基于内积谓词的属性基隐私保护加密方案

张志强[①] 朱友文*[①②] 王 箭[①] 张玉书[①]

[①](南京航空航天大学计算机科学与技术学院 南京 211106)

[②](桂林电子科技大学广西密码学与信息安全重点实验室 桂林 541010)

摘 要：隐私保护是信息安全中的热点话题，其中属性基加密(ABE)中的隐私问题可分为数据内容隐私、策略隐私及属性隐私。针对数据内容、策略和属性3方面隐私保护需求，该文提出基于内积谓词的属性基隐私保护加密方案(PPES)。所提方案利用加密算法的机密性保障数据内容隐私，并通过向量承诺协议构造策略属性及用户属性盲化方法，实现策略隐私及属性隐私。基于混合论证技术，该文证明了所提方案满足标准模型下适应性选择明文安全，且具备承诺不可伪造性。性能分析结果显示，与现有方法相比，所提方案具有更优的运行效率。

关键词：隐私保护；属性基加密；内积谓词；策略隐藏

中图分类号：TN918.4 **文献标识码**：A **文章编号**：1009-5896(2023)03-0828-08

DOI: 10.11999/JEIT221050

Attribute Based Privacy Protection Encryption Scheme Based on Inner Product Predicate

ZHANG Zhiqiang[①] ZHU Youwen[①②] WANG Jian[①] ZHANG Yushu[①]

[①](*College of Computer Science and Technology*, *Nanjing University of Aeronautics and Astronautics*, *Nanjing* 211106, *China*)

[②](*Guangxi Key Laboratory of Cryptography and Information Security*, *Guilin University of Electronic Technology*, *Guilin* 541010, *China*)

Abstract: Privacy protection is a hot topic in information security, where the privacy issues in Attribute Based Encryption(ABE) can be divided into data content privacy, policy privacy and attribute privacy. Considering the three privacy protection needs of data content, policy and attributes, an attribute-based Privacy-Preserving Encryption Scheme based on inner product predicates (PPES) is proposed. The privacy of data content is ensured by using confidentiality of encryption algorithm, furthermore the blind method of policy attributes and user attributes is constructed through vector commitment protocol to achieve policy privacy and attribute privacy. Based on the hybrid argument technology, adaptive chosen plaintext security of the scheme is proved under standard model. Besides commitment unforgeability of the scheme is also illustrated. The performance analysis results show that the proposed scheme has better operation efficiency compared to existing methods.

Key words: Privacy protection; Attribute Based Encryption(ABE); Inner product predicate; Policy hiding

收稿日期：2022-08-10；改回日期：2022-11-01；网络出版：2022-11-05

*通信作者： 朱友文 zhuyw@nuaa.edu.cn

基金项目：国家重点研发计划(2021YFB3100400)，国家自然科学基金(62172216, 62032025, 62071222, U20A201092)，广东省重点研发计划(2020B0101090002)，江苏省自然科学基金(BK20211180)，广西密码学与信息安全重点实验室开放课题(GCIS202107)

Foundation Items: The National Key Research and Development Program of China (2021YFB3100400), The National Natural Science Foundation of China (62172216, 62032025, 62071222, U20A201092), The Key R&D Program of Guangdong Province (2020B0101090002), The Natural Science Foundation of Jiangsu Province (BK20211180), The Research Fund of Guangxi Key Laboratory of Cryptography and Information Security (GCIS202107)

1　引言

2005年Sahai和Waters[1]在基于身份加密的基础上，提出了属性基加密(Attribute-Based Encryption, ABE)，ABE机制中包含属性及访问策略，其中属性描述事物的客观特征信息，策略则是特征之间的关系；若用户属性满足策略设置的最低阈值，那么则可成功解密。ABE机制凭借其1对多、细粒度的访问控制特点，受到业内学者的广泛关注，而后又延伸出了谓词加密、对偶策略、函数加密、匹配加密[2]等密码原语。在诸多ABE方案中，考虑到隐私保护，一般分3个层面，分别是数据内容隐私、策略隐私以及属性隐私。

数据内容隐私通过加密算法所具备的机密性来实现，将隐私性绑定到密码系统的安全性上，而密码系统的安全性则依赖已知难解的困难问题及密钥的安全管理。在医疗数据隐私[3]、外包安全计算[4]等应用领域，使用ABE不仅确保了数据内容隐私的机密性，且能够提供细粒度的访问控制。通过加密来保障数据隐私的方法[5–7]本质上是一种风险转移，将棘手的隐私数据保护转换为更易操作的ABE方案构造，但同时也带了新的问题，即ABE中的策略隐私与属性隐私。

策略隐私保护中主要有两种方式，分别是部分策略隐藏及完全策略隐藏。常见的部分策略隐藏方法有通配符替代、属性名与属性值分割[8–10]等；完全策略隐藏大都采用对原始属性做映射变换的方式[11]。Lai等人[12]结合双系统加密技术，基于合数阶群提出了标准模型下的策略隐藏ABE方案，对策略属性进行映射变换，加密中需要使用两个秘密向量，虽然安全性较好，但也导致密文长度增加。Hur[13]同样采用策略属性映射的方式进行方案构造，相比于文献[11]效率更优，但该方案依赖于一般群模型构造，未能达到可证明安全。Michalevsky等人[14]基于内积谓词加密构造了支持接收者隐私的策略隐藏方案，对不属于加密策略的属性进行0值填充，但大量无效属性值导致策略冗余较为明显。Qian等人[15]构造了策略完全隐藏的ABE方案，并额外给出了零知识性的密钥生成协议，但未验证其协议效率以及在完整方案中的可行性。

属性隐私具体指用户在向授权机构申请密钥阶段，自身属性信息的隐私性。Han等人[16]较早关注到这一问题，提出了一种保护隐私的去中心化密钥策略ABE方案，通过在用户与授权机构之间进行零知识性的密钥协商协议，完成密钥的分发工作。该方案构造的零知识密钥协商保护了用户属性隐私不被授权机构泄露，但协议过程太过复杂，且被文献[17]指出其方案不具备用户合谋安全性：即通过更改与特定密钥相关联的标识符来删除单个用户密钥之间的关联性，进而未满足解密条件的多个用户可通过密钥聚合的方式完成解密操作。紧接着，Han等人[18]对原工作做了改进，但方案中并未对原密钥协商协议进行简化，并且被文献[19]指出该方案仍不具备用户合谋安全性。

