一种支持树形访问结构的属性基可净化签名方案

莫 若[1],马建峰[1,3],刘西蒙[2],张 涛[3]
(1. 西安电子科技大学网络与信息安全学院,陕西西安 710071; 2. 新加坡管理大学信息系统学院,新加坡 178902;
3. 西安电子科技大学计算机学院,陕西西安 710071)

摘 要: 在电子医疗档案系统中,用户会频繁更新自己的健康数据. 若直接使用现有签名方案保证这些数据的可认证性,在泄露用户身份隐私的同时,也需要大量的计算开销. 为了解决上述问题,我们利用属性集合来模糊用户的身份信息,并引入可授权第三方—净化者,提出了一个属性基的可净化签名方案. 安全性分析证明,本方案保护了用户的匿名性,同时在标准模型下针对给定策略选择消息攻击具有不可伪造性. 通过方案对比分析表明,本方案在有效降低用户签名计算开销的同时,还支持树形访问结构,能在大规模属性集下提供灵活的细粒度访问控制.

关键词: 基于属性的签名; 可净化签名; 电子医疗档案; 标准模型; 不可伪造性; 匿名性
中图分类号: TP309 **文献标识码:** A **文章编号:** 0372-2112 (2017)11-2715-06
电子学报 URL: http://www.ejournal.org.cn **DOI:** 10.3969/j.issn.0372-2112.2017.11.019

An Attribute-Based Sanitizable Signature Supporting Dendritic Access Structure

MO Ruo[1], MA Jian-feng[1,3], LIU Xi-meng[2], ZHANG Tao[3]
(1. *School of Cyber Engineering, Xidian University, Xi'an, Shaanxi* 710071, *China*;
2. *School of Information systems, Singapore Management University, Singapore* 178902, *Singapore*;
3. *School of Computer Science and Technology, Xidian University, Xi'an, Shaanxi* 710071, *China*)

Abstract: In the Electronic Health Record system, users update their health data frequently. If users keep the authentication of these data with the signature scheme in existence, it will lead to the leakage of their identity privacy and huge computation cost. Aiming at tackling the problems above, we propose a novel scheme called attribute-based sanitizable signature supporting dendritic access structure which obfuscates the user identity with attribute sets and introduces an authorized semi-trust third-party—sanitizer. The security analysis demonstrates that our scheme achieves the anonymity of users and is unforgeable under selective-predicate chosen-message attack in the standard model. Through comparison, our scheme not only reduces the signing computation overhead of users, but also supports the dendritic access structure which can provide flexibly fine-grained access control under large-scale attribute sets.

Key words: attribute-based signature; sanitizable signature; electronic health records; standard model; unforgeable; anonymity

1 引言

电子医疗档案[1]将患者的医疗数据通过电子数据的形式进行系统化存储,提高了医疗保健的质量,从而引起了广泛的关注[2~4].

用户利用数字签名,对医疗数据进行签名并上传,确保医疗数据的可认证性. 医疗人员将信息下载到本地时,可以验证签名者的身份判断该信息来源是否合法. 因此数字签名方案被广泛应用于电子医疗档案系统. 然而,传统的数字签名暴露了用户的身份信息,会造成用户的隐私泄露. 同时,用户的健康数据会频繁更新,如果每次上传都需要对更新后的消息重新生成签名,无疑会造成大量的计算开销. 例如一个心脏病患者会随时上传自己的心跳频率,血氧含量,这些签名的私钥

收稿日期:2016-07-25;修回日期:2017-01-09;责任编辑:蓝红杰
基金项目:国家自然基金(No. U1135002, No. U1405255);国家 863 高技术研究发展计划(No. 2015AA016007, No. 2015AA017203)

中包含了用户的姓名,工作单位等医生不应该知道的身份信息.因此如何减少签名过程中用户的计算开销,同时保护其身份隐私,是电子医疗档案系统中的一个关键问题.

针对上述问题,我们将用户的身份私钥替换为用户所拥有的属性私钥,使签名本身仅证实了用户所拥有的部分属性,同时引入授权半可信第三方—净化者,在原始签名生成后根据用户需求直接更新签名中的部分信息并生成对应的签名,提出了一种支持树形访问结构的属性基可净化签名方案(Attribute-Based Sanitizable Signature supporting Dendritic Access Structure,DAS-ABSS).方案的主要工作可以概括为三个方面:(1)在原始签名的净化过程中,净化者不需要和用户进行交互获得私钥即可生成对应的有效签名.利用基于属性的访问控制,使满足访问结构的用户可以使用部分属性私钥生成签名.(2)在标准模型下证明本方案在给定策略选择消息攻击具有不可伪造性,同时具有匿名性,保护了用户的身份隐私.(3)通过对比分析,本方案在有效地降低了用户的计算开销的同时,支持树形访问结构,在大规模属性集下提供灵活的访问控制.

