e,g,g_1,g_2,Z,H_1,H_2,H_3,\{P_k\}_{k=1,\ldots,n},\{T_{j,k}\}_{j\in\omega_k\cup\Omega_k,k=1,\ldots,n},q\rangle$.
- 秘密参数: $privates=\langle\{t_{j,k}\}_{j\in\omega_k\cup\Omega_k,k=1,\ldots,n},\{a_{k,0},x_k\}_{k=1,\ldots,n}\rangle$.

3.2 密钥分发 *KeyGen*(ω_{ID_i})

每个 AA_k 随机选择一个 d_k-1 次多项式 $q_k(\cdot)$(严格保密),满足 $q_k(0)=a_{k,0}$.任意 l 个管理不同属性子集的 AA_k 即可组成集合 *Team*,负责系统中所有用户任意属性密钥的分发和管理,从而可以避免因不可抗力因素导致部分 AA_k 无法正常工作,使得整个系统崩溃的情况发生.当用户 ID_i(拥有属性集合 $\omega_{ID_i}=\{\omega_{ID_i,k}\}_{k\in Team}$)向 *Team* 中各成员发出密钥分发请求时,*Team* 中的各 AA_k 首先为其计算对应的身份标识 $\{\lambda_{i,k}=PRF_{x_k}(ID_i)\}_{k\in Team}$,然后计算属性 $j\in\{\omega_{ID_i,k}\cup\Omega_k\}_{k\in Team}$ 对应的密钥:

$$\{S_{1,j,k}=H_2(j)^{t_{j,k}}g_2^{H_1(\lambda_{i,k})q_k(j)}\}_{j\in\omega_{ID_i,k}\cup\Omega_k,k\in Team},\{S_{2,k}=g_1^{-x_k}g_2^{H_1(\lambda_{i,k})a_{k,0}+a_{k,0}}\}_{k\in Team}.$$

最后,用户 ID_i 得到属性密钥集合 $SK=\langle\{S_{1,j,k}\}_{j\in\omega_{ID_i,k}\cup\Omega_k,k\in Team}\{S_{2,k}\}_{k\in Team}\rangle$.

3.3 签名 *Sign*($\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$, *params*, *m*, *SK*)

用户 ID_i 根据声明断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$ 对消息 m 进行签名,首先选择签名属性集合 $\{\omega'_{ID_i,k}\}_{k\in Team}$,其中,$\omega'_{ID_i,k}\subseteq\omega_{ID_i,k}\cap\omega_k^*$ 且 $|\omega'_{ID_i,k}|=t_k$;然后,从各缺省属性集合 Ω_k 中随机选择 d_k-t_k 个缺省属性构成集合 $\{\Omega_{ID_i,k}\}_{k\in Team}$;其次,选取 Z_q^* 上的随机数 v,z(用户身份模糊因子)及随机数集合 $\{r_{j,k}\}_{j\in\omega_k^*\cup\Omega_{ID_i,k},k\in Team}$,计算 m 相应的签名:

$$\sigma_1=g_2^zH_3(m)^v\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}S_{1,j,k}^{\Delta_{j,\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(0)\cdot\Delta_{k,Team}(0)}\prod_{j\in\omega_k^*\cup\Omega_{ID_i,k}}H_2(j)^{r_{j,k}}\right),$$

$$\sigma_2=g_2^z\prod_{k\in Team}(P_kS_{2,k})^{\Delta_{k,Team}(0)},$$

$$\sigma_3=g^v.$$

- 对于任意属性 $j\in\{\omega'_{ID_i,k}\cup\Omega_{ID_i,k}\}_{k\in Team}$,计算 $\sigma_{4,j,k}=T_{j,k}^{\Delta_{j,\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(0)\cdot\Delta_{k,Team}(0)}g^{r_{j,k}}$.
- 对于任意属性 $j\in\{\omega_k^*\setminus\omega'_{ID_i,k}\}_{k\in Team}$,计算 $\sigma_{4,j,k}=g^{r_{k,j}}$.

最后,将消息 m、签名 $\sigma=\langle\sigma_1,\sigma_2,\sigma_3,\{\sigma_{4,j,k}\}_{j\in\omega_k^*\cup\Omega_{ID_i,k},k\in Team}\rangle$ 和集合 $\{\Omega_{ID_i,k}\}_{k\in Team}$ 公开.

3.4 验证 *Verify*($\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$, *params*, *m*, σ)

验证者通过以下步骤判定签名 $\sigma=\langle\sigma_1,\sigma_2,\sigma_3,\{\sigma_{4,j,k}\}_{j\in\omega_k^*\cup\Omega_{ID_i,k},k\in Team}\rangle$ 是否为消息 m 的合法签名.

1) 判断不等式 $\{d_k-|\Omega_{ID_i,k}|\geqslant t_k\}_{k\in Team}$ 是否成立(验证签名是否满足声明断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$).

2) 若不等式成立,判断等式 $\frac{e(g,\sigma_2)e(H_3(m),\sigma_3)\prod_{k\in Team}\prod_{j\in\omega_k^*\cup\Omega_{ID_i,k}}e(H_2(j),\sigma_{4,j,k})}{e(g,\sigma_1)}=Z$ 是否成立:若等式成立,则接受σ作为 m 的合法签名;否则拒绝.

3.5 正确性分析

方案正确性验证如下:

$$\frac{e(g,\sigma_2)e\left(H_3(m),\sigma_3\right)\prod_{k\in Team}\prod_{j\in\omega_k^*\cup\Omega_{ID_i,k}}e\left(H_2(j),\sigma_{4,j,k}\right)}{e(g,\sigma_1)}=$$

$$\frac{e\left(g,g_2^z\prod_{k\in Team}(P_kS_{2,k})^{\Delta_{k,Team}(0)}\right)e\left(H_3(m),g^v\right)\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}e\left(H_2(j),T_{j,k}^{\Delta_{j,\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(0)\cdot\Delta_{k,Team}(0)}\right)\prod_{j\in\omega_k^*\cup\Omega_{ID_i,k}}e\left(H_2(j),g^{r_{j,k}}\right)\right)}{e\left(g,g_2^zH_3(m)^v\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}S_{1,j,k}^{\Delta_{j,\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(0)\cdot\Delta_{k,Team}(0)}\prod_{j\in\omega_k^*\cup\Omega_{ID_i,k}}H_2(j)^{r_{j,k}}\right)\right)}=$$

$$\frac{e\left(g,\prod_{k\in Team}(g_2^{H_1(\lambda_{i,k})a_{k,0}+a_{k,0}})^{\Delta_{k,Team}(0)}\right)\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}e(H_2(j),g^{t_{j,k}\cdot\Delta_{j,\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(0)\cdot\Delta_{k,Team}(0)})\right)}{e\left(g,\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(H_2(j)^{t_{j,k}}g_2^{H_1(\lambda_{i,k})q_k(j)})^{\Delta_{j,\omega'_{ID_i,k}\cup\Omega_{ID_i,k}}(0)\cdot\Delta_{k,Team}(0)}\right)\right)}=$$

$$\frac{e(g,g_2^{a_0})e\left(g,\prod_{k\in Team}g_2^{H_1(\lambda_{i,k})a_{k,0}\cdot\Delta_{k,Team}(0)}\right)}{e\left(g,\prod_{k\in Team}g_2^{H_1(\lambda_{i,k})a_{k,0}\cdot\Delta_{k,Team}(0)}\right)}=e(g_1,g_2)=Z.$$

3.6 批验证

很多情况下,验证者需要同时验证大量签名.然而,基于属性的环签名体制需要进行计算代价较高的双线性对运算,因此极大地限制了该体制的应用.本文借鉴文献[26]的批验证思想,基于定义 3,提出了一种适用于本方案的批验证算法,该算法能够将验证计算量由由 $nO(\cdot)$降为 $O(\cdot)+n$,有效地提高了验证效率.