ABE隐私保护研究中部分工作侧重点是数据内容隐私[3–7]；针对策略隐私的研究较多[8–15]，但未兼顾用户属性隐私，方案中均假设授权机构完全可信且不涉及用户属性窃听及泄露；文献[16–19]从用户属性隐私的角度出发，但构造中未考虑策略隐私。究其原因，加解密用户分别在策略保护与属性保护中进行随机化操作后，很难将解密等式构造成功。

针对以上存在的问题，本文同时兼顾数据内容、用户属性、访问策略3方面隐私保护需求，构造了基于内积谓词的属性基隐私保护加密方案(attribute-based Privacy Protection Encryption Scheme based on inner product predicate, PPES)。概况地说，本文的主要工作有以下3点：

(1) 基于谓词加密算法保障了数据内容隐私，通过向量承诺协议将访问策略与用户属性分别进行盲化，兼顾了属性隐私和策略隐私；同时，改进了Catalano协议，使其适配于属性盲化承诺，能够在不暴露关键隐私信息的前提下，完成承诺验证。

(2) 借助内积向量的线性运算模式，实现了ABE隐私保护中多方随机元素消去操作，使得加解密双方分别进行随机化后，仍然能够进行解密等式构造(详见5.1节)。

(3) 基于判定性子群假设证明了所提方案满足标准模型下适应性选择明文安全，并且承诺具备不可伪造性。性能分析结果显示，所提方案比现有方案效率更高。

2　预备知识

本节给出本文中用于构建PPES方案所用到的基础定义及基础协议。

2.1　基础定义

定义1　(合数阶双线性映射)给定安全参数λ，令Setup(λ)表示双线性群生成算法，输出阶为合数$N=pqr$的乘法循环群G, G_T, p, q, r为互不相同的3个素数，g为群G生成元。定义双线性映射e:$G\times G\to G_T$满足如下性质：

(1)可计算性：双线性映射e在多项式时间内可被有效计算。

(2)双线性：$\forall g,h\in G$；$a,b\in Z_N$有$e(g^a,h^b)=e(g,h)^{ab}$。

(3)非退化性：$e(g,g)\neq 1$。

定义2 (判定性子群假设)给定群生成器Setup(λ)定义其子群分布为

$$(N=pqr,G,G_T,e)\xleftarrow{R}\text{Setup} \tag{1}$$

$$g_1\xleftarrow{R}G_P,g_3\xleftarrow{R}G_R,g_{1,2}\xleftarrow{R}G_pG_Q \tag{2}$$

$$D=(g_1,g_3,g_{1,2}) \tag{3}$$

$$T_0\xleftarrow{R}G_P,T_1\xleftarrow{R}G_pG_Q \tag{4}$$

对于公开元组D，任意概率多项式敌手A能够正确区分T_0与T_1的优势定义为

$$\text{Adv}(\lambda):=|\Pr[A(D,T_0)=1]-\Pr[A(D,T_1)=1]| \tag{5}$$

2.2 基础协议

协议1 向量承诺协议(Vector Commitment, VC)。协议主体由4个多项式算法构成[20]，分别是承诺密钥生成算法、承诺计算算法、承诺打开算法以及承诺验证算法。

PPES方案中，将加解密用户的盲化操作利用承诺协议进行提交，用于公开验证盲化操作的合法性。向量承诺协议能够对指定位置i处进行承诺验证，提供了位置绑定特性；由承诺封装带来的消息隐藏特性，能够确保所参与承诺的元素与机密信息无关，进而真实的属性信息不会被泄露。

协议2 谓词加密[7](Predicate Encryption, PE)是基于属性加密的延伸和扩展，内积谓词则是PE的构造形式之一，其中密钥对应布尔函数表示的谓词$\mathbb{F}$，密文则与属性集合Σ相关。当密钥SK_f对应谓词$f\in\mathbb{F}$，且密文关联属性$I\in\Sigma$满足$f(I)=1$时解密成功。

3 模型定义

本节给出论文中的模型定义，包括系统模型、安全模型及算法模型。

3.1 系统模型

如图1所示，PPES方案涉及5个实体，分别是属性授权中心、云服务提供商、第三方验证者、数据用户及数据属主。考虑到策略隐私及属性隐私，DO需使用盲化后的属性构造访问策略；DU使用盲化后的属性申请私钥，并对盲化结果做出承诺。

属性授权中心(Attribute Authority, AA)：该实体完全可信，负责系统初始化、主密钥、公共参数及用户公私钥生成。

云服务提供商(Cloud Service Provider, CSP)：该实体为半可信服务器，为用户提供密文存储及下载服务。

第三方验证者(Third Party Verifier, TPV)：向加解密双方提出验证请求，对加解密双方所提交承诺的有效性做验证。

数据用户(Data User, DU)：从CSP下载密文，若满足解密要求，可对其进行解密；作为用户证明者(User Prover, U-Prover)回答验证者请求。

数据属主(Data Owner, DO)：加密数据并上传到CSP；作为属主证明者(Owner Prover, O-Prover)回答验证者请求。

3.2 安全模型

定义3 (数据内容隐私) 给定安全参数n，对任意多项式时间敌手A，如果在下述游戏中的优势是可忽略的，那么称PPES方案满足数据内容隐私。

(1)挑战者C运行初始化算法Setup(1^n)，获得公共参数$pp:\{N=pqr,G,G_T,e(\cdot)\}$，$g_pg_qg_r$分别对应3个子群生成元。