净化签名的概念[5]最早在2005年由Ateniese等提出,该方案基于变色龙哈希函数[6],作者同时提出了不同条件下净化签名可能满足的四个性质:不变性,隐私性,可追责性和透明性;Canard等[7]对传统的单签名者——单净化者的条件进行扩展,提出了多签名者-多净化者这一概念;针对净化签名的四个性质,Brzuska等[8~10]引入了两个新的性质:非交互可追责性和不可连接性.Agrawal等在文献[11]中对透明性这一性质进行加以细分,同时提出了具体的满足透明性的净化签名方案,并证明该方案在标准模型下的不可伪造性.

基于属性的访问控制[12]分为基于属性的加密(Attribute-Based Encryption,ABE)和基于属性的签名(Attribute-Based Signature,ABS).ABS的概念在2008年由Yang等[13]提出,支持单授权机构和单层访问结构;Shahandashti和Safavi-Naini提出了基于门限的ABS方案[14];Maji等提出了面向多授权机构的ABS方案[15];随后,在2014年,Su等考虑树性访问结构并设计了对应的ABS方案[16].

2 背景知识

2.1 双线性映射

双线性映射具有双线性、非退化性、可计算性,相关知识请参考文献[17].

2.2 系统模型

DAS-ABSS方案由以下6个算法组成:

初始化 $Setup(1^{\lambda})\rightarrow(Mk,params)$. *Setup* 算法输入安全参数 λ,输出主密钥 Mk 和公开参数 *params*.

属性签名私钥生成 $SignKey(Mk,\omega)\rightarrow sk_{\omega}$. *SignKey* 算法输入主密钥 Mk,用户的属性集合 ω,输出用户签名的属性私钥 sk_{ω}.

验证公钥生成 $VeriKey(params,Mk,\Gamma)\rightarrow Vk$. *VeriKey* 算法输入公开参数 *params*、主密钥 Mk 和树形访问结构 Γ,生成验证公钥 Vk.

签名 $Sign(params,sk_{\omega},M)\rightarrow\delta$. *Sign* 算法输入公开参数 *params*、消息 M 和属性签名私钥 sk_{ω},生成签名 δ.

验证 $Verify(Vk,\delta)\rightarrow accept/reject$. *Verify* 算法输入公钥 Vk,签名 δ,输出验证结果 *accept/reject*.

净化 $Sanitize(M,\delta,SI,params)\rightarrow(M',\delta')$. *Sanitize* 算法输入原始消息 M,签名 δ,状态信息 *SI* 和公开参数 *params*,生成净化后的消息 M' 和净化签名 δ'. 其中 *SI* 为状态信息,表示原始消息中需要净化的比特.

2.3 安全模型

定义1(正确性) 如果对于 $(Mk,params)\leftarrow Setup(1^{\lambda})$,消息 M,用户属性集 ω,签名私钥 $sk_{\omega}\leftarrow SignKey(Mk,\omega)$,验证密钥 $Vk\leftarrow VeriKey(params,Mk,\Gamma)$ 和访问结构 Γ,有 $Verify(Vk,Sign(sk_{\omega},M))\rightarrow accept$,则称方案是正确的.

定义2(匿名性) 如果对于 $(Mk,params)\leftarrow Setup(1^{\lambda})$,所有满足的属性集 ω_0 和 ω_1,签名私钥 $sk_{\omega_0}\leftarrow SignKey(Mk,\omega_0)$ 和 $sk_{\omega_1}\leftarrow SignKey(Mk,\omega_1)$,验证公钥 $Vk\leftarrow VeriKey(params,Mk,\Gamma)$,使签名 $\delta_{\omega_0}\leftarrow Sign(params,sk_{\omega_0},M)$ 和 $\delta_{\omega_1}\leftarrow Sign(params,sk_{\omega_1},M)$ 具有相同的分布,则称方案满足匿名性.

定义3(不可伪造性) 如果任意的多项式时间敌手 $\mathcal{A}$ 以如下选择策略的攻击方式攻破我们的净化签名方案的概率是可以忽略的,我们称该方案具有不可伪造性:

设定阶段 $\mathcal{A}$ 定义新的访问结构 Γ^*,用来生成伪造签名.

初始化阶段 挑战者 $\mathcal{C}$ 选择足够大的安全参数 λ 并运行 *Setup* 算法,生成公开参数 *params* 和主密钥 Mk,将公开参数发给敌手 $\mathcal{A}$.

查询阶段 收到公开参数后,敌手 $\mathcal{A}$ 可以利用 ω 和 (M,Γ) 向挑战者发出签名私钥查询请求和签名查询请求,挑战者根据主密钥 Mk,分别运行 *KeyGen* 算法和 *Sign* 算法生成签名私钥 sk_{ω} 和签名 δ,发给敌手 $\mathcal{A}$.

