计算机研究与发展
Journal of Computer Research and Development
DOI: 10.7544/issn1000-1239.202220212
60(12): 2737−2748, 2023

前向安全的高效属性基可净化签名方案

朱留富[1] 李继国[1,2,3] 陆 阳[4] 张亦辰[1,2]

[1](福建师范大学计算机与网络空间安全学院 福州 350117)

[2](福建省网络安全与密码技术重点实验室(福建师范大学) 福州 350117)

[3](分析数学及应用教育部重点实验室(福建师范大学) 福州 350117)

[4](南京师范大学计算机与电子信息学院/人工智能学院 南京 210023)

Efficient and Forward-Secure Attribute-Based Sanitizable Signature Scheme

Zhu Liufu[1], Li Jiguo[1,2,3], Lu Yang[4], and Zhang Yichen[1,2]

[1](*College of Computer and Cyber Security*, *Fujian Normal University*, *Fuzhou* 350117)

[2](*Fujian Provincial Key Laboratory of Network Security and Cryptology* (*Fujian Normal University*), *Fuzhou* 350117)

[3](*Key Laboratory of Analytical Mathmatics and Applications* (*Fujian Normal University*), *Minstry of Education*, *Fuzhou* 350117)

[4](*School of Computer and Electronic Information/School of Artificial Intelligence*, *Nanjing Normal University*, *Nanjing* 210023)

Abstract In the attribute-based signature (ABS) scheme, the secret key of the signer is generated by attribute authority with different attributes, and the signature can be generated successfully only when the attributes meet the given signing policy. The verifier does not need to know the identity of the signer to determine whether the signature is valid. As a result, ABS has attracted wide attention due to its anonymity and fine-grained access control. In ABS scheme, once the key leakage occurs, the attacker can use the leaked key to generate a valid signature. The original message often contains some sensitive information. For example, in e-health or electronic finance scenario, personal privacy information is contained in personal medical records or transaction records. If the original message is not desensitized, sensitive personal information will be leaked. In order to solve the problems of key leakage and sensitive information leakage, an efficient and forward-secure attribute-based sanitizable signature (FABSS) scheme is proposed. The security of FABSS is reduced to the η-DHE (η-Diffie-Hellman exponent) assumption problem under the standard model. The proposed scheme not only protects signer privacy and supports fine-grained access control, but also has the ability to hide sensitive information and resist key leakage. In addition, the length of signature is constant, and only a constant number of pairing operations need to be calculated in the verification stage. Experimental analysis shows that the performance of the proposed scheme is efficient.

Key words attribute-based signature; forward security; sanitizablity; access control; standard-model

摘 要 在属性基签名(attribute-based signature, ABS)方案中,签名者密钥由不同的属性生成,只有当所拥有的属性满足给定的签名策略时才能够产生有效签名.验证者不需要知道签名者真实身份就能判断签名是否有效.所以ABS因其匿名性而受到广泛关注.在ABS方案中,一旦密钥发生泄露,那么获得密钥的攻击者就可以生成一个有效签名.原始消息中往往包含一些敏感信息,例如在电子医疗或电子金融场景中,个人的医疗记录或交易记录中包含个人隐私信息,若未经脱敏处理将会导致个人敏感信息泄露.为了解决密钥泄露和敏感信息泄露问题,提出了一种前向安全的高效属性基可净化签名(forward-secure attribute-

收稿日期: 2022-03-14; **修回日期**: 2022-12-23

基金项目: 国家自然科学基金项目(62072104, 61972095, U21A20465, U1736112, 61972190); 福建省自然科学基金项目(2020J01159)

This work was supported by the National Natural Science Foundation of China (62072104, 61972095, U21A20465, U1736112, 61972190) and the Natural Science Foundation of Fujian Province (2020J01159).

通信作者: 李继国(ljg1688@163.com)

based sanitizable signature, FABSS）方案.基于 η-DHE（η-Diffie-Hellman exponent）困难问题假设，在标准模型下证明了该方案的安全性.提出的方案不仅可以抵抗密钥泄露，保护签名者隐私，同时还具有敏感信息隐藏功能.此外，提出的方案具有固定签名长度，并且在验证阶段只需要计算常数个配对运算.实验分析表明提出方案的性能是高效的.

关键词 属性基签名；前向安全；可净化性；访问控制；标准模型

中图法分类号 TP391

自 2005 年 Sahai 等人[1]提出模糊身份基加密方案后，属性基密码体制成为研究的热点.属性基密码体制使用一组关联属性代替用户的身份信息，密文或密钥与一个事先定义的访问策略或是谓词结构相关联，当用户的属性满足访问策略或谓词结构时就可以进行解密.因此属性基密码克服了身份基密码一对一的通信限制，只要用户拥有满足访问策略或谓词结构的属性集就可以进行通信，从而实现了一对多的通信并实现了细粒度的访问控制[2-3].为了满足不同的应用需求，一些新型的属性基加密方案[4-11]和属性基签名方案[12-15]相继被提出.

在属性基签名方案中，由于使用一组属性集代替用户，隐藏了真实的身份信息从而获得了匿名性.签名者根据属性授权机构颁发的属性密钥对消息进行签名，属性密钥由属性授权机构产生并秘密发送给签名者，一旦属性密钥发生泄露或密钥传输时遭受主动攻击被截获，那么获得密钥的任何人都能产生一个有效签名.与此同时，签名数据中可能包含一些敏感信息，例如身份证号、手机号或者个人金融交易记录等.这些敏感信息泄露可能会带来个人隐私泄露甚至是国家机密泄露的极大风险.因此属性基签名中的密钥泄露和敏感信息泄露问题是亟待解决的关键问题.

本文的主要贡献包括 3 个方面：

1）提出了前向安全的高效属性基可净化签名（efficient and forward-secure attribute-based sanitizable signature, FABSS）方案，并在标准模型下证明该方案的安全性.方案的安全性可规约到 η-DHE（η-Diffie-Hellman exponent）困难问题假设.

2）提出的方案利用属性集合和谓词结构提供细粒度访问控制，保护签名者的隐私；利用前向安全技术解决了密钥泄露问题；利用可净化签名技术对原始数据进行脱敏，解决了敏感数据泄露问题.

3）提出的方案具有固定签名长度，并且在验证阶段只需要常数个配对运算，使得通信开销和计算开销低，因此提出的方案具有高效性.

1 相关工作

属性基加密方案根据访问策略的不同布置可分为密钥策略的属性基加密方案[2]和密文策略的属性基加密方案[16].在密钥策略的属性基加密方案中，用户访问策略与密钥关联，一组属性集与密文相关联.当密文中的属性集满足访问策略时，用户可以正确解密该密文.在密文策略的属性基加密方案中，事先定义的一个访问策略嵌入到密文中，密钥由用户属性集标识，只有当标识密钥的属性集满足密文中的访问策略时用户才能正确解密.

为了解决数据完整性、认证性以及用户细粒度访问控制问题，Maji 等人[17]在 2011 年首次提出属性基签名方案，并在一般群模型中证明了该方案的安全性.Okamoto 等人[18]基于 CDH（computational Diffie-Hellman）困难问题假设，提出了标准模型下证明安全的属性基签名方案.标准模型下证明安全的方案通常需要大量的计算开销，其中配对运算的代价尤其高昂.为了提高效率，Gagn 等人[19]设计了具有短配对运算的高效属性基签名方案.为了进一步提高效率，Anada 等人[20]提出了无配对运算的属性基签名方案.然而文献 [19-20] 中的方案仅仅考虑性能的提升而没有考虑密钥泄露问题.在密钥颁发和存储过程中，可能会遭受主动攻击或者由于管理不当造成密钥泄露，恶意攻击者在获得密钥后就能产生任意时间片段签名.为了解决密钥泄露问题，在 2015 年，Wei 等人[21]提出了门限结构的前向安全属性基签名方案，并在标准模型下给出了安全性证明.另一个解决密钥泄露的方法是密钥隔离技术，2017 年，Rao[22]提出一个签名策略的属性基密钥隔离签名，将密钥分为长期密钥和短期密钥，并将长期密钥保存在一个安全的设备中，从而保证了密钥的安全.然而在签名方案中，可能发生泄露的不仅仅有签名者密钥，同时还包括消息中的一些敏感信息，例如个人医疗记录信息、金融机构交易信息以及政府部门政务信息等.这些信息一旦发生泄露将会给个人、金融市场或者政府部

门带来极大的安全风险. 因此我们需要对数据中的敏感数据进行编辑从而隐藏真实信息，这样的方法可称之为“净化”. 在可净化签名中，净化者可以在不知道签名者密钥的前提下对数据进行编辑并重新生成一个有效签名. Ateniese 等人[23]首次提出可净化签名概念，利用变色龙哈希设计了可净化签名方案并在随机预言模型下给出了安全性证明. Agrawal 等人[24]提出了在标准模型下证明安全的可净化签名方案，方案的安全性规约到 CDH 困难问题假设. 但该方案需要大量的配对运算和指数运算，具有较高的运算开销. 为了改进效率，Pöhls 等人[25]提出了高效的可净化方案. 可审计性要求签名者可以对净化者的行为进行追责，2017 年，Beck 等人[26]提出一个具有强审计性的可净化签名，不仅实现对净化者的追责，同时也防止签名者对净化者的恶意指责. 为了获得细粒度访问控制和以及签名者隐私，刘西蒙等人[27]给出属性基可净化签名方案的构造并在标准模型下给出了方案的安全性证明. 文献 [25] 利用门限结构作为访问策略，为了获得更丰富和灵活的访问结构，莫若等人[28]和 Mo 等人[29]先后给出了基于树形访问结构的属性基可净化签名方案和具有灵活访问结构的属性基可净化签名方案，方案支持与门、或门和门限结构. 为了同时获得访问控制和可审计性，Samelin 等人[30]提出了属性基可净化签名并实现了对净化者的追责. 为了解决属性基签名中签名者滥用签名问题，李继国等人[31]提出了可追踪的属性基可净化签名方案，不仅实现了恶意用户追踪，而且还保证了敏感数据的隐私.

2 预备知识

本节介绍 FABSS 方案中使用的相关密码学知识，其中包括双线性映射、拉格朗日插值、η-DHE假设.

2.1 双线性映射

令G_1和G_2是 2 个 p阶乘法循环群，p是大素数.g是G_1的一个生成元. 一个双线性映射$e:G_1\times G_1\to G_2$具有 3 个性质：

1）双线性. 对任意$a,b\in\mathbb{Z}_p$, 都有$e\left(g^a,g^b\right)=e(g,g)^{ab}$.

