抗共谋攻击的多授权电子健康记录共享方案

王经纬[1,3],吴静雯[1],殷新春[1,2,3]
(1. 扬州大学信息工程学院,江苏扬州 225127; 2. 扬州大学广陵学院,江苏扬州 225128;
3. 广东省信息安全技术重点实验室,广东广州 510275)

摘 要: 为解决属性基加密方案中用户权限变更不灵活以及无法抵抗共谋攻击的问题,本文提出一种抗共谋攻击的多授权电子健康记录共享方案. 采用版本控制的方式实现属性撤销,属性授权中心为非撤销用户提供更新密钥并更新密文,而没有更新密钥的用户将无法继续获取数据. 为了保证数据访问的效率,系统将大部分计算外包至云服务器执行. 此外,所有属性授权中心需要生成各自的公私钥对以抵抗共谋攻击. 本方案在随机谕言模型下满足选择明文攻击不可区分安全,与其他多中心方案相比,功能更加实用且解密开销至少降低了45.9%.

关键词: 属性基加密;多授权中心;抗共谋攻击;属性撤销;外包解密;外包可验证
基金项目: 广东省信息安全技术重点实验室开放基金(No.2020B1212060078)
中图分类号: TP309.7 **文献标识码:** A **文章编号:** 0372-2112(2023)05-1179-08
电子学报URL:http://www.ejournal.org.cn **DOI:**10.12263/DZXB.20220769

Collusion-Resistant Multi-Authority Electronic Health Records Sharing Scheme

WANG Jing-wei[1,3], WU Jing-wen[1], YIN Xin-chun[1,2,3]
(1. *College of Information Engineering, Yangzhou University, Yangzhou, Jiangsu* 225127, *China*;
2. *Guangling College of Yangzhou University, Yangzhou, Jiangsu* 225128, *China*;
3. *Guangdong Provincial Key Laboratory of Information Security Technology, Guangzhou, Guangdong* 510275, *China*)

Abstract: To achieve flexible user revocation and collusion attack resistance, this paper proposes a collusion- resistant multi-authority EHRs (Electronic Health Records) sharing scheme. Version control is used to achieve user revocation. Attribute authorities need to distribute update keys for non-revoked users as well as update the ciphertexts in the cloud, and users without update keys will not be able to access data. To guarantee the performance of data retrieval, most of the computation is outsourced to the cloud. Besides, all the attribute authorities need to generate a pair of public key and secret key to resist collusion attacks. The proposed scheme is indistinguishably secure against chosen-plaintext attack under the random oracle model. Compared to other multi-authority schemes, the proposed scheme is practical in function and the overhead of the decryption is reduced by at least 45.9%.

Key words: attribute-based encryption; multi-authority; anti-collusion attack; attribute revocation; outsource decryption; outsource verification
Foundation Item(s): Opening Project of Guangdong Provincial Key Laboratory of Information Security Technology (No.2020B1212060078)

1 引言

随着云计算技术的不断成熟,越来越多的软件开始提供数据传输、存储、共享等服务. 在医疗行业,各类传感器24小时不间断地监测患者的生理状态,自动将产生的电子健康记录(Electronic Health Records, EHRs)存储在指定的第三方服务器中供医护人员诊断. 尽管这有助于提高医护人员的工作效率,但将患者的EHRs存储在第三方云服务器使患者失去了对数据的管理能力,带来了安全方面的问题[1~4]. 针对这些问题,研究人员基于属性基加密(Attribute-Based Encryption, ABE)提出了大量的EHRs访问控制方案[5~10]. 然而,这些方案大多采用单授权中心结构,并不适合多授

收稿日期:2022-07-01;修回日期:2022-11-21;责任编辑:覃怀银

权中心[11~13]的场景.

在多授权中心的研究方面,Lewko等[14]提出了去中心化的ABE方案,但其中每个授权中心只能管理一个属性,实用性较差. Rouselakis等[15]改进了文献[14]中的方案,消除了授权中心管理属性数量的限制. 文献[16~19]提出了各具特色的多授权ABE方案,但这些方案均无法抵抗共谋攻击. 在撤销方面,文献[20,21]分别提出了一个支持属性撤销的ABE方案,但计算开销较大. 文献[22,23]中的方案计算效率较高,但安全与实用性存在缺陷. 为解决上述问题,本文提出一个抗共谋攻击的多授权电子健康记录共享(Collusion-resistant Multi-authority EHRs Sharing, CM-EHRS)方案,在抵抗共谋攻击的同时提供外包解密、外包可验证以及属性撤销功能,可以保证方案的安全与执行效率.

2 CM-EHRS方案

2.1 实体介绍

本方案包括以下4类实体:

(1) 属性授权中心(Attribute Authority, AA):AA负责生成系统参数、为用户生成部分属性私钥以及实现属性撤销. AA是半可信的.

(2) 数据拥有者(Data Owner, DO):DO负责制定访问策略、加密EHRs并上传至云服务器进行存储和共享. DO是可信的.

(3) 数据用户(Data User, DU):DU可以按照其属性的权限访问云服务器中的数据. DU是不可信的.

(4) 云服务器(Cloud Server, CS):CS负责存储DU上传的密文、执行外包解密、密文更新等算法. CS是半可信的.

2.2 安全目标

(1) 选择明文攻击不可区分(Indistinguishable Chosen-Plaintext Attack, IND-CPA)安全:给定2个等长的明文,使用相同的访问策略加密后,未授权的DU无法在两者之间进行区分.

(2) 抗用户共谋攻击:即使未授权DU通过与不满足访问策略的DU合并属性私钥也无法恢复该未授权DU本身无法解密的数据.

(3) 抗用户与属性授权中心共谋攻击:即使未授权DU与AA进行共谋(要求该未授权DU的属性集合与AA负责属性的并集无法满足访问策略)也无法恢复未授权DU本身无法解密的数据.

2.3 安全性假设

在q-DPBDHE2(q-Decisional Parallel Bilinear Diffie-Hellman Exponent2)假设[15]中,挑战者选择阶为p的群G和G_T,构造双线性映射$e: G\times G\to G_T$,随机选择$s,a,b_1,b_2,\cdots,b_q\in\mathbf{Z}_p, g\in G, Y\in G_T$. 令

$$T=(G,G_T,p,e,g),T_0=g^s \tag{1}$$

$$T_1=\{g^{a^i}\}_{i\in[2q],i\neq q+1} \tag{2}$$

$$T_2=\{g^{b_j a^i}\}_{(i,j)\in[2q,q],i\neq q+1},T_3=\{g^{s/b_j}\}_{j\in[q]} \tag{3}$$

$$T_4=\{g^{sa^i b_j/b_{j'}}\}_{(i,j,j')\in[q+1,q,q],j\neq j'} \tag{4}$$

Y为群G_T中的一个随机元素. 令元组$D=(T,T_0,T_1,T_2,T_3,T_4),r=a^{q+1}$,攻击者无法在多项式时间内区分$(D,e(g,g)^{sr})$与$(D,Y)$.