(2)随机选择$t\in G_P$，$Q_1,Q_2\in G_Q$，$s,\theta\in Z_p$，将$(N,G,G_T,e(\cdot),g_p,g_q,g_r,t,g_p^s,t^sQ_1,g_p^\theta Q_2,e(g_p,t)^\theta)$公开，并选择随机比特$b\in\{0,1\}$，如果$b=0$，将$e(g_p,t)^{\theta s}$发送给敌手A，如果$b=1$，则发送$\mathbb{G}_T$中的随机元素。

(3)敌手A输出比特b'，当$b=b'$时，攻击成功。

上述游戏中，敌手A的优势可定义为

$$\text{Adv}=|\Pr[b=b']-1/2| \tag{6}$$

定义4 (策略隐私) 设谓词集合为$\mathbb{F}$，属性集合为$\mathbb{S}$，安全参数为n。对任意多项式时间敌手A，在下述游戏中优势可忽略，那么称该谓词加密方案满足策略隐私。

(1)挑战者C运行初始化算法Setup(1^n)生成公钥PK，私钥SK，大整数N，并将其发送给敌手A。

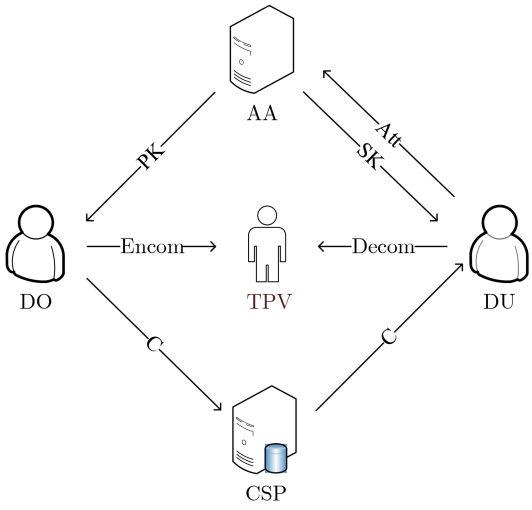

图 1 系统模型

(2)敌手A输出$\boldsymbol{x},\boldsymbol{y}\in Z_N^n$。

(3)敌手A对向量$\boldsymbol{v}_1$,$\boldsymbol{v}_2$,$\cdots$,$\boldsymbol{v}_l\in Z_N^n$所对应密钥做适应性请求，其中所有的$i$都需满足$<\boldsymbol{v}_i,\boldsymbol{x}>=0 \bmod N$，当且仅当$<\boldsymbol{v}_i,\boldsymbol{y}>=0 \bmod N$。挑战者C运行$\mathrm{Genkey}_{\mathrm{SK}}(\mathrm{f}_{\mathrm{v}_i})$算法将对应的私钥$\mathrm{SK}_{\mathrm{v}_i}$返回给敌手A。

(4)挑战者C随机选择$b\in\{0,1\}$，当$b=0$时，输出密文$C=\mathrm{Enc}_{\mathrm{PK}}(\boldsymbol{x})$；当$b=1$时，输出密文$C=\mathrm{Enc}_{\mathrm{PK}}(\boldsymbol{y})$。

(5)在第(3)步的限制条件下，敌手A继续对其他谓词向量进行适应性私钥询问。

(6)敌手A输出b'，若满足$b=b'$，那么敌手攻击成功。

上述游戏中，敌手A的优势可定义为

$$\mathrm{Adv}=|\Pr[b=b']-1/2| \tag{7}$$

定义5 (属性隐私) 给定安全参数n，q阶循环群G_1，其生成元为P。对任意多项式时间敌手A，在下述游戏中的优势是可忽略的，那么称PPES方案满足属性隐私。

(1)挑战者C运行初始化算法$\mathrm{Setup}(1^n)$，生成公共参数$\mathrm{pp}=\{G_1,q,P\}$。

(2)挑战者C随机选择$a,b\in Z_q^*$，计算$(aP,bP)\in G_1$并公开。选择随机比特$b\in\{0,1\}$，如果$b=0$，将abP发送给敌手A，如果$b=1$，则发送G_1中的随机元素。

(3)敌手A输出比特b'，当$b=b'$时，攻击成功。

上述游戏中，敌手A的优势可定义为

$$\mathrm{Adv}=|\Pr[b=b']-1/2| \tag{8}$$

3.3 算法模型

(1)系统初始化算法$\mathrm{Setup}(1^n)\rightarrow(\mathrm{pp},\mathrm{MPK},\mathrm{MSK})$：该算法由可信授权中心执行，输入安全参数，输出公共参数pp及系统主公钥与主私钥。

(2)加密算法$\mathrm{Encrypt}(\mathrm{MPK},\mathrm{MSK},M,(A,\rho),\boldsymbol{x})\rightarrow(C)$：该算法由数据属主执行，首先将加密所需属性向量$\boldsymbol{x}$盲化为$\boldsymbol{h}$；使用盲化后的属性向量$\boldsymbol{h}$构造LSSS访问策略，完成对谓词向量的张成，将明文M加密为密文C。

(3)用户属性盲化算法$\mathrm{User\text{-}Blind}(\boldsymbol{v})\rightarrow(\boldsymbol{u})$：该算法由数据用户执行，用户将自身属性向量$\boldsymbol{v}$盲化为$\boldsymbol{u}$，然后将其发送给授权机构生成私钥。

(4)密钥生成算法$\mathrm{KeyGen}(\mathrm{MPK},\mathrm{MSK},\boldsymbol{u})\rightarrow(\mathrm{SK})$：该算法由授权机构执行，根据数据用户的属性$\boldsymbol{u}$生成数据用户私钥SK。

(5)解密算法$\mathrm{Decrypt}(\mathrm{SK},C)\rightarrow(M)$：该算法由数据用户执行，输入私钥SK与密文$C$，若属性满足谓词授权集合，输出解密结果$M$。

(6)承诺提交及验证算法：$\mathrm{Verify}(\mathrm{Com},s_i,\mathrm{Aux})\rightarrow(\mathrm{Result})$：该算法为证明者与验证者之间的交互。首先要求作为证明者的U-Prover与O-Prover在盲化操作完成后，分别提交盲化承诺，而后交由第三方验证。