签名伪造 $\mathcal{A}$ 生成消息 M^* 关于访问结构 Γ^* 的签名 δ^*. 如果消息 M^* 关于访问结构 Γ^* 的签名 δ^* 是有效的,且 (M^*,Γ^*) 未曾出现在签名查询中,签名私钥查询中用到的属性集 ω^* 不能满足访问结构 Γ^*,即 $\Gamma^*(\omega^*)\neq 1$,则称敌手在游戏模拟中获胜.敌手的优势定义为 $|\Pr[Verify(\delta^*,M^*,\Gamma^*)]=1|$.

3　DAS-ABSS 方案

3.1　算法设计

初始化:给出$\mathbb{G}_1$,$\mathbb{G}_2$两个阶循环乘法群,g 是$\mathbb{G}_1$的生成元,$g_1=g^a$,其中 $a\in\mathbb{Z}_p^*$. 随机选取一个元素 g_2,u',$\cdots$,$u_k\in\mathbb{G}_1$,k 为消息 M 的长度,最后计算双线性函数 $Z=e(g_1,g_2)$. 主密钥 $Mk=a$,公开参数 $params=(p,\mathbb{G}_1,\mathbb{G}_2,e,g,g_1,g_2,u',u_1,\cdots,u_k,Z)$.

属性签名私钥生成　设用户属性集为 ω,访问结构 Γ 中的叶子属性集为 ω'. 随机选择 $r\in\mathbb{Z}_p$,计算 $d=g_2^{r+a}$. 对属性集为 ω 的用户,对每个属性 $i\in\omega$,随机选择 $\beta_i\in\mathbb{Z}_p$,$\gamma_i\in\mathbb{Z}_p$,$r_i\in\mathbb{Z}_p$,分别计算

$$\{d_{i0}=g_2^{r/a}\cdot(g^{\beta i})^{ri},d_{i1}=g^{ri}\}_{i\in\omega'},$$

$$\{d_{i0}=g_2^{r/a}\cdot(g_1^{-\beta i}g^{\gamma i})^{ri},d_{i1}=g^{ri}\}_{i\in\omega/\omega\cap\omega'}.$$

用户的签名私钥为 $sk_\omega=(\{d_{i0},d_{i1}\}_{i\in\omega})$.

验证公钥生成　将访问结构 Γ 定义为由所有属性通过门限组成的属性树,对访问结构中每个节点建立阶数为 d_x 的多项式 q_x,其中 $d_x=k_x-1$,k_x 为每个节点的门限值. 定义访问结构的根节点多项式和阶数分别为 $q_{root}(0)=a$ 和 d_{root},然后通过自顶向下的方式构造其余节点的 $q_x(0)=q_{parent(x)}(index(x))$. 公钥 gpk 定义为 $\{D_x=g^{px(0)},h_i=g^{\beta ipx(0)}\}$,其中 $i=attr(x)$ 并且 x 是一个叶子节点.

签名　随机选择 $s\in\mathbb{Z}_p$,计算 $M=m_1\cdots m_k$ 的签名 $\delta_0=\left(m'\sum_{k=1}^{n}u_k^{m_k}\right)^S d,\delta_0'=g^S$. 用 ω' 表示访问结构 Γ 中的所有属性,对每个 $i\in\omega'$,随机选择 $r_i'\in\mathbb{Z}_p$并计算

$$\{\delta_{i0}=d_{i0}g^{\beta r'_i},\delta_{i1}=d_{i1}g^{r'_i}\}_{i\in\omega\cap\omega'},$$

$$\{\delta_{i0}=g^{\beta r'_i},\delta_{i1}=g^{r'_i}\}_{i\in\omega'/\omega\cap\omega'}.$$

最后,用户生成签名$(\delta_0,\{\delta_{i0},\delta_{i1}\}_{i\in\omega'},\delta_0')$.

验证　定义递归函数 $VerNode(\delta,gpk,x)$,x 是访问结构中的一个节点,该函数可能生成$\mathbb{G}_2$中的一个元素或者,表示生成结果无效,计算终止.

