软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2012,23(9):2449−2464 [doi: 10.3724/SP.J.1001.2012.04172]

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

一个可追踪身份的基于属性签名方案*

张秋璞[1,2], 徐 震[3+], 叶顶锋[1,2]

[1](信息安全国家重点实验室(中国科学院 研究生院),北京 100049)

[2](中国科学院 数据与通信保护研究教育中心,北京 100049)

[3](信息安全国家重点实验室(中国科学院 软件研究所),北京 100190)

Identity Traceable Attribute-Based Signature Scheme

ZHANG Qiu-Pu[1,2], XU Zhen[3+], YE Ding-Feng[1,2]

[1](State Key Laboratory of Information Security (Graduate University, The Chinese Academy of Sciences), Beijing 100049, China)

[2](The Data Assurance and Communication Security Research Center, The Chinese Academy of Sciences, Beijing 100049, China)

[3](State Key Laboratory of Information Security (Institute of Software, The Chinese Academy of Sciences), Beijing 100190, China)

+ Corresponding author: E-mail: xuzhen@is.iscas.ac.cn

Zhang QP, Xu Z, Ye DF. Identity traceable attribute-based signature scheme. *Journal of Software*, 2012, 23(9):2449−2464 (in Chinese). http://www.jos.org.cn/1000-9825/4172.htm

Abstract: In an attribute-based signature (ABS) scheme, the signer's identity keeps anonymous. To prevent the signer from abusing this property, Escala, Herranz, and Morillo proposed an identity traceable attribute-based signature scheme (EHM-ABS). Their scheme used an automorphic signature, and applied the non-interactive witness indistinguishable (NIWI) proofs many times. Inspired by Boyen, and Waters' identity-based compact group signature scheme, the study presents an identity traceable ABS scheme in the standard model. When issuing the attribute private key, the signer's identity is embedded. By using the NIWI proof of encrypting each bit of identity, this scheme achieves the traceability. To compare with EHM-ABS, this scheme reduces the number of applying the NIWI proofs when the order of the claimed attributes set is bigger than the quarter of the bit length of identity, and do not need to use automorphic signature. The security of this proposed scheme is based on the subgroup dicision and the computational diffie-Hellman assumptions.

Key words: attribute-based signature; traceability; unlinkability; non-frameability; bilinear pairings

摘 要: 基于属性的签名(attribute-based signature,简称 ABS)方案可以隐藏签名者的身份.为了防止签名者滥用签名,Escala,Herranz 和 Morillo 提出了一种可追踪签名者身份的基于属性签名方案(EHM-ABS),其中使用了自同构签名,并多次使用了非交互证据不可区分(non-interactive witness indistinguishable,简称 NIWI)的证明.在 Boyen 和 Waters 的基于 ID 的紧致群签名方案的基础上,在标准模型下提出了一种可追踪身份的 ABS 方案.在颁发属性私钥时嵌入签名者的身份,并对身份使用比特加密的 NIWI 证明来实现可追踪性.与 EHM-ABS 相比,当声明的属性集合的阶大于 ID 的比特长度的 1/4 时,该方案减少了使用 NIWI 证明的次数,且无须使用自同构签名.该方案的安全性基于子群判定假设和 CDH 假设.

关键词: 基于属性签名;可追踪性;不可联系性;不可陷害性;双线性对

* 收稿时间: 2011-07-04; 定稿时间: 2011-12-21

中图法分类号: TP309 文献标识码: A

自从 Sahai 和 Waters 提出基于属性的加密(attribute-based encryption,简称 ABE)方案[1]以来,基于属性的密码体系成为最近研究的热点之一,其访问控制权限依赖于指定的属性集合与访问策略是否匹配.Goyal 等人在文献[2]中将 key-policy ABE 的概念作了形式化的定义:访问策略和私钥绑定,属性和密文绑定.Bethencourt 等人在文献[3]中提出了 ciphertext-policy ABE 的概念:访问策略和密文绑定,属性和私钥绑定.Ostrovsky 等人提出了支持非单调的访问结构的 ABE 方案[4],其中可以支持负的访问条款.在文献[2−4]中,使用访问树(access tree)自顶向下(top-down)颁发属性私钥.在上述 ABE 方案中,都使用了线性秘密共享方案(linear secret sharing scheme,简称 LSSS),Cheung 和 Newport 则提出了不使用线性秘密共享的 ABE 方案[5].文献[6]则对近年来的 ABE 方案做了较完整的总结.

除了 ABE 之外,大量的基于属性的签名(attribute-based signature,简称 ABS)方案也被提出.在基于属性的签名方案中,PKG(private key generator)颁发属性私钥给用户.在对消息签名时,签名者使用某一签名策略对消息签名,验证者则可以验证该签名是否满足签名者声明的签名策略.在文献[7]中,Yang 等人提出了模糊的基于身份的签名(fuzzy identity-based signature)方案,该方案可以看作是基于属性的签名方案.文献[8]提出了基于属性的群签名方案,其中使用了自底向上(bottom-up)的方式来构造访问树,并使用了哑属性.在文献[9,10]提出的 ABS 方案中,需要对每一个属性单独签名,其签名数据太长.Li 等人在文献[11]中对文献[10]中的 ABS 方案提出了一种改进,在签名时,将多个属性分量的签名数据聚合到一起.文献[10,11]中都使用了哑属性.文献[12]提出了使用门限的基于属性的签密方案,其中使用了与文献[11]类似的聚合多个属性分量运算的技术.Maji 等人在文献[13]中给出了一般的基于属性的签名方案的构造方法.

基于属性的签名方案具有匿名性,可以隐藏签名者的身份,但是签名者可以利用这一特性滥用签名.可追踪身份的基于属性的签名方案则可以防止签名者滥用签名,给定一个合法签名,PKG 可以使用追踪密钥确定签名者的身份;但是对于不知道追踪密钥的其他验证者,则无法确认多个使用相同签名策略的签名是否是由同一签名者签署的.在不需要完全匿名性的应用场景,可追踪身份的基于属性签名方案非常具有吸引力.

Escala,Herranz 和 Morillo 在文献[14]中给出了可由 PKG 追踪签名者身份的基于属性签名方案(EHM-ABS),其中,对是否拥有某一属性使用比特加密的非交互证据不可区分(non-interactive witness indistinguishable,简称 NIWI)的证明[15],用以保证敌手无法区分签名者是否拥有该属性;同时,使用了自同构签名(automorphic signature)[16],用于保证签名的可追踪性(traceability)和不可陷害性(non-frameability).另外,还使用 Groth 和 Sahai 的关于双线性对群中等式可满足性的 NIWI 证明[17],用于保证签名的不可联系性.

在群签名[18]中,允许群中的成员代表群来进行签名,只有管理员可以揭露群中签名者的身份.在文献[19]中,Bellare 等人通过使用非交互零知识证明(non-interactive zero knowledge,简称 NIZK),可以将任意的签名方案转换成群签名方案.在文献[20]中,Boyen 和 Waters 利用 BGN 密码体系[21]对文献[19]的效率做了改进.可追踪身份的基于属性签名和群签名有类似之处,二者都可以隐藏签名者的身份,且在一定条件下都可以追踪签名者身份.二者的区别是基于属性签名并不代表群,而是声明其拥有的属性集合满足某一签名策略,从而隐藏了签名者的身份.

本文在标准模型下,提出了一种新的构造可追踪身份的基于属性签名方案的方法.将用户 ID 嵌入到属性私钥中,然后利用身份的比特加密的 NIWI 证明达到可追踪性和不可联系性,从而构造出可追踪身份的 ABS 方案.

我们首先使用文献[11]的思想,构造门限的带 ID 的基于属性签名(threshold-ID-ABS)方案.

设门限为 d,用户 u 拥有属性集合 Ω,在生成属性私钥时,将 ID 信息 u 嵌入属性私钥中,在签名时,签名者选取属性集合 $\gamma\subseteq\Omega$,其中,$|\gamma|\geq d$.同时选取任意的属性集合 γ',其中 $\gamma\cap\gamma'=\varnothing$,签名者声明至少拥有 $\gamma\cup\gamma'$ 中的 d 个属性,而敌手无法确认签名者具体拥有哪些属性.与文献[11]相比,我们的方案没有使用哑属性.在 Threshold-ID-ABS 的基础上,本文利用文献[20]的思想,构造门限的可追踪身份的基于属性签名(threshold-traceable-ABS)方案,其中使用了 BGN 密码体系[21]加密用户的身份 u,并提供 NIWI 证明[15],用于保证 ID 的不可联系性和可追踪性(PKG

可追踪 ID 身份).在 Threshold-Traceable-ABS 方案的基础上,我们进一步给出两个通用的可追踪身份的基于属性签名(traceable-ABS)方案:一个基于访问树结构,其中除了需要使用属性私钥树[2−4],还构造了签名策略树,该方案适用于由任意的 AND,OR 与门限组成的单调的访问结构;另一个则适用于可由任意线性秘密共享方案表达的访问结构.我们方案的安全性可规约到子群判定假设和 CDH 假设.

与文献[14]相比,本文不需要使用自同构签名[16],本文是对用户 ID 的每一个比特使用 NIWI 证明,而文献[14]的 EHM-ABS 则是对声明的属性集合中的每一个属性使用 NIWI 证明;同时,EHM-ABS 比我们的方案还多使用了两个 Groth 和 Sahai 的关于双线性对群中等式可满足性的 NIWI 证明(GS-NIWI)[17].在通用的签名策略下,EHM-ABS 还需要对声明的属性集合中的分量对应的签名策略值做 NIWI 证明,而我们的方案则无需对签名策略做 NIWI 证明.设声明的属性集合的阶为 n,ID 的比特长度为 n_u,在通用的签名策略下,EHM-ABS 做 NIWI 证明的次数为 $4n$,而我们的方案做 NIWI 证明的次数为 n_u.即,我们的方案做 NIWI 证明的次数仅依赖于 ID 的比特长度,而与属性集合及签名策略无关.与 EHM-ABS 相比,当声明的属性集合的阶大于 ID 的比特长度的 1/4 时,我们的方案减少了使用 NIWI 证明的次数.

本文第 1 节介绍相关的预备知识和复杂性假设.第 2 节给出可追踪身份的基于属性签名方案的形式化定义和安全模型.第 3 节给出 Threshold-ID-ABS 方案.第 4 节给出 Threshold-Traceable-ABS 方案及其安全性证明.第 5 节将 Threshold-Traceable-ABS 推广到通用的 Traceable-ABS 方案.第 6 节总结全文.

1 预备知识

1.1 双线性对

设 G 和 G_T 是两个阶为 n 的乘法循环群,其中,n 可以为素数或合数[21].g 为 G 的生成元,双线性对 $e:G\times G\to G_T$ 是一个具有如下性质的双线性映射:

(1) 双线性:对于任意的 $u,v\in G,a,b\in Z_n$,有 $e(u^a,v^b)=e(u,v)^{ab}$;

(2) $e(g,g)$是 G_T 的生成元.

一般的双线性对要求 G 和 G_T 是素数阶的.在本文使用的双线性对中,乘法循环群除了可以是素数阶的,还可以是合数(两个大素数之积)阶的.

1.2 子群判定假设

子群判定(subgroup dicision,简称 SD)假设[21]:设 p,q 为两个大素数,$n=pq$,G 是阶为 n 的循环群,G_p,G_q 分别表示 G 的阶为 p,q 的子群.子群判定假设是指随机选择 $h\in G$ 或 $h\in G_p$,难以判定 $h\in G_p$ 是否成立.

在我们的方案中,为了保证签名的不可联系性,使用该假设构造非交互证据不可区分的证明.

1.3 CDH假设

计算性 Diffie-Hellman(the computational diffie-Hellman,简称 CDH)假设:G 为阶为 p 的循环群,g 为 G 的生成元,对于$\alpha,\beta\in_R Z_p$,CDH 假设是指,给定(g^α,g^β),不存在多项式有界的算法,能够以不可忽略的概率计算出 $g^{\alpha\beta}$.