定义1 对于任意多项式时间算法,如果其成功解决q-DPBDHE2问题的优势是可忽略的,则称q-DPBDHE2困难性假设成立.

2.4 方案设计

CM-EHRS方案包括系统初始化、用户注册、EHRs上传、EHRs访问和属性撤销5个阶段,方案执行步骤如图1所示.

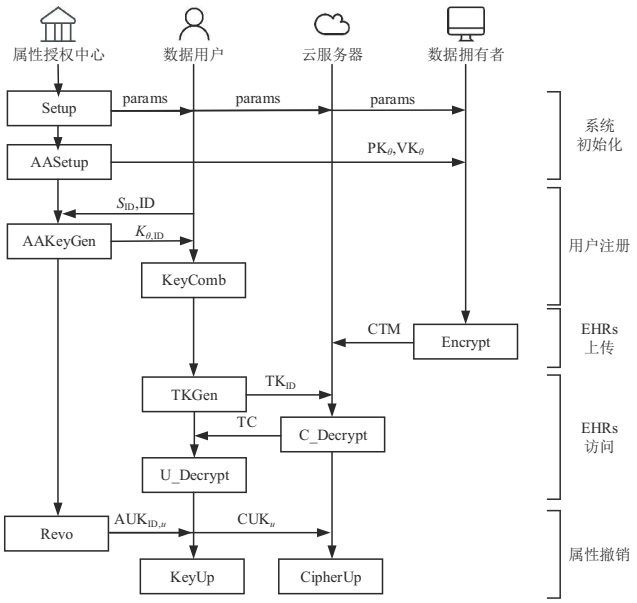


图1 方案执行步骤图

2.4.1 系统初始化

该阶段包括2个步骤,主要目的是生成并公开系统参数.

步骤1 Setup(λ)$\to$params

AA根据输入的安全参数λ生成群参数(G,G_T,p,e). 随机选择$g\in G$以及3个安全的哈希函数$H:\{0,1\}^*\to G, T:\{0,1\}^*\to G, H_1:\{0,1\}^*\to\{0,1\}^*$. 最终生成的系统公共参数为params$=\{(G,G_T,p,e),g,H,T,H_1\}$(params为其他算法的默认输入).

步骤2 AASetup(S_θ)$\to\{PK_\theta,MSK_\theta,VK_\theta,v_\theta\}$

该算法由所有的$\{AA_\theta\}_{\theta\in[n]}$执行,输入$AA_\theta$管理的属性集合$S_\theta$. AA_θ随机选择$\alpha_\theta,\beta_\theta\in\mathbf{Z}_p$,计算$PK_{\theta,1}=e(g,g)^{\alpha_\theta}, PK_{\theta,2}=g^{\beta_\theta}$. 令$AA_\theta$的公钥为$PK_\theta=\{PK_{\theta,1},PK_{\theta,2}\}$,

主私钥为$\mathrm{MSK}_\theta=\{\alpha_\theta,\beta_\theta\}$. 对于属性$u\in S_\theta$,$\mathrm{AA}_\theta$随机选择$u$的初始版本私钥$v_{v,u}\in\mathbf{Z}_p$,计算版本公钥$\mathrm{VK}_{v,u}=e(g,T(u))^{v_{v,u}}$. AA_θ公开PK_θ以及S_θ的版本公钥$\mathrm{VK}_\theta=\{\mathrm{VK}_{v,u}\}_{u\in S_\theta}$,保存$\mathrm{MSK}_\theta$以及$S_\theta$的版本私钥$v_\theta=\{v_{v,u}\}_{u\in S_\theta}$,其中下标$v$为版本号,初值为0.

2.4.2　用户注册

该阶段包括2个步骤,AA通过AAKeyGen为DU生成部分属性私钥,DU再通过KeyComb组合部分属性私钥为完整属性私钥.

步骤3　$\mathrm{AAKeyGen}(S_{\mathrm{ID}},S_\theta,\mathrm{ID},\mathrm{MSK}_\theta,v_\theta)\rightarrow K_{\theta,\mathrm{ID}}$

该算法由AA_θ执行,输入$\mathrm{DU}_{\mathrm{ID}}$的属性集合$S_{\mathrm{ID}}$,$\mathrm{AA}_\theta$的属性集合$S_\theta$,$\mathrm{DU}_{\mathrm{ID}}$的身份标识ID,$\mathrm{AA}_\theta$的主私钥$\mathrm{MSK}_\theta$以及版本私钥$v_\theta$. 对于$u\in S_{\mathrm{ID}}\cap S_\theta$,$\mathrm{AA}_\theta$随机选择$t_u\in\mathbf{Z}_p$,保存$\{\mathrm{ID},u,t_u\}$. 按式(5)和式(6)计算属性$u$的私钥$\{K_{\mathrm{ID},u},K_{v,u}\}$:

$$K_{\mathrm{ID},u}=g^{\alpha_\theta}H(\mathrm{ID})^{\beta_\theta}T(u)^{v_{v,u}(t_u+1)}\tag{5}$$

$$K_{v,u}=g^{v_{v,u}t_u}\tag{6}$$

AA_θ将部分属性私钥$K_{\theta,\mathrm{ID}}=\{K_{\mathrm{ID},u},K_{v,u}\}_{u\in S_{\mathrm{ID}}\cap S_\theta}$发送给$\mathrm{DU}_{\mathrm{ID}}$.

步骤4　$\mathrm{KeyComb}(\{K_{\theta,\mathrm{ID}}\}_{\theta\in\mathrm{AAList}})\rightarrow K_{\mathrm{ID}}$

该算法由$\mathrm{DU}_{\mathrm{ID}}$执行,令AAList为AA编号的集合,算法输入各AA为$\mathrm{DU}_{\mathrm{ID}}$生成的部分属性私钥$\{K_{\theta,\mathrm{ID}}\}_{\theta\in\mathrm{AAList}}$. $\mathrm{DU}_{\mathrm{ID}}$将所有$K_{\theta,\mathrm{ID}}$组合后即可得到完整的属性私钥$K_{\mathrm{ID}}=\{K_{\mathrm{ID},u},K_{v,u}\}_{u\in S_{\mathrm{ID}}}$.