2）非退化性. $e(g,g)\neq 1$.

3）可计算性. 对所有$g_1,g_2\in G_1$, 存在多项式时间算法计算$e(g_1,g_2)$.

2.2 拉格朗日插值

设p为素数，$S\subseteq\mathbb{Z}_p$, 拉格朗日系数定义为$\Delta_i^S(x)=\prod_{j\in S,\,j\neq i}\frac{x-j}{i-j}$, 其中$i\in\mathbb{Z}_p$. 给定$\mathbb{Z}_p$上的$d$个点$(1,q_1),(2,q_2),\cdots,(d,q_d)$, $d-1$次多项式$q(x)$可以重构为$q(x)=\sum_{i\in S}q(i)\Delta_i^S(x)$, 其中$|S|=d$.

2.3 η-DHE 问题和困难问题假设

η-DHE 问题. G_1是一个 p阶群，g 是G_1的一个生成元，随机选取$a\in\mathbb{Z}_p$.给定元组$(g,g^a,g^{a^2},\cdots,g^{a^\eta},g^{a^{\eta+2}},\cdots,g^{a^{2\eta}})$, 计算$g^{a^{\eta+1}}$.

ε-(η-DHE) 困难问题假设. 若不存在多项式时间算法以不可忽略的概率ε解决G_1上的 η-DHE 困难问题，则称ε-η-DHE 困难问题假设在群G_1上是成立的.

3 形式化定义和安全模型

借鉴文献 [21] 中前向安全的属性基签名的形式化定义，本节给出 FABSS 方案的形式化定义和安全模型.

3.1 FABSS 方案的形式化定义

FABSS 方案包括设置、密钥生成、密钥更新、签名、净化和验证 6 个算法，每个算法的定义为：

1）设置. 算法输入安全参数λ、系统时间片段总数T、系统门限值d，输出公共参数$params$和主密钥msk.

2）密钥生成. 该算法由属性授权中心执行. 算法输入公共参数 $params$、主密钥msk、签名者属性集w_{a}以及初始时间片段t_0, 输出初始时间片段密钥SK_{t_0}.

3）密钥更新. 该算法由签名者执行. 算法输入公共参数 $params$、当前时间片段t_j的密钥SK_{t_j}以及时间片段$t_{j'}$, 其中$t_j<t_{j'}$.算法输出时间片段$t_{j'}$的密钥$SK_{t_{j'}}$.

4）签名. 算法输入公共参数 $params$、当前时间片段t_j的密钥SK_{t_j}、消息M、签名者属性集w_{a}、净化者属性集w_τ以及签名策略$\Gamma_{d,S}(\cdot)$. 若签名者属性集w_{a}满足签名策略$\Gamma_{d,S}(\cdot)$, 即$|w_{\mathrm{a}}\cap S|\geqslant d$, 算法输出消息$M$的签名$\sigma$以及秘密值集合$SI$. 其中$d$是门限值，$S$是谓词结构中的属性集合.

5）净化. 该算法由净化者执行. 签名者公开声明允许净化的消息索引集合$I_N\subseteq\{1,2,\cdots,n_m\}$, 其中$N\leqslant n_m$.净化者获得由签名者发送的秘密值集合$SI$. 算法输入消息$M$、签名$\sigma$、签名者属性集$w_{\mathrm{a}}$、净化者属性集$w_\tau$以及秘密值集合$SI$. 算法输出净化消息$M'$和净化签名$\sigma'$.

6）验证. 算法输入公共参数 $params$、当前时间片段t_j、消息M'以及签名σ'. 若验证签名有效，输出 accept; 否则，输出 reject.

FABSS 系统框架如图 1 所示. 签名者将属性集w_{a}以及初始时间片段t_0发送给属性授权中心，属性授权中心为签名者生成时间片段t_0的密钥SK_{t_0}. 签名者

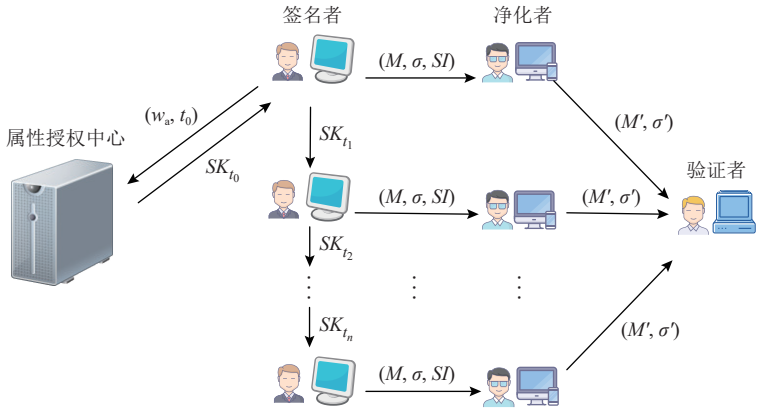


Fig. 1 The framework of FABSS

图 1 FABSS 框架

用私钥SK_{t_0}对消息M进行签名获得σ, 并生成秘密值集合SI, 将(M, σ, SI)通过安全信道发送给净化者. 净化者对允许净化范围内的消息进行修改, 重新生成关于净化后消息M'的签名σ'. 净化者将(M', σ')发送给验证者, 验证者通过验证算法判断签名是否有效. 此后, 签名者通过密钥更新算法生成时间片段t_1的密钥SK_{t_1}, 并重复上述过程.

3.2 安全模型

借鉴文献 [21] 的思想, 给出 FABSS 方案的前向安全性和不变性安全模型.

3.2.1 前向安全性

FABSS 方案满足传统 ABS 方案不可伪造性的同时达到了前向安全性. FABSS 方案的前向安全性可以通过挑战者 B 和敌手 A 之间的游戏来刻画.

基于文献 [21] 给出的安全模型, 定义 FABSS 的前向安全性游戏.

1)初始化. A 将需要挑战的签名策略$\Gamma_{d^*,S^*}(\cdot)$和时间片段t_{j^*}发送给 B.

2)设置. B 运行设置算法, 生成公共参数 $params$ 和主密钥msk, 设置初始时间片段t_0. 挑战者 B 将公共参数 $params$发送给 A, 主密钥msk保密.

3)密钥生成询问. A 自适应选择属性w_a和时间片段t_j, 将w_a和t_j交给 B. 通过密钥生成算法, B 生成对应的密钥SK_{t_j}并发送给 A.

4)密钥更新询问. A 随机选择一个新时间片段t_j并要求 B 执行密钥更新算法, 此时当前时间片段t_j被更新为后一时间片段$t_{j'}$, B 将更新后的密钥$SK_{t_{j'}}$发送给 A.

5)签名询问. A 自适应地选择签名者属性集w_a, 净化者属性集w_τ, 消息M和签名策略$\Gamma_{d,S}(\cdot)$并发送给 B, B 通过签名算法产生当前时间片段t_j的签名σ, 并发送给 A.

6)伪造. A 生成关于消息$M^* = \{m_1^*, m_2^*, \cdots, m_{n_m}^*\}$, 签名策略$\Gamma_{d^*,S^*}(\cdot)$在时间片段$t_{j^*}$的签名$\sigma^*$. 若满足条件①~③, 则称 A 赢得前向安全性游戏.

① σ^*是一个有效签名;

② A 没有对(w_a, t_j)进行密钥生成询问, 其中属性集w_a满足签名策略$\Gamma_{d^*,S^*}(\cdot)$并且$t_j \leqslant t_{j^*}$;

③ A 没有在时间片段t_{j^*}对消息$M^* = \{m_1^*, m_2^*, \cdots, m_{n_m}^*\}$进行签名询问.

定义 1. 对于任意概率多项式时间t的敌手, 如果赢得上述游戏的概率ε是可忽略的, 那么就称 FABSS 方案满足前向安全性.

3.2.2 不变性

FABSS 方案的不变性要求净化者只能对允许净化范围内的消息进行修改, 无法对净化范围之外的消息进行任何操作. 不变性可以通过敌手 A 和挑战者 B 之间的游戏来刻画.

1)初始化. A 将挑战索引集合I_N^*和签名策略$\Gamma_{d^*,S^*}(\cdot)$发送给 B, 其中I_N^*表示净化者可以执行净化操作的消息索引集合.

2)设置. B 执行设置算法产生公开参数 $params$和主密钥msk, 将公开参数 $params$发送给 A, 主密钥msk保密.

3)询问. A 自适应地进行多项式次密钥生成询问, 密钥更新询问和签名询问. 其中 A 可以进行q_s次签名询问, 在第j次签名询问中, A 询问关于消息$M_j = \{m_{j,1}, m_{j,2}, \cdots, m_{j,n_m}\}$的签名$\sigma_j$. B 将签名σ_j和秘密值集合SI发送给 A.

4)伪造. A 输出关于消息$M^* = \{m_1^*, m_2^*, \cdots, m_{n_m}^*\}$, 时间片段$t_{j^*}$和签名策略$\Gamma_{d^*,S^*}(\cdot)$的签名$\sigma^*$, 若满足条件①~③, 则称 A 赢得不变性游戏.

① σ^*是一个有效签名；

② A 没有对(w_a, t_j)进行密钥生成询问，其中属性集合w_a满足签名策略$\Gamma_{d^*,S^*}(\cdot)$并且$t_j \leqslant t_{j^*}$；

③ 对于任何$j \in \{1, 2, \cdots, q_s\}$，存在$i \notin I_N^*$使得$m_{j,i} \neq m_i^*$.

定义 2. 如果任意概率多项式时间t的敌手进行至多q_k次密钥询问和至多q_s次签名询问，最终赢得不变性游戏的概率ε是可忽略的，则 FABSS 方案具有ε-不变性.