在本文中,将在素数阶的子群中使用 CDH 假设来证明签名的存在不可伪造性.

1.4 BGN密码体系

Boneh,Goh 和 Nissi 在文献[21]中介绍了一种密码体系,该密码体系是基于子群判定假设的,本文使用了该密码体系的比特加密形式.

- KeyGen:设 p,q 为两个大素数,$n=pq$.G 和 G_T 是两个阶为 n 的乘法循环群,$e:G\times G\to G_T$ 为双线性映射.G_p,G_q 分别为 G 的阶为 p,q 的子群.随机选取 G 的生成元 g 以及 G_q 的生成元 h.私钥为 $D=q$,公钥为 $PK=(n,G,G_T,e,g,h)$.
- Encrypt:加密 1 个比特 $m\in\{0,1\}$,随机选取 $r\in Z_n$,密文为 $c=g^m h^r$.
- Decrypt:为了解密密文 c,计算 c^q.如果 $c^q=g^0$,则输出 0;如果 $c^q=g^q$,则输出 1;如果是其他值,则返回失败.

其中,由于 h 是 G_q 的生成元,即 h 的阶为 q,则有 $c^q=(g^m h^r)^q=(g^q)^m$.

在我们的方案中,使用 BGN 密码体系构造用户身份 u 的比特加密的 NIWI 证明.

1.5 比特加密的非交互证据不可区分证明

在文献[15]中,Groth,Ostrovsky 和 Sahai 介绍了如何使用 BGN 密码体系为任何一个 NP 语言构造一个有效的统计零知识证明系统.在本文中,我们使用其中的关于比特加密的 NIWI 证明.

- Common reference string:基本同第 1.4 节中的 KeyGen,公共参考串(common reference string,简称 CRS)为 $CRS=(n,G,G_T,e,g,h)$.
- Statement:基本同第 1.4 节中的 Encrypt.对 $m\in\{0,1\}$,声明为 $c=g^m h^r$,其中,$r\in Z_n$.
- Proof:输入为(CRS,c,m,r).对声明 $c=g^m h^r$,其 NIWI 证据为$\pi=(g^{2m-1}h^r)^r$.
- Verify:输入为(CRS,c,π).验证 $e(c,c/g)=e(h,\pi)$成立.

由文献[15]可知,该证明是正确的、完备的,且是证据不可区分的.文献[14,20]同样使用了该 NIWI 证明.

1.6 访问结构

访问结构(access structure)[22]:设 $\Psi=\{att_1,att_2,\ldots,att_n\}$为属性集合,$\Phi$是 Ψ的一些子集的非空集合,即 $\Phi\subseteq 2^{\Psi}\setminus\{\varnothing\}$,且$\Phi$满足单调性:如果 $A_1\in\Phi$,且 $A_1\subseteq A_2$,则 $A_2\in\Phi$.那么,Φ是关于 Ψ的满足单调性的访问结构.

2 形式化定义和安全模型

本文采用文献[14]给出的形式化定义,并做了简单修改.基于属性签名方案使用签名策略$(\Psi,term,\Phi)$,其中,Ψ为某一属性集合,Φ为满足条件 $term$ 的 Ψ的一些子集的非空集合,即 $\Phi\subseteq 2^{\Psi}\setminus\{\varnothing\}$,且$\Phi$具有单调性.设签名者的属性集合为$\Omega$,一个有效的签名意味着签名者拥有$\Phi$中某一元素($\Phi$的元素为属性集合)中的全部属性,即存在属性集合$\gamma\subseteq\Omega$,满足$\gamma\in\Phi$.签名策略的典型例子为门限策略,设 Ψ为包含 n 个属性的集合,门限为 d,则$\Phi=\{A\subseteq\Psi:|A|\geqslant d\}$.我们用$(\Psi,d,\Phi)$表示门限策略,其含义为签名者至少拥有属性集合 Ψ中的 d 个属性.

2.1 形式化定义

一个可追踪身份的基于属性签名方案由以下算法组成.由于需要追踪身份,因此显式使用了用户的身份 u:

- Setup:给定安全参数,生成公共参数 PK、主密钥 MK 和追踪密钥 TK.
- KeyGen:该函数的输入为身份 u、属性集合Ω、公共参数 PK 和主密钥 MK,输出私钥 $D_{u,\Omega}$.
- Sign:签名者使用私钥 $D_{u,\Omega}$对消息 m 签名,签名策略为$(\Psi,term,\Phi)$,输出签名数据σ.
- Verify:该函数的输入为消息 m,签名策略$(\Psi,term,\Phi)$和签名σ,返回是否接受该签名.
- Trace:该函数的输入为签名σ和追踪密钥 TK,返回签名者的身份 u.

2.2 不可伪造性

在选择签名策略和选择消息攻击模型下,基于属性的签名方案的存在不可伪造性是指:如果不知道签名者的私钥,且没有询问过该签名者对消息 m 关于签名策略$(\Psi,term,\Phi)$做的签名,则敌手不能伪造该签名者的关于签名策略$(\Psi,term,\Phi)$的消息签名对(m,σ).对于该安全模型,用户 u 是适应性的.

定义 1. 一个基于属性的签名方案,在选择签名策略和选择消息攻击模型下是存在不可伪造的,当且仅当不存在多项式有界的敌手,在下述游戏中有不可忽略的优势:

- Init:首先敌手声明他将要挑战的签名策略$(\Psi^*,term^*,\Phi^*)$.
- Setup:挑战者生成公共参数 PK、主密钥 MK 和追踪密钥 TK,将公共参数发送给敌手.
- Query:敌手可进行多项式界次数的询问:KeyGen 询问、Sign 询问和 Trace 询问.其中,在对用户 u、属性集合Ω进行 KeyGen 询问时,要求不存在属性集合$\gamma\subseteq\Omega$,使$\gamma\in\Phi^*$.即,Ω不满足签名策略$(\Psi^*,term^*,\Phi^*)$.
- Forge:敌手输出伪造的关于用户 u^*、消息 m^*、签名策略$(\Psi^*,term^*,\Phi^*)$的签名σ^*.要求敌手没有询问过 u^*的私钥,且敌手没有对用户 u^*询问过关于消息 m^*、签名策略$(\Psi^*,term^*,\Phi^*)$的签名.若σ^*能通过签名

验证,则敌手获胜.

敌手在上述游戏中的优势定义为敌手赢得上述游戏的概率.

2.3 不可联系性

不可联系性(unlinkability)是指给出两个使用同一签名策略的有效签名,在不知道追踪密钥的前提下,即使敌手知道签名者的私钥,敌手也无法区分这两个签名是否是由同一个签名者签署的.

定义 2. 一个基于属性的签名方案,在选择签名策略和选择消息攻击模型下是不可联系的,当且仅当不存在多项式有界的敌手,在下述游戏中有不可忽略的优势:

- Init:首先,敌手声明他将要挑战的签名策略为$(\Psi^*,term^*,\Phi^*)$.
- Setup:同定义 1 的 Setup.
- Phase 1:同定义 1 的 Query.
- Challenge:敌手选择用户 u_0(其属性集合为Ω_0),要求存在属性集合$\gamma\subseteq\Omega_0$,满足$(\Psi^*,term^*,\Phi^*)$.敌手选择$u_1\neq u_0$,选择$\Omega_1\in\Phi^*$.敌手对$(u_0,\Omega_0),(u_1,\Omega_1)$询问 KeyGen.挑战者任选 $b\in\{0,1\}$,生成关于(u_b,Ω_b)、消息 m、$(\Psi^*,term^*,\Phi^*)$的签名σ^*,并将$\sigma^*,(u_0,\Omega_0),(u_1,\Omega_1)$发送给敌手.
- Phase 2:基本同 Phase 1,除了敌手不能对σ^*做 Trace 询问.
- Guess:敌手输出对 b 的猜测 b'.若 $b'=b$,则敌手获胜.

敌手在上述游戏中的优势定义为$|2Pr[b'=b]-1|$.

2.4 不可陷害性

不可陷害性(non-frameability)是指对可以做合谋攻击的敌手,即使敌手知道追踪密钥 TK,敌手也无法伪造一个有效签名,对该签名做 Trace 运算,得到 u'.其中,u'没有参与合谋攻击.

定义 3. 一个基于属性的签名方案,在选择签名策略和选择消息攻击模型下是不可陷害的,当且仅当不存在多项式有界的敌手,在下述游戏中有不可忽略的优势:

- Init:首先,敌手声明他将要挑战的签名策略$(\Psi^*,term^*,\Phi^*)$.
- Setup:基本同定义 1 的 Setup,且敌手拥有追踪密钥 TK.
- Query:敌手可以对 KeyGen,Sign 进行多项式界次数的询问.此时,敌手不需要询问 Trace,因为敌手拥有追踪密钥 TK.令 U_{KeyGen} 表示做过 KeyGen 询问的身份 u 的集合.
- Forge:敌手输出对消息 m^*伪造的签名σ^*,其中,签名策略为$(\Psi^*,term^*,\Phi^*)$.若敌手伪造的σ^*能通过签名验证,且对该σ^*做 Trace 运算,得到 $u'\notin U_{\mathrm{KeyGen}}$,则敌手获胜.

敌手在上述游戏中的优势定义为敌手赢得上述游戏的概率.

3 门限的带 ID 的基于属性签名方案

本节给出一个门限的带 ID 的基于属性签名方案,简称 Threshold-ID-ABS,该方案是文献[11]中门限的基于属性签名方案的变形.在此基础上,第 4 节给出门限的可追踪身份的基于属性签名方案.

3.1 方案构造

Setup:设 p 为大素数.G 和 G_T 是两个阶为 p 的乘法循环群,$e:G\times G\to G_T$ 为双线性映射.设 $S\subseteq Z_p$,且 $i\in S$,定义拉格朗日系数为 $\Delta_{i,S}(x)=\prod_{j\in S,j\neq i}\frac{x-j}{i-j}$.

设系统支持的属性集合为 Z_p^*.定义 $K=\{1,\ldots,k,k+1\}$,对 $i\in K$,随机选取 $t_i\in G$,定义 $T(X)=g_2^{X^k}\prod_{i=1}^{k+1}t_i^{\Delta_{i,K}(X)}$.

定义门限为 d,即用户至少有 d 个属性才可以签名.PKG 随机选择 G 的生成元 g,并随机选择 $\alpha\in Z_p^*$.令 $g_1=g^\alpha$,同时随机选择 G 中的元素 g_2.此外,随机选择 $u',m'\in G$,以及长度分别为 n_u 与 n_m 的向量 $U=\{u_i\}$与 $M=\{m_i\}$,其中,$u_i,m_i\in_R G$.则公共参数为 $PK=(d,g,g_1,g_2,t_1,\ldots,t_{k+1},e,u',U,m',M)$,主密钥 MK 为 α.

在本文中,设用户 u 用长为 n_u 的二进制字符串表示,令 $u[i]$表示 u 的第 i 个比特,定义 $U\subset\{1,\ldots,n_u\}$为满足 $u[i]=1$ 的序号 i 的集合.定义 $W(u)=u'\prod_{i\in U}u_i$.设消息 m 是长度为 n_m 的比特串,令 $m[i]$表示 m 的第 i 个比特,定义 $M\subset\{1,\ldots,n_m\}$为满足 $m[i]=1$ 的序号 i 的集合.定义 $V(m)=m'\prod_{i\in M}m_i$.

KeyGen:该函数的输入为用户 u 及其对应的属性集合Ω、主密钥 MK 和公共参数 PK.

首先,PKG 随机选择一个 d–1 次多项式 $q(x)$,其中,$q(0)=\alpha$.对每个用户 u,随机选取唯一的 $s\in Z_p$,计算 $D_u=g^s$.

对于属性 $i\in\Omega$,PKG 随机选取唯一的 $r_i\in Z_p$,计算 $D_{i,1}=g^{r_i}$,$D_{i,2}=g_2^{q(i)}\cdot T(i)^{r_i}\cdot W(u)^s$.