对于大量消息-签名对 $\{m_i,\sigma_i=\langle\sigma_{1,i},\sigma_{2,i},\sigma_{3,i},\{\sigma_{4,j,k,i}\}_{j\in\omega_{i,k}^*\cup\Omega_{i,k},k\in Team_i}\rangle\}_{1\leqslant i\leqslant n}$,其中,$n$ 为消息-签名对的数量,$\mu=(\mu_1,\ldots,\mu_n)$为 Z_q^* 上的随机向量.具体验证过程如下:

$$\frac{e(g,\sigma_{2,1}^{\mu_1}\ldots\sigma_{2,n}^{\mu_n})\prod_{1\leqslant i\leqslant n}e(H_3(m_i),\sigma_{3,i}^{\mu_i})\prod_{k\in\bigcup_{1\leqslant i\leqslant n}\{Team_i\}}\prod_{j\in\bigcup_{1\leqslant i\leqslant n}\{\omega_{i,k}^*\cup\Omega_{i,k}\}}e(H_2(j),\sigma_{4,j,k,1}^{\mu_1}\ldots\sigma_{4,j,k,\kappa}^{\mu_\kappa})}{e(g,\sigma_{1,1}^{\mu_1}\ldots\sigma_{1,n}^{\mu_n})}=Z^{\sum_{i=1}^n\mu_i},$$

其中,κ为任意属性对应子签名的数量,满足 $1\leqslant\kappa\leqslant n$.若等式成立,说明$\{\sigma_1,\sigma_2,\ldots,\sigma_n\}$是消息$\{m_1,m_2,\ldots,m_n\}$对应的合法签名;否则,说明$\{\sigma_1,\sigma_2,\ldots,\sigma_n\}$中存在$\sigma_i$不是对应消息 m_i 的合法签名.针对这种情况,可以通过二分法快速查找非法消息-签名对,算法具体细节请参考文献[26],在此不再赘述.

4 安全性分析

定理 1(无条件强匿名性). 本文所提出的分布式无中心授权的属性基可变门限环签名方案具备无条件强匿名性.

证明:因为从签名属性集合 $\{\omega_k^*\}_{k\in Team}$ 中任意选取满足断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$ 的属性子集 $\{\omega'_{ID_i,k}\}_{k\in Team}$ 作为实际签名属性集合均可产生合法的签名,且验证签名无需使用 $\{\omega'_{ID_i,k}\}_{k\in Team}$,所以任何敌手均无法获得 $\{\omega'_{ID_i,k}\}_{k\in Team}$

的任何信息.接下来只需证明通过签名无法揭露签名者的实际身份 ID_i,即可证明该方案具备无条件强匿名性.

1) 初始化

A 声明挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in Team}$.挑战者 C 运行初始化算法,并将生成的系统公开参数 *params* 和系统秘密参数 *privates* 全部发送给 A,因此,A 可以生成系统中所有用户的任意属性密钥.

2) 挑战阶段

A 随机选择消息 m^*和用户 ID_1(属性集合为 ω_{ID_1}),ID_2(属性集合为 ω_{ID_2}),满足 $\Upsilon_{t_k,\omega_k^*}(\omega_{ID_1})=\Upsilon_{t_k,\omega_k^*}(\omega_{ID_2})=1$,并将 $m^*,(ID_1,\omega_{ID_1}),(ID_2,\omega_{ID_2})$ 发送给 C.

- C 首先运行密钥生成算法生成相应的密钥集合:

$$SK_1=\langle\{S_{1,j,k}^1\}_{j\in\omega_{ID_1,k}\cup\Omega_{ID_1,k},k\in Team}\{S_{2,k}^1\}_{k\in Team}\rangle, SK_2=\langle\{S_{1,j,k}^2\}_{j\in\omega_{ID_2,k}\cup\Omega_{ID_2,k},k\in Team}\{S_{2,k}^2\}_{k\in Team}\rangle.$$

- 然后抛掷一枚公平硬币 $b\in\{1,2\}$,调用签名算法使用 SK_b 生成 m^*相应的签名:

$$\sigma_b^*=\langle\sigma_1^{b*},\sigma_2^{b*},\sigma_3^{b*},\{\sigma_{4,j,k}^{b*}\}_{j\in\omega_k^*\cup\Omega_{ID_b,k},k\in Team}\rangle.$$

- 最后,将 σ_b^* 发送给 A 进行猜测.其中,

$$\sigma_1^{b*}=g_2^{z_b+\sum_{k\in Team}H_1(\lambda_{b,k})a_{k,0}\cdot\Delta_{k,Team}(0)}H_3(m^*)^{v_b}\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_b,k}\cup\Omega_{ID_b,k}}(H_2(j)^{t_{j,k}})^{\Delta_{j\in\omega'_{ID_b,k}\cup\Omega_{ID_b,k}}(0)\cdot\Delta_{k,Team}(0)}\prod_{j\in\omega_k^*\cup\Omega_{ID_b,k}}H_2(j)^{r_{j,k}^b}\right),$$

$$\sigma_2^{b*}=g_2^{z_b+a_0+\sum_{k\in Team}H_1(\lambda_{b,k})a_{k,0}\cdot\Delta_{k,Team}(0)},$$

$$\sigma_3^{b*}=g^{v_b},$$

$$\{\sigma_{4,j,k}^{b*}=T_{j,k}^{b\ \Delta_{j,\omega'_{ID_b,k}\cup\Omega_{ID_b,k}}(0)\cdot\Delta_{k,Team}(0)}g^{r_{j,k}^b}\}_{j\in\omega'_{ID_b,k}\cup\Omega_{ID_b,k},k\in Team},$$

$$\{\sigma_{4,j,k}^{b*}=g^{r_{j,k}^b}\}_{j\in\omega_k^*\setminus\omega'_{ID_b,k},k\in Team}.$$

3) 猜测阶段

A 输出对 b 的猜测 b',若 $b=b'$,则 A 赢得游戏,说明本方案不具备无条件强匿名性.

下面分析 A 不可能赢得游戏的原因.

假设 C 在 b=1 的条件下选取 Z_q^* 上的随机数 v_1,z_1 及随机数集合 $\{r_{j,k}^1\}_{j\in\omega_k^*\cup\Omega_{ID_1,k},k\in Team}$,使用 SK_1 生成 m^*相应的签名 σ_1^*,但该签名与 C 选取 $\{\omega'_{ID_2,k}\cup\Omega_{ID_2,k}\}_{k\in Team}=\{\omega'_{ID_1,k}\cup\Omega_{ID_1,k}\}_{k\in Team}$,$z_2=z_1+\sum_{k\in Team}H_1(\lambda_{1,k})a_{k,0}\cdot\Delta_{k,Team}(0)-\sum_{k\in Team}H_1(\lambda_{2,k})a_{k,0}\cdot\Delta_{k,Team}(0)$,$v_2=v_1$,$\{r_{j,k}^2\}_{j\in\omega_k^*\cup\Omega_{ID_1,k},k\in Team}=\{r_{j,k}^1\}_{j\in\omega_k^*\cup\Omega_{ID_2,k},k\in Team}$,使用 SK_2 为 m^*生成的相应签名 σ_2^* 相等,因此,C 也可以声明该签名是在 b=2 的条件下生成的.同理可证:C 在 b=2 的条件下生成签名 σ_2^*,其同样可以声明该签名是在 b=1 条件下产生的.