定义 $i=attr(x)$. 如果 x 是一个叶子节点,那么

$$VerNode(\delta,gpk,x)=\frac{e(\delta_{i0},D_x)}{e(\delta_{i1},h_i)},$$

if $e(\delta_{i0},D_x)/e(\delta_{i1},h_i)\neq1$

$\perp$, otherwise

我们注意到如果 $i\in\omega\cap\omega'$,$e(\delta_{i0},D_x)/e(\delta_{i1},h_i)=e(g_1,g_2)^{r/aqx(0)}$. 如果 $i\in\omega'\cap\omega\cap\omega'$,$e(\delta_{i0},D_x)/e(\delta_{i1},h_i)=1$. 如果 x 是一个非叶子节点,我们采用自底向上方式进行递归:对于所有 x 节点的子节点 z,调用 $VerNode(\delta,gpk,x)$ 函数并存为 F_z. 定义 $i=index(z)$,$S_x'=\{index(z):z\in S_x\}$ 并计算

$$F_x=\prod_{z\in S_x}F_z^{\Delta_{i,S'_x(0)}}=\prod_{z\in S_x}e(g,g_2)^{\frac{r}{aq_z(i)\Delta_{i,S'_x(0)}}}$$

$$=e(g,g_2)^{r/aq_x(0)}.$$

计算出 F_{root},并核对下列等式:

$$\frac{e(g,\delta_0)}{F_{root}\cdot e\left(u'\sum_{k=1}^{n}u_k^{m_k},\delta_0'\right)}=Z.$$

如果等式满足,则接受改签名,证明该签名确实是由满足访问结构的用户生成的,如果等式不满足,说明该签名无效,拒绝该签名.

净化　净化者从签名者接受签名$\{\delta_0,\delta_0'\}$和状态信息 SI. 首先净化者验证签名是否有效. 定义 $I_1=\{k\in I:m_k=0,m'_k=1\}$ 和 $I_2=\{k\in I:m_k=1,m'_k=0\}$. 净化者随机选择 $\tilde{s}\in\mathbb{Z}_p$并计算

$$\delta_S=\delta_0\frac{\prod_{k\in I_1}u_k^S}{\prod_{k\in I_2}u_k^S}u'^{\tilde{S}}\prod_{k=1}^{n}u_k^{m'_k\tilde{S}},\delta_S'=\delta_0'g^{\tilde{S}}.$$

3.2　安全性证明

定理 1　DAS-ABSS 方案满足定义 1 的正确性.

证明　当且仅当用户的属性 ω 满足访问结构 Γ,即 $\Gamma(\omega)=1$,生成的签名可以通过验证. 根据拉格朗日插值定理,$e(g,g_2)^{r/ap_{root}(0)}=e(g,g_2)^r$. 因此,

$$\frac{e(g,\delta_0)}{F_{root}\cdot e\left(u'\prod_{k=1}^{n}u_k^{m_k},\delta_0'\right)}=\frac{e\left(g,\left(u'\prod_{k=1}^{n}u_k^{m_k}\right)^S d\right)}{e(g,g_2)^r\cdot e\left(u'\prod_{k=1}^{n}u_k^{m_k},g^S\right)}$$

$$=e(g_1,g_2)$$

$$=Z.$$

签名的正确性得到验证.

净化签名的格式为:

$$\delta_S=\delta_0\frac{\prod_{k\in I_1}u_k^S}{\prod_{k\in I_2}u_k^S}u'^{\tilde{S}}\prod_{k=1}^{n}u_k^{m'_k\tilde{S}},\delta_S'=\delta_0'g^{\tilde{S}},$$

其中 $I_1=\{k\in I:m_k=0,m'_k=1\}$,$I_2=\{k\in I:m_k=1,m'_k=0\}$. 不难发现 $K\in I_1$ 时,$m'_k-m_k=1$;$K\in I_2$ 时,$m'_k-m_k=-1$;否则 $m'_k-m_k=0$. 由此我们可以推出:

$$\delta_S=\delta_0\frac{\prod_{k\in I_1}u_k^S}{\prod_{k\in I_2}u_k^S}u'^{\tilde{S}}\prod_{k=1}^{n}u_k^{m'_k\tilde{S}}=g_2^{r+a}u^{\tilde{S}+S}\prod_{k=1}^{n}u_k^{m'_k(\tilde{S}+S)}.$$

$$\delta_k'=\delta_0'g^{\tilde{S}}=g^{(\tilde{S}+S)}.$$

可以看到净化签名和原始签名具有相同分布,因此净化签名的正确性得到验证.

定理 2　DAS-ABSS 方案满足定义 2 的匿名性.

证明　在 DAS-ABSS 方案中,任何满足访问结构 Γ 的属性集都可以生成签名. 因此我们仅需在 $\omega=\omega'$的情况下证明方案满足签名者隐私性,ω'表示访问结构 Γ 中的所有属性.