4 方案构造

根据文献 [32] 给出的二叉树结构，利用该结构分配时间片段. 在二叉树结构中，如图 2 所示，将完整时间片段T分解为$t_0, t_1, \cdots, t_{T-1}$时间片段. 每个时间片段对应一个层数为$l$的满二叉树的叶子节点. 其中根节点用一个空串$\gamma$标记，$k(1 \leqslant k \leqslant l)$层上的每个节点$v$用一个二进制比特串$b_v \in \{0, 1\}^k$表示，$b_v$与节点$v$到根节点的路径相关，其中 0 表示左子节点，1 表示右子节点. 对每个二进制串$b \in \{0, 1\}^k$，都对应二叉树第k层上的一个节点，将这个节点记为v_b，并令$b_v[i]$表示b_v中的第i位. 例如初始时间片段t_0对应节点v_{t_0}，$b_{v_{t_0}} = 0^l$；t_1时间片段的节点为v_{t_1}，$b_{v_{t_1}} = 0^{l-1}1$. 用$Path_v$表示节点v到根节点路径上包含的所有节点的集合，$R(v)$表示v的右子节点. 对于时间片段t_j及其对应的节点v_{t_j}，定义集合$V_{t_j} = \{R(v) | v \in Path_{v_{t_j}}, R(v) \notin Path_{v_{t_j}}\} \cup \{v_{t_j}\}$. 如图 2 所示，$Path_{v_{t_0}} = \{\gamma, v_0, v_{00}, v_{t_0}\}$，$V_{t_0} = \{v_1, v_{01}, v_{t_1}, v_{t_0}\}$. 基于上述构造，可得引理 1.

引理 1. 存在时间t_j和$t_{j'}$，若$t_{j'} > t_j$，对于每个节点$v' \in V_{t_{j'}}$，存在一个节点$v \in V_{t_j}$，有$b_{v'} = b_v \| b^*$. 其中，$b^* \in \{0, 1\}^k$，$k = |b_{v'}| - |b_v|$.

1）设置. 选取安全参数λ，生成p阶双线性群G_1和G_2，其中p是大素数；$e: G_1 \times G_1 \to G_2$是双线性映射. 令$T = 2^l$为总时间片段，$U = \{1, 2, \cdots, n+d\}$表示属性域，其中$n$为常数. $\Omega = \{\omega_1, \omega_2, \cdots, \omega_{d-1}\}$为缺省属性集，$\omega_i \in \mathbb{Z}_p$. 设$S \subseteq \mathbb{Z}_p$，且$i \in S$，定义拉格朗日系数$\Delta_i^S(x) = \prod_{j \in S, j \neq i} \frac{x-j}{i-j}$. 随机选取$\alpha \in \mathbb{Z}_p^*$，计算$Z = e(g, g)^\alpha$，其中$g$是$G_1$的生成元. 随机选取群元素$f_a, f_\tau$和群元素集合$H = \{h_1, h_2, \cdots, h_l\}$，$W = \{w_1, w_2, \cdots, w_{n_m}\}$，$F = \{f_1, f_2, \cdots, f_\eta\}$，其中$n_m$是消息长度，$\eta = n + d - 1$. 则 $params = \{G_1, G_2, e, g, h_0, w_0, f_a, f_\tau, H, W, F, T, U, \Omega, Z\}$是公共参数，主密钥为$\alpha$.

2）密钥生成. 算法输入签名者属性集$w_a \subseteq U$，主密钥α，公共参数$params$和初始时间片段t_0. 首先选择一个$d-1$次多项式$q(x)$，满足$q(0) = \alpha$. 随机选取$r_i \in \mathbb{Z}_p$，其中$i \in w_a$；随机选取$r_{i,v} \in \mathbb{Z}_p$，其中$v \in V_{t_0}$. 计算$\mu_i = g^{r_i}$；$\varphi_i = \{f_1^{r_i}, f_2^{r_i}, \cdots, f_{i-1}^{r_i}, f_{i+1}^{r_i}, .., f_\eta^{r_i}\}$；$sk_{i,v} = (g^{q(i)}(f_a f_i)^{r_i} \cdot \left(h_0 \prod_{k=1}^{|b_v|} h_k^{b_v[k]}\right)^{r_{i,v}}, g^{r_{i,v}}, h_{|b_v|+1}^{r_{i,v}}, \cdots, h_l^{r_{i,v}})$.因此$t_0$时间片段的密钥$SK_{t_0} = \{\mu_i, \varphi_i, \{sk_{i,v} | v \in V_{t_0}\}\}$，其中$i \in w_a$.

3）密钥更新. 算法输入当前时间片段t_j的密钥SK_{t_j}，后续时间片段$t_{j'}$和公共参数$params$. 将当前时间片段密钥SK_{t_j}表示成：

$sk_{i,v} = \{a_{i,0}, a_{i,1}, a_{i,|b_v|+1}, \cdots, a_{i,l}\}$，$SK_{t_j} = \{\mu_i, \varphi_i, \{sk_{i,v} | v \in V_{t_j}\}\}$，因为$t_{j'} > t_j$，由文献 [32] 可得，对每个节点$v' \in V_{t_{j'}}$，一定存在节点$v \in V_{t_j}$，有$b^*$满足$b_{v'} = b_v \| b^*$. 随机选取$r_i' \in \mathbb{Z}_p$，其中$i \in w_a$；随机选取$r_{i,v'} \in \mathbb{Z}_p$，其中$v' \in V_{t_{j'}}$. 计算$\mu_i' = \mu_i \times g^{r_i'}$；$\varphi_i' = \{f_1^{r_i} f_1^{r_i'}, f_2^{r_i'}, \cdots, f_{i-1}^{r_i} f_{i-1}^{r_i'}, f_{i+1}^{r_i} f_{i+1}^{r_i'}, \cdots, f_\eta^{r_i} f_\eta^{r_i'}\}$；$sk_{i,v'} = \left\{a_{i,0}(f_a f_i)^{r_i'} \left(h_0 \prod_{k=1}^{|b_{v'}|} h_k^{b_{v'}[k]}\right)^{r_{i,v'}} \prod_{k=|b_v|+1}^{|b_{v'}|} a_{i,k}^{b_{v'}[k]}, a_{i,1} g^{r_i'}, a_{i,|b_{v'}|+1} h_{|b_{v'}|+1}^{r_{i,v'}}, \cdots, a_{i,l} h_l^{r_{i,v'}}\right\} = \{a_{i,0}', a_{i,1}', a_{i,2}', a_{i,|b_{v'}|+1}', \cdots, a_{i,l}'\}$. 时间片段$t_{j'}$的密钥为$SK_{t_{j'}} = \{\mu_i', \varphi_i', \{sk_{i,v'} | v' \in V_{t_{j'}}\}\}$，删除当前时间片段$t_j$的密钥$SK_{t_j}$.

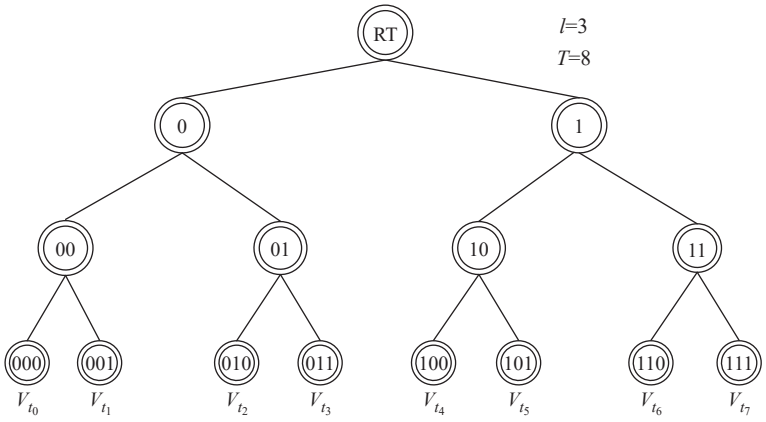


Fig. 2 Binary evolutionary tree of time

图 2 时间的二叉进化树

4)签名. 算法输入消息$M=\{m_1,m_2,\cdots,m_{n_m}\}$, 签名策略$\Gamma_{d,S}(\cdot)$, 签名者属性集$w_{\mathrm{a}}$, 净化者属性集$\widehat{w_\tau}$, 密钥$SK_{t_j}$, 要求属性集$w_{\mathrm{a}}$满足$\Gamma_{d,S}(w_{\mathrm{a}})=1$, 即$|w_{\mathrm{a}}\cap S|\geqslant d$. 因此存在属性$w'_{\mathrm{a}}\subseteq w_{\mathrm{a}}\cap S$, 其中$\left|w'_{\mathrm{a}}\right|=d$. 选取缺省属性集$\Omega'\subset\Omega$, 满足$w'_{\mathrm{a}}\cap\Omega'=\varnothing$. 令$\widehat{w_{\mathrm{a}}}=w'_{\mathrm{a}}\cup\Omega'$, 当$i\in\widehat{w_{\mathrm{a}}}$, 计算$\bar{a}_{i,0}=a_{i,0}\prod_{j\in\widehat{w_{\mathrm{a}}},j\neq i}f_j^{r_i}=\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{r_{i,v_{t_j}}}g^{q(i)}\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_i}$; $a_0=\prod_{i\in\widehat{w_{\mathrm{a}}}}\left(\bar{a}_{i,0}\right)^{\Delta_i^{\widehat{w_{\mathrm{a}}}}(0)}=\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{r}\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r'}\cdot g^{\alpha}$; $a_1=\prod_{i\in\widehat{w_{\mathrm{a}}}}\left(a_{i,1}\right)^{\Delta_i^{\widehat{w_{\mathrm{a}}}}(0)}=g^{r}$; $\mu'=\prod_{i\in\widehat{w_{\mathrm{a}}}}(\mu_i)^{\Delta_i^{\widehat{w_{\mathrm{a}}}}(0)}=g^{r'}$. 此时有$r=\sum_{i\in\widehat{w_{\mathrm{a}}}}\Delta_i^{\widehat{w_{\mathrm{a}}}}(0)\cdot r_{i,v_{t_j}}$; $r'=\sum_{i\in\widehat{w_{\mathrm{a}}}}\Delta_i^{\widehat{w_{\mathrm{a}}}}(0)\cdot r_i$. 随机选取$r_{\mathrm{a}}, s, z, r_\tau\in\mathbb{Z}_p$, 计算$\sigma_0=a_0\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s}\left(w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)^{z}\cdot\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}$; $\sigma_1=a_1g^{s}$; $\sigma_2=\mu'\cdot g^{r_{\mathrm{a}}}$; $\sigma_3=g^{r_\tau}$; $\sigma_4=g^{z}$. 因此在当前时间片段t_j产生的签名为$\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$. 签名者计算秘密值$SI_i=w_i^{z}$, 其中$i\in I_N$. 用$SI$表示秘密值集合, 即$SI=\{SI_1,SI_2,\cdots,SI_{|I_N|}\}$, $I_N=\{1,2,\cdots,N\}$表示签名者允许净化的消息索引集合, 其中$N\leqslant n_m$.