因为 σ_b^* 中仅有 $\sigma_1^{b*},\sigma_2^{b*}$ 中包含用户的身份信息,所以,这里仅对 σ_1^{b*}和σ_2^{b*} 的正确性进行验证.

$$\begin{aligned}\sigma_1^{1*}&=g_2^{z_1+\sum_{k\in Team}H_1(\lambda_{1,k})a_{k,0}\cdot\Delta_{k,Team}(0)}H_3(m^*)^{v_1}\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_1,k}\cup\Omega_{ID_1,k}}(H_2(j)^{t_{j,k}})^{\Delta_{j\in\omega'_{ID_1,k}\cup\Omega_{ID_1,k}}(0)\cdot\Delta_{k,Team}(0)}\prod_{j\in\omega_k^*\cup\Omega_{ID_1,k}}H_2(j)^{r_{j,k}^1}\right)\\&=g_2^{z_2+\sum_{k\in Team}H_1(\lambda_{2,k})a_{k,0}\cdot\Delta_{k,Team}(0)}H_3(m^*)^{v_2}\prod_{k\in Team}\left(\prod_{j\in\omega'_{ID_2,k}\cup\Omega_{ID_2,k}}(H_2(j)^{t_{j,k}})^{\Delta_{j\in\omega'_{ID_2,k}\cup\Omega_{ID_2,k}}(0)\cdot\Delta_{k,Team}(0)}\prod_{j\in\omega_k^*\cup\Omega_{ID_2,k}}H_2(j)^{r_{j,k}^2}\right)\\&=\sigma_1^{2*},\end{aligned}$$

$$\sigma_2^{1*}=g_2^{z_1+a_0+\sum_{k\in Team}H_1(\lambda_{1,k})a_{k,0}\cdot\Delta_{k,Team}(0)}=g_2^{z_2+a_0+\sum_{k\in Team}H_1(\lambda_{2,k})a_{k,0}\cdot\Delta_{k,Team}(0)}=\sigma_2^{2*}$$

成立.证毕. □

定理 2(适应性选择消息和断言攻击下存在性不可伪造). 本文所提出的分布式无中心授权的属性基可变

门限环签名方案在适应性选择消息和断言攻击下是存在性不可伪造的.

证明:在随机预言机模型及适应性选择消息和断言攻击条件下,若攻击者 A 能够以一个不可忽略的优势 ε 在多项式时间内攻破本方案,则存在算法 C,能够以不可忽略的优势 ε' 在多项式时间内解决 CDH 困难问题,其中,

$$\varepsilon' \approx \frac{\varepsilon}{q_{H_2} q_{H_3} \prod_{k\in\psi\cup\bar{I}} \binom{d_k - t_k}{d_k - 1}}.$$

1) 系统建立:假设攻击者 A 已经攻破 l–1 个属性授权机构,不失一般性,假设这些已被攻破的属性授权机构组成集合 $\Psi=\{AA_1,AA_2,\ldots,AA_{l-1}\}$,其余未被攻破的属性授权机构组成集合 $T=\{AA_l,AA_{l+1},\ldots,AA_n\}$.因此,攻击者 A 只需再攻破集合 T 中任何一个成员 $AA_{\bar{I}}$,就可以成功地伪造任意消息的合法签名.

A 声明挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$,其中,$1\leqslant t_k\leqslant d_k$,$d_k$ 为 AA_k 预设门限值.挑战者 C 运行初始化算法 $Setup(d)$,生成系统的公开参数 $params=\langle e,g,g_1,g_2,Z,H_1,H_2,H_3,\{P_k\}_{k=1,\ldots,n},\{T_{j,k}\}_{j\in\omega_k\cup\Omega_k,k=1,\ldots,n},q\rangle$ 以及秘密参数 $privates=\langle\{t_{j,k}\}_{j\in\omega_k\cup\Omega_k,k=1,\ldots,n},\{a_{k,0},x_k\}_{k=1,\ldots,n}\rangle$,并将 $params$ 和集合 Ψ 中成员的秘密参数 $\langle\{t_{j,k}\}_{j\in\omega_k\cup\Omega_k,k\in\psi},\{a_{k,0},x_k\}_{k\in\psi}\rangle$ 发送给攻击者 A.

2) 预言仿真阶段:假设攻击者 A 分别可以进行 $q_{H_1},q_{H_2},q_{H_3},q_k,q_s$ 次 $H_i(i=1,2,3)$ 预言仿真、密钥解析预言仿真和签名预言仿真.挑战者 C 将 $H_i(i=1,2,3)$ 预言仿真和密钥解析预言仿真的结果分别存储于列表 $List_i(i=1,2,3)$ 和 $List_{key}$ 中.

a) H_1-询问:C 维护一个包含数组 $(ID_i,AA_k,H_{1,j,k})$ 的列表 $List_1$.当 A 对 $(ID_\varsigma,AA_{\bar{I}})$ 进行 H_1 询问时,C 进行如下操作.

- C 首先检查列表 $List_1$,若 $List_1$ 中存在数组 $(ID_\varsigma,AA_{\bar{I}},H_{1,\varsigma,\bar{I}})$,则将 $H_{1,\varsigma,\bar{I}}$ 作为对 $(ID_\varsigma,AA_{\bar{I}})$ 进行 H_1 询问的应答发送给 A.
- 否则,C 随机选取 $\alpha_{\varsigma,\bar{I}}\in Z_q^*$,把 $H_{1,\varsigma,\bar{I}}=\alpha_{\varsigma,\bar{I}}$ 作为对 $(ID_\varsigma,AA_{\bar{I}})$ 进行 H_1 询问的应答发送给 A,并将数组 $(ID_\varsigma,AA_{\bar{I}},H_{1,\varsigma,\bar{I}})$ 存入列表 $List_1$.

b) H_2-询问:C 维护一个包含数组 $(j_k,H_{2,j,k})$ 的列表 $List_2$.当 A 对属性 $j_{\bar{I}}$ 进行 H_2 询问时,C 随机选取缺省属性集合 $\Omega_{\bar{I}}^*$,满足 $|\Omega_{\bar{I}}^*|=d_{\bar{I}}-t_{\bar{I}}$,进行如下操作.

- C 首先检查列表 $List_2$:如果 $List_2$ 中存在数组 $(j_{\bar{I}},H_{2,j,\bar{I}})$,则将 $H_{2,j,\bar{I}}$ 作为对 $j_{\bar{I}}$ 进行 H_2 询问的应答发送给 A.
- 否则,若 $j_{\bar{I}}\in\omega_{\bar{I}}^*\cup\Omega_{\bar{I}}^*$,$C$ 随机选取 $\beta_{\bar{I},j}\in Z_q^*$,把 $H_{2,j,\bar{I}}=g^{\beta_{\bar{I},j}}$ 作为对 $j_{\bar{I}}$ 进行 H_2 询问的应答发送给 A,并将数组 $(j_{\bar{I}},H_{2,j,\bar{I}})$ 存入列表 $List_2$.
- 否则,$j_{\bar{I}}\notin\omega_{\bar{I}}^*\cup\Omega_{\bar{I}}^*$,$C$ 随机选取 $\beta_{\bar{I},j},\gamma_{\bar{I},j}\in Z_q^*$,把 $H_{2,j,\bar{I}}=g_1^{-\beta_{\bar{I},j}}g^{\gamma_{\bar{I},j}}$ 作为对 $j_{\bar{I}}$ 进行 H_2 询问的应答发送给 A,并将数组 $(j_{\bar{I}},H_{2,j,\bar{I}})$ 存入列表 $List_2$.

c) H_3-询问:C 维护一个包含数组 $(m_i,H_{3,i})$ 的列表 $List_3$,并选取一个随机数 $\delta\in[1,q_{H_3}]$.当 A 对 m_ς 进行 H_3 询问时,C 进行如下操作.