4　方案构造

本节给出方案的具体构造，并对算法模型中的多项式算法做进一步阐述。

(1)$\mathrm{Setup}(1^n)\rightarrow(pp,\mathrm{MPK},\mathrm{MSK})$：运行初始化算法$\mathrm{Setup}(1^n)$，记属性全集为$S$，获得公共参数$pp:\{N=pqr,G,G_T,e(\cdot),g,G_1\}$。

$G=G_P\times G_Q\times G_R$，$g_pg_qg_r$分别对应3个子群生成元，加法循环群$G_1$生成元为$g$。随机选择$r_{1,i},r_{2,i}\in G_R$，$p_{1,i},p_{2,i},t\in G_P$，$r_0\in G_R$，$\theta\in Z_N$，其中$i\in[1,n]$。生成系统公钥：$\mathrm{MPK}=\{g_p,g_r,g,T=e(g_p,t)^{\theta},Q=g_qr_0,\{P_{1,i}=p_{1,i}\cdot r_{1,i},P_{2,i}=p_{2,i}\cdot r_{2,i}\}_{i=1}^n\}$。

系统主密钥$\mathrm{MSK}=(p,q,r,g_q,t^{-\theta},\{p_{1,i},p_{2,i}\}_{i=1}^n)$。

(2)$\mathrm{Encrypt}(\mathrm{MPK},\mathrm{MSK},M,(A,\rho),\boldsymbol{x})\rightarrow(C)$：定义访问策略属性向量$\boldsymbol{x}=(x_1,x_2,\cdots,x_n)\in S$，随机选择$z\in Z_N$，计算$h_i=z\cdot x_i\cdot g$，$x_i\in Z_N$，$i\in[1,n]$。

定义LSSS访问策略$(\boldsymbol{A},\rho)$，其中$\boldsymbol{A}=(\boldsymbol{A}_{n,m})\subset\boldsymbol{Z}_N^{l\times|S|}$为$n\times m$矩阵，线性映射函数$\rho$将$\boldsymbol{A}$的每一行$\boldsymbol{A}_i$映射到一个盲化后属性$\rho(h_i)$，记为$\rho(i)$。随机选择$s,\alpha,\beta\in Z_N,r_{3,i},r_{4,i}\in G_R$，对明文消息$M$进行加密，输出密文为：$C=C'=M\cdot T^s$，$C_0=g_p^s$，$\{C_{1,i}=P_{1,i}^s\cdot Q^{\alpha\cdot\rho(i)}\cdot r_{3,i}\}_{i=1}^n$，$\{C_{2,i}=P_{2,i}^s\cdot Q^{\beta\cdot\rho(i)}\cdot r_{4,i}\}_{i=1}^n$。

(3)$\mathrm{User\text{-}Blind}(\boldsymbol{v})\rightarrow(\boldsymbol{u})$：用户定义属性向量$\boldsymbol{v}=(v_1,v_2,\cdots,v_n)\in S$，随机选择$y\in Z_N$，计算$u_i=y\cdot v_i\cdot g$，将盲化后的属性$\boldsymbol{u}=(u_1,u_2,\cdots,u_n)$发送给授权机构获取私钥。

(4)$\mathrm{KeyGen}(\mathrm{MPK},\mathrm{MSK},\boldsymbol{u})\rightarrow(\mathrm{SK})$：随机选择$\gamma_{1,i},\gamma_{2,i}\in Z_p$，$f_1,f_2\in Z_q$，$r_5\in G_R$，$\vartheta\in G_Q$，计算用户私钥：$\mathrm{SK}=\{K=r_5\cdot\vartheta\cdot t^{-\theta}\cdot\prod_{i=1}^n p_{1,i}^{-\gamma_{1,i}}\cdot p_{2,i}^{-\gamma_{2,i}},\{K_{1,i}=g_p^{\gamma_{1,i}}\cdot g_q^{f_1\cdot u_i}\}_{i=1}^n,\{K_{2,i}=g_p^{\gamma_{2,i}}\cdot g_q^{f_2\cdot u_i}\}_{i=1}^n\}$。

(5)$\mathrm{Decrypt}(\mathrm{SK},C)\rightarrow(M)$：记密文为：$C=(C',C_0,\{C_{1,i},C_{2,i}\}_{i=1}^n)$，密钥为$\mathrm{SK}=(K,\{K_{1,i},K_{2,i}\}_{i=1}^n)$，若解密属性满足访问结构，则通过线性计算后的属性向量之间仍满足正交关系，即存在$<\boldsymbol{x},\boldsymbol{v}>=0$，那么解密计算后可获得明文$M$，即

$$C'\cdot e(C_0,K)\cdot\prod_{i=1}^n e(C_{1,i},K_{1,i})\cdot e(C_{2,i},K_{2,i})=M \tag{9}$$

(6)$\mathrm{Verify}(\mathrm{Com},s_i,\mathrm{Aux})\rightarrow(\mathrm{Result})$：首先声明属性全集$S=\{s_1,s_2,\cdots,s_q\}$及承诺向量$\{\boldsymbol{u},\boldsymbol{h}\}$。AA发布承诺凭证

$$\mathrm{Cre}=\left\{\mathrm{EnCre}=\prod_{i=1}^{q}h_i,\mathrm{DeCre}=\prod_{i=1}^{q}u_i\right\} \tag{10}$$

并将Cre作为公开信息。作为证明者的O-Prover与U-Prover提交属性承诺

$$\mathrm{Com}=\left\{\mathrm{EnCom}=\prod_{i=1}^{q}h_i,\ \mathrm{DeCom}=\prod_{i=1}^{q}u_i\right\} \tag{11}$$

验证者将其与承诺凭证比对后输出承诺有效性声明。而后验证者任选属性$\boldsymbol{s}_i$将其发送给证明者，证明者计算辅助信息$\mathrm{Aux}=\{\mathrm{EnAux}_j=\prod_{j=1,j\neq i}^{q}h_j,\ \mathrm{DeAux}_j=\prod_{j=1,j\neq i}^{q}u_j\}$并返回给验证者，验证者进行计算验证$e(\mathrm{Com}/h_i,g)=e(\mathrm{Aux},g),e(\mathrm{Com}/u_i,g)=e(\mathrm{Aux},g)$判断结果是否正确，否则承诺无效。