2.4.3　EHRs上传

令D表示EHRs,基于密钥封装的思想,我们首先使用对称密钥ck加密D生成对称密文$E_{\mathrm{ck}}(D)$,然后利用ABE加密ck生成部分密文CT.

步骤5　$\mathrm{Encrypt}(\mathrm{PK}_\theta,\mathrm{VK}_\theta,(\boldsymbol{M},\rho,F),\mathrm{ck},E_{\mathrm{ck}}(D))\rightarrow$

CTM**该算**法由DO执行,输入AA_θ的公钥PK_θ和版本公钥VK_θ,访问策略$(\boldsymbol{M},\rho,F)$,对称密钥ck,对称密文$E_{\mathrm{ck}}(D)$. 令$s\in\mathbf{Z}_p$为秘密值,算法选择向量$\boldsymbol{h}=(s,h_2,\cdots,h_n)$,$\boldsymbol{f}=(0,f_2,\cdots,f_n)$,其中$h_i,f_i\in\mathbf{Z}_p$. 令$\boldsymbol{M}_i$为矩阵$\boldsymbol{M}$第$i$行构成的向量,对$i\in[l]$,算法计算$\lambda_i=\boldsymbol{M}_i\cdot\boldsymbol{h}$,$o_i=\boldsymbol{M}_i\cdot\boldsymbol{f}$,随机选择$r_i\in\mathbf{Z}_p$,按式(7)和式(8)计算:

$$C_0=\mathrm{ck}e(g,g)^s,C_{i,1}=e(g,g)^{\lambda_i}(\mathrm{PK}_{\theta,1}\mathrm{VK}_{v,u})^{r_i}\tag{7}$$

$$C_{i,2}=g^{-r_i},C_{i,3}=\mathrm{PK}_{\theta,2}^{r_i}g^{o_i},C_{i,4}=T(\rho(i))^{r_i}\tag{8}$$

则部分密文为$\mathrm{CT}=\{C_0,\{C_{i,1},C_{i,2},C_{i,3},C_{i,4}\}_{i\in[l]}\}$. 算法计算用于验证的信息摘要$H_1(\mathrm{ck}\|E_{\mathrm{ck}}(D))$,将密文$\mathrm{CTM}=\{\mathrm{CT},(\boldsymbol{M},\rho,F),H_1(\mathrm{ck}\|E_{\mathrm{ck}}(D)),E_{\mathrm{ck}}(D)\}$上传至CS存储.

2.4.4　EHRs访问

该阶段包括3个步骤,DU首先通过TKGen生成用于外包解密的传输密钥并发送给CS,CS通过C_Decrypt计算半解密密文,将计算结果返回给DU后,DU执行U_Decrypt获取解密结果. 为验证CS是否忠实地执行了外包解密的步骤,DU在解密完成后可以计算一个信息摘要与密文中的摘要进行对比,只有当两者一致时DU才接受解密结果.

步骤6　$\mathrm{TKGen}(K_{\mathrm{ID}},\mathrm{ID})\rightarrow\{\mathrm{TK}_{\mathrm{ID}},\mu\}$

该算法由DU执行,输入完整属性私钥K_{ID}以及用户身份ID. 算法随机选择$\mu\in\mathbf{Z}_p$作为用户秘密值,计算$\mathrm{TK}_{\mathrm{HID}}=H(\mathrm{ID})^\mu$,对$u\in S_{\mathrm{ID}}$,按式(9)计算:

$$\mathrm{TK}_{\mathrm{ID},u}=(K_{\mathrm{ID},u})^\mu,\mathrm{TK}_{v,u}=(K_{v,u})^\mu\tag{9}$$

则半解密私钥为:

$$\mathrm{TK}_{\mathrm{ID}}=\{\mathrm{TK}_{\mathrm{HID}},\{\mathrm{TK}_{\mathrm{ID},u},\mathrm{TK}_{v,u}\}_{u\in S_{\mathrm{ID}}}\}\tag{10}$$

DU将$\mathrm{TK}_{\mathrm{ID}}$发送给CS,自己保存$\mu$.

步骤7　$\mathrm{C\_Decrypt}(\mathrm{CTM},\mathrm{TK}_{\mathrm{ID}})\rightarrow\mathrm{TC}/\perp$

该算法由CS执行,输入完整密文CTM以及$\mathrm{TK}_{\mathrm{ID}}$. 若$\mathrm{TK}_{\mathrm{ID}}$中的属性能够满足CTM中的访问策略,对$i\in[l]$,算法选择常数$w_i\in\mathbf{Z}_p$使得$\sum_{i\in[l]}w_i\boldsymbol{M}_i=(1,0,\cdots,0)$,否则输出$\perp$. 随后令$P_i=e(\mathrm{TK}_{\mathrm{ID},\rho(i)},C_{i,2})e(\mathrm{TK}_{\mathrm{HID}},C_{i,3})e(\mathrm{TK}_{v,\rho(i)},C_{i,4})$,计算$\mathrm{TP}_1=\prod_{i\in[l]}P_i^{w_i}$,$\mathrm{TP}_2=\prod_{i\in[l]}C_{i,1}^{w_i}$. CS将半解密密文$\mathrm{TC}=\{\mathrm{TP}_1,\mathrm{TP}_2,H_1(\mathrm{ck}\|E_{\mathrm{ck}}(D)),E_{\mathrm{ck}}(D),C_0\}$发送给$\mathrm{DU}_{\mathrm{ID}}$.

步骤8　$\mathrm{U\_Decrypt}(\mathrm{TC},\mu)\rightarrow\mathrm{ck}$

该算法由DU执行,输入TC和用户秘密值μ. 算法计算$\mathrm{TP}=\mathrm{TP}_2(\mathrm{TP}_1)^{1/\mu}$,$R=C_0/\mathrm{TP}$. 如果$H_1(\mathrm{ck}\|E_{\mathrm{ck}}(D))=H_1(R\|E_{\mathrm{ck}}(D))$,则C_Decrypt计算过程无误,$R$即为对称密钥ck.