属性中心运行 *Setup* 函数,生成公开参数和主密钥 a 并交给敌手 $\mathcal{A}$. 敌手 $\mathcal{A}$ 输出两个满足访问结构 Γ 的

属性集 ω_0 和 ω_1 并进行属性私钥查询,分别获得

$$sk_{\omega_0}=(d^0,\{d_{i0}^0,d_{i1}^0\}_{i\in\omega_0}),$$

$$sk_{\omega_1}=(d^1,\{d_{i0}^1,d_{i1}^1\}_{i\in\omega_1}).$$

令 $\eta\in\{0,1\}$,随机选取 $\beta_i,r_\eta,r_i^\eta\in\mathbb{Z}_p$,对每个 $i\in\omega_\eta$,计算 $d^\eta=g_2^{r_\eta+a}$,$d_{i0}^\eta=g_2^{r_i/a}\cdot(g^{\beta_i})^{r_i^\eta}$,$d_{i1}^\eta=g^{r_i^\eta}$. 挑战者随机选择一个字节 $b\in\{0,1\}$ 和消息 M 进行签名查询,生成私钥 sk_{ω_η} 关于消息 M 的签名

$$\delta^*=\left(g_2^{r+a}\cdot\left(u'\prod_{k=1}^{n}u_k^{m_k}\right)^S,\{\delta_{i0}=d_{i0}g^{\beta r_i},\right.$$

$$\left.\delta_{i1}=d_{i1}g^{r_i}\right\}_{i\in\omega',g^S}.$$

私钥 sk_{ω_η} 可能来自 sk_{ω_0} 或者 sk_{ω_1},那么该签名即可能是由生成 sk_{ω_0} 也有可能是由 sk_{ω_1} 生成,方案的匿名性得到验证.

定理 3 假设敌手能够在最多进行 q_k 次属性私钥查询和 q_s 次签名查询的前提下,在时间 t 以 ε 的概率攻破我们的签名方案,那么存在算法 B 在时间 $t'<t+(2q_k+4q_s)t_{exp}$ 内,以 $\varepsilon'\geqslant\frac{\varepsilon}{4(n+1)q_s}$ 的优势攻破 CDH 问题,其中 t_{exp} 表示在 $\mathbb{G}_1$ 中进行幂运算所需的最大时间.

证明 假设敌手 $\mathcal{A}$ 可以以一定优势攻破我们的 DAS-ABSS 方案,那么我们可以构造一个算法 B 利用敌手 $\mathcal{A}$ 攻破 CDH 问题. 即令 B 在获得 $(g,X=g^\alpha,Y=g^\beta)\in\mathbb{G}_1$ 的前提下计算 $g^{\alpha\beta}$.

初始化:$\mathcal{A}$ 定义一个挑战访问结构树 Γ^*,用 ω^* 表示 Γ^* 中的属性叶子节点. B 令 $X=g_1,Y=g_2$.

属性签名私钥生成查询 $\mathcal{A}$ 可以对属性集 ω 的签名私钥进行 q_k 次查询,ω 满足 $\Gamma^*(\omega)\neq1$,因为 $\Gamma^*(\omega)\neq1$ 且 $\omega\cap\omega^*\subseteq\omega$ 所以 $\Gamma^*(\omega\cap\omega^*)\neq1$. 假设 S 是满足访问结构 Γ^* 的属性集合并且 $\omega\cap\omega^*\subseteq S$,随机选择 $\beta_i\in\mathbb{Z}_p,\gamma_i\in\mathbb{Z}_p,r_i\in\mathbb{Z}_p$,按照如下方法生成 d_{i0},d_{i1}:

如果 $i\in S$,有 $d_{i0}=g_2^{r/a}\cdot(g^{\beta_i})^{r_i}$,$d_{i1}=g^{r_i}$,

如果 $i\notin S$,有 $d_{i0}=g_2^{r/a}\cdot(g_1^{-\beta_i}g^{\gamma_i})^{r_i}$,$d_{i1}=g^{r_i}$.

签名查询 假设签名查询的次数为 q_s,定义 $l=2q_s$. B 随机选择整数 t 满足 $0\leqslant t\leqslant n$,n 为消息长度. 对于给定的 q_s 和 n,假设 $l(n+1)<p$. 随机选择:$x'\in\mathbb{Z}_l$,$\hat{x}_k\in\mathbb{Z}_p,\hat{y}_k\in\mathbb{Z}_p$. 对消息 $M=(m_1,m_2,\cdots,m_n)$ 定义下列函数:

$$F(M)=x'+\sum_{k=1}^{n}\hat{x}_km_k-lt,$$

$$J(M)=y'+\sum_{k=1}^{n}\hat{y}_km_k.$$

B 构造以下公开参数:

$$u'=g_2^{x'-lt}g^{y'},\ u_k=g_2^{\hat{x}_k}g^{\hat{y}_k},\ k=1,\cdots,n.$$

我们可以得到下列等式:

$$u'\prod_{k=1}^{n}u_k^{m_k}=g_2^{F(M)}g^{J(M)}.$$

计算出以上公开参数后,B 将 $g_1=g^\alpha,g_2=g^\beta,u'\prod_{k=1}^{n}u_k^{m_k}$ 交给敌手 $\mathcal{A}$,然后由 $\mathcal{A}$ 进行签名查询.