属性私钥为 $D_{u,\Omega}=(D_u,\{(D_{i,1},D_{i,2})_{i\in\Omega}\})$.

Sign:用户 u 对消息 m 签名,签名者随机选择$\gamma\subseteq\Omega$,其中,$|\gamma|\geqslant d$.再随机选择属性集合γ',其中,$\gamma\cap\gamma'=\varnothing$,令 $\Psi=\gamma\cup\gamma'$,则签名策略为(Ψ,d,Φ),即签名者至少拥有属性集合 Ψ中的 d 个属性.签名者执行如下步骤:

(1) 令$\delta_1=D_u=g^s$;

(2) 随机选取 $s_2\in Z_p$,计算 $\delta_2=g^{s_2}$;

(3) 对所有的 $i\in\Psi$,随机选取 $r_i'\in Z_p$,当 $i\in\gamma$时,计算 $\delta_{3,i}=D_{i,1}^{\Delta_{i,\gamma}(0)}\cdot g^{r_i'}=g^{r_i\Delta_{i,\gamma}(0)+r_i'}$;当 $i\in\gamma'$时,计算 $\delta_{3,i}=g^{r_i'}$;

(4) 计算 $\delta_4=V(m)^{s_2}\cdot\prod_{i\in\gamma}D_{i,2}^{\Delta_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}$.

最终输出签名$\delta=(\delta_1,\delta_2,\{\delta_{3,i}\}_{i\in\Psi},\delta_4)$.

Verify:该函数的输入为δ,返回是否接受签名.验证者验证下式是否成立:若成立则接受签名,否则拒绝签名.

$$\frac{e(\delta_4,g)}{(\prod_{i\in\Psi}e(T(i),\delta_{3,i}))\cdot e(W(u),\delta_1)\cdot e(V(m),\delta_2)}=e(g_1,g_2).$$

3.2 正确性

对于常数函数 $f(\cdot)=1$,有 $f(0)=\sum_{i\in\gamma}(f(i)\cdot\Delta_{i,\gamma}(0))=\sum_{i\in\gamma}\Delta_{i,\gamma}(0)=1$.因此有,

$$\begin{aligned}\delta_4&=V(m)^{s_2}\cdot\prod_{i\in\gamma}D_{i,2}^{\Delta_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\&=V(m)^{s_2}\cdot\prod_{i\in\gamma}(g_2^{q(i)}\cdot T(i)^{r_i}\cdot W(u)^s)^{\Delta_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\&=g_2^{\alpha}\cdot V(m)^{s_2}\cdot W(u)^s\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'},\end{aligned}$$

$$\frac{e(\delta_4,g)}{(\prod_{i\in\Psi}e(T(i),\delta_{3,i}))\cdot e(W(u),\delta_1)\cdot e(V(m),\delta_2)}=$$

$$\frac{e(g_2^{\alpha}\cdot V(m)^{s_2}\cdot W(u)^s\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'},g)}{(\prod_{i\in\gamma}e(T(i),g^{r_i\Delta_{i,\gamma}(0)+r_i'}))\cdot(\prod_{i\in\gamma'}e(T(i),g^{r_i'}))\cdot e(W(u),g^s)\cdot e(V(m),g^{s_2})}=e(g_1,g_2).$$

3.3 不可伪造性

在选择签名策略和选择消息攻击模型下,该签名方案的存在不可伪造性可以规约到标准的 CDH 假设.其安全性证明与文献[11]中的证明以及本文中后续给出的 Threshold-Traceable-ABS 方案的存在不可伪造性证明非常类似,在此省略证明过程.

4 门限的可追踪身份的基于属性签名方案

本节在 Threshold-ID-ABS 方案的基础上,给出门限的可追踪身份的属性签名(threshold-traceable-ABS)方案,并给出了 Threshold-Traceable-ABS 方案的安全性分析.

4.1 Threshold-Traceable-ABS方案

Setup:设 p,q 为两个大素数,$n=pq$.G 和 G_T 是两个阶为 n 的乘法循环群,$e:G\times G\to G_T$ 为双线性映射.G_p,G_q 分别为 G 的阶为 p,q 的子群.设 $S\subseteq Z_n$,且 $i\in S$,拉格朗日系数的定义同第 3.1 节.

设系统支持的属性集合为 Z_n^* .$T(X)$的定义基本同第 3.1 节,除了要求 t_i 为从 G 中随机选取的生成元.

定义门限为 d.PKG 随机选择 G 的生成元 g,并选择 $\alpha \in_R Z_n^*$,令 $g_1=g^\alpha$,同时随机选择 G 的生成元 g_2.PKG 随机选择 G_q 的生成元 h.此外,随机选择 G 的生成元 u',m',以及长度分别为 n_u 与 n_m 的向量 $U=\{u_i\}$与 $M=\{m_i\}$,其中,u_i,m_i 均为 G 的生成元.则主密钥 MK 为α,追踪密钥 TK 为 q,公共参数 $PK=(d,g,g_1,g_2,h,t_1,\ldots,t_{k+1},e,u',U,m',M)$.

$W(u)$与 $V(m)$的定义同第 3.1 节.

KeyGen:该函数的输入为用户 u 及其对应的属性集合Ω、主密钥 MK 和公共参数 PK.

PKG 随机选择一个 $d-1$ 次多项式 $q(x)$,其中,$q(0)=\alpha$.对每个用户 u,随机选取唯一的 $s\in Z_n$,计算 $D_{u,1}=g^s$,$D_{u,2}=h^s$.

对于属性 $i\in\Omega$,PKG 随机选取唯一的 $r_i\in Z_n$,计算 $D_{i,1}=g^{r_i}$,$D_{i,2}=g_2^{q(i)}\cdot T(i)^{r_i}\cdot W(u)^s$.

则私钥为 $D_{u,\Omega}=(D_{u,1},D_{u,2},\{(D_{i,1},D_{i,2})_{i\in\Omega}\})$.

Sign:用户 u 对消息 m 签名,签名者随机选择$\gamma\subseteq\Omega$,其中,$|\gamma|\geq d$.再随机选择属性集合γ',其中,$\gamma\cap\gamma'=\varnothing$.令 $\Psi=\gamma\cup\gamma'$,签名策略为(Ψ,d,Φ),即签名者至少拥有属性集合 Ψ中的 d 个属性.签名者执行如下步骤:

(1) 对 u 的每一个比特 $u[i](i=1,\ldots,n_u)$,随机选取$\theta_i\in Z_n$,计算 $c_i=u_i^{u[i]}\cdot h^{\theta_i}$,$\pi_i=(u_i^{2u[i]-1}\cdot h^{\theta_i})^{\theta_i}$,其中,$c_i$ 是 $u[i]\in\{0,1\}$的承诺,π_i是 c_i的证据.签名者计算:

$$\theta=\sum_{i=1}^{n_u}\theta_i,c=u'\prod_{i=1}^{n_u}c_i=(u'\prod_{i=1}^{n_u}u_i^{u[i]})\cdot h^\theta=(u'\prod_{i\in U}u_i)\cdot h^\theta=W(u)\cdot h^\theta.$$

即 c 可以看作是对 $W(u)$使用 h^θ进行随机化的结果;

(2) 随机选取 $s_1'\in Z_n$,令 $s_1=s+s_1'$,计算 $\sigma_1=D_{u,1}\cdot g^{s_1'}=g^s\cdot g^{s_1'}=g^{s_1}$;

(3) 随机选取 $s_2\in Z_n$,计算 $\sigma_2=g^{s_2}$;

(4) 对所有的 $i\in\Psi$,随机选取 $r_i'\in Z_n$,当 $i\in\gamma$时,计算 $\sigma_{3,i}=D_{i,1}^{A_{i,\gamma}(0)}\cdot g^{r_i'}=g^{r_iA_{i,\gamma}(0)+r_i'}$;当 $i\in\gamma'$时,计算 $\sigma_{3,i}=g^{r_i'}$;

(5) 计算 $\sigma_4=V(m)^{s_2}\cdot(\prod_{i\in\gamma}D_{i,2}^{A_{i,\gamma}(0)})\cdot D_{u,2}^\theta\cdot c^{s_1'}\cdot\prod_{i\in\Psi}T(i)^{r_i'}$.

最终输出签名 $\sigma=(\sigma_1,\sigma_2,\{\sigma_{3,i}\}_{i\in\Psi},\sigma_4,c_1,...,c_{n_u},\pi_1,...,\pi_{n_u})$.

Verify:该函数的输入为σ,返回是否接受签名.验证者计算 $c=u'\prod_{i=1}^{n_u}c_i$,并且对所有的 $i=1,\ldots,n_u$,验证者验证 $e(c_i,u_i^{-1}c_i)=e(h,\pi_i)$ 是否成立.若成立,则证明了对于所有的 $u[i]\in\{0,1\}$,有 $c_i=u_i^{u[i]}\cdot h^{\theta_i}$ 成立.因此,验证者计算出来的 c 具有正确的格式.验证者验证下式是否成立,若成立则接受签名,否则拒绝签名.

$$\frac{e(\sigma_4,g)}{(\prod_{i\in\Psi}e(T(i),\sigma_{3,i}))\cdot e(c,\sigma_1)\cdot e(V(m),\sigma_2)}=e(g_1,g_2)\tag{1}$$

Trace:该函数的输入为σ和追踪密钥 TK,返回签名者的身份 u.PKG 首先验证签名是合法的,然后对每一个 c_i,计算$(c_i)^q$.若$(c_i)^q=g^0$,则 $u[i]=0$;若$(c_i)^q=(u_i)^q$,则 $u[i]=1$.从而可以恢复签名者的身份 u.

对身份 u 的每一个比特 $u[i]$,有 $e(c_i,u_i^{-1}c_i)=e(h,\pi_i)$ 成立.由 $h\in G_q$,则 $e(h,\pi_i)$在 G_T 中的阶为 q,因此有 $c_i\in G_q$ 或 $u_i^{-1}c_i\in G_q$.若 $c_i\in G_q$,则有$(c_i)^q=g^0$;若 $c_i\notin G_q$,则有 $u_i^{-1}c_i\in G_q$,即可表示为 $u_i^{-1}c_i=h^{\theta_i}$,$c_i=u_ih^{\theta_i}$,其中,θ_i 未知.此时,$(c_i)^q=(u_ih^{\theta_i})^q=(u_i)^q$.

综上所述,可以保证 Trace 算法的正确性.文献[20]中给出了对所有的(c_i,π_i)同时快速验证的方法以及对长消息签名的优化方法,这些方法同样适用于本方案.

4.2 正确性

$$\begin{aligned}
\sigma_4&=V(m)^{s_2}\cdot(\prod_{i\in\gamma}D_{i,2}^{A_{i,\gamma}(0)})\cdot D_{u,2}^\theta\cdot c^{s_1'}\cdot\prod_{i\in\Psi}T(i)^{r_i'}=V(m)^{s_2}\cdot\prod_{i\in\gamma}(D_{i,2}\cdot D_{u,2}^\theta\cdot c^{s_1'})^{A_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\
&=V(m)^{s_2}\cdot\prod_{i\in\gamma}(g_2^{q(i)}\cdot T(i)^{r_i}\cdot W(u)^s\cdot h^{\theta\cdot s}\cdot c^{s_1'})^{A_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\
&=V(m)^{s_2}\cdot\prod_{i\in\gamma}(g_2^{q(i)}\cdot T(i)^{r_i}\cdot c^s\cdot c^{s_1'})^{A_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\
&=V(m)^{s_2}\cdot\prod_{i\in\gamma}(g_2^{q(i)}\cdot T(i)^{r_i}\cdot c^{s_1})^{A_{i,\gamma}(0)}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\
&=g_2^\alpha\cdot V(m)^{s_2}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_iA_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'},
\end{aligned}$$

$$\frac{e(\sigma_4,g)}{(\prod_{i\in\Psi'}e(T(i),\sigma_{3,i}))\cdot e(c,\sigma_1)\cdot e(V(m),\sigma_2)}=$$
$$\frac{e(g_2^{\alpha}\cdot V(m)^{s_2}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_iA_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'},g)}{(\prod_{i\in\gamma}e(T(i),g^{r_iA_{i,\gamma}(0)+r_i'}))\cdot(\prod_{i\in\gamma'}e(T(i),g^{r_i'}))\cdot e(c,g^{s_1})\cdot e(V(m),g^{s_2})}=e(g_1,g_2).$$

4.3 不可联系性

定理 1. 对于循环群 G,如果子群判定假设成立,则我们的属性签名方案满足不可联系性(unlinkability).