2.4.5　属性撤销

该阶段包含3个步骤,当AA需要撤销拥有属性u的DU时,负责管理u的$\mathrm{AA}_{F(u)}$首先通过Revo更新u的版本私钥,分别将属性更新密钥和密文更新密钥发送给非撤销用户和CS. 非撤销用户通过KeyUp更新属性私钥,CS通过CipherUp更新密文.

步骤9　$\mathrm{Revo}(v_{F(u)},t_u,u)\rightarrow\{\mathrm{AUK}_{\mathrm{ID},u},\mathrm{CUK}_u\}$

该算法由$\mathrm{AA}_{F(u)}$执行,输入$\mathrm{AA}_{F(u)}$的版本私钥集合$v_{F(u)}$、用户随机数t_u以及待撤销属性u. 算法为u选择新的版本私钥$v_{v+1,u}\in\mathbf{Z}_p$替换$v_{F(u)}$中的旧版本私钥,计算并公布u的新版本公钥$\mathrm{VK}_{v+1,u}=e(g,T(u))^{v_{v+1,u}}$. 对系统中的非撤销用户,计算属性更新密钥以及密文更新密钥如式(11)~(13).

$$\mathrm{AUK}_{\mathrm{ID},u,1}=T(u)^{(v_{v+1,u}-v_{v,u})(t_u+1)}\tag{11}$$

$$\mathrm{AUK}_{\mathrm{ID},u,2}=g^{(v_{v+1,u}-v_{v,u})t_u}\tag{12}$$

$$\mathrm{CUK}_u=T(u)^{v_{v,u}-v_{v+1,u}}\tag{13}$$

$\mathrm{AA}_{F(u)}$将$\mathrm{AUK}_{\mathrm{ID},u}=\{\mathrm{AUK}_{\mathrm{ID},u,1},\mathrm{AUK}_{\mathrm{ID},u,2}\}$发送给所有非撤销用户,将$\mathrm{CUK}_u$发送给CS.

步骤 10 $\mathrm{KeyUp}(\mathrm{AUK}_{\mathrm{ID},u'},K_{\mathrm{ID}})\rightarrow K_{\mathrm{ID}}$

该算法由 DU 执行，令 u' 为待更新属性，输入 $\mathrm{AUK}_{\mathrm{ID},u'}$ 以及 K_{ID}. 解析 K_{ID} 为 $\{K_{\mathrm{ID},u},K_{v,u}\}_{u\in S_{\mathrm{ID}}}$，选择其中与 u' 相关的私钥 $\{K_{\mathrm{ID},u'},K_{v,u'}\}$，按式(14)和式(15)计算：

$$K_{\mathrm{ID},u'}=K_{\mathrm{ID},u'}\mathrm{AUK}_{\mathrm{ID},u',1} \tag{14}$$

$$K_{v+1,u'}=K_{v,u'}\mathrm{AUK}_{\mathrm{ID},u',2} \tag{15}$$

输出更新后的完整属性私钥：

$$K_{\mathrm{ID}}=\{\{K_{\mathrm{ID},u},K_{v,u}\}_{u\in S_{\mathrm{ID}}\backslash\{u'\}},\{K_{\mathrm{ID},u'},K_{v+1,u'}\}\} \tag{16}$$

步骤 11 $\mathrm{CipherUp}(\mathrm{CUK}_{u'},\mathrm{CTM})\rightarrow \mathrm{CTM}$

该算法由 CS 执行，输入 $\mathrm{CUK}_{u'}$ 和 CTM，其中 u' 为待更新属性，已知 $\mathrm{CUK}_{u'}=T(u')^{v_{v,u'}-v_{v+1,u'}}$，$\mathrm{CTM}=\{\mathrm{CT},(\boldsymbol{M},\rho,F),H_1(\mathrm{ck}\|E_{\mathrm{ck}}(D)),E_{\mathrm{ck}}(D)\}$，$\mathrm{CT}=\{C_0,\{C_{i,1},C_{i,2},C_{i,3},C_{i,4}\}_{i\in[l]}\}$，对于 $i\in[l]$，若 $\rho(i)=u'$ 则计算并更新 $C_{i,1}=C_{i,1}e(C_{i,2},\mathrm{CUK}_{u'})$，输出更新后的密文 CTM.

3 安全性分析

3.1 IND-CPA 安全

定理 1 若 q-DPBDHE2 假设成立，面对规模最大为 $q\times q$ 的线性秘密共享矩阵，本方案是 IND-CPA 安全的.

证明 令 A 为多项式时间的攻击者，C 为挑战者，可模拟本方案中的所有算法. S 为系统中属性的集合，$\boldsymbol{M}$ 表示大小为 $l\times n$ 的访问控制矩阵，$M_{i,j}$ 为矩阵 $\boldsymbol{M}$ 中第 i 行第 j 个元素. 令 c 表示受被妥协 AA 管理属性的数量，$n'=n-c$，对矩阵 $\boldsymbol{M}$ 作行变换可得等价矩阵 $\boldsymbol{M}'$ 使得其中前 $c\times n'$ 个元素全为 0，矩阵 $\boldsymbol{M}$ 以及 $\boldsymbol{M}'$ 见式(17)和式(18).

$$\boldsymbol{M}=\begin{bmatrix}M_{1,1}&\cdots&M_{1,n}\\ \vdots&\ddots&\vdots\\ M_{l,1}&\cdots&M_{l,n}\end{bmatrix} \tag{17}$$

$$\boldsymbol{M}'=\begin{bmatrix}0&\cdots&0&M'_{1,n'+1}&\cdots&M'_{1,n}\\ 0&\cdots&0&M'_{2,n'+1}&\cdots&M'_{2,n}\\ \vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\ M'_{c+1,1}&\cdots&M'_{c+1,n'}&M'_{c+1,n'+1}&\cdots&M'_{c+1,n}\\ \vdots&\ddots&\vdots&\vdots&\ddots&\vdots\\ M'_{l,1}&\cdots&M'_{l,n'}&M'_{l,n'+1}&\cdots&M'_{l,n}\end{bmatrix} \tag{18}$$

初始化阶段 A 提交要挑战的访问策略 $(\boldsymbol{M},\rho,F)$. 令 AA_C 表示妥协的 AA 集合，AA_N 表示正常的 AA 集合. C 运行 Setup 算法生成群参数 (G,G_T,p,e)，随机选择 $g\in G$ 以及安全的哈希函数 $H:\{0,1\}^*\rightarrow G$，$T:\{0,1\}^*\rightarrow G$，$H_1:\{0,1\}^*\rightarrow\{0,1\}^*$，生成公共参数 $\mathrm{params}=\{(G,G_T,p,e),g,H,T,H_1\}$.