5 方案分析

本节对论文方案做综合分析，包括正确性证明、安全性证明及实验评估。

5.1 正确性证明

给定密文C与用户私钥SK，由合数阶各子群正交性质，解密等式推导为

$$\begin{aligned}
&C'\cdot e(C_0,K)\cdot\prod_{i=1}^{n}e(C_{1,i},K_{1,i})\cdot e(C_{2,i},K_{2,i})\\
&=\left(\begin{array}{l}M\cdot T^s\cdot e(g_p^s,r_5\vartheta t^{-\theta}\prod_{i=1}^{n}p_{1,i}^{-\gamma_{1,i}}p_{2,i}^{-\gamma_{2,i}})\\ \cdot\prod_{i=1}^{n}e(P_{1,i}^sQ^{\alpha\cdot\rho(i)}r_{3,i},g_p^{\gamma_{1,i}}g_q^{f_1\cdot u_i})\\ \cdot e(P_{2,i}^sQ^{\beta\cdot\rho(i)}r_{4,i},g_p^{\gamma_{2,i}}g_q^{f_2\cdot u_i})\end{array}\right)\\
&=\left(\begin{array}{l}M\cdot T^s\cdot e(g_p^s,t^{-\theta}\prod_{i=1}^{n}p_{1,i}^{-\gamma_{1,i}}p_{2,i}^{-\gamma_{2,i}})\\ \cdot\prod_{i=1}^{n}e(p_{1,i}^sg_q^{\alpha\cdot\rho(i)},g_p^{\gamma_{1,i}}g_q^{f_1\cdot u_i})\\ \cdot e(p_{2,i}^sg_q^{\beta\cdot\rho(i)},g_p^{\gamma_{2,i}}g_q^{f_2\cdot u_i})\end{array}\right)\\
&=M\cdot T^s\cdot e(g_p,t)^{-\theta s}\cdot\prod_{i=1}^{n}e(g_q,g_q)^{(\alpha f_1+\beta f_2)\rho(i)u_i}\\
&=M\cdot e(g_q,g_q)^{(\alpha f_1+\beta f_2)<\boldsymbol{\rho},\boldsymbol{u}>}\\
&=M\cdot e(g_q,g_q)^{\mathrm{cons}<\boldsymbol{x},\boldsymbol{v}>}=M
\end{aligned}\tag{12}$$

若满足解密条件，则$(\alpha f_1+\beta f_2)<\boldsymbol{\rho},\boldsymbol{u}>$可看作线性变换后$<\boldsymbol{x},\boldsymbol{v}>$与常数系数cons的乘积，即$\mathrm{cons}<\boldsymbol{x},\boldsymbol{v}>$，由$<\boldsymbol{x},\boldsymbol{v}>=0$可得解密结果$M$。

在承诺验证阶段，已知承诺Com与辅助信息Aux, U-Prover承诺验证推导为

$$e(\mathrm{Com}/u_i,g)=e\left(\prod_{j=1,j\neq i}^{q}u_j,g\right)=e(\mathrm{Aux},g) \tag{13}$$

O-Prover承诺验证推导为

$$e(\mathrm{Com}/h_i,g)=e\left(\prod_{j=1,j\neq i}^{q}h_j,g\right)=e(\mathrm{Aux},g) \tag{14}$$

5.2 安全性证明

本节通过定理1与定理2证明了PPES方案的不可区分性及承诺不可伪造性，进而满足数据内容隐私、策略隐私及属性隐私。

5.2.1 不可区分性证明

本节通过构造7个游戏，证明密文的不可区分性，即所提PPES方案满足标准模型下的适应性选择明文安全。

定理1 如果PPES方案满足定义3与定义4，那么称该谓词加密方案满足数据内容隐私及策略隐私。

游戏定义：

游戏0：随机选择$s,\alpha,\beta\in Z_N$，$r_{3,i},r_{4,i}\in G_R$并且利用向量$\boldsymbol{x}$生成M_0的挑战密文：$C=\{C'=M_0\cdot T^s,C_0=g_p^s\{C_{1,i}=P_{1,i}^s\cdot Q^{\alpha\cdot x_i}\cdot r_{3,i}\}_{i=1}^n\}\ \{C_{2,i}=P_{2,i}^s\cdot Q^{\beta\cdot x_i}\cdot r_{4,i}\}_{i=1}^n\}$。

游戏1：选择G_T中的随机元素作为密文C'的取值，其余密文元组仍然按照游戏0利用向量$\boldsymbol{x}$生成：$C=\{C'\in G_T,C_0=g_p^s,\{C_{1,i}=P_{1,i}^s\cdot Q^{\alpha\cdot x_i}\cdot r_{3,i}\}_{i=1}^n,\{C_{2,i}=P_{2,i}^s\cdot Q^{\beta\cdot x_i}\cdot r_{4,i}\}_{i=1}^n\}$。

游戏2：当使用$\boldsymbol{0}$进行加密生成密文元组$\{C_{2,i}\}$时，随机选择$s,\alpha\in Z_N$，$r_{3,i},r_{4,i}\in G_R$，$C'\in G_T$计算密文如下：$C=\{C'\in G_T,C_0=g_p^s,\{C_{1,i}=P_{1,i}^s\cdot Q^{\alpha\cdot x_i}\cdot r_{3,i}\}_{i=1}^n\{C_{2,i}=P_{2,i}^s\cdot r_{4,i}\}_{i=1}^n\}$。

游戏3：当使用$\boldsymbol{y}$进行加密生成密文元组$\{C_{2,i}\}$时，随机选择$s,\alpha,\beta\in Z_N$，$r_{3,i},r_{4,i}\in G_R$，$C'\in G_T$计算密文如下：$C=\{C'\in G_T,C_0=g_p^s,\{C_{1,i}=P_{1,i}^sQ^{\alpha\cdot x_i}r_{3,i}\}_{i=1}^n\{C_{2,i}=P_{2,i}^sQ^{\beta\cdot y_i}r_{4,i}\}_{i=1}^n\}$。