证明:考察签名σ.其中,$\sigma_1=g^{s_1},\sigma_2=g^{s_2}$ 是随机的.对于$\{\sigma_{3,i}\}_{i\in\Psi}$,每一个$\sigma_{3,i}$都被 r_i' 随机化.因此,每一个$\sigma_{3,i}$也是随机的.且在σ_4中,s_1',s_2,θ,r_i' 都为随机数,因此对于敌手,σ_4与随机数是不可区分的.

由文献[15]可知,基于子群判定假设,对所有的 i=1,…,n_u,c_i 是 $u[i]\in\{0,1\}$的承诺,π_i 是 c_i 非交互证据不可区分的证据.因此,(c_i,π_i)不会泄露 $u[i]\in\{0,1\}$的任何信息.

综上所述,我们的属性签名方案满足不可联系性.显然,不可联系性蕴含着匿名性. □

4.4 不可伪造性

定理 2. 在选择签名策略和选择消息攻击模型下,使用存在不可伪造安全模型,如果敌手可以攻破本方案,则可以构造一个多项式有界的模拟器,以不可忽略的优势解决 CDH 问题.

证明:模拟器已知 p,q 为两个大素数,$n=pq$,G 和 G_T 是两个阶为 n 的乘法循环群,$e:G\times G\to G_T$ 为双线性映射.G_p,G_q 分别为 G 的阶为 p,q 的子群,G_{Tp},G_{Tq} 分别为 G_T 的阶为 p,q 的子群.h 为 G_q 的生成元.挑战者生成随机的(g,g^{α},g^{β}),其中,g 为 G_p 的生成元,$\alpha,\beta\in_R Z_p^*$,将(g,g^{α},g^{β})发送给模拟器.若敌手可以攻破本方案,则可以利用敌手构造模拟器解决 G_p 子群中的 CDH 问题.该证明的思想参考自文献[1,20,23,24]. □

Init:敌手选定他要挑战的签名策略(Ψ^*,d,Φ^*).

Setup:模拟器收到(g,g^{α},g^{β}),令 $g_1=g^{\alpha},g_2=g^{\beta}$,目标是计算出 $g^{\alpha\beta}$.

模拟器随机选择 k 次多项式 $f(X)$,并按如下方式计算 k 次多项式$\varphi(X)$:当 $X\in\Psi^*$时,令$\varphi(X)=-X^k$;否则,令$\varphi(X)\neq -X^k$.由于$\varphi(X)$和$-X^k$是两个 k 次多项式,因此它们最多有 k 个点相同,或者二者为相同的多项式.上述构造方式保证了对于多项式$\varphi(X)$,当且仅当 $X\in\Psi^*$时,有$\varphi(X)=-X^k$.

对 i=1,…,k+1,模拟器令 $t_i=g_2^{\varphi(i)}g^{f(i)}$.由于 $f(X)$是 k 次随机多项式,因此 t_i 是独立的,并有 $T(i)=g_2^{i^k+\varphi(i)}g^{f(i)}$.

假设敌手最多询问 q_k 次 KeyGen 运算、q_s 次 Sign 运算.参考文献[24],令 $l_u=2(q_k+q_s)$,$l_m=2q_s$,设 $l_u(n_u+1)<p$,$l_m(n_m+1)<p$,模拟器随机选择:

(1) 两个整数 k_u 和 k_m,其中,$0\leqslant k_u\leqslant n_u$,$0\leqslant k_m\leqslant n_m$;

(2) 整数 $x'\in Z_{l_u}$ 和一个 n_u 维向量 $X=(x_i)(x_i\in Z_{l_u})$;

(3) 整数 $z'\in Z_{l_m}$ 和一个 n_m 维向量 $Z=(z_i)(z_i\in Z_{l_m})$;

(4) 两个整数 $y',w'\in Z_p$,一个 n_u 维向量 $Y=(y_i)(y_i\in Z_p)$和一个 n_m 维向量 $W=(w_i)(w_i\in Z_p)$.

关于身份 u、消息 m 的函数定义如下:

$$F(u)=-l_uk_u+x'+\sum_{i\in U}x_i,$$
$$J(u)=y'+\sum_{i\in U}y_i,K(m)=-l_mk_m+z'+\sum_{i\in M}z_i,$$
$$L(m)=w'+\sum_{i\in M}w_i.$$

模拟器设置下列公共参数并将其发送给敌手,令

$$u'=g_2^{-l_uk_u+x'}g^{y'},$$
$$u_i=g_2^{x_i}g^{y_i}(1\leqslant i\leqslant n_u),$$
$$m'=g_2^{-l_mk_m+z'}g^{w'},$$
$$m_i=g_2^{z_i}g^{w_i}(1\leqslant i\leqslant n_m).$$

则对于任意的身份 u 和消息 m,有

$$W(u)=u'\prod_{i\in U}u_i=g_2^{F(u)}g^{J(u)},V(m)=m'\prod_{i\in M}m_i=g_2^{K(m)}g^{L(m)}.$$

KeyGen 询问:敌手最多询问 q_k 次 KeyGen.

对于用户 u,设其属性集合为 Ω.若 $|\Omega\cap\Psi^*|\geqslant d$,则 Ω 满足签名策略 (Ψ^*,d,Φ^*),模拟器终止;否则,敌手可以对属性集合 Ω 询问 KeyGen.在不知道主密钥的情况下,模拟器按如下方式模拟 $D_{u,\Omega}$.值得指出的是,与文献[24]不同,当 $|\Omega\cap\Psi^*|<d$ 时,无论 $F(u)=0$ 是否成立,都可以询问 KeyGen.

首先定义 3 个集合 Γ,Γ' 和 S,其中,$\Gamma=\Omega\cap\Psi^*$.选取 Γ' 为满足 $\Gamma\subseteq\Gamma'\subseteq\Omega$ 的任意集合,其中,$|\Gamma'|=d-1$.令 $S=\Gamma'\cup\{0\}$.

对于用户 u,随机选取唯一的 $s\in Z_p$,计算 $D_{u,1}=g^s,D_{u,2}=h^s$.

对于属性 $i\in\Gamma'$,模拟器随机选择 $r_i,\eta_i\in Z_p$,令 $D_{i,1}=g^{r_i},D_{i,2}=g_2^{\eta_i}\cdot T(i)^{r_i}\cdot W(u)^s$.即,当属性 $i\in\Gamma'$ 时,随机选择 $d-1$ 次多项式 $q(x)$ 上的 $d-1$ 个点 $q(i)=\eta_i$.此外,期望多项式 $q(x)$ 满足 $q(0)=\alpha$.

对于属性 $i\in\Omega-\Gamma'$,模拟器随机选择 $r_i'\in Z_p$,令

$$D_{i,1}=(g_1^{-1/(i^k+\varphi(i))}g^{r_i'})^{\Delta_{0,S}(i)},D_{i,2}=(\prod_{j\in\Gamma'}g_2^{q(j)\Delta_{j,S}(i)})\cdot(g_1^{-f(i)/(i^k+\varphi(i))}(g_2^{i^k+\varphi(i)}g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}\cdot W(u)^s.$$

由 $\varphi(X)$ 的构造,对所有的 $i\notin\Psi^*$,包括 $i\in\Omega-\Gamma'$,有 $i^k+\varphi(i)\neq 0$.

令 $r_i=(r_i'-\alpha/(i^k+\varphi(i)))\cdot\Delta_{0,S}(i)$,由于 $q(i)=q(0)\Delta_{0,S}(i)+\sum_{j\in\Gamma'}(q(j)\Delta_{j,S}(i))$,因此有:

$$D_{i,1}=(g_1^{-1/(i^k+\varphi(i))}g^{r_i'})^{\Delta_{0,S}(i)}=(g^{r_i'-\alpha/(i^k+\varphi(i))})^{\Delta_{0,S}(i)}=g^{r_i},$$

$$\begin{aligned}D_{i,2}&=(\prod_{j\in\Gamma'}g_2^{q(j)\Delta_{j,S}(i)})\cdot(g_1^{-f(i)/(i^k+\varphi(i))}(g_2^{i^k+\varphi(i)}g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}\cdot W(u)^s\\&=(\prod_{j\in\Gamma'}g_2^{q(j)\Delta_{j,S}(i)})\cdot(g_2^{\alpha}(g_2^{i^k+\varphi(i)}g^{f(i)})^{-\alpha/(i^k+\varphi(i))}(g_2^{i^k+\varphi(i)}g^{f(i)})^{r_i'})^{\Delta_{0,S}(i)}\cdot W(u)^s\\&=(\prod_{j\in\Gamma'}g_2^{q(j)\Delta_{j,S}(i)})\cdot g_2^{\alpha\cdot\Delta_{0,S}(i)}\cdot(T(i)^{r_i'-\alpha/(i^k+\varphi(i))})^{\Delta_{0,S}(i)}\cdot W(u)^s=g_2^{q(i)}\cdot T(i)^{r_i}\cdot W(u)^s.\end{aligned}$$

因此,对于敌手而言,模拟器计算的 $D_{u,\Omega}$ 与真正的 $D_{u,\Omega}$ 是不可区分的.

Sign 询问:假设敌手最多询问 q_s 次 Sign 运算,生成关于消息 m 的签名数据,其中,签名者的身份为 u,属性集合为 Ω,签名策略为 (Ψ,d,Φ).若 $|\Omega\cap\Psi|<d$,则 Ω 不满足签名策略 (Ψ,d,Φ),模拟器终止;否则,当 $|\Omega\cap\Psi|\geqslant d$ 时,模拟器选择 $\gamma\subseteq(\Omega\cap\Psi)$,此时 $|\gamma|\geqslant d$,并选择 $\gamma'=\Psi-\gamma$,按如下方式模拟对消息 m 的签名数据:

- 当 $|\Omega\cap\Psi^*|<d$ 时,模拟器询问 KeyGen,得到用户 u 的私钥 $D_{u,\Omega}$.模拟器按原始方案直接生成签名数据;
- 当 $|\Omega\cap\Psi^*|\geqslant d$ 时,若 $K(m)=0 \bmod l_m$,则模拟器放弃;否则,模拟器按如下方式模拟签名数据:

(1) 对 u 的每一个比特 $u[i](i=1,\ldots,n_u)$,随机选取 $\theta_i\in Z_p$,计算 $c_i=u_i^{u[i]}\cdot h^{\theta_i},\pi_i=(u_i^{2u[i]-1}\cdot h^{\theta_i})^{\theta_i}$,并计算

$$\theta=\sum_{i=1}^{n_u}\theta_i,c=u'\prod_{i=1}^{n_u}c_i=(u'\prod_{i=1}^{n_u}u_i^{u[i]})\cdot h^{\theta}=(u'\prod_{i\in U}u_i)\cdot h^{\theta}=W(u)\cdot h^{\theta};$$

(2) 随机选取 $s_1,s_2'\in Z_p$,计算 $\sigma_1=g^{s_1},\sigma_2=g_1^{-1/K(m)}g^{s_2'}$;

(3) 对于 $i\in\Psi$,随机选取 $r_i,r_i'\in Z_p$,当 $i\in\gamma$ 时,计算 $\sigma_{3,i}=g^{r_i\Delta_{i,\gamma}(0)+r_i'}$;当 $i\in\gamma'$ 时,计算 $\sigma_{3,i}=g^{r_i'}$;

(4) 计算 $\sigma_4=g_1^{-L(m)/K(m)}\cdot(g_2^{K(m)}g^{L(m)})^{s_2'}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'}$.