查询阶段 1 A 发起如下询问.

属性授权中心及版本密钥询问：A 向 C 提交由 AA_i 管理的属性 u. 在运行 AASetup 算法时，如果 $\mathrm{AA}_i\in\mathrm{AA}_C$，则由 A 随机选择 $\alpha_i,\beta_i\in\mathbf{Z}_p$，生成 $\mathrm{PK}_i=\{e(g,g)^{\alpha_i},g^{\beta_i}\}$ 并发送给 C. 如果 $\mathrm{AA}_i\in\mathrm{AA}_N$ 且挑战访问策略与 AA_i 有关，C 随机选取 $\alpha_i,\beta_i\in\mathbf{Z}_p$，生成 $\mathrm{PK}_i=\{e(g,g)^{\alpha_i},g^{\beta_i}\}$；如果与挑战访问策略无关，$C$ 设置集合 $X=\{i|F(i)\}$，其中函数 F 可以将 i 映射到负责属性 $\rho(i)$ 的 AA. 此时 C 构造 $\alpha_i=\sum_{i\in X}b_ia^{q+1}M'_{i,1}$，$\beta_i=\sum_{i\in X}\sum_{j=2}^{n'}b_ia^{q+2-j}M'_{i,j}$. 令 AA_i 的公钥如式(19)：

$$\mathrm{PK}_i=\{\prod_{i\in X}e(g^{b_ia},g^{a^q})^{M'_{i,1}},\prod_{i\in X}\prod_{j=2}^{n'}(g^{b_ia^{q+2-j}})^{M'_{i,j}}\} \tag{19}$$

对 $u\in S$，如果 $\mathrm{AA}_i\in\mathrm{AA}_C$，$C$ 随机选取 $T(u)\in G$. 否则，C 设置集合 $X=\{i|F(i)\}\backslash\{\rho(i)=u\}$，该集合包含除 u 所在的行以外所有由 AA_i 管理的行. 此时，C 设 $T(u)=g\prod_{i\in X}\prod_{j\in[1,n']}(g^{b_ia^{q+1-j}})^{M'_{i,j}}$. 最后，$C$ 选择 $v_{v,u}\in\mathbf{Z}_p$，公开相应的 $\mathrm{VK}_{v,u}=e(g,T(u))^{v_{v,u}}$，$C$ 将 PK_i 和 $\mathrm{VK}_{v,u}$ 发送给 A.

属性私钥询问：A 向 C 提交用户身份 ID 及其对应的属性集合 S_{ID}. 对于 S_{ID} 中不与挑战访问策略相关的属性，C 随机选择 $J_i\in\mathbf{Z}_p$，输出 $H(\mathrm{ID}_i)=g^{J_i}$. 对于其他属性，C 构造向量如式(20)：

$$\boldsymbol{d}_i=(1,d_{i,2},\cdots,d_{i,n'},0,\cdots,0) \tag{20}$$

$d_{i,j}$ 为 $\boldsymbol{d}_i$ 的第 j 个元素且 $d_{i,j}\in\mathbf{Z}_p$. 选取 $J_i\in\mathbf{Z}_p$，输出 $H(\mathrm{ID}_i)=g^{J_i}\prod_{k=2}^{n'}(g^{a^{k-1}})^{d_{i,k}}$. 令 AA_u 表示管理 u 的 AA，当 C 为 u 生成属性私钥时，考虑以下情况.

(1) 如果挑战访问策略与 AA_u 无关. C 随机选取 $t_u\in\mathbf{Z}_p$，输出 $K_{\mathrm{ID},u}=g^{\alpha_i}H(\mathrm{ID})^{\beta_i}T(u)^{v_{v,u}(t_u+1)}$，$K_{v,u}=g^{v_{v,u}t_u}$.

(2) 如果挑战访问策略与 AA_u 有关. 此时有式(21)和式(22)：

$$H(\mathrm{ID}_i)=g^{J_i}\prod_{k=2}^{n'}(g^{a^{k-1}})^{d_{i,k}} \tag{21}$$

$$T(u)=g\prod_{i\in X}\prod_{j\in[1,n']}(g^{b_ia^{q+1-j}})^{M'_{i,j}} \tag{22}$$

C 构造 $t_u=-\sum_{k\in[1,n']}a^kd_{i,k}/v_{u,v}$，令属性私钥为 $K_{\mathrm{ID},u}=g^{\alpha_\theta}H(\mathrm{ID})^{\beta_\theta}T(u)^{v_{u,v}(t_u+1)}$，$K_{v,u}=g^{v_{u,v}t_u}$. 但由于 C 不掌握 $g^{b_ia^{q+1}}(i\in X)$，因此无法为 A 生成 u 的属性私钥.

A 收到各个 AA 生成的部分属性私钥后，通过 KeyComb 算法获取完整的属性私钥.

挑战阶段 A 选择 2 个等长的消息提交给 C，C 随机选择 $b\in\{0,1\}$，计算 $C_0=m_bY$，其中 Y 由 q-DPBDHE2 问题提供. C 构造 $z=sa^{q+1}$，并设向量

$$\boldsymbol{h}=(sa^{q+1},0,\cdots,0),\boldsymbol{f}=(0,sa^q,\cdots,sa^{q-n'+2},0,\cdots,0).$$

对于被妥协 AA 所掌控的行 i^*，根据已有条件可知 $\lambda_{i^*}=\boldsymbol{M}_{i^*}\cdot\boldsymbol{h}=0$，$o_{i^*}=\boldsymbol{M}_{i^*}\cdot\boldsymbol{f}=0$. C 随机选取 $r_{i^*}\in\mathbf{Z}_p$，计算 $C_{1,i^*}=e(g,g)^{\alpha_{F(i^*)}r_{i^*}}e(g,T(\rho(i^*)))^{v_{u,v}r_{i^*}}$，$C_{2,i^*}=g^{-r_{i^*}}$，$C_{3,i^*}=g^{\beta_{F(i^*)}r_{i^*}}$，$C_{4,i^*}=T(\rho(i^*))^{r_{i^*}}$.