- C 首先检查列表 $List_3$:若 $List_3$ 中存在数组 $(m_\varsigma,H_{3,\varsigma})$,则将 $H_{3,\varsigma}$ 作为对 m_ς 进行 H_3 询问的应答发送给 A.
- 否则,若 $\varsigma=\delta$,C 随机选取 $\eta_\delta\in Z_q^*$,把 $H_{3,\varsigma}=g^{\eta_\delta}$ 作为对 m_ς 进行 H_3 询问的应答发送给 A,并将数组 $(m_\varsigma,H_{3,\varsigma})$ 存入列表 $List_3$.
- 否则,$\varsigma\neq\delta$,C 随机选取 $\theta_\varsigma,\eta_\varsigma\in Z_q^*$,把 $H_{3,\varsigma}=g_1^{\theta_\varsigma}g^{\eta_\varsigma}$ 作为对 m_ς 进行 H_3 询问的应答发送给 A,并将数组 $(m_\varsigma,H_{3,\varsigma})$ 存入列表 $List_3$.

d) 密钥解析询问:C 维护一个包含数组 $(\omega_{ID_i,k},ID_i,\{T_{k,j},S_{k,j}\}_{j\in\omega_{ID_i,k}\cup\Omega_k^*},P)_k$ 的列表 $List_{key}$.当 A 输入 $(\omega_{ID_\varsigma,\bar{I}},ID_\varsigma)$ 进行密钥解析询问时,C 进行如下操作.

- C 检查列表 $List_{key}$:若 $List_{key}$ 中存在数组 $\left(\omega_{ID_\varsigma,\bar{I}}, ID_\varsigma, \{T_{\bar{I},j}, S_{\bar{I},j}\}_{j\in\omega_{ID_\varsigma,\bar{I}}\cup\Omega_{\bar{I}}^*}, P_{\bar{I}}\right)$,则将 $\{T_{\bar{I},j}, S_{\bar{I},j}\}_{j\in\omega_{ID_\varsigma,\bar{I}}\cup\Omega_{\bar{I}}^*}$ 和 $P_{\bar{I}}$ 作为对 $(\omega_{ID_\varsigma,\bar{I}}, ID_\varsigma)$ 进行密钥解析询问的应答发送给 A.
- 否则,若 $|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|<t_{\bar{I}}$,$C$ 随机选取缺省属性集合 $\Omega_{\bar{I}}^*$,满足 $|\Omega_{\bar{I}}^*|=d_{\bar{I}}-t_{\bar{I}}$. 定义 3 个属性集合 $\Gamma_{\bar{I}},\Gamma'_{\bar{I}},S_{\bar{I}}$,其中,$\Gamma_{\bar{I}}\subseteq\Gamma'_{\bar{I}}\subset S_{\bar{I}}, \Gamma_{\bar{I}}=\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*\cup\Omega_{\bar{I}}^*, |\Gamma'_{\bar{I}}|=d_{\bar{I}}-1, S_{\bar{I}}=\Gamma'_{\bar{I}}\cup\{0\}$.由拉格朗日插值公式可知,$a_0=\sum_{k\in\Psi\cup\bar{I}}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)$,由于 A 已经攻破集合 Ψ 中所有属性授权机构,因此,$AA_{\bar{I}}$ 的部分密钥满足等式 $a_{\bar{I},0}=\dfrac{a_0-\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}$.

对于属性 $j_{\bar{I}}\in\Gamma'_{\bar{I}}$,$C$ 首先随机选取 $x'_{\bar{I}},\tau_{j,\bar{I}},t_{j,\bar{I}}\in Z_q^*$,等价于隐性地令 $q_{\bar{I}}(j)=\tau_{j,\bar{I}}$,然后分别对 ID_ς 和 $j_{\bar{I}}$ 进行预言机询问得到 $H_1(\lambda_\varsigma)$ 和 $H_2(j_{\bar{I}})$ 的仿真结果,最后 C 生成相应属性的密钥.

$$\{S_{1,j,\bar{I}}=H_2(j)^{t_{j,\bar{I}}}g_2^{H_1(\lambda_{\varsigma,\bar{I}})\tau_{j,\bar{I}}}\}_{j\in\Gamma'},S_{2,\bar{I}}=g_1^{-x'_{\bar{I}}}g_2^{\frac{-(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}},\{T_{1,j,\bar{I}}=g^{t_{j,\bar{I}}}\}_{\xi\in\Gamma'},P_{\bar{I}}=g_1^{x'_{\bar{I}}}.$$

正确性验证:令 $x_{\bar{I}}=\dfrac{(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot b_0}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+x'_{\bar{I}}$,则下列等式成立.

$$S_{2,\bar{I}}=g_1^{-x'_{\bar{I}}}g_2^{\frac{-(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}}=g_1^{-\left(x_{\bar{I}}-\frac{(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot b_0}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\right)}g_2^{\frac{-(H_1(\lambda_{\varsigma,\bar{I}})+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}}=g_1^{-x_{\bar{I}}}g_2^{H_1(\lambda_{\varsigma,\bar{I}})a_{\bar{I},0}+a_{\bar{I},0}}.$$

对于属性 $\xi_{\bar{I}}\notin\Gamma'$,为了确保等式 $q_{\bar{I}}(0)=a_{\bar{I},0}$ 成立,C 随机选取 $t'_{\xi,\bar{I}}\in Z_p^*$,计算相应的属性密钥:

$$S_{1,\xi,\bar{I}}=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t'_{\xi,\bar{I}}}g_2^{\gamma_{\bar{I},\xi}\cdot\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+H_1(\lambda_{\varsigma,\bar{I}})\left(\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)-\frac{\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\Delta_{0,S_{\bar{I}}}(\xi)\right)},T_{1,\xi,\bar{I}}=g_2^{\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}}g^{t'_{\xi,\bar{I}}}.$$

正确性验证:令 $t_{\xi,\bar{I}}=\dfrac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\cdot b_0+t'_{\xi,\bar{I}}$,由于 $q_{\bar{I}}(\xi)=\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)+q_{\bar{I}}(0)\Delta_{0,S_{\bar{I}}}(\xi)$,故下列等式成立.

$$\begin{aligned}S_{1,\xi,\bar{I}}&=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t'_{\xi,\bar{I}}}g_2^{\gamma_{\bar{I},\xi}\cdot\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+H_1(\lambda_{\varsigma,\bar{I}})\left(\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)-\frac{\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\Delta_{0,S_{\bar{I}}}(\xi)\right)}\\&=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t_{\xi,\bar{I}}-\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\cdot b_0}g_2^{\gamma_{\bar{I},\xi}\cdot\frac{H_1(\lambda_{\varsigma,\bar{I}})\Delta_{0,S_{\bar{I}}}(\xi)}{\beta_{\bar{I},\xi}\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}+H_1(\lambda_{\varsigma,\bar{I}})\left(\sum_{j\in\Gamma'_{\bar{I}}}q_{\bar{I}}(j)\Delta_{j,S_{\bar{I}}}(\xi)-\frac{\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\Delta_{0,S_{\bar{I}}}(\xi)\right)}\\&=(g_1^{-\beta_{\bar{I},\xi}}g^{\gamma_{\bar{I},\xi}})^{t_{\xi,\bar{I}}}g_2^{H_1(\lambda_{\varsigma,\bar{I}})q_{\bar{I}}(\xi)}.\end{aligned}$$

把相应密钥集合发送给 A,并将数组 $\left(\omega_{ID_\varsigma,\bar{I}}, ID_\varsigma, \{T_{j,\bar{I}}, S_{j,\bar{I}}\}_{j\in\omega_{ID_\varsigma,\bar{I}}\cup\Omega_{\bar{I}}^*}, P_{\bar{I}}\right)$ 存入列表 $List_{key}$.

- 否则,$|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|\geqslant t_{\bar{I}}$,$C$ 停止仿真,将该事件记为 E_1.

e) 签名询问:A 输入 $(\omega_{ID_\varsigma}, ID_\varsigma, m_\varsigma)$ 进行签名询问,C 进行如下操作.