5)净化. 净化者获得签名σ和秘密值集合SI, 首先通过验证算法判断签名是否有效, 若是有效签名, 定义此次需要净化的消息索引集$I\subseteq I_N$. 令$I_1=\{i\in I:m_i=0,m'_i=1\}$; $I_2=\{i\in I:m_i=1,m'_i=0\}$. 净化者随机选取$r'_{\mathrm{a}}$, $s',z',r'_\tau\in\mathbb{Z}_p$, 计算$\sigma'_0=\sigma_0\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r'_{\mathrm{a}}}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s'}\cdot\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r'_\tau}\frac{\prod_{i\in I_1}SI_i}{\prod_{i\in I_2}SI_i}\left(\prod_{j=1}^{n_m}w_j^{m'_i}\cdot w_0\right)^{z'}$; $\sigma'_1=\sigma_1g^{s'}$; $\sigma'_2=\sigma_2g^{r'_{\mathrm{a}}}$; $\sigma'_3=\sigma_3g^{r'_\tau}$; $\sigma'_4=\sigma_4g^{z'}$. 净化后的签名为$\sigma'=\{\sigma'_0,\sigma'_1,\sigma'_2,\sigma'_3,\sigma'_4\}$.

6)验证. 为了验证签名是否有效, 需要计算等式$Z=\dfrac{e(\sigma'_0,g)}{e\left(\sigma'_1,h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)e\left(\sigma'_2,f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)}\cdot\dfrac{1}{e\left(\sigma'_3,f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)e\left(\sigma'_4,w_0\prod_{j=1}^{n_m}w_j^{m'_i}\right)}$是否成立. 若等式成立, 则签名有效; 否则拒绝该签名. 验证算法不仅可用于验证净化消息签名对, 同时也可以验证非净化的消息签名是否有效.

5 安全性分析

本节将分别给出FABSS方案的安全性分析.

5.1 正确性

验证方程既能验证原始签名σ, 同时也能验证净化签名σ'. 首先给出对原始签名σ的验证过程, 在5.2节中给出净化签名的净化性分析. 给定签名$\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, 通过证明等式(1)成立, 表明FABSS方案满足正确性要求. 下面分别验证方程中的每一部分.

$$(\sigma_0,g)=e\left(g,\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}+r'}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s+r}\cdot\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\left(w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)^{z}g^{\alpha}\right)=$$
$$e(g^{\alpha},g)e\left(\left(w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)^{z},g\right)e\left(g,\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\cdot\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}+r'}\right)e\left(g,\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s+r}\right);$$

$$e\left(\sigma_1,h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)=e\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]},g^{r+s}\right)=e\left(\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{r+s},g\right);$$

$$e\left(\sigma_2,f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)=e\left(g^{r_{\mathrm{a}}+r'},f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)=e\left(g,\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}+r'}\right);$$

$$e\left(\sigma_3,f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)=e\left(g^{r_b},f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)=e\left(g,\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\right);$$

$$e\left(\sigma_4,w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)=e\left(w_0\prod_{j=1}^{n_m}w_j^{m_i},g^{z}\right)=e\left(g,\left(w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)^{z}\right);$$

因此有

$$\frac{e(\sigma_0, g)}{e\left(\sigma_1, h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)e\left(\sigma_2, f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)e\left(\sigma_3, f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)}\cdot\frac{1}{e\left(\sigma_4, w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)}=e(g,g)^{\alpha}=Z. \tag{1}$$

综上所述，方案满足正确性.

5.2 净化性

净化者操作后的净化签名为$\sigma'=\{\sigma'_0,\sigma'_1,\sigma'_2,\sigma'_3,\sigma'_4\}$.当$i\in I_1$时，$m'_i-m_i=1$，$\sigma'$记为 1；当$i\in I_2$时，$m'_i-m_i=-1$，$\sigma'$记为 0. $\sigma'_0=\sigma_0\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r'_{\mathrm{a}}}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s'}\cdot\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r'_\tau\prod_{i\in I_1}SI_i\Big/\prod_{i\in I_2}SI_i}\left(w_0\prod_{j=1}^{n_m}w_j^{m'_i}\right)^{z'}=\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau+r'_\tau}\cdot g^{\alpha}\cdot\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}+r'+r'_{\mathrm{a}}}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s+r+s'}\cdot\left(w_0\prod_{j=1}^{n_m}w_j^{m'_i}\right)^{z+z'}$；$\sigma'_1=\sigma_1g^{s'}=g^{r+s+s'}$，$\sigma'_2=\sigma_2g^{r'_{\mathrm{a}}}=g^{r_{\mathrm{a}}+r'+r'_{\mathrm{a}}}$，$\sigma'_3=\sigma_3g^{r'_\tau}=g^{r_\tau+r'_\tau}$，$\sigma'_4=\sigma_4g^{z'}=g^{z+z'}$. 综上所述，净化后的签名$\sigma'=\{\sigma'_0,\sigma'_1,\sigma'_2,\sigma'_3,\sigma'_4\}$与原始签名$\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$有相同的分布. 因此签名$\sigma'$和$\sigma$都能通过验证方程.

5.3 前向安全性

定理 1. 在ε'-(η-DHE)困难问题假设下，提出的 FABSS 方案具有$(\varepsilon, q_{\mathrm{s}})$-前向安全性. 其中$\varepsilon'\geqslant\dfrac{\varepsilon}{4T\times q_{\mathrm{s}}\times(n_m+1)}$，$T$是时间片段总数，$n_m$是消息的长度，$q_{\mathrm{s}}$是敌手$A$进行签名询问的次数.

证明. 通过敌手A和挑战者B之间的交互游戏证明定理 1.

1）初始化. 给B一个η-DHE困难问题的随机实例$\{g, g_1=g^a, g_2=g^{a^2},\cdots,g_\eta=g^{a^\eta}, g_{\eta+2}=g^{a^{\eta+2}},\cdots,g_{2\eta}=g^{a^{2\eta}}\}$，其中$g$是素数阶群$G_1$的生成元，$a\in\mathbb{Z}_p$. A选择挑战签名谓词$\Gamma_{d^*,S^*}(\cdot)$和时间片段t_{j^*}并发送给B，其中$0\leqslant t_{j^*}\leqslant T=2^l-1$. 同时定义属性域$U=\{1,2,\cdots,n+d\}$，其中$n$是常数. 选择缺省属性集$\Omega=\{\omega_1,\omega_2,\cdots,\omega_{d-1}\}$. 在以下交互中，$B$尝试计算得到$g_{\eta+1}=g^{a^{\eta+1}}$.

2）设置. B通过如下方式生成公共参数$params$和主密钥msk. B随机选取$\alpha',\delta_{\mathrm{a}},\delta_\tau,\delta_1,\cdots,\delta_\eta\in\mathbb{Z}_p$，计算$f_i=g^{\delta_i}g_{\eta-i+1}$，其中$1\leqslant i\leqslant\eta$；选择缺省属性子集$\Omega^{*'}\subset\Omega$，计算$f_{\mathrm{a}}=g^{\delta_{\mathrm{a}}}\prod_{i\in S^*\cup\Omega^{*'}}f_i^{-1}$；令$w_\tau\subseteq U$，计算$f_\tau=g^{\delta_\tau}\prod_{i\in w_\tau}f_i^{-1}$；随机选取$\theta_0,\theta_1,\cdots,\theta_l\in\mathbb{Z}_p$，计算$h_k=g^{\theta_k}g_{\eta-k+1}^{-1}$，$h_0=g^{\theta_0}\prod_{k=1}^{l}g_{\eta-k+1}^{b_{v_{t_{j^*}}}[k]}$，其中$1\leqslant k\leqslant l$；随机选取$\zeta\in\{0,1,\cdots,n_m\}$以及 2 个随机数集合$X=\{x_0,x_1,\cdots,x_{n_m}\}$和$Y=\{y_0,y_1,\cdots,y_{n_m}\}$，其中$x_i\in\mathbb{Z}_{2q_{\mathrm{s}}-1}$，$y_i\in\mathbb{Z}_p$；计算$w_i=g_1^{x_i}g^{y_i}$，$w_0=g_1^{x_0-2\zeta q_{\mathrm{s}}}g^{y_0}$，其中$1\leqslant i\leqslant n_m$；计算$Z=e\left(g_1,g_\eta\right)e(g,g)^{\alpha'}=e(g,g)^{\alpha'+a^{\eta+1}}$. 最后$B$设置$params=\{G_1,G_2,e,g,f_{\mathrm{a}},f_\tau,h_0,w_0,U,\Omega,T,H,W,Z\}$为公共参数，主密钥$msk$为$\alpha=\alpha'+a^{\eta+1}$. 定义 2 个函数，$J(M)=x_0+\sum_{j=1}^{n_m}x_jm_j-2\zeta q_{\mathrm{s}}$；$K(M)=y_0+\sum_{j=1}^{n_m}y_jm_j$. 此时$w_0\prod_{j=1}^{n_m}w_j^{m_i}=g_1^{J(M)}g^{K(M)}$.

3）密钥生成询问. A最多进行q_{k}次密钥生成询问. A询问属性集w_{a}在时间片段t_j的密钥SK_{t_j}，此时必须满足$|w_{\mathrm{a}}\cap S^*|<d^*$或者$|w_{\mathrm{a}}\cap S^*|\geqslant d^*$，$t_j>t_{j^*}$. 下面分别讨论这 2 种情况.

①当$|w_{\mathrm{a}}\cap S^*|<d^*$时，$B$定义 3 个属性集合$\Gamma,\Gamma',S$，使$\Gamma=(w_{\mathrm{a}}\cap S^*)\cup\Omega^{*'}$，$\Gamma\subseteq\Gamma'\subseteq S$，其中$|\Gamma'|=d^*-1$. 令$S=\Gamma'\cup\{0\}$. 同时随机选取一个$d^*-1$次多项式$q(x)$，满足$q(0)=\alpha=\alpha'+a^{\eta+1}$.