令 $s_2=s_2'-\alpha/K(m)$,则有,

$$\sigma_2=g_1^{-1/K(m)}\cdot g^{s_2'}=g^{s_2'-\alpha/K(m)}=g^{s_2},$$

$$\begin{aligned}\sigma_4&=g_1^{-L(m)/K(m)}\cdot(g_2^{K(m)}g^{L(m)})^{s_2'}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'}\\&=g_2^{\alpha}\cdot(g_2^{K(m)}g^{L(m)})^{-\alpha/K(m)}\cdot(g_2^{K(m)}g^{L(m)})^{s_2'}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'}\\&=g_2^{\alpha}\cdot(g_2^{K(m)}g^{L(m)})^{s_2'-\alpha/K(m)}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'}\\&=g_2^{\alpha}\cdot V(m)^{s_2}\cdot c^{s_1}\cdot\prod_{i\in\gamma}T(i)^{r_i\Delta_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T(i)^{r_i'}.\end{aligned}$$

最终模拟的签名为 $\sigma=(\sigma_1,\sigma_2,\{\sigma_{3,i}\}_{i\in\Psi},\sigma_4,c_1,\ldots,c_{n_u},\pi_1,\ldots,\pi_{n_u})$.

容易验证,模拟器计算的 σ 可以通过签名验证,且模拟器计算的 σ 与原始方案的 σ 是不可区分的.

Trace 询问:对于 Trace 询问,直接按原始方案运算,并返回相关结果即可.

Forge:设敌手可以成功伪造出满足签名策略(Ψ^*,d,Φ^*)的关于消息 m^*的合法签名σ^*.模拟器知道追踪密钥 TK,首先调用 Trace 算法计算出u^*.模拟器检查敌手没有询问过u^*的私钥,且敌手没有对用户 u^*做过关于消息m^*,签名策略(Ψ^*,d,Φ^*)的 Sign 询问.

由$\varphi(X)$的构造,对所有的 $i\in\Psi^*$,有 $i^k+\varphi(i)=0$.此时,$T(i)=g_2^{i^k+\varphi(i)}g^{f(i)}=g^{f(i)}$.

若 $F(u^*)\neq 0 \bmod p$ 或 $K(m^*)\neq 0 \bmod p$,则模拟器放弃;否则,有 $F(u^*)=0 \bmod p, K(m^*)=0 \bmod p$.同文献[24]分析,$F(u)=0 \bmod p\Rightarrow F(u)=0 \bmod l_u$,因此有 $F(u)\neq 0 \bmod l_u\Rightarrow F(u)\neq 0 \bmod p$.同理,有 $K(m)=0 \bmod p\Rightarrow K(m)=0 \bmod l_m$, $K(m)\neq 0 \bmod l_m\Rightarrow K(m)\neq 0 \bmod p$.

因此,当 $F(u^*)=0 \bmod p, K(m^*)=0 \bmod p$ 时,有

$$W(u^*)=g^{J(u^*)}, V(m^*)=g^{L(m^*)}, c^*=u'\prod_{i=1}^{n_u}c_i^*=W(u^*)\cdot h^\theta=g^{J(u^*)}\cdot h^\theta,\ \text{其中,}\theta\text{未知.}$$

由于 $g,g_1,g_2,T(i),W(u^*),V(m^*)\in G_p$,因此有 $e(\sigma_4^*,g),e(T(i),\sigma_{3,i}^*),e(W(u^*),\sigma_1^*),e(V(m^*),\sigma_2^*),e(g_1,g_2)\in G_{Tp}$,由等式(1)成立,有

$$\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(T(i),\sigma_{3,i}^*))\cdot e(c^*,\sigma_1^*)\cdot e(V(m^*),\sigma_2^*)}=\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(T(i),\sigma_{3,i}^*))\cdot e(W(u^*),\sigma_1^*)\cdot e(h^\theta,\sigma_1^*)\cdot e(V(m^*),\sigma_2^*)}=e(g_1,g_2).$$

因此有 $e(h^\theta,\sigma_1^*)\in G_{Tp}$,否则,$\sigma^*$无法通过等式(1)的验证.而 $h\in G_q$,因此 $e(h^\theta,\sigma_1^*)\in G_{Tq}$.由 $G_{Tp}\cap G_{Tq}=1$,可以得到 $e(h^\theta,\sigma_1^*)=1$.

$$\begin{aligned}\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(T(i),\sigma_{3,i}^*))\cdot e(c^*,\sigma_1^*)\cdot e(V(m^*),\sigma_2^*)}&=\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(T(i),\sigma_{3,i}^*))\cdot e(W(u^*),\sigma_1^*)\cdot e(h^\theta,\sigma_1^*)\cdot e(V(m^*),\sigma_2^*)}\\&=\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(g^{f(i)},\sigma_{3,i}^*))\cdot e(g^{J(u^*)},\sigma_1^*)\cdot e(g^{L(m^*)},\sigma_2^*)}\\&=\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(g,(\sigma_{3,i}^*)^{f(i)}))\cdot e(g,(\sigma_1^*)^{J(u^*)})\cdot e(g,(\sigma_2^*)^{L(m^*)})}\\&=e\left(\frac{\sigma_4^*}{(\prod_{i\in\Psi^*}(\sigma_{3,i}^*)^{f(i)})\cdot(\sigma_1^*)^{J(u^*)}\cdot(\sigma_2^*)^{L(m^*)}},g\right)\\&=e(g_1,g_2)\\&=e(g^{\alpha\beta},g).\end{aligned}$$

因此有 $\frac{\sigma_4^*}{(\prod_{i\in\Psi^*}(\sigma_{3,i}^*)^{f(i)})\cdot(\sigma_1^*)^{J(u^*)}\cdot(\sigma_2^*)^{L(m^*)}}=g^{\alpha\beta}$ 成立,成功解决 CDH 问题.矛盾.

假设敌手能够以ε的概率伪造签名,则模拟器不放弃的条件为:

(1) 在做 KeyGen 询问时,要求$|\Omega\cap\Psi^*|<d$;

(2) 在做 Sign 询问时,当$|\Omega\cap\Psi^*|\geq d$ 时,要求 $K(m)\neq 0 \bmod l_m$;

(3) 在 Forge 阶段,要求 $F(u^*)=0 \bmod p, K(m^*)=0 \bmod p$.

在选择签名策略模型下,敌手在询问 KeyGen 之前就可以自己验证$|\Omega\cap\Psi^*|\geq d$ 是否成立.因此,我们假设在做 KeyGen 询问时,敌手选择的属性集合Ω满足$|\Omega\cap\Psi^*|<d$.设在做 Sign 询问(要求满足条件$|\Omega\cap\Psi^*|\geq d$)时询问了 q_m 个不同的消息,显然有 $q_m\leqslant q_s$.定义下列事件:

(1) E_i:$K(m_i)\neq 0 \bmod l_m$,其中,$i=1,\ldots,q_m$;

(2) E':$K(m^*)=0 \bmod p$;

(3) E'':$F(u^*)=0 \bmod p$.

则模拟器不放弃的概率为 $\Pr[\overline{abort}]\geqslant\Pr[\wedge_{i=1}^{q_m}E_i\wedge E'\wedge E'']$.

同文献[24]的分析,有 $\Pr[E']=1/(l_m(n_m+1))$,$\Pr[E'']=1/(l_u(n_u+1))$.同时,对所有的 $i=1,\ldots,q_m$,事件 E_i 与 E'是独立

的.因此有,

$$\begin{aligned}\Pr[\overline{abort}] &\geqslant \Pr[\wedge_{i=1}^{q_m} E_i \wedge E' \wedge E''] = \Pr[\wedge_{i=1}^{q_m} E_i \wedge E'] \cdot \Pr[E''] = \Pr[E'] \cdot \Pr[\wedge_{i=1}^{q_m} E_i \mid E'] \cdot \Pr[E''] \\ &= \Pr[E'] \cdot (1 - \Pr[\vee_{i=1}^{q_m} \overline{E_i} \mid E']) \cdot \Pr[E''] \geqslant \Pr[E'] \cdot (1 - \sum_{i=1}^{q_m} \Pr[\overline{E_i} \mid E']) \cdot \Pr[E''] \\ &= \frac{1}{l_m(n_m+1)} \cdot \left(1 - \frac{q_m}{l_m}\right) \cdot \frac{1}{l_u(n_u+1)} \\ &\geqslant \frac{1}{2q_s(n_m+1)} \cdot \left(1 - \frac{q_s}{2q_s}\right) \cdot \frac{1}{2(q_k+q_s)(n_u+1)} \\ &= \frac{1}{8q_s(q_k+q_s)(n_u+1)(n_m+1)}.\end{aligned}$$

即若敌手能够以ε的概率伪造签名,则模拟器成功解决 CDH 问题的概率至少为 $\frac{\varepsilon}{8q_s(q_k+q_s)(n_u+1)(n_m+1)}$.

4.5 不可陷害性

定理 3. 如果敌手可以攻破本方案的不可陷害性(non-frameability),则可以构造一个多项式有界的模拟器,以不可忽略的优势攻破 Threshold-ID-ABS 方案的存在不可伪造性.

证明:假设敌手可以攻破本方案,则我们可以利用敌手来构造模拟器,攻破 Threshold-ID-ABS 方案的存在不可伪造性.该证明的思想源自文献[20].

Setup:模拟器已知 p,q 为两个大素数,$n=pq$,G 和 G_T 是两个阶为 n 的乘法循环群,$e:G\times G\to G_T$ 为双线性映射.G_p,G_q 分别为 G 的阶为 p,q 的子群,则 G 为 G_p,G_q 的直积.

挑战者首先调用 Threshold-ID-ABS 方案中的 Setup.随机选取 G_p 的生成元 $\tilde{g}$ 以及$\alpha\in_R Z_p$,计算 $\tilde{g}_1=\tilde{g}^{\alpha}$.挑战者随机选取 $(\tilde{g}_2,\tilde{t}_1,...,\tilde{t}_{k+1},\tilde{u}',\tilde{U},\tilde{m}',\tilde{M})\in G_p$,则$\alpha$为主密钥,$\alpha$不发送给模拟器,公共参数为

$$\widetilde{PK}=(d,\tilde{g},\tilde{g}_1,\tilde{g}_2,\tilde{t}_1,...,\tilde{t}_{k+1},e,\tilde{u}',\tilde{U},\tilde{m}',\tilde{M}).$$

记 $\tilde{T}(X)=\tilde{g}_2^{X^k}\prod_{i=1}^{k+1}(\tilde{t}_i)^{\Delta_{i,K}(X)},\tilde{W}(u)=\tilde{u}'\prod_{i\in U}\tilde{u}_i,\tilde{V}(m)=\tilde{m}'\prod_{i\in M}\tilde{m}_i$.

模拟器随机选取 $(f,h,t_1',...,t_{k+1}',\xi',\xi_1,...,\xi_{n_u},v',v_1,...,v_{n_m})\in G_q$,并随机选取$\beta\in_R Z_q$.记

$$T'(X)=f^{X^k}\prod_{i=1}^{k+1}(t_i')^{\Delta_{i,K}(X)},W'(u)=\xi'\prod_{i\in U}\xi_i,V'(m)=v'\prod_{i\in M}v_i.$$

模拟器计算: $g=\tilde{g}\cdot f,g_1=\tilde{g}_1f^{\beta},g_2=\tilde{g}_2f,u'=\tilde{u}'\xi',m'=\tilde{m}'v'$.对于 i=1,…,k,k+1,令 $t_i=\tilde{t}_it_i'$;对于 i=1,…,n_u,令 $u_i=\tilde{u}_i\xi_i$;对于 i=1,…,n_m,令 $m_i=\tilde{m}_iv_i$.那么, $T(X)=\tilde{T}(X)\cdot T'(X),W(u)=\tilde{W}(u)\cdot W'(u),V(m)=\tilde{V}(m)\cdot V'(m)$.