游戏4、游戏5：与游戏2、游戏3对称，继续选择G_T中的随机元素作为密文C'的取值，但游戏5将使用$\boldsymbol{y}$对G_T中的随机元素做正确加密。

游戏6：使用$\boldsymbol{y}$生成M_1的正确挑战密文。

证明 借鉴Katz等人[7]中证明思路，若游戏0与游戏1在定义3下是不可区分的，那么游戏1与游戏5也满足不可区分性，而游戏5与游戏6的不可区分性证明与游戏0和游戏1对称。因此，以游戏0与游戏1为例展开不可区分性证明。

根据定义4，挑战者C将$\{N=pqr,G,G_T,e(\cdot),g_p,g_q,g_r,t,g_p^s,t^sQ_1,g_p^\theta Q_2,e(g_p,t)^\theta$以及与$e(g_p,t)^{\theta s}$等长的元素$L$公开给敌手，其中$L$满足$G_T$中均匀分布。

初始化 敌手A输出$\boldsymbol{x},\boldsymbol{y}\in Z_N^n$，将其发送给挑战者C。

挑战者随机选择$\omega_{1,i},\omega_{2,i}\in Z_N$，$r_{1,i},r_{2,i},r_0\in G_R$，设置公钥：$\mathrm{PK}=\{g_p,g_r,g,T=e(g_p,t)^\theta Q=g_qr_0,$

$\{P_{1,i}=t^{x_i}g_p^{\omega_{1,i}}r_{1,i}\}_{i=1}^n\{P_{2,i}=t^{x_i}g_p^{\omega_{2,i}}r_{2,i}\}_{i=1}^n\}$。与原方案公钥参数相对比，在$\{P_{1,i},P_{2,i}\}$的构造中，由$t^{x_i}g_p^{\omega_{1,i}}$，$t^{x_i}g_p^{\omega_{2,i}}$代替了$t_{1,i}t_{2,i}$，即$t_{1,i}=t^{x_i}g_p^{\omega_{1,i}}$，$t_{2,i}=t^{x_i}g_p^{\omega_{2,i}}$。

密钥生成　敌手A使用不同向量$\boldsymbol{v}$做私钥请求，其中$<\boldsymbol{v},\boldsymbol{x}>\neq 0$，挑战者C按照如下形式做构造密钥，对私钥请求做出回应：

令$k=1/2<\boldsymbol{x},\boldsymbol{v}>\bmod N$，在此条件下，如果$\gcd(<\boldsymbol{x},\boldsymbol{v}>,N)\neq 1$，敌手可对$N$做因子分解，但该情况发生概率可忽略不计。挑战者C随机选择$f_1',f_2',\{\gamma_{1,i}',\gamma_{2,i}'\}\in Z_N, qr\in G_{QR}$，计算

$$K=\begin{pmatrix} qr\cdot\prod_{i=1}^{n}((g_p^{\omega_{1,i}}t^{x_i})^{-\gamma_{1,i}'}\cdot(g_p^{\theta}Q_2)^{kv_i\omega_{1,i}}) \\ \cdot((g_p^{\omega_{2,i}}t^{x_i})^{-\gamma_{2,i}'}\cdot(g_p^{\theta}Q_2)^{kv_i\omega_{2,i}}) \end{pmatrix} \tag{15}$$

$$\begin{aligned} K_{1,i}=&(g_p^{\theta}Q_2)^{-kv_i}\cdot g_q^{f_1'v_i}g_p^{\gamma_{1,i}'} \\ =&g_p^{-kv_i\theta+\gamma_{1,i}'}g_q^{(f_1'-kc)\cdot v_i} \end{aligned} \tag{16}$$

$$\begin{aligned} K_{2,i}=&(g_p^{\theta}Q_2)^{-kv_i}g_q^{f_2'v_i}g_p^{\gamma_{2,i}'} \\ =&g_p^{-kv_i\theta+\gamma_{2,i}'}g_q^{(f_2'-kc)\cdot v_i} \end{aligned} \tag{17}$$

在化简中，将Q_2表示为c，其中$c=\log_{g_q}Q_2$。最终挑战者用$\mathrm{SK}=(K,\{K_{1,i},K_{2,i}\}_{i=1}^n)$回复敌手的密钥请求。

在上述模拟过程中与真实方案相比

$$f_1=f_1'-kc,\ \gamma_{1,i}=-kv_i\theta+\gamma_{1,i}' \tag{18}$$

$$f_2=f_2'-kc,\ \gamma_{2,i}=-kv_i\theta+\gamma_{2,i}' \tag{19}$$

因此密钥组件$\{K_{1,i},K_{2,i}\}$的构造满足Z_N中均匀独立分布。在对密钥组件K的构造中，由于

$$\begin{aligned} &\prod_{i=1}^{n}(g_p^{\omega_{1,i}}t^{x_i})^{-\gamma_{1,i}'}(g_p^{\theta})^{kv_i\omega_{1,i}} \\ &=\prod_{i=1}^{n}g_p^{-\omega_{1,i}\gamma_{1,i}'+k\theta v_i\omega_{1,i}}t^{-x_i\gamma_{1,i}'} \\ &=\prod_{i=1}^{n}g_p^{-\omega_{1,i}(\gamma_{1,i}+k\theta v_i)+k\theta v_i\omega_{1,i}}t^{-x_i(\gamma_{1,i}+k\theta v_i)} \\ &=\prod_{i=1}^{n}(t^{x_i}g_p^{\omega_{1,i}})^{-\gamma_{1,i}}t^{-\theta kv_ix_i}=t^{-\theta/2}\prod_{i=1}^{n}t_{1,i}^{-\gamma_{1,i}} \end{aligned} \tag{20}$$