B随机选取$r_i,\rho_i\in\mathbb{Z}_p$，令$q(i)=\rho_i$，其中$i\in\Gamma'$. 随机选取$r_{i,v}\in\mathbb{Z}_p$，其中$v\in V_{t_j}$. 计算密钥$SK_{t_j}=\{\mu_i,\varphi_i,\{sk_{i,v}|v\in V_{t_j}\}\}$，其中$\mu_i=g^{r_i}$，$\varphi_i=\{f_1^{r_i},f_2^{r_i},\cdots,f_{i-1}^{r_i},f_{i+1}^{r_i},\cdots,f_\eta^{r_i}\}$，$sk_{i,v}=\left\{g^{\rho_i}(f_af_i)^{r_i}\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r_{i,v}},g^{r_{i,v}},h_{|b_v|+1}^{r_{i,v}},\cdots,h_l^{r_{i,v}}\right\}=\{a_{i,0},a_{i,1},\cdots,a_{i,|b_v|+1},\cdots,a_{i,l}\}$. B随机选取$r'_i\in\mathbb{Z}_p$，其中$i\in(w_{\mathrm{a}}\cap\Omega)/\Gamma'$. 令$r_i=r'_i-\Delta_0^S(i)a^i$. 由拉格朗日插值可得$q(i)=\sum_{j\in S}q(j)\Delta_j^S(i)$. 随机选取$r_{i,v}\in\mathbb{Z}_p$，其中$v\in V_{t_j}$. 计算密钥$SK_{t_j}=\left\{\mu_i,\varphi_i,\left\{sk_{i,v}|v\in V_{t_j}\right\}\right\}$，其中$\mu_i=g^{r_i}=g^{r'_i}g^{-\Delta_0^S(i)}$；$\varphi_i=\left\{f_1^{r_i},f_2^{r_i},\cdots,f_{i-1}^{r_i},f_{i+1}^{r_i},\cdots,f_\eta^{r_i}\right\}=\{f_1^{r'_i}\left(g^{\delta_1}g_\eta\right)^{-\Delta_0^S(i)a^i},\cdots,f_{i-1}^{r'_i}\left(g^{\delta_\eta}g_1\right)^{-\Delta_0^S(i)a^i}(g_{\eta-i+2}g^{\delta_{i-1}})^{-\Delta_0^S(i)a^i}f_{i+1}^{r'_i}\left(g^{\delta_{i+1}}g_{\eta-i}\right)^{-\Delta_0^S(i)a^i},f_\eta^{r'_i}\}=\{f_1^{r'_i}\left(g^{\delta_1}g_{\eta+i}\right)^{-\Delta_0^S(i)},\cdots,f_{i-1}^{r'_i}\left(g^{\delta_{i-1}}g_{\eta+2}\right)^{-\Delta_0^S(i)},f_{i+1}^{r'_i}(g_\eta g^{\delta_{i+1}})^{-\Delta_0^S(i)},f_\eta^{r'_i}\left(g^{\delta_\eta}g_{i+1}\right)^{-\Delta_0^S(i)}\}$；$sk_{i,v}=\left\{g^{q(i)}(f_af_i)^{r_i}\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r_{i,v}},g^{r_{i,v}},h_{|b_v|+1}^{r_{i,v}},\cdots,h_l^{r_{i,v}}\right\}=\{a_{i,0},a_{i,1},a_{i,|b_v|+1},\cdots,a_{i,l}\}$. 此时，计算可得$a_{i,0}=g^{q(i)}(f_0f_i)^{r_i}\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r_{i,v}}=(f_0f_i)^{r'_i-\Delta_0^S(i)a^i}\cdot g^{\sum_{j\in\Gamma'}q(j)\Delta_j^S(i)+q(0)\Delta_0^S(i)}$；$\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r_{i,v}}=g^{\sum_{j\in\Gamma'}\rho_i\Delta_j^S(i)}g^{\alpha'\Delta_0^S(i)}\cdot g_{\eta+1}^{\Delta_0^S(i)}(f_af_i)^{r'_i}g_i^{-\delta_i\Delta_0^S(i)}\left(\prod_{k=1}^{|b_v|}h_k^{b_v[k]}h_0\right)^{r_{i,v}}\left(g_i^{\delta_{\mathrm{a}}}\prod_{j\in S^*\cup\Omega^{*'}}g_j^{\delta_j}g_{\eta-j+i+1}\right)^{\Delta_0^S(i)}$.

综上所述，模拟的密钥与原始方案生成的密钥具有相同的分布，因此对敌手而言模拟的密钥与原始密钥不可区分.

②当$w_{\mathrm{a}}\cap S^*\geqslant d^*$，$t_j>t_{j^*}$时，根据时间二进制树的定义可得，对节点$v\in V_{t_j}$，存在索引$\beta$使得$b_v[\beta]\neq b_{v_{t_{j^*}}}[\beta]$.

为简化分析, 令β为满足条件的最小索引值. B 定义 3 个属性集合Γ, Γ', S, 使得$\Gamma=(w_{\mathrm{a}}\cap S^*)\cup\Omega^{z'}$, $\Gamma\subseteq\Gamma'\subseteq S$, 其中$|\Gamma'|=d^*-1$. 令$S=\Gamma'\cup\{0\}$. 随机选取$d^*-1$次多项式$q(x)$, 满足$q(0)=\alpha=\alpha'+a^{\eta+1}$.

B 随机选取r_i, $\rho_i\in\mathbb{Z}_p$, 令$q(i)=\rho_i$, 其中$i\in\Gamma'$.随机选取$r_{i,v}\in\mathbb{Z}_p$, 其中$v\in V_{t_j}$. 计算密钥$SK_{t_j}=\{\mu_i,\varphi_i,\{sk_{i,v}|v\in V_{t_j}\}\}$, 其中$\mu_i=g^{r_i}$, $\varphi_i=\{f_1^{r_i},f_2^{r_i},\cdots,f_{i-1}^{r_i},f_{i+1}^{r_i},\cdots,f_\eta^{r_i}\}$, $sk_{i,v}=\left\{(g^{\rho_i}(f_{\mathrm{a}}f_i))^{r_i}\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r_{i,v}},g^{r_{i,v}},h_{|b_v|+1}^{r_{i,v}},\cdots,h_l^{r_{i,v}})\right\}=(a_{i,0},a_{i,1},\cdots,a_{i,|b_v|+1},\cdots,a_{i,l})$. B 随机选择$r_i\in\mathbb{Z}_p$, 其中$i\in(w_{\mathrm{a}}\cap\Omega)/\Gamma'$. 计算$\mu_i=g^{r_i}$, $\varphi_i=\{f_1^{r_i},f_2^{r_i},\cdots,f_{i-1}^{r_i},f_{i+1}^{r_i},\cdots,f_\eta^{r_i}\}$; 随机选取$r'_{i,v}\in\mathbb{Z}_p$, 其中$v\in V_{t_j}$. 令$r_{i,v}=a^\beta\Delta_0^S(i)/b_v[\beta]-b_{v_{t_{j^*}}}[\beta]+r'_{i,v}$.

此时$sk'_{i,v}=\{a_{i,0},\ a_{i,1},\ a_{i,|b_v|+1},\ \cdots,\ a_{i,l})=\left\{g^{q(i)}(f_{\mathrm{a}}f_i)^{r_i}\cdot\left(\prod_{k=1}^{|b_v|}h_k^{b_v[k]}h_0\right)^{r_{i,v}},g^{r_{i,v}},h_{|b_v|+1}^{r_{i,v}},\cdots,h_l^{r_{i,v}}\right\}$, 其中$q(i)=\sum_{j\in\Gamma'}q(j)\cdot\Delta_j^S(i)+q(0)\Delta_0^S(i)$. 此时

$$a_{i,0}=\left(g^{q(i)}(f_{\mathrm{a}}f_i)\right)^{r_i}\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r_{i,v}}=\left(g^{q(0)\Delta_0^S(i)}(f_{\mathrm{a}}f_i)\right)^{r_i}\cdot g^{\sum_{j\in\Gamma'}q(j)\Delta_j^S(i)}\left(\prod_{k=1}^{\beta-1}g_{\eta-k+1}^{b_{v_{t_{j^*}}}[k]-b_v[k]}\right)^{r_{i,v}}\left(g^{\theta_0+\sum_{k=1}^{\beta}b_v[k]\theta_k}\right)^{r_{i,v}}\cdot\left(g_{\eta-\beta+1}^{(b_{v_{t_{j^*}}}[k]-b_v[k])r_{i,v}}\right)^{r_{i,v}}\left(\prod_{k=\beta+1}^{l}g_{\eta-k+1}^{b_{v_{t_{j^*}}}[k]}\right)^{r_{i,v}}=$$

$$g^{\alpha'\Delta_0^S(i)}\left(g_\beta^{\frac{\Delta_0^S(i)}{b_v[k]-b_{v_{t_{j^*}}}[k]}}g^{r'_{i,v}}\right)^{\theta_0+\sum_{k=1}^{\beta}b_v[k]\theta_k}g^{\sum_{j\in\Gamma'}\rho_i\Delta_j^S(i)}\cdot g_{\eta-\beta+1}^{(b_{v_{t_{j^*}}}[k]-b_v[k])r'_{i,v}}\left(\prod_{k=\beta+1}^{l}g_{\eta-k+\beta+1}^{b_{v_{t_{j^*}}}[k]}\right)^{\frac{\Delta_0^S(i)}{b_v[k]-b_{v_{t_{j^*}}}[k]}}\cdot(f_0f_i)^{r_i}\left(\prod_{k=\beta+1}^{l}g_{\eta-k+\beta+1}^{b_{v_{t_{j^*}}}[k]}\right)^{r'_{i,v}};$$

$$a_{i,1}=g^{\frac{a^\beta\Delta_0^S(i)}{b_v[k]-b_{v_{t_{j^*}}}[k]}+r'_{i,v}}=g_\beta^{\Delta_0^S(i)/(b_v[k]-b_{v_{t_{j^*}}}[k])}g^{r'_{i,v}};$$

$$a_{i.k}=\left(g^{\theta_k}g_{\eta-k+1}^{-1}\right)^{a^\beta\Delta_0^S(i)/(b_v[k]-b_{v_{t_{j^*}}}[k])+r'_{i,v}}=\left(g_\beta^{\theta_k}g_{\eta-k+\beta+1}^{-1}\right)^{\Delta_0^S(i)/(b_v[k]-b_{v_{t_{j^*}}}[k])}\left(g^{\theta_k}g_{\eta-k+1}^{-1}\right)^{r'_{i,v}}.$$

最后 B 随机选取$r''_{i,v}\in\mathbb{Z}_p$, 计算$sk_{i,v}=\{a_{i,0}\prod_{k=\beta+1}^{|b_v|}a_{i,k}^{b_v[k]}\cdot\left(h_0\prod_{k=1}^{|b_v|}h_k^{b_v[k]}\right)^{r''_{i,v}},a_{i,1}g^{r''_{i,v}},a_{i,|b_v|+1}h_{|b_v|+1}^{r''_{i,v}},a_{i,|b_v|+2}h_{|b_v|+2}^{r''_{i,v}},\cdots,a_{i,l}h_l^{r''_{i,v}}\}$. 综上所述, B 成功模拟t_y时间片段密钥SK_{t_j}.