对由正常AA掌控的行i^*,已知有$\lambda_{i^*}=sa^{q+1}M'_{i^*,1}$,$o_{i^*}=\sum_{j=2}^{n'}sa^{q+2-j}M'_{i^*,j}$. C构造$r_{i^*}=-s/b_{i^*}$,令

$$\xi=\frac{sb_i a^{q+1}}{b_{i^*}},\psi=-\frac{T(u)v_{\rho(i^*),v}s}{b_{i^*}},Q=e(g,g) \tag{23}$$

按式(24)~(26)计算密文:

$$C_{1,i^*}=\prod_{i\in X\setminus\{i^*\}}Q^{-M'_{i,1}\xi}Q^{-\psi}\prod_{i\in X}\prod_{j\in[1,n']}Q^{-v_{\rho(i^*),v}M'_{i,j}\xi} \tag{24}$$

$$C_{2,i^*}=g^{-r_{i^*}}=g^{s/b_{i^*}},C_{3,i^*}=\prod_{i\in X\setminus\{i^*\}}\prod_{j=2}^{n'}(g^{\xi a^{1-j}})^{-M'_{i,j}} \tag{25}$$

$$C_{4,i^*}=g^{-T(u)s/b_{i^*}}\prod_{i\in X}\prod_{j\in[1,n']}(g^{\xi a^{-j}})^{-M'_{i,j}} \tag{26}$$

查询阶段2　与查询阶段1相同,但询问不能满足挑战访问策略.

猜测阶段　已知$z=sa^{q+1}$,$\prod_{i\in[1,q]}e(g,g)^{\lambda_i w_i}=e(g,g)^{sa^{q+1}}$,如果$Y=e(g,g)^{sa^{q+1}}$,则有式(27):

$$\frac{C_0}{e(g,g)^{sa^{q+1}}}=\frac{m_b Y}{e(g,g)^{sa^{q+1}}}=m_b \tag{27}$$

如果A不能正确地猜出b的值,则C认为Y是群G_T上的随机元素,如果A能以不可忽略的优势猜对b的值,则C认为$Y=e(g,g)^{sa^{q+1}}$.

综上,C解决q-DPBDHE2难题的能力可以被归约为A打破本方案不可区分性的能力. 由于q-DPBDHE2难题不可解,因此本方案是IND-CPA安全的.

证毕

3.2　抗用户共谋攻击

在本方案中,DU的属性私钥包括$K_{\mathrm{ID},u}=g^{\alpha_\theta}H(\mathrm{ID})^{\beta_\theta}T(u)^{v_{v,u}(t_u+1)}$,$K_{v,u}=g^{v_{v,u}t_u}$,其中$K_{\mathrm{ID},u}$不仅包括用户身份ID,还与$u$的版本私钥$v_{v,u}$和随机值$t_u$有关. 当恶意DU与其他DU实施共谋攻击时,由于ID、$v_{v,u}$和t_u均不相同且ID由AA的主私钥保护,恶意DU无法获得权限更高的合法属性私钥.

3.3　抗用户与属性授权中心共谋攻击

在为DU生成部分属性私钥之前,各个AA需要分别执行AASetup算法,为自己生成属性授权中心公私钥对及负责管理的属性的版本公私钥对. 随后,各个AA公开公钥以及负责属性的版本公钥,保存主私钥与属性的版本私钥. 在生成部分属性私钥时,需要输入AA的主私钥与对应属性的版本私钥,因此只要恶意AA不同时具备其他AA的主私钥与对应属性的版本私钥,则无法伪造由其他AA负责的部分属性私钥.

4　功能与性能分析

4.1　功能分析

CM-EHRS方案与同类方案[15~17,19~23]功能对比见表1. 相比于其他方案,CM-EHRS方案实现了属性撤销、外包解密和外包可验证的功能,不仅允许AA动态更新属性的版本实现属性撤销. 在安全性方面,我们的方案可以抵抗共谋攻击与选择明文攻击. 总体而言,本方案在功能上更加全面.

4.2　性能分析

4.2.1　统计分析

假设系统中有a个AA,k+1个用户(1个DO和k个DU). 在数据共享的过程中共需执行k次私钥生成算法和私钥合并算法(无计算开销),1次加密算法,k×n次数据解密操作(包括k×n次外包解密和k×n次用户解密). 为便于统计,假设DU属性的数量与访问策略中属性的数量同为80(t=i=80),访问策略均以AND互相连接,AA数量为5(a=5). 我们在表2中基于Charm[24]框架统计了私钥生成/i属性,加密/t属性,解密/t属性的时间开销. 结果显示,本方案在数据共享中的计算时间约为0.883k+0.442+0.146kn ms. 文献[15,16,18,19]的计算时间分别约为0.883k+0.626 +0.347kn ms, 0.667k+0.597+0.586kn ms, 0.473k+ 0.504+0.299kn ms, 0.504k+0.345+0.105kn ms. 因此,本方案的开销更低,同时随着数据用户进行解密的次数越多,本方案的优势将越来越明显.

表1　功能对比表

方案	撤销	多授权中心	外包解密	外包可验证	抗共谋攻击	选择明文攻击
文献[15]	×	√	×	×	×	√
文献[16]	×	√	√	√	√	√
文献[17]	属性撤销	√	×	×	√	√
文献[19]	×	√	×	×	×	√
文献[20]	属性撤销	√	×	×	√	√
文献[21]	属性撤销	×	×	×	√	√
文献[22]	用户撤销	√	×	×	√	√
文献[23]	用户撤销	×	×	×	√	√
CM-EHRS	属性撤销	√	√	√	√	√

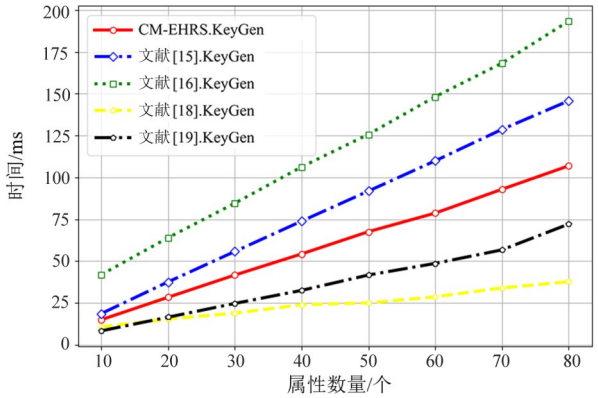
4.2.2　实验分析

为评估方案的实际性能,我们分别统计了本方案与文献[15,16,18,19]方案中私钥生成算法、加密算法以及解密算法的运行时间,如图2所示. 实验基于Charm框架使用Python3编程实现. 实验平台是一台Macbook Pro笔记本电脑,采用四核Inter Core i7(2.7 GHz)处理器,内存16 GB,显卡采用Intel Iris Plus Graphics 655(1 536 MB).