- 若 $|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|<t_{\bar{I}}$,$C$ 通过对 $(\omega_{ID_\varsigma,k}, ID_\varsigma)_{k\in\psi\cup\bar{I}}$ 进行密钥解析询问,获得相应属性的密钥,对 m_ς 进行 H_3 询问得到 $H_3(m_\varsigma)$ 的仿真结果,直接利用签名算法得到 m_ς 相应的签名,并发送给 A.
- 否则,$|\omega_{ID_\varsigma,\bar{I}}\cap\omega_{\bar{I}}^*|\geqslant t_{\bar{I}}$,若 $H_3(m_\varsigma)\neq g^{\eta_\delta}$,$C$ 首先随机选取属性集合 $\{\omega'_{ID_\varsigma,k}\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,其中,$\omega'_{ID_\varsigma,k}\subseteq\{\omega_{ID_\varsigma,k}\cap\omega_k^*\}$ 且 $|\omega'_{ID_\varsigma,k}\cup\Omega_k^*|=d_k$;然后,选随机数 $z,v'\in Z_q^*$ 和随机数集合 $\{r_{j,k}\in Z_q^*\}_{k\in\Psi\cup\bar{I},j\in\omega_k^*\cup\Omega_k^*}$;最后,通过下述方法生成 m_ς 对应的签名 $\sigma_\varsigma=\langle\sigma_1^\varsigma,\sigma_2^\varsigma,\sigma_3^\varsigma,\{\sigma_{4,j,k}^\varsigma\}_{j\in\omega_k^*\cup\Omega_k^*,k\in\psi\cup\bar{I}}\rangle$,其中,

$$\sigma_1 = g_2^{z-\frac{\eta_\varsigma \cdot H_1(\lambda_{i,\bar{I}})}{\theta_\varsigma}+\sum_{k\in\Psi}(H_1(\lambda_{i,k})-H_1(\lambda_{i,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v'}\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right),$$

$$\sigma_2 = g_2^{z-(H_1(\lambda_\varsigma)+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{k\in\Psi}(g_2^{H_1(\lambda_i)a_{k,0}+a_{k,0}})^{\Delta_{k,\Psi\cup\bar{I}}(0)},$$

$$\sigma_3 = g_2^{-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}}g^{v'}\left\{\sigma_{4,j,k}=(T_{j,k})^{\Delta_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\Delta_{k\in\Psi\cup\bar{I}}(0)}g_2^{r_{j,k}}\right\}_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*,k\in\Psi\cup\bar{I}}\{\sigma_{4,j,k}=g_2^{r_{j,k}}\}_{j\in\omega_k^*\setminus\omega'_{ID_\varsigma,k},k\in\psi\cap\bar{I}}.$$

正确性验证:令 $v=-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}\cdot b_0+v'$,则下列等式成立.

$$\sigma_1 = g_2^{z-\frac{\eta_\varsigma \cdot H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}+\sum_{k\in\Psi}(H_1(\lambda_{\varsigma,k})-H_1(\lambda_{\varsigma,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v'}\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^{z-\frac{\eta_\varsigma \cdot H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}+\sum_{k\in\Psi}(H_1(\lambda_{\varsigma,k})-H_1(\lambda_{\varsigma,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v+\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}\cdot b_0}$$

$$\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^{z+\sum_{k\in\Psi}(H_1(\lambda_{\varsigma,k})-H_1(\lambda_{\varsigma,\bar{I}}))a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v}g_2^{H_1(\lambda_{\varsigma,\bar{I}})\cdot\sum_{k\in\Psi\cup\bar{I}}a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)};$$

$$\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^{z+\sum_{k\in\Psi\cup\bar{I}}H_1(\lambda_{\varsigma,k})\cdot a_{k,0}\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}(g_1^{\theta_\varsigma}g^{\eta_\varsigma})^{v}\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(H_2(j)^{t_{j,k}})^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right)$$

$$= g_2^z H_3(m)^v\prod_{k\in\Psi\cup\bar{I}}\left(\prod_{j\in\omega'_{ID_\varsigma,k}\cup\Omega_k^*}S_{1,j,k}^{\Delta_{j,\omega'_{ID_\varsigma,k}\cup\Omega_k^*}(0)\cdot\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{j,k}}\right),$$

$$\sigma_2 = g_2^{z-(H_1(\lambda_\varsigma)+1)\cdot\sum_{k\in\Psi}a_{k,0}\Delta_{k,\Psi\cup\bar{I}}(0)}\prod_{k\in\Psi}(g_2^{H_1(\lambda_i)a_{k,0}+a_{k,0}})^{\Delta_{k,\Psi\cup\bar{I}}(0)} = g_2^z(P_{\bar{I}}S_{2,\bar{I}})^{\Delta_{\bar{I},\Psi\cup\bar{I}}(0)}\prod_{k\in\Psi}(P_kS_{2,k})^{\Delta_{k,\Psi\cup\bar{I}}(0)} = g_2^z\prod_{k\in\Psi\cup\bar{I}}(P_kS_{2,k})^{\Delta_{k,\Psi\cup\bar{I}}(0)},$$

$$\sigma_3 = g_2^{-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}}g^{v'} = g^{-\frac{H_1(\lambda_{\varsigma,\bar{I}})}{\theta_\varsigma}\cdot b_0+v'} = g_2^v.$$

- 否则,C 停止仿真,将该事件记为 E_2.

3) 伪造阶段:攻击者 A 在挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\bar{\Omega}_k\}_{k\in\psi\cup\bar{I}}$ 的条件下,成功地伪造了消息 m_ς^* 的签名 $\sigma_\varsigma^*=\langle\sigma_{1,\varsigma}^*,\sigma_{2,\varsigma}^*,\sigma_{3,\varsigma}^*,\{\sigma_{4,j,k}^*\}_{k\in\Psi\cup\bar{I},j\in\omega_k^*\cup\bar{\Omega}_k}\rangle$. 如果 $H_3(m_\varsigma^*)=g^{\eta_\delta}$ 且 $\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,则下列等式成立.

$$\frac{e(g,\sigma_{2,\varsigma}^*)e(g^{\eta_\delta},\sigma_{3,\varsigma}^*)\prod_{k\in\psi\cup\bar{I}}\prod_{j\in\omega_k^*\cup\Omega_k^*}e(g^{\beta_{k,j}^*},\sigma_{4,j,k}^*)}{e(g,\sigma_{1,\varsigma}^*)} = Z = e(g,g^{a_0\cdot b_0}).$$

因此,C 可以成功地解决 CDH 困难问题,其中, $g^{a_0\cdot b_0}=\frac{\sigma_{2,\varsigma}^*\cdot\sigma_{3,\varsigma}^{*\eta_\delta}\cdot\prod_{k\in\Psi\cup\bar{I}}\prod_{j\in\omega_k^*\cup\Omega_k^*}\sigma_{4,j,k}^{*\beta_{k,j}^*}}{\sigma_{1,\varsigma}^*}$.

下面分析 C 成功解决 CDH 困难问题的优势.

在伪造过程中要求 $H_3(m_\varsigma^*)=g^{\eta_\delta^*},\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$ 且 $H_2(j)$已知,因为$|\Omega_k|=d_k-1$,进行 H_2,H_3 预言仿真的次数分

别为 q_{H_2},q_{H_3},所以 C 成功解决 CDH 困难问题的优势为 $\varepsilon' \approx \dfrac{\varepsilon}{q_{H_2}q_{H_3}\prod\limits_{k\in\psi\cup\bar{I}}\binom{d_k-t_k}{d_k-1}}$. 证毕. □

定理 3(适应性选择消息和断言攻击下抗合谋攻击). 本文所提出的分布式无中心授权的属性基可变门限环签名方案在适应性选择消息和断言攻击下可以抵抗合谋攻击.