4)密钥更新询问. 为了从当前时间片段t_j获得后续时间片段$t_{j'}$的密钥$SK_{t_{j'}}$, A 向 B 进行密钥更新询问. B 通过原始方案计算更新密钥$SK_{t_{j'}}$并发送给 A.

5)签名询问. 给定消息$M=\{m_1,m_2,\cdots,m_{n_m}\}$和签名策略$\Gamma_{d,S}(\cdot)$, 若$J(M)=0$, 模拟终止; 否则, B 随机选取r_{a}, s, z', $r_\tau\in\mathbb{Z}_p$, 令$z=z'-\frac{a^\eta}{J(M)}$, 计算

$$\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4\}=\left\{\left(g_1^{J(M)}g^{K(M)}\right)^{z'}\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\cdot g^{a'}\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_a}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s}g_\eta^{-K(M)/J(M)},\ g^s,g^{r_{\mathrm{a}}},g^{r_\tau},g^{z'}g_\eta^{-1/J(M)}\right\},$$

此时,

$$\sigma_0=g^{a'}\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}}\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\left(g_1^{J(M)}g^{K(M)}\right)^{z'}g_\eta^{-\frac{K(M)}{J(M)}}\cdot\left(\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}h_0\right)^{s}=g^\alpha\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}}g_\eta^{-\frac{K(M)}{J(M)}}\left(g_1^{J(M)}g^{K(M)}\right)^{z'}\cdot\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s}g^{-a^{(\eta+1)}}g_\eta^{-\frac{K(M)}{J(M)}}=$$

$$g^\alpha\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}}}f_j\right)^{r_{\mathrm{a}}}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s}\left(w_0\prod_{j=1}^{n_m}w_j^{m_i}\right)^{z}\cdot\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau};$$

$$\sigma_4=g^{z'}g_\eta^{-1/J(M)}=g^z.$$

综上所述, 模拟签名与原始签名有相同的分布, 因此 B 将签名$\sigma=\{\sigma_0,\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$发送给 A.

6)伪造. 询问结束后, A 输出关于消息$M^*=\{m_1^*,m_2^*,\cdots,m_{n_m}^*\}$, 满足签名策略$\Gamma_{d^*,S^*}(\cdot)$和时间片段$t_{j^*}$的签名$\sigma^*=\{\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*,\}$. 伪造过程为: 选取$w_{\mathrm{a}}^*\subseteq S^*$以及$\Omega^*\subseteq\Omega$, 令$\widehat{w_{\mathrm{a}}^*}=w_{\mathrm{a}}^*\cup\Omega^*$. 要求 A 没有在t_{j^*}时间片段并且满足签名策略$\Gamma_{d^*,S^*}(\cdot)$的条件下对$M^*=\{m_1^*,m_2^*,\cdots,m_{n_m}^*\}$进行签名询问. 此时 B 检查$t_{j^*}=t_{j^*}$是否成立. 若不成立, 则模拟终止; 若成立, B 计算$J(M^*)$和$K(M^*)$. 若$J(M^*)\neq0$, 模拟终止; 否则 A 输出伪造签名$\sigma^*=\left\{\sigma_0^*,\ \sigma_1^*,\ \sigma_2^*,\ \sigma_3^*,\ \sigma_4^*\right\}=\left\{g^\alpha\left(f_{\mathrm{a}}\prod_{j\in\widehat{w_{\mathrm{a}}^*}}f_j\right)^{r_a}\cdot\left(g_1^{J(M^*)}g^{K(M^*)}\right)^{z'}\left(f_\tau\prod_{j\in\widehat{w_\tau}}f_j\right)^{r_\tau}\left(h_0\prod_{k=1}^{l}h_k^{b_{v_{t_j}}[k]}\right)^{s},g^s,g^{r_{\mathrm{a}}},g^{r_\tau},g^z\right\}=$

$$\left\{g^{a'}g_{\eta+1}g^{\delta_{\mathrm{a}}r_{\mathrm{a}}}\ \ g^{\delta_\tau r_\tau}g^{\left(\theta_0+\sum_{k=1}^{\beta}b_{t_{j^*}}[k]\theta_k\right)s}g^{zK(M^*)},\ g^s,\ g^{r_{\mathrm{a}}},\ g^{r_\tau},g^z\right\}=$$

$$\left\{g^{a'}g_{\eta+1}\left(\sigma_2^*\right)^{\delta_{\mathrm{a}}}(\sigma_3^*)^{\delta}\left(\sigma_1^*\right)^{\theta_0+\sum_{k=1}^{\beta}b_{t_{j^*}}[k]\theta_k}\left(\sigma_4^*\right)^{K(M^*)}\cdot,g^s,g^{r_{\mathrm{a}}},g^{r_\tau},g^z\right\}$$

B通过A提交的伪造签名计算$g^{a_{\eta+1}}=g_{\eta+1}=\dfrac{\sigma_0^*}{g^{a'}\left(\sigma_1^*\right)^{\theta_0+\sum_{k=1}^{\beta}b_{i_{j^*}[k]}\theta_k}\left(\sigma_2^*\right)^{\delta_a}\left(\sigma_3^*\right)^{\delta_\tau}\left(\sigma_4^*\right)^{K(M^*)}}$. 因此若$A$能够伪造一个消息的有效签名，那么$B$就能成功解决$\eta$-DHE困难问题. 证毕.

5.4 概率分析

为了在前向安全性游戏的交互中不发生终止，需要考虑3个事件：

1）事件E_1. 签名询问阶段，满足$J(M)\neq 0$，其中$i\in\{1,2,\cdots,q_s\}$；

2）事件E_2. 伪造阶段，满足$J(M^*)=0$；

3）事件E_3. 敌手猜测的时间t_{j^*}，满足$t_{j^*}=t_{j^*}$.

易见，B不发生终止的概率为$Pr\left[\overline{abort}\right]=Pr[\wedge_{i=1}^{q_s}E_{1i}\wedge E_2\wedge E_3]$. 同时，对于所有的$i=1,2,\cdots,q_s$，事件$E_{1i}$和事件$E_2$是相互独立的. 因此，$Pr\left[\overline{abort}\right]\geqslant Pr\left[\wedge_{i=1}^{q_s}E_{1i}\wedge E_2\right]Pr[E_3]=Pr[E_3]Pr\left[\left[\wedge_{i=1}^{q_s}E_{1i}\middle|E_2\right]P\right.$ $Pr[E_2]\geqslant Pr[E_2](1-\sum_{i=1}^{q_s}Pr[\overline{E_{1i}}|E_2]=\dfrac{1}{4Tq_s(n_m+1)}$.

综上所述，若存在概率多项式时间敌手以不可忽略概率ε赢得FABSS的前向安全性游戏，那么挑战者就能以$\varepsilon'\geqslant\dfrac{\varepsilon}{4T\times q_s\times(n_m+1)}$的概率解决$\eta$-DHE困难问题假设，其中$T$表示时间片段总数，$q_s$表示签名询问的次数，$n_m$表示消息的长度.

5.5 不变性

定理 2. FABSS方案在ε'-(η-DHE)困难问题假设下具有ε-不变性，其中存在常数ψ，满足$\varepsilon<\psi\varepsilon'$.

假设可净化集合$I_N\subseteq\{1,2,\cdots,n_m\}$，净化者已知秘密值集合$SI$，但无法对可净化集合范围之外的数据进行操作. 首先证明引理2.

引理 2. 若存在多项式时间的敌手A_1能够对可净化索引集合I_N中的κ位长度的消息进行操作，其中$0<\kappa\leqslant n_m$，并且以ε_{A_1}的优势赢得不变性游戏，那么就存在一个多项式时间敌手A在不可伪造游戏中以$\varepsilon_A\geqslant\varepsilon_{A_1}$的优势成功伪造一个长度为$n_m-\kappa$位消息的有效签名.

证明. 假设A_1在可净化范围内对κ位长度的消息进行操作，此时A对长度为$n_m-\kappa$位的消息进行前向安全游戏，在游戏中A模仿挑战者与A_1交互. 在收到A_1提交的相关询问操作后，A通过与前向安全游戏中的挑战者B交互并将结果发送给A_1.

1）设置阶段，A_1获得可净化索引集合I_N，其中$I_N\subseteq\{1,2,\cdots,n_m\}$. 为简化分析，令$I_N=\{n_m-\kappa+1,n_m-\kappa+2,\cdots,n_m\}$，$\kappa=|I_N|$. B将公共参数$params=\{G_1,G_2,e,g,f_a,f_\tau,h_0,w_0,U,\Omega,T,H,W_{n_m-\kappa},Z\}$发送给$A$，其中$W_{n_m-\kappa}=\{w_1,w_2,\cdots,w_{n_m-\kappa}\}$. A随机选取$s_i\in\mathbb{Z}_p$，计算$w_i'=g^{s_i}$，其中$i\in\{n_m-\kappa+1,n_m-\kappa+2,\cdots,n_m\}$. 令$W=W_{n_m-\kappa}\cup W_{n_m-\kappa+1}$，$W_{n_m-\kappa+1}=\{w_{n_m-\kappa+1},w_{n_m-\kappa+2},\cdots,w_{n_m}\}$. A将公共参数$params=\{G_1,G_2,e,g,f_a,f_\tau,h_0,w_0,U,\Omega,T,H,W,Z\}$发送给$A_1$.

在$j=1,2,\cdots,q_s$次的签名询问中，A通过与B的交互来回答A_1的询问. 首先A_1向A询问消息$M_j=\{m_{j,1},m_{j,2},\cdots,m_{j,n_m}\}$的签名，$A$收到询问后向$B$询问消息$\overline{M_j}=\{m_{j,1},m_{j,2},\cdots,m_{j,n_m-\kappa}\}$的签名. B将签名$\sigma=\{\sigma_{j,0},\sigma_{j,1},\sigma_{j,2},\sigma_{j,3},\sigma_{j,4}\}$发送给$A$，$A$计算$\sigma'_{j,0}=\sigma_{j,0}\prod_{i=n_m-\kappa+1}^{n_m}\sigma_{j,1}{}^{s_im_{j,i}}$，$\sigma'_{j,1}=\sigma_{j,1},\sigma'_{j,2}=\sigma_{j,2},\sigma'_{j,3}=\sigma_{j,3},\sigma'_{j,4}=\sigma_{j,4}$. A将签名$(\sigma'_{j,0},\sigma'_{j,1},\sigma'_{j,2},\sigma'_{j,3},\sigma'_{j,4})$以及秘密消息$\{\sigma_{j,1}{}^{s_im_{j,i}}|i=n_m-\kappa+1,n_m-\kappa+2,\cdots,n_m\}$发送给$A_1$.