令 PK=(d,g,g_1,g_2,h,t_1,….,t_{k+1},e,u',U,m',M),追踪密钥 TK 为 q,模拟器不知道主密钥.

KeyGen 询问:当敌手对 Threshold-Traceable-ABS 询问用户 u 的私钥时,模拟器首先对 Threshold-ID-ABS 询问用户 u 的私钥,得到 $\tilde{D}_{u,\Omega}=(\tilde{D}_u,\{(\tilde{D}_{i,1},\tilde{D}_{i,2})\}_{i\in\Omega})\in G_p^{1+2|\Omega|}$.

模拟器随机选择 $s\in Z_q$,计算 $D_{u,1}=\tilde{D}_u\cdot f^s,D_{u,2}=h^s$.模拟器随机选择 d–1 次多项式 $q'(x)$ mod Z_q,其中,$q'(0)=\beta$.对每一个 $i\in\Omega$,模拟器随机选择 $r_i\in Z_q$,计算 $D_{i,1}=\tilde{D}_{i,1}\cdot f^{r_i},D_{i,2}=\tilde{D}_{i,2}\cdot f^{q'(i)}\cdot T'(i)^{r_i}\cdot W'(u)^s$.

最终得到私钥 $D_{u,\Omega}$=($D_{u,1}$,$D_{u,2}$,{($D_{i,1}$,$D_{i,2}$)}$_{i\in\Omega}$).模拟器生成的 $D_{u,\Omega}$与原始方案的 $D_{u,\Omega}$是不可区分的,且敌手可以使用模拟的 $D_{u,\Omega}$按照原始方案生成合法的签名.其中,签名的流程为:

(1) 对 u 的每一个比特 $u[i]$,模拟器按照原始方案计算(c_i,π_i),并计算,

$$c=u'\prod_{i=1}^{n_u}c_i=W(u)\cdot h^{\theta}=\tilde{W}(u)\cdot W'(u)\cdot h^{\theta};$$

(2) 随机选取 $s_1'\in Z_n$,令 $s_1=s+s_1'$,计算 $\sigma_1=D_{u,1}\cdot g^{s_1'}=\tilde{D}_u\cdot f^s\cdot\tilde{g}^{s_1'}\cdot f^{s_1'}=\delta_1\cdot\tilde{g}^{s_1'}\cdot f^{s_1}$;

(3) 随机选取 $s_2\in Z_n$,计算 $\sigma_2=g^{s_2}=(\tilde{g}\cdot f)^{s_2}=\delta_2\cdot f^{s_2}$;

(4) 对 $i\in\Psi$,选取 $r_i'\in_R Z_n$,当 $i\in\gamma$时,计算 $\sigma_{3,i}=D_{i,1}^{\Delta_{i,\gamma}(0)}\cdot g^{r_i'}=\tilde{D}_{i,1}^{\Delta_{i,\gamma}(0)}f^{r_i\Delta_{i,\gamma}(0)}\cdot\tilde{g}^{r_i'}\cdot f^{r_i'}=\delta_{3,i}\cdot f^{r_i\Delta_{i,\gamma}(0)+r_i'}$;当 $i\in\gamma'$时,

计算 $\sigma_{3,i}=g^{r_i'}=\delta_{3,i}\cdot f^{r_i'}$;

(5) 计算 $\sigma_4=V(m)^{s_2}\cdot(\prod_{i\in\gamma}D_{i,2}^{A_{i,\gamma}(0)})\cdot D_{u,2}^{\theta}\cdot c^{s_1'}\cdot\prod_{i\in\Psi}T(i)^{r_i'}$,则

$$\begin{aligned}\sigma_4&=V(m)^{s_2}\cdot(\prod_{i\in\gamma}D_{i,2}^{A_{i,\gamma}(0)})\cdot D_{u,2}^{\theta}\cdot c^{s_1'}\cdot\prod_{i\in\Psi}T(i)^{r_i'}\\&=\tilde{V}(m)^{s_2}\cdot V'(m)^{s_2}\cdot(\prod_{i\in\gamma}(\tilde{D}_{i,2}\cdot f^{q'(i)}\cdot T'(i)^{r_i}\cdot W'(u)^{s})^{A_{i,\gamma}(0)})\cdot D_{u,2}^{\theta}\cdot c^{s_1'}\cdot(\prod_{i\in\Psi}\tilde{T}(i)^{r_i'})\cdot\prod_{i\in\Psi}T'(i)^{r_i'}\\&=\tilde{V}(m)^{s_2}\cdot(\prod_{i\in\gamma}(\tilde{D}_{i,2})^{A_{i,\gamma}(0)})\cdot(\prod_{i\in\Psi}\tilde{T}(i)^{r_i'})\cdot V'(m)^{s_2}\cdot(\prod_{i\in\gamma}(f^{q'(i)}\cdot T'(i)^{r_i}\cdot W'(u)^{s})^{A_{i,\gamma}(0)})\cdot D_{u,2}^{\theta}\cdot c^{s_1'}\cdot\prod_{i\in\Psi}T'(i)^{r_i'}\\&=\delta_4\cdot V'(m)^{s_2}\cdot f^{\beta}\cdot W'(u)^{s}\cdot h^{s\theta}\cdot\tilde{W}(u)^{s_1'}\cdot W'(u)^{s_1'}\cdot h^{s_1'\theta}\cdot\prod_{i\in\gamma}T'(i)^{r_iA_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T'(i)^{r_i'}\\&=\delta_4\cdot\tilde{W}(u)^{s_1'}\cdot V'(m)^{s_2}\cdot f^{\beta}\cdot W'(u)^{s_1}\cdot h^{s_1\theta}\cdot\prod_{i\in\gamma}T'(i)^{r_iA_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T'(i)^{r_i'}.\end{aligned}$$

最终得到签名 $\sigma=(\sigma_1,\sigma_2,\{\sigma_{3,i}\}_{i\in\Psi},\sigma_4,c_1,...,c_{n_u},\pi_1,...,\pi_{n_u})$.

不妨设 g_0 为 G 的生成元,对于任意的 $x\in G_p,y\in G_q$,则可以设 $x=(g_0)^{aq},y=(g_0)^{bp}$,其中,$a,b\in Z_n$ 且 a,b 未知,则有 $e(x,y)=e(g_0^{aq},g_0^{bp})=e(g_0,g_0)^{abpq}=e(g_0,g_0)^{abn}=1$.因此,签名验证的正确性可按如下流程验证:

$$\frac{e(\sigma_4,g)}{(\prod_{i\in\Psi}e(T(i),\sigma_{3,i}))\cdot e(c,\sigma_1)\cdot e(V(m),\sigma_2)}=$$

$$\frac{e(\delta_4\cdot\tilde{W}(u)^{s_1'},\tilde{g})\cdot e(V'(m)^{s_2}\cdot f^{\beta}\cdot W'(u)^{s_1}\cdot h^{s_1\theta}\cdot\prod_{i\in\gamma}T'(i)^{r_iA_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T'(i)^{r_i'},f)}{(\prod_{i\in\Psi}e(T(i),\sigma_{3,i}))\cdot e(\tilde{W}(u),\delta_1\cdot\tilde{g}^{s_1'})\cdot e(W'(u)\cdot h^{\theta},f^{s_1})\cdot e(V(m),\sigma_2)}=$$

$$\frac{e(\delta_4,\tilde{g})\cdot e(f^{\beta},f)\cdot e(V'(m)^{s_2}\cdot\prod_{i\in\gamma}T'(i)^{r_iA_{i,\gamma}(0)+r_i'}\cdot\prod_{i\in\gamma'}T'(i)^{r_i'},f)}{(\prod_{i\in\Psi}e(\tilde{T}(i),\delta_{3,i}))\cdot(\prod_{i\in\gamma}e(T'(i),f^{r_iA_{i,\gamma}(0)+r_i'}))\cdot(\prod_{i\in\gamma'}e(T'(i),f^{r_i'}))\cdot e(\tilde{W}(u),\delta_1)\cdot e(\tilde{V}(m),\delta_2)\cdot e(V'(m),f^{s_2})}=$$

$$\frac{e(\delta_4,\tilde{g})}{(\prod_{i\in\Psi}e(\tilde{T}(i),\delta_{3,i}))\cdot e(\tilde{W}(u),\delta_1)\cdot e(\tilde{V}(m),\delta_2)}\cdot e(f^{\beta},f)=e(\tilde{g}_1,\tilde{g}_2)\cdot e(f^{\beta},f)=e(\tilde{g}_1\cdot f^{\beta},\tilde{g}_2\cdot f)=e(g_1,g_2).$$

Sign 询问:敌手询问关于用户 u(属性集合为Ω),消息 m,签名策略(Ψ,d,Φ)的签名.模拟器按如下步骤模拟:

(1) 对 u 的每一个比特 $u[i]$,模拟器按照原始方案计算(c_i,π_i),并计算

$$c=u'\prod_{i=1}^{n_u}c_i=W(u)\cdot h^{\theta}=\tilde{W}(u)\cdot W'(u)\cdot h^{\theta}.$$

(2) 模拟器对 Threshold-ID-ABS 询问关于用户 u(对应的属性集合为Ω)、消息 m、签名策略(Ψ,d,Φ)的签名,得到签名 $\delta=(\delta_1,\delta_2,\{\delta_{3,i}\}_{i\in\Psi},\delta_4)\in G_p^{3+|\Psi|}$.

(3) 模拟器选取 $s_1,s_2\in_R Z_q$,计算 $\sigma_1=\delta_1\cdot f^{s_1},\sigma_2=\delta_2\cdot f^{s_2}$.对 $i\in\Psi$,模拟器选择 $r_i'\in_R Z_q$,计算 $\sigma_{3,i}=\delta_{3,i}\cdot f^{r_i'}$.并计算 $\sigma_4=\delta_4\cdot f^{\beta}\cdot(\prod_{i\in\Psi}T'(i)^{r_i'})\cdot W'(u)^{s_1}\cdot h^{\theta\cdot s_1}\cdot V'(m)^{s_2}$.

最终签名为 $\sigma=(\sigma_1,\sigma_2,\{\sigma_{3,i}\}_{i\in\Psi},\sigma_4,c_1,...,c_{n_u},\pi_1,...,\pi_{n_u})$.

与 KeyGen 询问中的签名验证类似,对于任意的 $x\in G_p,y\in G_q$,有 $e(x,y)=1$.由于 $\delta=(\delta_1,\delta_2,\{\delta_{3,i}\}_{i\in\Psi},\delta_4)\in G_p^{3+|\Psi|}$,$f\in G_q$,因此,模拟器计算的签名$\sigma$的正确性可按如下流程验证:

$$\frac{e(\sigma_4,g)}{(\prod_{i\in\Psi}e(T(i),\sigma_{3,i}))\cdot e(c,\sigma_1)\cdot e(V(m),\sigma_2)}=$$

$$\frac{e(\delta_4\cdot f^{\beta}\cdot(\prod_{i\in\Psi}T'(i)^{r_i'})\cdot W'(u)^{s_1}\cdot h^{\theta\cdot s_1}\cdot V'(m)^{s_2},\tilde{g}\cdot f)}{(\prod_{i\in\Psi}e(\tilde{T}(i)\cdot T'(i),\delta_{3,i}\cdot f^{r_i'}))\cdot e(\tilde{W}(u)\cdot W'(u)\cdot h^{\theta},\delta_1\cdot f^{s_1})\cdot e(\tilde{V}(m)\cdot V'(m),\delta_2\cdot f^{s_2})}=$$

$$\frac{e(\delta_4,\tilde{g})\cdot e(f^{\beta}\cdot(\prod_{i\in\Psi}T'(i)^{r_i'})\cdot W'(u)^{s_1}\cdot h^{\theta\cdot s_1}\cdot V'(m)^{s_2},f)}{(\prod_{i\in\Psi}e(\tilde{T}(i),\delta_{3,i}))\cdot(\prod_{i\in\Psi}e(T'(i),f^{r_i'}))\cdot e(\tilde{W}(u),\delta_1)\cdot e(W'(u)\cdot h^{\theta},f^{s_1})\cdot e(\tilde{V}(m),\delta_2)\cdot e(V'(m),f^{s_2})}=$$

$$\frac{e(\delta_4,\tilde{g})}{(\prod_{i\in\Psi}e(\tilde{T}(i),\delta_{3,i}))\cdot e(\tilde{W}(u),\delta_1)\cdot e(\tilde{V}(m),\delta_2)}\cdot e(f^{\beta},f)=e(\tilde{g}_1,\tilde{g}_2)\cdot e(f^{\beta},f)=e(\tilde{g}_1\cdot f^{\beta},\tilde{g}_2\cdot f)=e(g_1,g_2).$$

Forge:假设敌手可以成功伪造出满足签名策略(Ψ^*,d,Φ^*)的关于消息 m^*的合法签名σ^*.模拟器在收到σ^*后,首先验证σ^*是合法的签名,然后使用 Trace 运算计算出 u^*.如果敌手询问过 u^*的私钥,或者敌手询问过关于用户

u^*、消息 m^*、签名策略(Ψ^*,d,Φ^*)的签名,则模拟器放弃;否则,模拟器计算如下:

对身份 u 的每一个比特 $u[i]$,有 $e(c_i,u_i^{-1}c_i)=e(h,\pi_i)$ 成立,因此 $c_i=u_i^{u[i]}\cdot h^{\theta_i}$ 成立,其中,θ_i 未知.那么,

$$c=u'\prod_{i=1}^{n_u}c_i=W(u)\cdot h^{\theta}=\tilde{W}(u)\cdot W'(u)\cdot h^{\theta},$$

其中,θ未知.