证明:假设存在攻击者 A 分别可以进行 $q_{H_1},q_{H_2},q_{H_3},q_k,q_s$ 次 $H_i(i=1,2,3)$预言仿真、密钥解析预言仿真和签名预言仿真.若该攻击者 A 能够在适应性选择消息和断言攻击的条件下,以一个不可忽略的优势ε在多项式时间内攻破本方案,则存在算法 C 可以在多项式时间内以不可忽略的优势ε'解决 CDH 困难问题,其中,

$$\varepsilon' \approx \frac{\varepsilon}{q_{H_2}q_{H_3}\prod\limits_{k\in\psi\cup\bar{I}}\binom{d_k-t_k}{d_k-1}}.$$

1) 系统建立

同定理 2 的系统建立过程.

2) 预言仿真阶段

同定理 2 的预言仿真阶段.

3) 挑战阶段

攻击者 A 在挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\bar{\Omega}_k\}_{k\in\psi\cup\bar{I}}$ 的条件下,挑战该方案的抗合谋攻击性.

A 首先随机选取用户 ID_1(属性集合为ω_1),ID_2(属性集合为ω_2),满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega_1)\neq 1,\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega_2)\neq 1$,且存在属性集合 $\omega'_{1,\bar{I}}\subseteq\omega_{1,\bar{I}},\omega'_{2,\bar{I}}\subseteq\omega_{2,\bar{I}}$,满足 $\Upsilon_{t_{\bar{I}},\omega_{\bar{I}}^*}(\omega'_{1,\bar{I}}\cup\omega'_{2,\bar{I}})=1$;

然后,分别对 $(ID_1,AA_{\bar{I}}),(ID_2,AA_{\bar{I}})$ 进行 H_1 询问,得到 $H_1(\lambda_{1,\bar{I}}),H_1(\lambda_{2,\bar{I}})$ 的仿真结果 $\alpha_{1,\bar{I}}$ 和 $\alpha_{2,\bar{I}}$;

对 $(\omega'_{1,\bar{I}},ID_1),(\omega'_{2,\bar{I}},ID_2)$ 进行密钥解析询问得到密钥集合:

$$\{S^1_{1,j,\bar{I}}=H_2(j)^{t_{j,\bar{I}}}g_2^{\alpha_{1,\bar{I}}\cdot q_{\bar{I}}(j)},S^1_{2,\bar{I}}=g_1^{-x_{\bar{I}}}g_2^{\alpha_{1,\bar{I}}\cdot a_{\bar{I},0}+a_{\bar{I},0}},T_{j,\bar{I}}=g^{t_{j,\bar{I}}},P_{\bar{I}}=g_1^{x_{\bar{I}}}\}_{j\in\omega'_{1,\bar{I}}\cup\bar{\Omega}_{1,\bar{I}}},$$

$$\{S^2_{1,j,\bar{I}}=H_2(j)^{t_{j,\bar{I}}}g_2^{\alpha_{2,\bar{I}}\cdot q_{\bar{I}}(j)},S^2_{2,\bar{I}}=g_1^{-x_{\bar{I}}}g_2^{\alpha_{2,\bar{I}}\cdot a_{\bar{I},0}+a_{\bar{I},0}},T_{j,\bar{I}}=g^{t_{j,\bar{I}}},P_{\bar{I}}=g_1^{x_{\bar{I}}}\}_{j\in\omega'_{2,\bar{I}}\cup\bar{\Omega}_{2,\bar{I}}};$$

其次,为用户 ID_2 生成新的属性密钥集合:

$$\left\{S^{2'}_{1,j,\bar{I}}=S^2_{1,j,\bar{I}}{}^{\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}=H_2(j)^{t_{j,\bar{I}}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}g_2^{\alpha_{1,\bar{I}}\cdot q_{\bar{I}}(j)},S^{2'}_{2,\bar{I}}=S^1_{2,\bar{I}}=g_1^{-x_{\bar{I}}}g_2^{\alpha_{1,\bar{I}}\cdot a_{\bar{I},0}+a_{\bar{I},0}},T'_{j,\bar{I}}=T^{\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}_{j,\bar{I}}=g^{t_{j,\bar{I}}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}},P_{\bar{I}}=g_1^{x_{\bar{I}}}\right\}_{j\in\omega'_{2,\bar{I}}\cup\bar{\Omega}_{2,\bar{I}}};$$

最终,A 可以获得签名密钥集合 $\{S^1_{1,j,k}\cup S^{2'}_{1,j,\bar{I}},S^1_{2,k},T_{j,k}\cup T'_{j,\bar{I}},P_k\}_{j\in\omega'_{1,k}\cup\omega'_{2,\bar{I}}\cup\bar{\Omega}_k,k\in\psi\cup\bar{I}}$.

4) 伪造阶段

攻击者 A 在挑战断言 $\{\Upsilon_{t_k,\omega_k^*}(\cdot)\}_{k\in\psi\cup\bar{I}}$ 和缺省属性集合 $\{\bar{\Omega}_k\}_{k\in\psi\cup\bar{I}}$ 的条件下,成功地伪造消息 m^*的签名$\sigma^*=\langle\sigma_1^*,\sigma_2^*,\sigma_3^*,\{\sigma_{4,j,k}^*\}_{j\in\omega_k^*\cup\bar{\Omega}_k,k\in\psi\cup\bar{I}}\rangle$,并将$\sigma^*$发送给 C 进行验证.如果 $H_3(m^*)=g^{\eta_\delta}$ 且 $\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,则下列等式成立:

$$\frac{e(g,\sigma_2^*)e(g^{\eta_\delta},\sigma_3^*)\prod\limits_{k\in\psi\cup\bar{I}}\prod\limits_{j\in\omega_k^*\cup\Omega_k^*}e(g^{\beta_{k,j}},\sigma_{4,j,k}^*)}{e(g,\sigma_1^*)}=Z=e(g,g^{a_0\cdot b_0}).$$

因此,C 可以成功地解决 CDH 困难问题,其中, $g^{a_0\cdot b_0}=\dfrac{\sigma_2^*\cdot\sigma_3^{*\eta_\delta}\cdot\prod\limits_{k\in\psi\cup\bar{I}}\prod\limits_{\xi\in\omega_k^*\cup\Omega_k^*}\sigma_{4,j,k}^{*\beta_{k,j}}}{\sigma_1^*}$.

正确性验证如下:

$$\frac{e(g,\sigma_2^*)e(H_3(m^*),\sigma_3^*)\prod_{k\in\psi\cup\bar{I}}\prod_{j\in\omega_k^*\cup\Omega_k^*}e(H_2(j),\sigma_{4,j,k}^*)}{e(g,\sigma_1^*)}=$$

$$\frac{e\left(g,\prod_{k\in\psi\cup\bar{I}}(P_kS_{2,k}^1)^{\Delta_{k,\psi\cup\bar{I}}(0)}\right)\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}e\left(H_2(j),T_{j,k}^{\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\prod_{j\in\omega_{2,\bar{I}}'}e\left(H_2(j),T_{j,\bar{I}}'^{\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)\prod_{j\in\omega_k^*\cup\Omega_k^*}e(H_2(j),g^{r_{k,j}})\right)}{e\left(g,\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}S_{1,j,k}^{1\ \Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\prod_{j\in\omega_{2,\bar{I}}'}S_{1,j,\bar{I}}^{2'\ \Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\prod_{j\in\omega_k^*\cup\Omega_k^*}H_2(j)^{r_{k,j}}\right)\right)}=$$

$$\frac{e\left(g,\prod_{k\in\psi\cup\bar{I}}(g_2^{\alpha_{1,k}\cdot a_{k,0}+a_{k,0}})^{\Delta_{k,\psi\cup\bar{I}}(0)}\right)\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}e\left(H_2(j),g^{t_{j,k}\cdot\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\right)\prod_{j\in\omega_{2,\bar{I}}'}e\left(H_2(j),g^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)}{e\left(g,\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}(H_2(j)^{t_{j,k}}g_2^{\alpha_{1,k}\cdot q_k(j)})^{\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\prod_{j\in\omega_{2,\bar{I}}'}\left(H_2(j)^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}}g_2^{\alpha_{1,\bar{I}}\cdot q_{\bar{I}}(j)}\right)^{\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)\right)}=$$