2）在伪造阶段，若A_1能够成功伪造消息$M^{*\prime}=\{m_0^{*'},m_1^{*'},\cdots,m_{n_m}^{*'}\}$的签名$(\sigma_{j,0}^{*}{}',\sigma_{j,1}^{*}{}',\sigma_{j,2}^{*}{}',\sigma_{j,3}^{*}{}',\sigma_{j,4}^{*}{}')$. A利用该签名进行以下计算. 对于$i=1,2,\cdots,q_s$，$\exists i\notin\{n_m-\kappa+1,n_m-\kappa+2,\cdots,n_m\}$，有$m_{j,i}\neq m_i^{*\prime}$. 令消息$M^*=\{m_0^*,m_1^*,\cdots,m_{n_m}^*\}$，当$i\in\{1,2,\cdots,n_m-\kappa\}$时，$m_i^*=m_i^{*'}$. A计算$\sigma_0^*=\dfrac{\sigma_0^{*\prime}}{\prod_{i=n_m-\kappa+1}^{n_m}\sigma_{j,1}{}^{s_im_i^{*\prime}}}$，$\sigma_1^*=\sigma_1^{*\prime}$，$\sigma_2^*=\sigma_2^{*\prime}$，$\sigma_3^*=\sigma_3^{*\prime}$，$\sigma_4^*=\sigma_4^{*\prime}$. A将有效签名$\sigma^*=\{\sigma_0^*,\sigma_1^*,\sigma_2^*,\sigma_3^*,\sigma_4^*\}$发送给$B$. 此时$\forall j\in\{1,2,\cdots,q_s\}$，$\exists i\in\{n_m-\kappa+1,n_m-\kappa+2,\cdots,n_m\}$满足$m_{j,i}\neq m_i^{*\prime}$. 可以发现，如果$A_1$伪造的签名能够通过验证，那么$A$生成的签名也可以通过验证. 因此$A$赢得前向安全性游戏的优势$\varepsilon_A$，满足$\varepsilon_A\geqslant\varepsilon_{A_1}$，其中$\varepsilon_{A_1}$表示$A_1$赢得不变性游戏的优势.

由定理1可得，敌手A赢得前向安全游戏的优势是可忽略的. 因此由引理2可知，敌手A_1赢得不变性游戏的优势也是可忽略的. 证毕.

6 方案分析

FABSS方案不仅获得细粒度访问控制，缓解了密钥泄露问题，而且具有可净化性，解决了敏感信息泄露问题. 表1给出FABSS方案与文献[21,29,31,33]在匿名性、净化性、前向安全性、透明性以及访问控制方面的优势比较分析. 其中文献[33]给出了支持非单调谓词的高效属性基签名方案，提供签名者的匿名性，同时具有细粒度访问控制，但无法提供前向

Table 1 Comparison of Schemes

表 1 方案比较

方案	匿名性	净化性	前向安全性	透明性	访问控制
文献 [21]	√	×	√	×	√
文献 [29]	√	√	×	√	√
文献 [31]	√	√	×	√	√
文献 [33]	√	×	×	×	√
FABSS	√	√	√	√	√

注: "√"表示方案支持该性质; "×"表示方案不支持该性质.

性和净化性. 文献 [21] 提出具有前向安全的属性基签名方案, 在获得细粒度访问控制的同时缓解了密钥泄露问题, 但无法解决敏感信息泄露问题. 文献 [29] 构造了具有灵活访问结构的属性基可净化签名方案, 不仅提供灵活细粒度访问控制, 而且还实现了敏感信息隐藏, 但无法解决密钥泄露问题. 文献 [31] 提出可追踪的属性基可净化签名方案, 提供净化功能从而实现敏感信息隐藏, 同时具有恶意用户追踪功能, 避免签名滥用, 但无法缓解密钥泄露问题. 本文提出的 FABSS 方案, 不仅具有细粒度访问控制, 还具有前向安全性和净化性, 而且缓解了密钥泄露问题并保护了敏感数据的隐私.

7 性能分析

基于 Ubuntu 18.4, 在 Charm0.5 框架下实现了 FABSS 方案. 利用 Charm 库中的超奇异椭圆曲线 (SS512) 测试方案. 实验中群G_1和G_2的阶为 p, p为 512 b 的大素数. 在此参数的计算机上测试主要密码学操作开销, 经过 1 000 次测量取平均值后, 得到实验中计算双线配对所需时间为 1.45 ms, 在群G_1和G_2中执行指数运算所需时间分别为 1.998 ms 和 0.2 ms. FABSS 与文献 [29,31] 的通信开销和计算开销比较如表 2 和表 3 所示, 其中$|G_1|$表示群G_1中元素的大小, $|\widehat{\omega}_{\mathrm{a}}|$表示签名者属性数量, $|\widehat{\omega}_{\tau}|$表示净化者属性数量, l表示时间二叉树层数. 由表 2 可知, 提出的 FABSS 方案具有固定的签名长度, 减少了通信开销. 由表 3 可知, 提出的方案在验证阶段和净化阶段的指数和配对运算与属性数量无关, 降低了计算开销. 实验结果如图 3~6 所示, 由图 3 和图 4 可知, 随着用户属性数量增加, 提出的方案在密钥生成和签名阶段比文献 [29,31] 需要更大的计算开销, 但是密钥生成算法一般只执行 1 次, 所以对方案的性能影响不大; 由图 5 和图 6 可知, 提出的方案在净化以及验证阶段所需的计算时间要小于文献 [29,31], 具有较小的计算开销.

8 结束语

本文形式化了前向安全的属性基可净化签名安全模型. 提出了一种前向安全的高效属性基可净化签名方案, 不仅缓解了密钥泄露问题, 而且还实现了敏感信息隐藏功能. 基于 η-DHE 困难问题假设, 在标准模型下证明了本文方案的安全性. 通过与现有方案的对比分析可知, 提出的方案更适用于电子医疗、电子政务等特殊应用场景中.

Table 2 Comparison of Communication Cost

表 2 通信开销比较

方案	密钥	签名	净化签名
FABSS	$[\lvert\widehat{\omega}_{\mathrm{a}}\rvert+\eta-1+(l+2)\lvert\widehat{\omega}_{\mathrm{a}}\rvert]\lvert G_1\rvert$	$5\lvert G_1\rvert$	$5\lvert G_1\rvert$
文献 [29]	$(2+\lvert\widehat{\omega}_{\mathrm{a}}\rvert)\lvert G_1\rvert$	$(2\lvert\widehat{\omega}_{\mathrm{a}}\rvert^2+2)\lvert G_1\rvert$	$(2\lvert\widehat{\omega}_{\mathrm{a}}\rvert^2+2)\lvert G_1\rvert$
文献 [31]	$(2\lvert\widehat{\omega}_{\mathrm{a}}\rvert+2)\lvert G_1\rvert+\lvert\mathbb{Z}_p^*\rvert$	$(3\lvert\widehat{\omega}_{\mathrm{a}}\rvert+\lvert\widehat{\omega}_{\tau}\rvert+3)\lvert G_1\rvert$	$(3\lvert\widehat{\omega}_{\mathrm{a}}\rvert+\lvert\widehat{\omega}_{\tau}\rvert+3)\lvert G_1\rvert$

注: $|G_1|$表示群G_1中元素的大小, $|\mathbb{Z}_p^*|$表示环$\mathbb{Z}_p^*$中元素的比特大小, $|\widehat{\omega}_{\mathrm{a}}|$表示签名者属性数量, $|\widehat{\omega}_{\tau}|$表示净化者属性数量, l表示时间二叉树层数, $\eta=n+d-1$, n是常数, d是门限值.

Table 3 Comparison of Computation Cost

表 3 计算开销比较

方案	密钥生成	签名	验证	净化
FABSS	$[(4+\eta+l)\lvert\widehat{\omega}_{\mathrm{a}}\rvert]$E	$[(3+l)\lvert\widehat{\omega}_{\mathrm{a}}\rvert+\lvert\widehat{\omega}_{\tau}\rvert+13+n_m]$E	$(l+n_m)$E+5P	$(8+l+I+n_m)$E
文献 [29]	$(\lvert\widehat{\omega}_{\mathrm{a}}\rvert+1)$E	$(3\lvert\widehat{\omega}_{\mathrm{a}}+n_m+2)$E	$(3+\lvert\widehat{\omega}_{\mathrm{a}}\rvert)$P+$(\lvert\widehat{\omega}_{\mathrm{a}}\rvert+n_m)$E	$(\lvert\widehat{\omega}_{\mathrm{a}}\rvert+I+n_m)$E
文献 [31]	$(3+3\lvert\widehat{\omega}_{\mathrm{a}}\rvert)$E	$(3\lvert\widehat{\omega}_{\mathrm{a}}\rvert+2\lvert\widehat{\omega}_{\tau}\rvert+l+4v+6)$E	$(\lvert\widehat{\omega}_{\mathrm{a}}\rvert+\lvert\widehat{\omega}_{\tau}\rvert+3)$P+$l$E	$(\lvert\widehat{\omega}_{\mathrm{a}}\rvert+\lvert\widehat{\omega}_{\tau}\rvert+\lvert l\rvert+l+4)$E

注: n_m表示消息长度, I表示可净化范围集合, E 表示G_1中的指数运算, P 表示配对运算, $|\widehat{\omega}_{\mathrm{a}}|$表示签名者属性数量, $|\widehat{\omega}_{\tau}|$表示净化者属性数量, l表示时间二叉树层数, $\eta=n+d-1$, n是常数, d是门限值.