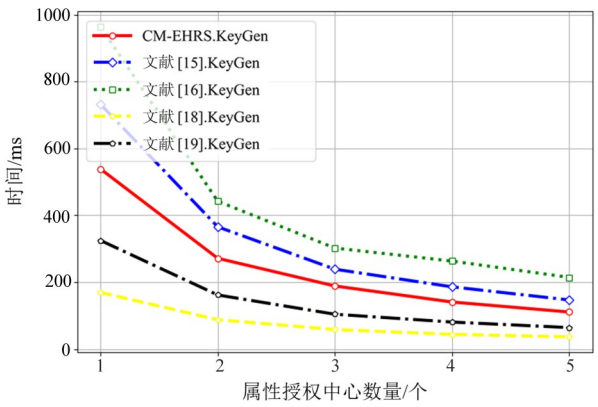
各方案私钥生成算法运行时间随用户属性数量变化的情况如图2(a)所示. 约定AA的数量为5,用户属性数量从10~80递增,5个AA各自管理一个互不相交

表2 计算开销统计分析对比表 单位:ms

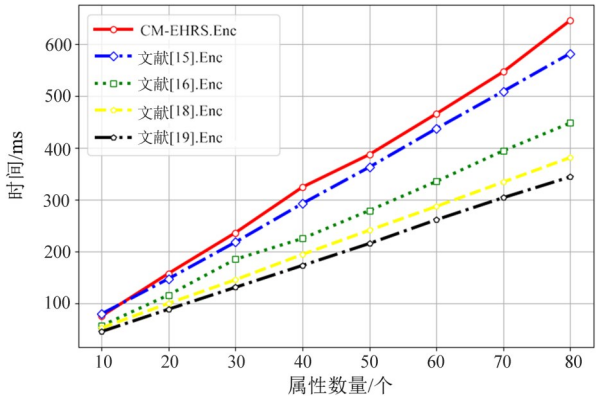
方案	私钥生成	加密	外包解密	用户解密
文献[15]	0.011 04i	0.007 827 9t+0.000 138 6	0.0043 422t	
文献[16]	0.011 55a+0.007 62i	0.007 35t+0.009 279 3	0.007 222 2t+0.003 368 6	0.004 878 6
文献[18]	0.006 3a +0.005 52i	0.006 3t+0.000 069 3a+0.002 238 6	0.003 656 5t+0.001 337 9a+0.000 138 6	
文献[19]	0.006 3i	0.004 2t+0.001 407 2a+0.002 169 3	0.001 268 6t+0.000 634 3a+0.000 138 6	
CM-EHRS	0.011 04i	0.005 527 1t+0.000 138 6	0.001 833 6t	0.000 207 9



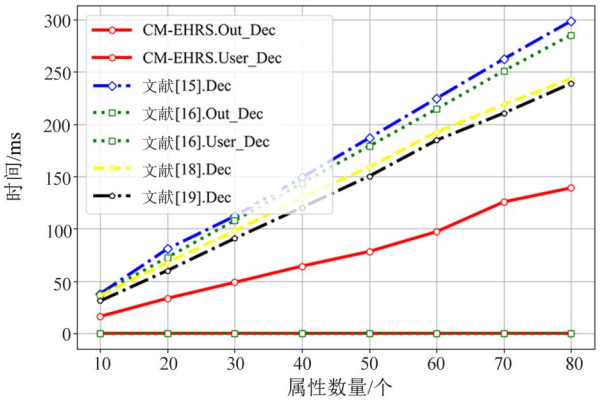
(*a*) 私钥生成时间随属性数量变化情况



(*b*) 私钥生成时间随属性授权中心数量变化情况



(*c*) 加密时间随属性数量变化情况



(*d*) 解密时间随属性数量变化情况

图2 运行时间对比图

的属性集合,每个属性集合中属性的数量基本一致. 结果显示本方案相比于文献[15,16]中的方案计算开销更低,但高于文献[18,19]. 这是由于本方案需要比文献[18]的方案多计算1个私钥成分,比文献[19]的方案多计算属性版本信息. 由于本方案的功能与文献[16]更为接近,因此将文献[16]中的方案作为主要的对比对象. 当AA数量为5、用户属性数量为80时,本方案的私钥生成时间为106.91 ms,而文献[16]中的方案为193.31 ms,计算开销降低了(193.31-106.91)/193.31=44.6%. 各方案私钥生成算法运行时间随AA数量变化的情况如图2(*b*)所示. 当属性数量固定为80、AA数量从1~5递增时,约定每个AA管理的属性数量分别为80、40、26、20、16. 结果显示各方案的运行时间排列与图2(*a*)一致且随着AA的增加,各AA单独的计算时间逐渐下降. 各方案在加密算法中的计算开销如图2(*c*)所示. 在加密阶段,约定访问策略中属性数量从10~80递增. 各方案解密算法的运行时间如图2(*d*)所示. 在解密阶段,约定解密私钥中属性的数量从10~80递增. 由于文献[16]中的方案与本方案均支持外包解密功能,我们分别展示了这两个方案在外包解密和用户解密阶段的运行时间. 结果显示,当访问策略的属性数量为80时,本方案的解密时间为129.04 ms,而文献[15,16,18,19]方案中的解密时间分别为298.55 ms、285.28 ms、243.41 ms、238.90 ms. 因此本方案在解密阶段的计算开销至少降低了(238.90−129.04)/238.90=45.9%.

5 总结

为抵抗共谋攻击,实现灵活的用户权限管理,本文提出一种多授权电子健康记录共享方案并基于Charm框架通过Python对方案进行实现. 安全性分析表明本方案在随机谕言模型下满足IND-CPA安全. 实验证明本方案显著降低了用户在数据访问时的计算开销.