B 在收到 $\mathcal{A}$ 对消息 M_j 的第 j 次签名查询后,在 $F(M_j)\neq0 \bmod p$ 的情况下,随机选取 $s_j\in\mathbb{Z}_p,r\in\mathbb{Z}_p$ 并生成签名

$$\delta_{0,j}=g^{-\frac{r(J(M_j)}{F(M_j)}}g_1^{-\frac{J(M_j)}{F(M_j)}}\left(g_2^{F(M_j)}g^{J(M_j)}\right)^{s_j},$$

$$\delta'_{0,j}=g^{-\frac{r}{F(M_j)}}g_1^{-\frac{1}{F(M_j)}}g^{s_j}.$$

令 $\hat{s}_j=s_j-\frac{a+r}{F(M_j)}$,可以推导出:

$$\begin{aligned}\delta_{0,j}&=g^{-\frac{r(J(M_j)}{F(M_j)}}g^{-\frac{a(J(M_j)}{F(M_j)}}\left(g_2^{F(M_j)}g^{J(M_j)}\right)^{s_j}\\&=g_2^{a+r}\left(g_2^{F(M_j)}g^{J(M_j)}\right)^{\hat{s}_j},\end{aligned}$$

$$\delta'_{0,j}=g^{sj-\frac{a+r}{F(M_j)}}g^{\hat{s}_j}.$$

如果 $F(M_j)=0 \bmod p$,那么上述计算无法运行,模拟中止.

根据假设 $l(n+1)<p,x'<l,\hat{x}_k<l$,可以推出 $0\leqslant lt<p,0\leqslant x'+\sum_{k=1}^{n}\hat{x}_km_k<p$,可以得出 $-p<F(M_j)<p$,那么只要 $F(M_j)=0 \bmod p$ 就有 $F(M_j)=0 \bmod l$. 相反,如果 $F(M_j)\neq0 \bmod l$ 那么 $F(M_j)\neq0 \bmod p$. 因此只要 $F(M_j)\neq0 \bmod l$(事件 A_j)就可以进行模拟.

生成签名 最后,敌手 $\mathcal{A}$ 根据之前的查询生成属性 ω' 集和消息 M^* 的签名

$$\delta^*=(\delta_0^*,\{\delta_{i0}^*,\delta_1^*\}_{i\in\omega^*},\delta_0^{*'})=g_2^{a+r}\left(g_2^{F(M^*)}g^{J(M^*)}\right)^{s^*},$$

$$\left\{g_2^{r/a}(g^{\beta_i})^{r_i+r'_i},g^{r_i+r'_i}\right\}_{i\in\omega^*},g^{s^*}),$$

如果 $F(M^*)=0 \bmod p$(事件 A^*)则继续模拟,我们可以得到:

$$\delta_0^*=g_2^{a+r}\left(g_2^{F(M^*)}g^{J(M^*)}\right)^{s^*}=g_2^{a+r}g^{J(M^*)s^*},$$

$$\delta_0^{*'}=g^{s^*}.$$

B 模拟递归函数 $ReNode(x,\Gamma^*)$,其中 x 是访问结构 Γ^* 中的一个节点,该函数生成 $\mathbb{G}_1$ 中的元素. 如果 x 是 Γ^* 中的叶子节点,令

$i=attr(x)$,$ReNode(x,\Gamma^*)=((\delta_{i1}^*)^{\beta_i}/(\delta_{i0}^*))^{q_x(0)}=g_2^{-rq_x(0)/a}$.

对每个非叶子结点 x,假设 z 是 x 的子节点,调用函数 $ReNode(x,\Gamma^*)$,将输出记为 R_z. 定义元素个数为 k_x 的集合 S_x 包含所有的 z 节点. 令 $i=index(z)$ 和 $S'_x=\{index(z):z\in S_x\}$ 并计算

$$R_x=\prod_{z\in S_x}R^{\Delta_{i,S'_x}(0)}=\prod_{z\in S_x}g_2^{-\frac{rq_x(i)\Delta_{i,S'_x}(0)}{a}}=g^{-rq_x(0)/a}.$$

因此,$R_{root}=g_2^{-rq_{root}(0)/a}=g_2^{-r}$. 最后 B 计算 $g^{\alpha\beta}=R_{root}\cdot\frac{\delta_0^*}{(\delta_0^{*'})^{J(M^*)}}$.