模拟器选取$\lambda\in Z_n$,且满足$\lambda=0 \mod q$,$\lambda=1 \mod p$,则对于任意的 $x\in G$,$y\in G_q$,有 $e(x,y)^{\lambda}=1$;且对于任意的 $x',y'\in G_p$,有 $e(x',y')^{\lambda}=e(x',y')$.因此有,

$$\left(\frac{e(\sigma_4^*,g)}{(\prod_{i\in\Psi^*}e(T(i),\sigma_{3,i}^*))\cdot e(c^*,\sigma_1^*)\cdot e(V(m^*),\sigma_2^*)}\right)^{\lambda}=$$

$$\left(\frac{e(\sigma_4^*,\tilde{g})\cdot e(\sigma_4^*,f)}{(\prod_{i\in\Psi^*}e(\tilde{T}(i)\cdot T'(i),\sigma_{3,i}^*))\cdot e(\tilde{W}(u^*)\cdot W'(u^*)\cdot h^{\theta},\sigma_1^*)\cdot e(\tilde{V}(m^*)\cdot V'(m^*),\sigma_2^*)}\right)^{\lambda}=$$

$$\frac{e((\sigma_4^*)^{\lambda},\tilde{g})}{(\prod_{i\in\Psi^*}e(\tilde{T}(i),(\sigma_{3,i}^*)^{\lambda}))\cdot e(\tilde{W}(u^*),(\sigma_1^*)^{\lambda})\cdot e(\tilde{V}(m^*),(\sigma_2^*)^{\lambda})}=e(g_1,g_2)^{\lambda}=e(\tilde{g}_1f^{\beta},\tilde{g}_2f)^{\lambda}=e(\tilde{g}_1,\tilde{g}_2)^{\lambda}=e(\tilde{g}_1,\tilde{g}_2).$$

因此,$((\sigma_1^*)^{\lambda},(\sigma_2^*)^{\lambda},\{(\sigma_{3,i}^*)^{\lambda}\}_{i\in\Psi},(\sigma_4^*)^{\lambda})\in G_p^{3+|\Psi|}$ 是 Threshold-ID-ABS 的一个成功的伪造.

5 通用的可追踪身份的基于属性签名方案

本节在 Threshold-Traceable-ABS 方案的基础上,给出两个通用的可追踪身份的基于属性签名(traceable-ABS)方案.

5.1 基于访问树的访问结构

访问树[2−4]:设 T 是一个表示访问结构的树,树中的每一个非叶子节点表示门限,由其孩子个数和门限值来描述:num_x 是节点 x 的孩子个数;d_x 是门限值,$0<d_x\leqslant num_x$.当 $d_x=1$ 时,该门限的含义为 OR 结构;当 $d_x=num_x$ 时,该门限的含义为 AND 结构.每个叶子节点 x 由属性值描述,其门限值为 $d_x=1$.

对访问树,定义函数如下:$parent(x)$表示节点 x 的父节点.当 x 是叶子节点时,$att(x)$表示与 x 相关联的属性.访问树 T 中,每个节点 x 的孩子的次序定义为从 1~num_x,用 $index(x)$来表示.

设访问树 T 的根为 R,T_x 表示 T 的以 x 为根的子树,则 T 可以表示为 T_R.如果属性集合γ满足访问树 T_x,则记为 $T_x(\gamma)=1$.$T_x(\gamma)$的计算方式如下:如果 x 是非叶子节点,则计算节点 x 的所有孩子 x'的 $T_{x'}(\gamma)$值;当至少有 d_x 个孩子的 $T_{x'}(\gamma)=1$ 返回 1 时,$T_x(\gamma)$返回 1;如果 x 是叶子节点,则当且仅当 $att(x)\in\gamma$时,$T_x(\gamma)=1$.

Setup:同 Threshold-Traceable-ABS 的 Setup.

KeyGen:设用户 u 的属性集合为Ω,我们使用 top-down 方式为用户 u 颁发属性私钥.

令 T_Ω为属性私钥树,对 T_Ω中的每一个节点 x,从 T_Ω的根开始按如下方式选择多项式 q_x:对树中的每一个节点 x,其门限值为 d_x,设多项式 q_x 的次数 d_x-1.对树的根 R,令 $q_R(0)=\alpha$,再随机选择 d_R-1 个多项式 q_R 上的其他点,则多项式 q_R 定义完毕.对其他节点 x,令 $q_x(0)=q_{parent(x)}(index(x))$,并随机选择 d_x-1 个多项式 q_x 上的其他点,则多项式 q_x 定义完毕.当所有的多项式定义完毕后,则可以得到所有叶子节点的属性私钥.与 Threshold-Traceable-ABS 方案相比,$D_{u,1}$,$D_{u,2}$ 的计算方法不变;对叶子节点,$D_{i,1}$ 的计算方法也不变,而 $D_{i,2}=g_2^{q_x(0)}\cdot T(i)^{r_i}\cdot W(u)^s$.

Sign:对于用户 u,由 T_Ω的构造结构可知,叶子节点集合对应的属性集合即为Ω.

设 T_Ω的高度为 h_T,根节点所在的层数为顶层 0,叶子节点所在层数为 h_T-1.用户的属性集合Ω被分解为 h_T-2 个不相交的子集的并,即 $\Omega=\Omega_1\cup...\cup\Omega_{h_T-2}$,且对于所有的 $j_1,j_2=1,...,h_T-2$,$j_1\neq j_2$,有 $\Omega_{j_1}\cap\Omega_{j_2}=\varnothing$.

签名者使用如下方式构造签名策略树 T_Ψ:T_Ψ的根节点同 T_Ω的根节点,设根节点 R 要求的门限为 d_R,则只需在 T_Ω的 R 的孩子中选择至少 d_R 个节点,即可构成 T_Ψ的第 1 层节点.自顶向下继续上述操作,直至确定了所有需要签名的属性集合子集.

不妨设最终选定的属性集合子集为 $\gamma_1,...,\gamma_{n_s}$,其中,$n_s\leqslant h_T-2$,且对于 $j=1,...,n_s$,满足$\gamma_j\subseteq\Omega_j$.此时,$T_\Omega$中的其他叶

子节点及其对应的属性都不在 T_Ψ中.由访问树的构造结构可知,对于所有的 $j_1,j_2=1,...,n_s,j_1\neq j_2$,有 $\gamma_{j_1}\cap\gamma_{j_2}=\varnothing$.对每一个$\gamma_j$,选取 $\gamma'_j\cap\Omega=\varnothing$,显然有 $\gamma'_j\cap\gamma_j=\varnothing$,且对所有的 $j_1,j_2=1,...,n_s,j_1\neq j_2$,要求 $\gamma'_{j_1}\cap\gamma'_{j_2}=\varnothing$.令 $\Psi_j=\gamma_j\cup\gamma'_j$,设 Ω_j 的父节点为 x_j,x_j 要求的门限为 d_j,则 x_j 对应的签名策略为(Ψ_j,d_j,Φ_j).由上述的构造方式可知,对所有的 $j_1,j_2=1,...,n_s,j_1\neq j_2$,有 $\Psi_{j_1}\cap\Psi_{j_2}=\varnothing$.对于 $j\in\{1,\ldots,n_s\}$,使用 Ψ_j 替换γ_j,则签名策略树 T_Ψ构造完毕.每次签名时构造的签名策略树可以不同.

签名者使用签名策略树 T_Ψ对消息 m 做签名.对每一个 $\Psi_j(j=1,\ldots,n_s)$,分别采用 Threshold-Traceable-ABS 签名方案.最终的签名为 $\sigma=(\sigma_1,\sigma_2,\{\sigma_{3,i}\}_{i\in\Psi},\{\sigma_{4,j}\}_{j=1,\ldots,n_s},c_1,...,c_{n_u},\pi_1,...,\pi_{n_u})$,其中,$\sigma_{4,j}$ 为签名策略(Ψ_j,d_j,Φ_j)对应的签名数据,其计算方式与 Threshold-Traceable-ABS 方案中σ_4的计算方式相同.

Verify:验证者计算 $c=u'\prod_{i=1}^{n_u}c_i$,并对 $i=1,\ldots,n_u$,验证 $e(c_i,u_i^{-1}c_i)=e(h,\pi_i)$ 是否成立,若不成立则拒绝签名.

对 T_Ψ中的节点 x,定义函数 $VerifyNode(\sigma,x,T_\Psi)$.

对 $j=1,\ldots,n_s$,设 Ψ_j 对应的父节点为 x_j(即Ω_j 的父节点 x_j),x_j 所在的层数为 h_T–2,计算:

$$VerifyNode(\sigma,x_j,T_\Psi)=\frac{e(\sigma_{4,j},g)}{(\prod_{i\in\Psi_j}e(T(i),\sigma_{3,i}))\cdot e(c,\sigma_1)\cdot e(V(m),\sigma_2)}=e(g,g_2)^{q_{x_j}(0)}.$$

对 h_T–3 层及其上层的非叶子节点 x,递归计算如下:对 x 的所有孩子 x',计算 $VerifyNode(\sigma,x',T_\Psi)$,令 S_x 为节点 x 的所有孩子 x'组成的集合,$i=index(x')$, $S'_x=\{index(x'):x'\in S_x\}$,验证者计算

$$VerifyNode(\sigma,x,T_\Psi)=\prod_{x'\in S_x}VerifyNode(\sigma,x',T_\Psi)^{\Delta_{i,S'_x}(0)}=\prod_{x'\in S_x}(e(g,g_2)^{q_{x'}(0)})^{\Delta_{i,S'_x}(0)}=$$

$$\prod_{x'\in S_x}(e(g,g_2)^{q_{parent(x')}(index(x'))})^{\Delta_{i,S'_x}(0)}=\prod_{x'\in S_x}(e(g,g_2)^{q_x(i)})^{\Delta_{i,S'_x}(0)}=e(g,g_2)^{q_x(0)}.$$

当递归计算到根节点时,若 $F_R=e(g_1,g_2)$成立则接受签名,否则拒绝签名.

Trace:同 Threshold-Traceable-ABS 的 Trace.

与 Threshold-Traceable-ABS 方案相比,该方案的签名仅多了 n_s–1 个分量.该方案适用于由任意的 AND、OR 与门限组成的单调的访问结构.该方案的安全性分析与 Threshold-Traceable-ABS 的安全性分析类似.