$$\frac{e\left(g,g_2^{a_0}\prod_{k\in\psi\cup\bar{I}}g_2^{\alpha_{1,\bar{I}}\cdot a_{k,0}\cdot\Delta_{k,\psi\cup\bar{I}}(0)}\right)\prod_{k\in\psi\cup\bar{I}}\left(\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}e\left(H_2(j),g^{t_{j,k}\cdot\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\right)\prod_{j\in\omega_{2,\bar{I}}'}e\left(H_2(j),g^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}\cdot\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)}{e\left(g,\prod_{k\in\psi\cup\bar{I}}\left(g_2^{\alpha_{1,\bar{I}}\cdot a_{k,0}\cdot\Delta_{k,\psi\cup\bar{I}}(0)}()\prod_{j\in\omega_{1,k}'\cup\Omega_k^*}H_2(j)^{t_{j,k}\cdot\Delta_{j,\omega_{1,k}'\cup\omega_{2,\bar{I}}'\cup\Omega_k^*(0)\cdot\Delta_{k,\psi\cup\bar{I}}(0)}}\right)\prod_{j\in\omega_{2,\bar{I}}'}H_2(j)^{t_{j,k}\cdot\frac{\alpha_{1,\bar{I}}}{\alpha_{2,\bar{I}}}\cdot\Delta_{j,\omega_{1,\bar{I}}'\cup\omega_{2,\bar{I}}'\cup\Omega_{\bar{I}}^*(0)\cdot\Delta_{\bar{I},\psi\cup\bar{I}}(0)}}\right)}=$$

$e(g,g_2^{a_0})=e(g,g^{a_0\cdot b_0})$.

下面分析 C 成功解决 CDH 困难问题的优势.

在合谋攻击过程中,要求 $H_3(m^*)=g^{\eta_\delta},\{\bar{\Omega}_k=\Omega_k^*\}_{k\in\psi\cup\bar{I}}$,$H_2(j)$ $H_2(j)$,由于$|\Omega_k|=d_k-1$,进行 H_2,H_3 预言仿真的次数分别为 q_{H_2},q_{H_3},因此,C 成功解决 CDH 困难问题的优势为 $\varepsilon'\approx\dfrac{\varepsilon}{q_{H_2}q_{H_3}\prod_{k\in\psi\cup\bar{I}}\binom{d_k-t_k}{d_k-1}}$. 证毕. □

5 效率比较与性能分析

本节将从效率和性能两方面与现有方案进行对比,进而得出本方案的综合评估结果.评估过程所用符号及其定义见表 1,效率比较见表 2,性能比较见表 3.

Table 1 Definition of related symbols

表 1 相关符号定义

符号	定义	符号	定义
A	签名者拥有属性集合	d	预定义数值
B	断言声明属性集合	t	断言中声明的门限值
D	系统缺省属性集	T_p	双线性对运算所需时间复杂度
T	签名所需 AA_k 组成的集合	T_e	倍点运算所需时间复杂度
A	签名者拥有属性集合	–	–

Table 2 Efficiency comparison of ABRS schemes

表 2 ABRS 方案效率比较

方案	密钥长度/bit	签名长度/bit	签名计算量	验证计算量
文献[13]中方案	$2(\|A\|+d-1)\|G_1\|$	$3d\|G_1\|$	$5dT_e$	dT_e+3dT_p
文献[14]中方案	$2\|A\|\|G_1\|$	$3\|A\|\|G_1\|$	$(2\|A\|+1)T_e$	$3dT_p+(d+1)T_e$
文献[16]中方案	$(\|A\|+d+1)\|G_1\|$	$2\|G_1\|$	$4T_e$	$3T_p+1T_e$
文献[17]中方案	$2(\|A\|+d-1)\|G_1\|$	$(\|B\|+d-t+2)\|G_1\|$	$(2\|B\|+4d-2t+2)T_e$	$(\|B\|+d-t+2)T_p$
文献[18]中方案	$(\|A\|+d)\|G_1\|$	$3\|G_1\|$	$5T_e$	$4T_p+1T_e$
文献[19]中方案	$(\|A\|+d-1)(\|B\|+d-t)\|G_1\|$	$3\|G_1\|$	$(2d+4)T_e$	$3T_p$
文献[20]中方案	$(\|A\|+d)\|G_1\|$	$(\|B\|+d-t+2)\|G_1\|$	$(\|B\|+2d-2t+2)T_e$	$(\|B\|+d-t+2)T_p+(\|B\|+d-t)T_e$
文献[21]中方案	$(2\|A\|+\|T\|^2)\|G_1\|$	$(\|B\|+2)\|G_1\|$	$(2\|B\|+2d+2)T_e$	$(\|B\|+2)T_p$
本文方案	$(\|A\|+d-1+\|T\|)\|G_1\|$	$(\|B\|+d-t+3)\|G_1\|$	$(2\|B\|+4d-2t+4+\|T\|)T_e$	$(\|B\|+d-t+3)T_p$

Table 3 Performance comparison of ABRS schemes

表 3 ABRS 方案性能比较

方案	不可伪造性	匿名性	抗合谋攻击性	签名门限可变	属性密钥托管问题	批验证	安全模型
文献[13]中方案	CDH	弱匿名性	×	√	存在	×	标准模型
文献[14]中方案	CDH	强匿名性	×	×	存在	×	标准模型
文献[16]中方案	SDH	弱匿名性	×	×	存在	×	标准模型
文献[17]中方案	CDH	强匿名性	×	√	存在	×	标准模型#
文献[18]中方案	CDH	弱匿名性	×	×	存在	×	标准模型
文献[19]中方案	q-DHE	强匿名性	×	√	存在	×	标准模型
文献[20]中方案	CDH	计算匿名性	√	√	存在	×	ROM
文献[21]中方案	CDH**	强匿名性	√#	×	不存在	√	ROM
本文方案	CDH	强匿名性	√	√	不存在	√	ROM

注:×代表不支持该性能,√代表支持该性能,**代表形式化证明不完整,#代表未给出形式化证明.

综合表 2 和表 3 的结果可知,虽然文献[20,21]中的方案和本文方案的形式化安全证明均基于随机预言机模型,但是目前仅有这 3 个方案可以抵抗合谋攻击,因此下面主要针对这 3 个方案进行分析.当$|T|=1$时,即本文所提出的方案与文献[20]中的方案均使用单属性授权机构为相应属性分发密钥,此时,本方案密钥长度与文献[20]中的方案相等,签名长度仅比文献[20]中的方案多 $1|G_1|$bit,虽然就签名效率而言本方案不占优势,但是由于本文提出了一种高效地批验证方法,因此验证效率很高,且即便仅对单个签名进行验证,本方案的计算量也比文献[20]中的方案少$(|B|+d-t)T_e-1T_p$;同时,本方案匿名性明显优于文献[20]中的方案,且当$|T|\neq 1$ 时,本方案可以解决文献[20]中的方案存在的属性密钥托管问题.

若不考虑动态门限的实现,本方案签名长度和验证计算量与文献[21]中的方案相差不大,比文献[21]中的方案分别多 $1|G_1|$bit 和 $1T_p$,虽然签名计算量比文献[21]中的方案高$(2+|T|)T_e$,但是文献[21]中的方案引入了密钥匿名分发协议,因此就密钥长度而言,比本方案长$(|A|-|T|+|T|^2)|G_1|$bit,导致其 AA 与用户之间的通信代价很大.此外,该方案只能在单属性授权机构,即存在的属性密钥托管问题的安全模型下,被证明具备匿名性和不可伪造性,并未给出抗合谋攻击的形式化安全证明.而本文方案可以在克服密钥长度过长这一前提下,在假设存在 $l-1$ 个不可信授权属性机构的安全模型下,被证明同时具备无条件强匿名性、不可伪造性和抗合谋攻击性.