模拟的不中止概率取决于事件 A_j,A^*,其中:A_j 事件指 $F(M_j)\neq0 \bmod l$,其中 $j=1,\cdots,q_s$. A^* 事件指 F

$(M_j)=0 \bmod p$. 因此有 $\Pr[\overline{abort}]=\Pr[\bigwedge_{j=1}^{q_s} A_j \wedge A^*]$. 由于 $0<x'<l, 0<\hat{x}_i<l, 0\leqslant t\leqslant n$,可以得出 $0\leqslant F(M^*) \bmod p<l(n+1)$, $\Pr[A^*]=\frac{1}{l(n+1)}$. 同理可求得 $\Pr[\neg A_j]=\frac{1}{l}$. 又注意到 A_j 和 A^* 之间相互独立,可以求得:

$$\Pr[(\bigwedge_{j=1}^{q_s} A_j)\wedge A^*]\geqslant\frac{1}{l(n+1)}\left(1-\sum_{j=1}^{q_s}\Pr[\neg A_j|A^*]\right)=\frac{1}{4q_s(n+1)}.$$

3.3　性能分析

表 1 给出了 DAS-ABSS 方案与现有方案在功能上的对比. 可以看出 DAS-ABSS 方案在降低了用户端计算开销的同时,能够提供细粒度的访问控制,支持灵活的访问结构,且具有更高的安全性.

在表 2 中我们和现有方案进行了效率对比,首先将现有方案分为两类:支持单层访问结构和支持树形访问结构. 对于支持单层访问结构的方案[13,14],ω 表示签名者拥有的属性,$n+1$ 表示系统中所有的属性,d 表示门限值,m 表示消息的长度. 在方案[15]中,l 表示访问结构中的所有属性,t 是一个和门限相关的参数,最大值用 $t_{\max}$ 表示. 方案[16]中用 S 表示访问结构中用到的所有内节点的集合,令 $\zeta=|S|$. 在净化签名阶段用表示状态信息集合,令 $\theta=|I|$. 在计算开销部分,用 P 和 EXP 分别表示双线性对运算的次数和指数运算的次数.

通过比较可以看出,我们的方案在主密钥长度上具有优势,在公开参数、属性签名密钥和签名长度上和现有方案相当,保证了效率. 由于原始签名需要对消息的每个比特逐个进行计算,因此在签名生成和验证过程中的计算开销略长于现有方案,但用户端仅需生成一次签名,降低了用户的计算开销.

表 1　方案功能比较

	本文方案	方案[13]	方案[14]	方案[15]	方案[16]
降低用户开销	是	否	否	否	否
匿名性	是	否	是	是	是
细粒度访问控制	是	是	是	是	是
树形访问结构	是	否	否	是	是
安全模型	标准模型	标准模型	标准模型	一般群模型	随机谕言机模型

表 2　方案效率比较

	本文方案	方案[13]	方案[14]	方案[15]	方案[16]
公开参数 *params*	$(m+4)\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	$(m+\omega+4)\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$	$(n+5)\lvert\mathbb{G}_1\rvert$	$(3t_{\max}+4)\lvert\mathbb{G}_1\rvert$	$3\lvert\mathbb{G}_1\rvert+\lvert\mathbb{G}_2\rvert$
主密钥 *Mk*	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$	$3\lvert\mathbb{Z}_p\rvert$	$\lvert\mathbb{Z}_p\rvert$
属性签名密钥 sk_ω	$(2\omega+1)\lvert\mathbb{G}_1\rvert$	$2\omega\lvert\mathbb{G}_1\rvert$	$2\omega\lvert\mathbb{G}_1\rvert$	$(\omega+2)\lvert\mathbb{G}_1\rvert$	$(2\omega+1)\lvert\mathbb{G}_1\rvert$
验证密钥 *Vk*	$2l\lvert\mathbb{G}_1\rvert$	–	–	–	$2l\lvert\mathbb{G}_1\rvert$
签名长度	$(2l+2)\lvert\mathbb{G}_1\rvert$	$(3\omega)\lvert\mathbb{G}_1\rvert$	$(3\omega)\lvert\mathbb{G}_1\rvert$	$(l+t+2)\lvert\mathbb{G}_1\rvert$	$(2l+2)\lvert\mathbb{G}_1\rvert$
净化签名长度	$2\lvert\mathbb{G}_1\rvert$	–	–	–	–
签名生成开销	$(m+2l+2)EXP$	$(m+2\omega)EXP$	$(3\omega)EXP$	$(3lt+4l+2)EXP$	$(2l+2)EXP$
净化签名生成开销	$(m+\theta+2)EXP$	–	–	–	–
验证开销	$2lP+(\zeta+m)EXP$	$3dP+(m+d)EXP$	$(3d+1)P+2dEXP$	$(tl+t+3)P+(2lt+t)EXP$	$2lP+\zeta EXP$

4　总结

传统的签名方案并不适用电子医疗档案系统,因为数据频繁更新会增加用户端的计算开销,同时造成了用户的身份泄露. 针对上述问题,我们提出了一种支持树形访问结构的属性基净化签名方案. 理论分析表明,我们的方案在标准模型下针对给定策略选择消息攻击具有不可伪造性,并且保护了用户的身份隐私. 通过和现有方案进行比较,本方案减少了用户端的计算开销,同时支持更加灵活的树形访问结构,更适用电子医疗档案系统中.