5.2 可由任意线性秘密共享方案表达的访问结构

使用文献[2]中的方法,容易将 Threshold-Traceable-ABS 方案扩展到可由任意线性秘密共享方案表达的访问结构.文献[22]指出,对于可由任意线性秘密共享方案表达的访问结构,存在单调张成方案(monotone span program,简称 MSP),可以计算出对应的布尔函数值,反之亦然.

设 p,q 为两个大素数,$n=pq$,考虑 Z_n 循环群上的单调张成方案,对于矩阵 $\Lambda_{k_1\times k_2}$,行由属性值来标记,$span(\Lambda)$表示矩阵Λ的行向量生成的线性空间.则对于属性集合γ,若存在向量 $\tau_{1\times k_1}(\tau_j\in Z_n)$,其中,$\tau_j=0(j\notin\gamma)$,使得 $\tau\cdot\Lambda=\vec{1}$($\vec{1}$ 为全 1 向量),即存在单调布尔函数f_Λ,使得 $f_\Lambda(\gamma)=\vec{1}$,则签名者可使验证者确信他拥有属性集合$\gamma$[2].

Setup:基本同 Threshold-Traceable-ABS 的 Setup,除了不需要定义门限.

KeyGen:对于属性私钥 $D_{u,\Omega}=(D_{u,1},D_{u,2},\{(D_{i,1},D_{i,2})\}_{i\in\Omega})$,$D_{u,1},D_{u,2},D_{i,1}$ 的计算方法不变,$D_{i,2}$ 的计算方法如下:$D_{i,2}=g_2^{\Lambda_i\zeta}\cdot T(i)^{r_i}\cdot W(u)^s$,其中,向量 $\zeta_{k_2\times1}(\zeta_j\in Z_n)$ 满足 $\vec{1}\cdot\zeta=\alpha$ (α为主密钥).

Sign:用户 u 对消息 m 签名,签名者选择$\gamma\subseteq\Omega$,使得 $f_\Lambda(\gamma)=\vec{1}$.再随机选择属性集合$\gamma'$,其中,$\gamma\cap\gamma'=\varnothing$,令 $\Psi=\gamma\cup\gamma'$,签名策略为(Ψ,f_Λ,Φ).由 $f_\Lambda(\gamma)=\vec{1}$,即存在向量 $\tau_{1\times k_1}(\tau_j\in Z_n)$,其中,$\tau_j=0(j\notin\gamma)$,使得 $\tau\cdot\Lambda=\vec{1}$.签名者执行:

(1) 对于每一个 $j\in\gamma$,计算出τ_j,记 $s_3=\sum_{j\in\gamma}\tau_j$;

(2) 对 u 的每一个比特 $u[i](i=1,\ldots,n_u)$,按照原始方案计算(c_i,π_i),并计算θ和 c;

(3) 随机选取 $s'_1\in Z_n$,令 $s_1=s+s'_1$,计算 $\sigma_1=(D_{u,1}\cdot g^{s'_1})^{s_3}=(g^s\cdot g^{s'_1})^{s_3}=g^{s_1s_3}$;

(4) 随机选取 $s_2\in Z_n$,计算 $\sigma_2=g^{s_2}$;

(5) 对所有的 $i\in\Psi$,随机选取 $r'_i\in Z_n$,当 $i\in\gamma$时,计算 $\sigma_{3,i}=D_{i,1}^{\tau_i}\cdot g^{r'_i}=g^{r_i\tau_i+r'_i}$;当 $i\in\gamma'$时,计算 $\sigma_{3,i}=g^{r'_i}$;

(6) 计算 $\sigma_4 = V(m)^{s_2} \cdot (\prod_{i\in\gamma} D_{i,2}^{r_i}) \cdot (D_{u,2}^{\theta} \cdot c^{s_1'})^{s_3} \cdot \prod_{i\in\Psi} T(i)^{r_i'}$.

最终输出签名 $\sigma = (\sigma_1, \sigma_2, \{\sigma_{3,i}\}_{i\in\Psi}, \sigma_4, c_1, ..., c_{n_u}, \pi_1, ..., \pi_{n_u})$.

Verify:同 Threshold-Traceable-ABS 的 Verify.在此省略签名验证的正确性的计算过程.

Trace:同 Threshold-Traceable-ABS 的 Trace.

该方案的签名长度与Threshold-Traceable-ABS方案的签名长度相同.参考Threshold-Traceable-ABS与文献[2]的安全性分析,容易得到本方案的安全性证明.

6 结 论

本文在标准模型下,首先给出了一个门限的带ID的基于属性签名(threshold-ID-ABS)方案.签名者可以从他所拥有的属性集合中选取不小于门限的属性个数,并选择他所没有的任意属性,将其填充到他声明的属性集合中,从而使验证者无法确认签名者拥有哪些属性.在 Threshold-ID-ABS 方案的基础上,为了达到签名的不可联系性,并可由 PKG 追踪签名者的身份,我们使用了 Groth,Ostrovsky 和 Sahai 的关于比特加密的 NIWI 证明[15],将 Threshold-ID-ABS 方案扩展到 Threshold-Traceable-ABS 方案.再进一步,我们将 Threshold-Traceable-ABS 方案推广到更加通用的场景,适用于由任意的 AND、OR 与门限组成的单调的访问结构,以及可由任意线性秘密共享方案表达的访问结构.我们方案的安全性可以规约到子群判定假设和 CDH 假设.

References:

[1] Sahai A, Waters B. Fuzzy identity based encryption. In: Advances in Cryptology-EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 457−473.

[2] Goyal V, Pandey O, Sahai A, Waters B. Attribute-Based encryption for fine-grained access control of encrypted data. In: Proc. of the 13th ACM Conf. on Computer and Communications Security (CCS 2006). New York: ACM Press, 2006. 89−98. [doi: 10.1145/1180405.1180418]

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

[4] Ostrovsky R, Sahai A, Waters B. Attribute-Based encryption with non-monotonic access structures. In: Proc. of the 14th ACM Conf. on Computer and Communications Security (CCS 2007). New York: ACM Press, 2007. 195− 203. [doi: 10.1145/1315245.1315270]

[5] Cheung L, Newport C. Provably secure ciphertext policy ABE. In: Proc. of the 14th ACM Conf. on Computer and Communications Security (CCS 2007). New York: ACM Press, 2007. 456−465. [doi: 10.1145/1315245.1315302]

[6] Su JS, Cao D, Wang XF, Sun YP, Hu QL. Attribute-Based encryption schemes. Journal of Software, 2011,22(6):1299−1315 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3993.htm [doi: 10.3724/SP.J.1001.2011.03993]

[7] Yang P, Cao Z, Dong X. Fuzzy identity based signature with applications to biometric authentication. Computers & Electrical Engineering, 2011,37(4):532−540. [doi: 10.1016/j.compeleceng.2011.04.013]

[8] Emura K, Miyaji A, Omote K. A dynamic attribute-based group signature scheme and its application in an anonymous survey for the collection of attribute statistics. Journal of Information Processing, 2009,17:216−231. [doi: s10.2197/ipsjjip.17.216]

[9] Shahandashti SF, Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems. In: Proc. of the Progress in Cryptology-AFRICACRYPT 2009. Berlin, Heidelberg: Springer-Verlag, 2009. 198−216. [doi: 10.1145/1755688.1755697]

[10] Li J, Kim K. Hidden attribute-based signatures without anonymity revocation. Information Sciences, 2010,180:1681−1689. [doi: 10.1016/j.ins.2010.01.008]

[11] Li J, Au MH, Susilo W, Xie D, Ren K. Attribute-Based signature and its applications. In: Proc. of the 5th ACM Symp. on Information, Computer and Communications Security (ASIACCS 2010). New York: ACM Press, 2010. 60−69. [doi: 10.1145/1755688.1755697]

[12] Gagné M, Narayan S, Safavi-Naini R. Threshold attribute-based signcryption. In: Proc. of 7th Conf. on Security and Cryptography for Networks. Berlin, Heidelberg: Springer-Verlag, 2010. 154−171. [doi: 10.1007/978-3-642-15317-4_11]

[13] Maji HK, Prabhakaran M, Rosulek M. Attribute-Based signatures. In: Proc. of the Topics in Cryptology-CT-RSA 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 376−392. [doi: 10.1007/978-3-642-19074-2_24]

[14] Escala À, Herranz J, Morillo P. Revocable attribute-based signatures with adaptive security in the standard model. In: Proc. of the Progress in Cryptology-AFRICACRYPT 2011. Berlin, Heidelberg: Springer-Verlag, 2011. 224–241. [doi: 10.1007/978-3-642-21969-6_14]

[15] Groth J, Ostrovsky R, Sahai A. Perfect non-interactive zero knowledge for NP. In: Proc. of the Advances in Cryptology-EUROCRYPT 2006. Berlin, Heidelberg: Springer-Verlag, 2006. 339–358. [doi: 10.1007/11761679_21]

[16] Abe M, Fuchsbauer G, Groth J, Haralambiev K, Ohkubo M. Structure-Preserving signatures and commitments to group elements. In: Advances in Cryptology-CRYPTO 2010. Berlin, Heidelberg: Springer-Verlag, 2010. 209–236. [doi: 10.1007/978-3-642-14623-7_12]

[17] Groth J, Sahai A. Efficient non-interactive proof systems for bilinear groups. In: Advances in Cryptology-EUROCRYPT 2008. Berlin, Heidelberg: Springer-Verlag, 2008. 415–432. [doi: 10.1007/978-3-540-78967-3_24]

[18] Petersen H. How to convert any digital signature scheme into a group signature scheme. In: Proc. of the 5th Int'l Workshop on Security Protocols. Berlin, Heidelberg: Springer-Verlag, 1997. 177–190.

[19] Bellare M, Micciancio D, Warinschi B. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In: Advances in Cryptology-EUROCRYPT 2003. Berlin, Heidelberg: Springer-Verlag, 2003. 614–629. [doi: 10.1007/3-540-39200-9_38]

[20] Boyen X, Waters B. Compact group signatures without random oracles. In: Advances in Cryptology-EUROCRYPT 2006. Berlin, Heidelberg: Springer-Verlag, 2006. 427–444. [doi: 10.1007/11761679_26]

[21] Boneh D, Goh EJ, Nissim K. Evaluating 2-DNF formulas on ciphertexts. In: Proc. of the 2nd Theory of Cryptography Conf. (TCC 2005). Berlin, Heidelberg: Springer-Verlag, 2005. 325–341. [doi: 10.1007/978-3-540-30576-7_18]

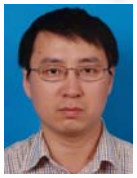
[22] Beimel A. Secure schemes for secret sharing and key distribution [Ph.D. Thesis]. Haifa: Israel Institute of Technology, 1996.

[23] Waters B. Efficient identity-based encryption without random oracles. In: Advances in Cryptology-EUROCRYPT 2005. Berlin, Heidelberg: Springer-Verlag, 2005. 114–127. [doi: 10.1007/11426639_7]

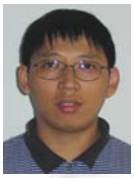
[24] Paterson KG, Schuldt JCN. Efficient identity-based signatures secure in the standard mode. In: Proc. of the11th Australasian Conf. on Information Security and Privacy (ACISP 2006). Berlin, Heidelberg: Springer-Verlag, 2006. 207–222. [doi: 10.1007/11780656_18]

附中文参考文献:

[6] 苏金树,曹丹,王小峰,孙一品,胡乔林.属性基加密机制.软件学报,2011,22(6):1299–1315. http://www.jos.org.cn/1000-9825/3993.htm [doi:10.3724/SP.J.1001.2011.03993]



张秋璞(1976－),男,河北高碑店人,博士生,主要研究领域为密码学.



叶顶锋(1966－),男,博士,教授,博士生导师,主要研究领域为密码分析,理论密码学.

徐震(1976－),男,博士,副研究员,CCF 会员,主要研究领域为网络与系统安全.