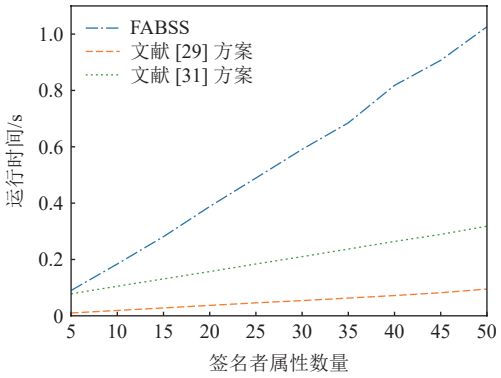


Fig. 3 Performance analysis of key generation algorithm

图 3 密钥生成算法性能分析

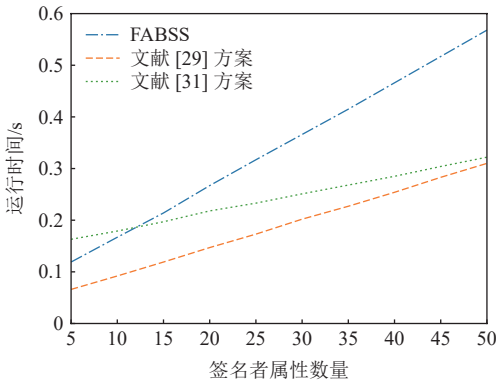


Fig. 4 Performance analysis of signing algorithm

图 4 签名算法性能分析

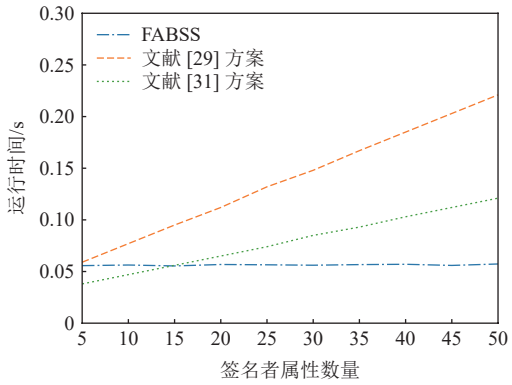


Fig. 5 Performance analysis of verifying algorithm

图 5 验证算法性能分析

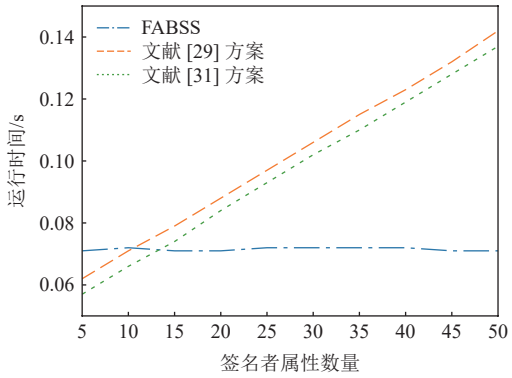


Fig. 6 Performance analysis of sanitization algorithm

图 6 净化算法性能分析

作者贡献声明：朱留富提出初步方案、实验设计，以及论文初稿撰写和修改；李继国负责论文思路构建、理论指导、方案分析和论文修改；陆阳和张亦辰负责论文方案分析、论文润色和修改.

参 考 文 献

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

[2] Goyal V, Pandey O, Saha A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C] //Proc of the 13th ACM Conf on Computer and Communications Security. New York: ACM, 2006: 89–98

[3] Li Jiguo, Yao Wei, Zhang Yichen, et al. Flexible and fine-grained attribute-based data storage in cloud computing[J]. IEEE Transactions on Services Computing, 2017, 10(5): 785−796

[4] Chen Ningyu, Li Jiguo, Zhang Yichen, et al. Efficient CP-ABE scheme with shared decryption in cloud storage[J]. IEEE Transactions on Computers, 2022, 71(1): 175−184

[5] Li Jiguo, Chen Ningyu, Zhang Yichen. Extended file hierarchy access control scheme with attribute based encryption in cloud computing[J]. IEEE Transactions on Emerging Topics in Computing, 2021, 9(2): 983−993

[6] Li Jiguo, Wang Yao, Zhang Yichen, et al. Full verifiability for outsourced decryption in attribute based encryption[J]. IEEE Transactions on Services Computing, 2020, 13(3): 478−487

[7] Li Jiguo, Yao Wei, Han Jinguang, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage[J]. IEEE Systems Journal, 2018, 12(2): 1767−1777

[8] Li Jiguo, Yu Qihong, Zhang Yichen. Hierarchical attribute based encryption with continuous leakage-resilience[J]. Information Sciences, 2019, 484: 113−134

[9] Li Jiguo, Zhang Yichen, Ning Jianting, et al. Attribute based encryption with privacy protection and accountability for cloudIoT[J]. IEEE Transactions on Cloud Computing, 2022, 10(2): 762−773

[10] Lin Suqing, Zhang Rui, Ma Hui, et al. Revisiting attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics & Security, 2017, 10(10): 2119−2130

[11] Liu Ximeng, Ma Jianfeng, Xiong Jinbo, et al. Ciphertext-policy hierarchical attribute-based encryption for fine-grained access control of encryption data[J]. International Journal of Network Security, 2014, 16(6): 437−443

[12] Chen Yu, Li Jiguo, Liu Chengdong, et al. Efficient attribute-based server-aided verification signature [J/OL]. IEEE Transactions on Services Computing, 2022, 15(6): 3224-3232

[13] Li Jiguo, Chen Yu, Han Jinguang, et al. Decentralized attribute-based server-aid signature in the Internet of things[J]. IEEE Internet of

Things Journal, 2021, 9(6): 4573−4583

[14] Okamoto T, Takashima K. Decentralized attribute-based signatures [C] //Proc of the 16th Int Conf on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2013: 125−142

[15] Sreenivasa R Y, Dutta R. Efficient attribute-based signature and signcryption realizing expressive access structures[J]. International Journal of Information Security, 2016, 15(1): 81−109

[16] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attribute-based encryption [C] //Proc of the 28th IEEE Symp on Security and Privacy (SP '07). Los Alamitos, CA: IEEE Computer Society, 2007: 321−334

[17] Maji K, Prabhakaran M, Rosulek M. Attribute-based signatures [C] //Proc of the 11th Int Conf on Topics in Cryptology. Berlin: Springer, 2011: 376−392

[18] Okamoto T, Takashima K. Efficient attribute-based signatures for non-monotone predicates in the standard model[C] //Proc of the 14th Int Conf on. Practice and Theory in Public Key Cryptography. Berlin: Springer, 2011: 125−142

[19] Gagn, Martin, Narayan S, et al. Short pairing-efficient threshold attribute-based signature[C] //Proc of the 5th Int Conf on Pairing-Based Cryptography. Berlin: Springer , 2012: 295−313

[20] Anada H, Arita S, Sakurai K. Attribute-based signatures without pairings via the fiat-shamir paradigm[C] //Proc of the 9th ACM Workshop on ASIA Public key Cryptography. New York: ACM 2014: 49−58

[21] Wei Jianghong, Liu Wenfen, Hu Xuexian. Forward-secure threshold attribute-based signature scheme[J]. The Computer Journal, 2015, 58(10): 2492−2506

[22] Rao Y S. Signature-policy attribute-based key-insulated signature[J]. IET Information Security, 2017, 11(1): 23−33

[23] Ateniese G, Chou D H, De Medeiros B, et al. Sanitizable signatures [C] //Proc of the 10th European Symp on Research in Computer Security. Berlin: Springer, 2005: 159−177

[24] Agrawal S, Kumar S, Shareef A, et al. Sanitizable signatures with strong transparency in the standard model[C] //Proc of the 5th Int Conf on Information Security and Cryptology. Berlin: Springer, 2009: 93−107

[25] Pöhls Henrich C, Samelin K, Posegga J. Sanitizable signatures in XML signature—Performance, mixing properties, and revisiting the property of transparency[C] //Proc of the 9th Int Conf on Applied Cryptography and Network Security. Berlin: Springer, 2011: 166−182

[26] Beck M T, Camenisch J, Derler D, et al. Practical strongly invisible and strongly accountable sanitizable signatures[C] //Proc of the 22nd Australasian Conf on Information Security and Privacy (ACISP 2017). Berlin: Springer, 2017: 437−452

[27] Liu Ximeng, Ma Jianfeng, Xiong Jinbo, et al. Attribute based sanitizable signature scheme[J]. Journal on Communications, 2013, 34(S1): 148−155 (in Chinese)
(刘西蒙, 马建峰, 熊金波, 等. 基于属性的可净化签名方案[J]. 通信学报, 2013, 34(S1): 148−155)

[28] Mo Ruo, Ma Jianfeng, Liu Ximeng, et al. An attribute-based sanitizable signature supporting dendritic access structure[J]. Acta Electronica Sinica, 2017, 45(11): 2715−2720 (in Chinese)
(莫若, 马建峰, 刘西蒙, 等. 一种支持树形访问结构的属性基可净化签名方案[J]. 电子学报, 2017, 45(11): 2715−2720)

[29] Mo Ruo, Ma Jianfeng, Liu Ximeng, et al. FABSS: Attribute-based sanitizable signature for flexible access structure[C] //Proc of the 19th Int Conf on Information and Communications Security. Berlin: Springer, 2018: 39−50

[30] Samelin K, Slamanig D. Policy-based sanitizable signatures [C] // Proc of the Cryptographers' Track at the RSA Conf . Berlin: Springer, 2020: 538−563

[31] Li Jiguo, Zhu Liufu, Liu Chengdong, et al. Provably secure traceable attribute-based sanitizable signature scheme in the standard model[J]. Journal of Computer Research and Development, 2021, 58(10): 2253−2264 (in Chinese)
(李继国, 朱留富, 刘成东, 等. 标准模型下证明安全的可追踪属性基净化签名方案[J]. 计算机研究与发展, 2021, 58(10): 2253−2264)

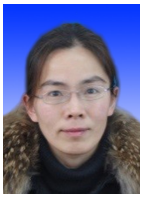
[32] Canetti R, Halevi S, Katz J. A forward-secure public-key encryption scheme[J]. Journal of Cryptology, 2007, 20(3): 265−294

[33] Zhang Jixin, Chen Jiageng, Meng Weizhi. Efficient attribute-based signature for monotone predicates[C] //Proc of the Int Conf on Provable Security (ProvSec 2021). Berlin: Springer, 2021: 346−362

Zhu Liufu, born in 1995. Master candidate. His main research interest includes public key cryptography.
朱留富, 1995 年生. 硕士研究生. 主要研究方向为公钥密码学.

Li Jiguo, born in 1970. PhD, professor. Member of CCF. His main research interests include public key cryptography and cloud computing security.
李继国, 1970 年生. 博士, 教授. CCF 会员. 主要研究方向为公钥密码学、云计算安全.

Lu Yang, born in 1977. PhD, professor. His main research interests include information security and cryptography, and cloud computing security.
陆　阳, 1977 年生. 博士, 教授. 主要研究方向为信息安全与密码学、云计算安全.



Zhang Yichen, born in 1971. PhD, associate professor. Her main research interests include public key cryptography and cloud computing security.
张亦辰, 1971 年生. 博士, 副教授. 主要研究方向为公钥密码学、云计算安全.