参考文献

[1] Hoerbst A, Ammenwerth E. Electronic health records[J]. Methods Inf Med, 2010, 49(4): 320 – 336.

[2] Sinsky C A, Beasley J W, Simmons G E, et al. Electronic health records: design, implementation, and policy for high-

er-value primary care[J]. Annals of Internal Medicine, 2014,160(10):727 – 728.
[3] Blumenthal D,Tavenner M. The "meaningful use" regulation for electronic health records[J]. New England Journal of Medicine,2010,363(6):501 – 504.
[4] Gellert G A,Ramirez R,Webster S L. The rise of the medical scribe industry:implications for the advancement of electronic health records[J]. JAMA,2015,313(13):1315 – 1316.
[5] Ateniese G,Chou D H,De Medeiros B,et al. Sanitizable signatures[A]. ESORICS 2005[C]. Berlin:Springer Heidelberg,2005. 159 – 177.
[6] Krawczyk H,Rabin T. Chameleon hashing and signatures [EB/OL]. http://eprint. iacr. org/1998/010,1998-03-17/2017-01-09.
[7] Canard S,Jambert A,Lescuyer R. Sanitizable signatures with several signers and sanitizers[A]. AFRICACRYPT 2012[C]. Berlin:Springer Heidelberg,2012. 35 – 52.
[8] Brzuska C,Fischlin M,Lehmann A,et al. Unlinkability of sanitizable signatures[A]. PKC 2010[C]. Berlin:Springer Heidelberg. 2010. 444 – 461.
[9] Brzuska C,Pøhls H C,Samelin K. Non-interactive public accountability for sanitizable signatures[A]. EuroPKI 2012[C]. Berlin:Springer Heidelberg,2013. 178 – 193.
[10] Brzuska C,P? hls H C,Samelin K. Efficient and perfectly unlinkable sanitizable signatures without group signatures[A]. EuroPKI 2013[C]. Berlin:Springer Heidelberg,2014. 12 – 30.
[11] Agrawal S,Kumar S,Shareef A,et al. Sanitizable signatures with strong transparency in the standard model[A]. Inscrypt 2009[C]. Berlin:Springer Heidelberg,2010. 93 – 107.
[12] 王小明,付红,张立臣. 基于属性的访问控制研究进展[J]. 电子学报,2010,38(7):1660 – 1667.
Wang Xiaoming,Fu Hong,Zhang Lichen. Research progress on attribute based access control[J]. Acta Electronica Sinica,2010,38(7):1660 – 1667. (in Chinese)
[13] Yang P,Cao Z,Dong X. Fuzzy identity based signature [EB/OL]. http://eprint. iacr. org/2008/002,2007-12-31/2017-01-09.
[14] Shahandashti S F,Safavi-Naini R. Threshold attribute-based signatures and their application to anonymous credential systems[A]. AFRICACRYPT 2009[C]. Berlin:Springer Heidelberg,2009. 198 – 216.
[15] Maji H K,Prabhakaran M,Rosulek M. Attribute-based signatures:achieving attribute-privacy and collusion-resistance[EB/OL]. http://eprint. iacr. org/2008/328,2008-07-29/2017-01-09.
[16] Su J,Cao D,Zhao B,et al. ePASS:An expressive attribute-based signature scheme with privacy and an unforgeability guarantee for the internet of things[J]. Future Generation Computer Systems,2014,33:11 – 18.
[17] 李琦,马建峰,熊金波,等. 一种素数阶群上构造的自适应安全的多授权机构 CP-ABE 方案[J]. 电子学报,2013,42(4):696 – 702.
Li Qi,Ma Jianfeng,Xiong Jinbo,et al. An adaptively secure multi-authority ciphertext-policy ABE scheme on prime order groups[J]. Acta Electronica Sinica,2013,42(4):696 – 702. (in Chinese)

作者简介

莫 若 男,1990 年生于陕西渭南. 西安电子科技大学网络与信息安全学院博士研究生. 研究方向为数字签名.
E-mail:593430655@qq.com

马建峰(通信作者) 男,1963 年生于陕西西安. 西安电子科技大学计算机学院、网络与信息安全学院教授、博士生导师. 研究方向为密码学、计算机网络与信息安全.
E-mail:jfma@mail.xidian.edu.cn