将K_p看作K在G_T群中的投影，那么同理可得

$$\begin{aligned} K_p=&\begin{pmatrix} \prod_{i=1}^{n}((g_p^{\omega_{1,i}}t^{x_i})^{-\gamma_{1,i}'}\cdot(g_p^{\theta})^{kv_i\omega_{1,i}}) \\ \cdot((g_p^{\omega_{2,i}}t^{x_i})^{-\gamma_{2,i}'}\cdot(g_p^{\theta})^{kv_i\omega_{2,i}}) \end{pmatrix} \\ =&t^{-\theta}\prod_{i=1}^{n}t_{1,i}^{-\gamma_{1,i}}t_{2,i}^{-\gamma_{2,i}} \end{aligned} \tag{21}$$

在上述化简中，用到了前面步骤中的隐含条件，即$t_{1,i}=t^{x_i}g_p^{\omega_{1,i}}$，$t_{2,i}=t^{x_i}g_p^{\omega_{2,i}}$，$<\boldsymbol{x},\boldsymbol{v}>=1/2k\bmod N$，进而得出最后化简结果，并可从等式中看出$K_p$和$K$满足均匀分布。

挑战密文生成　挑战者C随机选择$r_{7,i},r_{8,i}\in G_R$, $Q_1'\in G_Q$，令$C'=M_0\cdot L$, $C_0=g_p^s$，然后计算挑战密文如下：$C_{1,i}=(g_p^s)^{\omega_{1,i}}\cdot(t^sQ_1)^{x_i}\cdot r_{7,i}=(t^{x_i}g_p^{\omega_{1,i}})^s\cdot Q_1^{x_i}\cdot r_{7,i}=t_{1,i}^s\cdot Q_1^{x_i}\cdot r_{7,i}$；$C_{2,i}=(g_p^s)^{\omega_{2,i}}\cdot(t^sQ_1)^{x_i}\cdot(Q_1')^{x_i}\cdot r_{8,i}=(t^{x_i}g_p^{\omega_{2,i}})^s\cdot(Q_1Q_1')^{x_i}\cdot r_{8,i}=t_{2,i}^s\cdot(Q_1Q_1')^{x_i}\cdot r_{8,i}$。

通过观察挑战密文元组在群G_P,G_T,G_R中的投影，可以验证当$T=e(g_p,t)^{\theta s}$时，挑战密文的分布与游戏0相同。当T是从G_T群中随机选择的元素时，挑战密文的分布与游戏1相同。因此，在定义2下，游戏0与游戏1是不可区分的，即PPES方案满足不可区分性。　　证毕

5.2.2 承诺不可伪造性

定理2　如果PPES方案满足定义5，那么称该谓词加密方案满足属性隐私。

证明　已知$(P,aP,bP)\in G_1$，其中$a,b\in Z_q^*$为随机选取，则求解abP即为G_1群中的计算性迪菲-赫尔曼(Computational Diffie-Hellman, CDH)困难问题。方案承诺构造形式为：$\{\mathrm{EnCom}=\prod_{i=1}^{q}h_i,\ \mathrm{DeCom}=\prod_{i=1}^{q}u_i\}$。

其中$h_i=z_ix_ig$, $u_i=y_iv_ig$, g为群G_1生成元。当敌手试图伪造Com来通过验证时，需确保$e(\mathrm{Com}/h_i,g)=e(\mathrm{Aux},g)$或$e(\mathrm{Com}/u_i,g)=e(\mathrm{Aux},g)$成立。而辅助信息Aux由证明者计算生成，若使得验证等式成立，敌手需伪造与证明者相同的真实承诺值，其中$x_i,z_i,y_i,v_i\in Z_N$随机选取，即通过计算获取y_iv_ig与z_ix_ig是困难的。　　证毕

5.3 实验评估

本节对PPES方案进行效率分析，基于TypeA1型合数阶椭圆曲线，在i5-11300H处理器通过IntelliJ IDEA平台对方案进行实验对比。PPES基于合数阶群构造，因此只针对同类型方案进行分析。

表1给出了数值分析中所用到的符号描述，其中E表示指数运算，P表示双线性对运算，n表示方

表 1　符号描述

符号	含义
E	指数运算
P	双线性对运算
n	属性个数
$\lvert G\rvert$	群元素大小

案中涉及的属性个数，$|G|$表示子群元素大小。因为点乘运算耗时较小，相比于对运算与指数运算对方案总体效率影响不大，因此在表格中未作统计。

如表2密文及密钥长度对比所示，PPES方案用户私钥长度短于王悦等人方案[10]，相比于Zhang等人方案[11]、Lai方案[12]稍长，这是因为PPES方案中考虑到安全性，构造了两个属性相关的密钥组件；但在密文长度上，PPES方案均比对比方案更短，具备更好的存储性能，且兼顾策略隐私及属性隐私。

如表3方案计算开销对比所示，PPES方案构造了两个属性相关的密钥组件，在密钥生成阶段比Zhang等人方案[11]、Lai等人方案[12]开销略高，低于王悦等人方案[10]；但在加密阶段与解密阶段，PPES方案均优于对比方案，用到了更少的对运算及指数运算，在效率方面有显著优势。

对各方案主要阶段耗时进行数值对比，结果如图2、图3、图4所示，其中横轴代表属性个数，单位为个；纵轴代表耗时，单位为ms。

如图2密钥生成阶段，PPES方案低于王悦等人方案[10]，但略高于Zhang等人方案[11]、Lai等人方案[12]，这与表2及表3分析结果相吻合。如图3，在加密阶段，PPES方案耗时均低于对比方案。主要原因是PPES相比于王悦等人方案[10]减少了$8n$+1

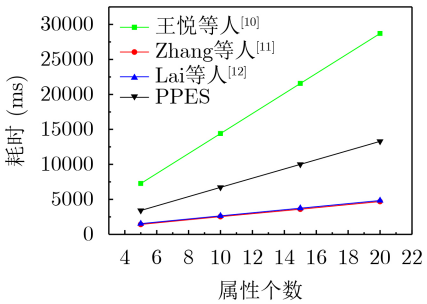

图 2 密钥生成阶段

表 2 密文及密钥长度对比

方案	用户私钥	密文长度
王悦等人[10]	$(4n+2)\|G\|$	$(4n+3)\|G\|$
Zhang[11]	$(n+2)\|G\|$	$(3n+4)\|G\|$
Lai[12]	$(n+2)\|G\|$	$(4n+4)\|G\|$
PPES	$(2n+1)\|G\|$	$(2n+2)\|G\|$