上述分析表明,综合考虑安全性和效率两方面性能,本文方案较现有方案具有更大优势.

6 总 结

本文针对现有基于属性的门限环签名方案无法同时具备无条件强匿名性和抗合谋攻击性,并且存在属性密钥托管、验证效率低、签名门限固定等问题,通过采用分布式密钥生成协议以及在属性密钥和签名中分别嵌入用户身份标识和用户身份模糊因子的方式,提出了一个分布式无中心授权的属性基可变门限环签名方案.该方案同时具备无条件强匿名性和抗合谋攻击性.在假设存在 $l-1$ 个不可信属性授权机构的前提下,该方案被证明在适应性选择消息和断言攻击下是存在性不可伪造的,并且能够抵抗由拥有互补属性集合的恶意用户发动合谋攻击.另外,还提出了一种适用于本方案的批验证算法,有效地提高了验证效率.

References:

[1] Sahai A, Waters B. Fuzzy identity-based encryption. In: Proc. of the 24th Annual Int'l Conf. on Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2005. 457−473. [doi: 10.1007/11426639_27]

[2] Attrapadung N, Libert B, De Panafieu E. Expressive key-policy attribute-based encryption with constant-size ciphertexts. In: Proc. of the 14th Int'l Conf. on Practice and Theory in Public Key Cryptography (PKC 2011). Berlin: Springer-Verlag, 2011. 90−108. [doi: 10.1007/978-3-642-19379-8_6]

[3] Han F, Qin J, Zhao H, Hu J. A general transformation from KP-ABE to searchable encryption. Future Generation Computing Systems, 2014,30(1):107−115. [doi: 10.1016/j.future.2013.09.013]

[4] Rouselakis Y, Waters B. Practical constructions and new proof methods for large universe attribute-based encryption. In: Proc. of the 2013 ACM SIGSAC Conf. on Computer and Communications Security. Berlin: ACM Press, 2013. 463−474. [doi: 10.1145/2508859.2516672]

[5] Bethencourt J, Sahai A, Waters B. Ciphertext-Policy attribute-based encryption. In: Proc. of the 2007 IEEE Symp. on Security and Privacy (SP 2007). Berkeley: IEEE Press, 2007. 321−334. [doi: 10.1109/SP.2007.11]

[6] Goyal V, Jain A, *et al*. Bounded ciphertext policy attribute based encryption. In: Proc. of the 35th Int'l Colloquium on Automata, Languages and Programming. Berlin: Springer-Verlag, 2008. 579−591. [doi: 10.1007/978-3-540-70583-3_47]

[7] Hong H, Sun Z, Liu X. A key-insulated CP-ABE with key exposure accountability for secure data sharing in the cloud. KSII Trans. on Internet and Information Systems, 2016,10(5):2394−2406. [doi: 10.3837/tiis.2016.05.024]

[8] Burnett A, Duffy A, Dowling T. A biometric identity based signature scheme. 2004. http://eprint.iacr.org/2004/176

[9] Guo SQ, Zeng YP. Attribute-Based signature scheme. In: Proc. of the 2nd Int'l Conf. on Information Security and Assurance. Busan. IEEE Press, 2008. 509−511. [doi: 10.1109/ISA.2008.111]

[10] Maji H, Prabhakaran M, Rosulek M. Attribute-Based signatures: Achieving attribute privacy and collusion-resistance. 2008. http://eprint.iacr.org/2008/328

[11] Rivest R, Shamir A, Tauman Y. How to leak a secret. In: Proc. of the Advances in Cryptology (ASIACRYPT 2001). Gold Coast: Springer-Verlag, 2001. 552−565. [doi: 10.1007/3-540-45682-1_32]

[12] Li J, Kim K. Attribute-Based ring signatures. 2008. http://eprint.iacr.org/2008/394

[13] Li J, Kim K. Hidden attribute-based signatures without anonymity revocation. Information Sciences, 2010,180(9):1681−1689. [doi: http://dx.doi.org/10.1016/j.ins.2010.01.008]

[14] Shahandashti SF, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems. In: Proc. of the Cryptology-Africacrypt 2009, Vol.5580. Berlin: Springer-Verlag, 2009. 198−216. [doi: 10.1007/978-3-642-02384-2_13]

[15] Wang WQ, Chen SZ. An efficient attribute-based ring signature scheme. In: Proc. of the Int'l Forum on Computer Science-Technology and Applications, Vol.1. Chongqing: IEEE Press, 2009. 147−150. [doi: 10.1109/IFCSTA.2009.43]

[16] Toluee R, Asaar MR, Salmasizadeh M. Attribute-Based ring signatures: Security analysis and a new construction. In: Proc. of the 10th Int'l ISC Conf. on Information Security and Cryptology (ISCISC). IEEE Press, 2014. 1−6. [doi: 10.1109/ISCISC.2013.6767342]

[17] Li J, Au MH, Susilo W, *et al*. Attribute-Based signatures and its applications. In: Proc. of the 5th ACM Symp. on Information, Computer and Communications Security (ASIACCS 2010). Beijing: ACM Press, 2010. 978−987.

[18] Wang WQ, Chen SZ. Attribute-Based ring signature scheme with constant-size signature. IET Information Security, 2010,4(2):104−110. [doi: 10.1049/iet-ifs.2009.0189]

[19] Ge AJ, Ma CG, Zhang ZF. Attribute-Based signature scheme with constant size signature in the standard model. Journal of IET Information Security, 2012,6(2):47−54. [doi: 10.1049/iet-ifs.2011.0094]

[20] Chen Z, Zhang WF, Wang XM. Attribute-Based alterable threshold ring signature scheme with conspiracy attack immunity. Journal on Communications, 2015,36(12):212−222 (in Chinese with English abstract).

[21] Li J, Chen XF, Huang XY. New attribute-based authentication and its application in anonymous cloud access service. Int'l Journal of Web and Grid Services, 2015,11(1):125−141. [doi: http://dx.doi.org/10.1504/IJWGS.2015.067161]

[22] Chase M. Multi-Authority attribute based encryption. In: Proc. of the 4th Theory of Cryptography Conf. Berlin: Springer-Verlag, 2007. 515−534. [doi: 10.1007/978-3-540-70936-7_28]

[23] Chase M, Chow S. Improving privacy and security in multi-authority attribute-based encryption, In: Proc. of the 16th ACM Conf. on Computer and Communications Security. Chicago: ACM Press, 2009. 121−130. [doi: 10.1145/1653662.1653678]

[24] Lin H, Cao ZF, Liang XH, *et al*. Secure threshold multi-authority attribute based encryption without a central authority. Journal of Information Sciences, 2010,180(13):2618−2632. [doi: http://doi.org/10.1016/j.ins.2010.03.004]

[25] Sun CX, Ma WP, Chen HF. Provable secure multi-authority attribute-based signature without a central authority. Journal of University of Electronic Science and Technology of China, 2012,41(4):552−556 (in Chinese with English abstract).

[26] Ferrara A, Green M, Hohenberger S, Pedersen M. Practical short signature batch verification. 2008. http://eprint.iacr.org/2008/015

附中文参考文献:

[20] 陈桢,张文芳,王小敏.基于属性的抗合谋攻击可变门限环签名方案.通信学报,2015,36(12):212−222.

[25] 孙昌霞,马文平,陈和风.可证明安全的无中心授权的多授权属性签名.电子科技大学学报,2012,41(4):552−556.

刘旭东(1990－),男,内蒙古呼和浩特人,硕士,主要研究领域为基于属性密码的密码体制,环签名.

张文芳(1978－),女,博士,副教授,主要研究领域为密码学,信息安全,分布式系统认证,密钥协商.

王小敏(1974－),男,博士,教授,博士生导师,主要研究领域为信息安全,轨道交通信息系统安全.