参考文献

[1] 沈剑, 周天祺, 曹珍富. 云数据安全保护方法综述[J]. 计算机研究与发展, 2021, 58(10): 2079-2098.
SHEN J, ZHOU T Q, CAO Z F. Protection methods for cloud data security[J]. Journal of Computer Research and Development, 2021, 58(10): 2079-2098. (in Chinese)

[2] 冯登国, 张敏, 张妍, 等. 云计算安全研究[J]. 软件学报, 2011, 22(1): 71-83.
FENG D G, ZHANG M, ZHANG Y, et al. Study on cloud computing security[J]. Journal of Software, 2011, 22(1): 71-83. (in Chinese)

[3] 张玉清, 王晓菲, 刘雪峰, 等. 云计算环境安全综述[J]. 软件学报, 2016, 27(06): 1328-1348.
ZHANG Y Q, WANG X F, LIU X F, et al. Survey on cloud computing security[J]. Journal of Software, 2016, 27 (06): 1328-1348. (in Chinese)

[4] LI H W, YANG Y, DAI Y S, et al. Achieving secure and efficient dynamic searchable symmetric encryption over medical cloud data[J]. IEEE Transactions on Cloud Computing, 2020, 8(2): 484-494.

[5] GE C P, SUSILO W, BAEK J, et al. Revocable attribute-based encryption with data integrity in clouds[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(5): 2864-2872.

[6] 牛淑芬, 谢亚亚, 杨平平, 等. 区块链上基于云辅助的属性基可搜索加密方案[J]. 计算机研究与发展, 2021, 58 (4): 811-821.
NIU S F, XIE Y Y, YANG P P, et al. Cloud-assisted attribute- based searchable encryption scheme on blockchain [J]. Journal of Computer Research and Development, 2021, 58(4): 811-821. (in Chinese)

[7] OSTROVSKY R, SAHAI A, WATERS B. Attribute-based encryption with non-monotonic access structures[C]//Proceedings of the 14th ACM Conference on Computer and Communications Security. New York: ACM, 2007: 195-203.

[8] HE K, GUO J, WENG J, et al. Attribute-based hybrid Boolean keyword search over outsourced encrypted data [J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(6): 1207-1217.

[9] 佘维, 霍丽娟, 刘炜, 等. 一种可隐藏敏感文档和发送者身份的区块链隐蔽通信模型[J]. 电子学报, 2022, 50(4): 1002-1013.
SHE W, HUO L J, LIU W, et al. A blockchain-based covert communication model for hiding sensitive documents and sender identity[J]. Acta Electronica Sinica, 2022, 50 (4): 1002-1013. (in Chinese)

[10] 赵志远, 朱智强, 王建华, 等. 属性可撤销且密文长度恒定的属性基加密方案[J]. 电子学报, 2018, 46(10): 2391-2399.
ZHAO Z Y, ZHU Z Q, WANG J H, et al. Attribute-based encryption with attribute revocation and constant-size ciphertext[J]. Acta Electronica Sinica, 2018, 46(10): 2391-2399. (in Chinese)

[11] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP ′07). Piscataway: IEEE Computer Society, 2007: 321-334.

[12] WATERS B. Ciphertext-policy attribute-based encryption: an expressive, efficient, and provably secure realization[C]//Proceedings of the 14th International Conference on Practice and Theory in Public Key Cryptography. Berlin: Springer, 2011: 53-70.

[13] ZENG P, ZHANG Z T, LU R X, et al. Efficient policy-hiding and large universe attribute-based encryption with public traceability for Internet of medical things[J]. IEEE Internet of Things Journal, 2021, 8(13): 10963-10972.

[14] LEWKO A B, WATERS B. Decentralizing attribute-based encryption[C]//Proceedings of the 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2011: 568-588.

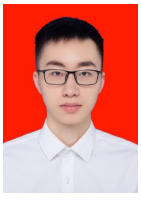
[15] ROUSELAKIS Y, WATERS B. Efficient statically-secure large-universe multi-authority attribute-based encryption[C]//Proceedings of the 19th International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2015: 315-332.

[16] 仲红, 崔杰, 朱文龙, 等. 高效且可验证的多授权机构属性基加密方案[J]. 软件学报, 2018, 29(7): 2006-2017.
ZHONG H, CUI J, ZHU W L, et al. Efficient and verifiable muti-authority attribute based encryption scheme[J]. Journal of Software, 2018, 29(7): 2006-2017. (in Chinese)

[17] MIAO Y B, DENG R H, LIU X M, et al. Multi-authority attribute-based keyword search over encrypted cloud data [J]. IEEE Transactions on Dependable and Secure Com-

puting, 2021, 18(4): 1667-1680.
[18] WEI J H, CHEN X F, HUANG X Y, et al. RS-HABE: Rrevocable-storage and hierarchical attribute-based access scheme for secure sharing of e-health records in public cloud[J]. IEEE Transactions on Dependable and Secure Computing, 2021, 18(5): 2301-2315.
[19] 闫玺玺, 刘媛, 李子臣, 等. 支持隐私保护的多机构属性基加密方案[J]. 计算机研究与发展, 2018, 55(4): 846-853.
YAN X X, LIU Y, LI Z C, et al. Multi-authority attribute-based encryption scheme with privacy protection[J]. Journal of Computer Research and Development, 2018, 55(4): 846-853. (in Chinese)
[20] YANG K, JIA X H. Expressive, efficient, and revocable data access control for multi-authority cloud storage[J]. IEEE Transactions on Parallel and Distributed Systems, 2014, 25(7): 1735-1744.
[21] VARRI U S, KASANI S, PASUPULETI S K, et al. FELT-ABKS: Fog-enabled lightweight traceable attribute-based keyword search over encrypted data[J]. IEEE Internet of Things Journal, 2022, 9(10): 7559-7571.
[22] CHEN J W, MA H D. Efficient decentralized attribute-based access control for cloud storage with user revocation[C]//2014 IEEE International Conference on Communications (ICC). Piscataway: IEEE, 2014: 3782-3787.
[23] HAN D Z, PAN N N, LI K C. A traceable and revocable ciphertext-policy attribute-based encryption scheme based on privacy protection[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(1): 316-327.
[24] AKINYELE J A, GARMAN C, et al. Charm: a framework for rapidly prototyping cryptosystems[J]. Journal of Cryptographic Engineering, 2013, 3(2): 111-128.

作者简介



王经纬 男, 1993 年 12 月出生于江苏省镇江市. 现为扬州大学信息工程学院博士生. 主要研究方向为属性基加密.
E-mail: M160437@yzu.edu.cn

吴静雯 女, 1996 年 3 月出生于江苏省扬州市. 主要研究方向为车联网安全、属性基加密.
E-mail: 2052229781@qq.com

殷新春(通讯作者) 男, 1962 年 2 月出生于江苏省姜堰市. 现为扬州大学信息工程学院博士生导师, 教授. 主要研究方向为密码学、软件质量保障、高性能计算.
E-mail: xcyin@yzu.edu.cn