表 3 方案计算开销对比

方案	密钥生成	加密阶段	解密阶段
王悦等人[10]	$(13n+1)$E	$(12n+3)$E	$(4n+2)$P
Zhang[11]	$(2n+3)$E	$(7n+4)$E	$(3n+1)$E+$(4n+1)$P
Lai[12]	$(2n+4)$E	$(10n+2)$E+2P	$(2n)$E+$(4n+2)$P
PPES	$(6n+1)$E	$(4n+2)$E	$(2n+1)$P

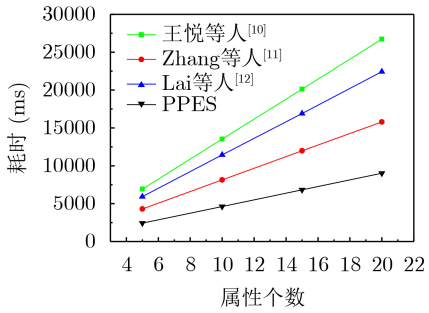

图 3 加密阶段

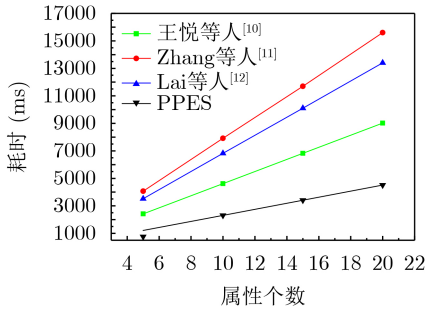

图 4 解密阶段

个指数运算，相比于Zhang等人方案[11]减少了$3n$+2个指数运算，相比于Lai等人方案[12]减少了$8n$个指数运算及2个双线性对运算。

同样，如图4解密阶段数值效率对比，PPES方案在解密运算中耗时均低于对比方案。PPES相比于王悦等人方案[10]减少了$2n$+1个双线性对运算，相比于Zhang等人方案[11]减少了$3n$+1个指数运算及$2n$个双线性对运算，相比于Lai等人方案[12]减少了$2n$个指数运算及$2n$+1个双线性对运算。

6 结束语

本文基于内积谓词与向量承诺协议构造了兼顾3方面隐私保护需求的属性基加密方案，并做了标准模型下的安全性证明及性能分析。一方面，向量承诺协议确保策略属性与用户属性盲化操作的可靠性；另一方面，借助内积操作的线性运算特性，为解决多方随机数消去的等式构造提供了新思路，达到支撑数据内容隐私、策略隐私以及属性隐私3方面隐私需求的目的。为进一步提高效率，未来将考虑标准模型下的素数阶方案构造。

参 考 文 献

[1] SAHAI A and WATERS B. Fuzzy identity-based encryption[C]. Proceedings of the 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, Aarhus, Denmark, 2005: 457–473. doi: 10.1007/11426639_27.

[2] ZHANG Yinghui, DENG R H, XU Shenmin, *et al.*

Attribute-based encryption for cloud computing access control: A survey[J]. *ACM Computing Surveys*, 2021, 53(4): 83. doi: 10.1145/3398036.

[3] LI Hang, YU Keping, LIU Bing, *et al*. An efficient ciphertext-policy weighted attribute-based encryption for the internet of health things[J]. *IEEE Journal of Biomedical and Health Informatics*, 2022, 26(5): 1949–1960. doi: 10.1109/JBHI.2021.3075995.

[4] XU Runhua, JOSHI J, and KRISHNAMURTHY P. An integrated privacy preserving attribute-based access control framework supporting secure deduplication[J]. *IEEE Transactions on Dependable and Secure Computing*, 2021, 18(2): 706–721. doi: 10.1109/TDSC.2019.2946073.

[5] WANG Jin, CHEN Jiahao, XIONG N, *et al*. S-BDS: An effective blockchain-based data storage scheme in zero-trust IoT[J]. *ACM Transactions on Internet Technology*, To be published. doi: 10.1145/3511902..

[6] ZHANG Yinghui, CHEN Xiaofeng, LI Jin, *et al*. Ensuring attribute privacy protection and fast decryption for outsourced data security in mobile cloud computing[J]. *Information Sciences*, 2017, 379: 42–61. doi: 10.1016/j.ins.2016.04.015.

[7] KATZ J, SAHAI A, and WATERS B. Predicate encryption supporting disjunctions, polynomial equations, and inner products[C]. The 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques on Advances in Cryptology, Istanbul, Turkey, 2008: 146–162. doi: 10.1007/978-3-540-78967-3_9.

[8] 赵志远, 王建华, 朱智强, 等. 面向物联网数据安全共享的属性基加密方案[J]. 计算机研究与发展, 2019, 56(6): 1290–1301. doi: 10.7544/issn1000-1239.2019.20180288.
ZHAO Zhiyuan, WANG Jianhua, ZHU Zhiqiang, *et al*. Attribute-based encryption for data security sharing of internet of things[J]. *Journal of Computer Research and Development*, 2019, 56(6): 1290–1301. doi: 10.7544/issn1000-1239.2019.20180288.

[9] 张嘉伟, 马建峰, 马卓, 等. 云计算中基于时间和隐私保护的可撤销可追踪的数据共享方案[J]. 通信学报, 2021, 42(10): 81–94. doi: 10.11959/j.issn.1000-436x.2021206.
ZHANG Jiawei, MA Jianfeng, MA Zhuo, *et al*. Time-based and privacy protection revocable and traceable data sharing scheme in cloud computing[J]. *Journal on Communications*, 2021, 42(10): 81–94. doi: 10.11959/j.issn.1000-436x.2021206.

[10] 王悦, 樊凯. 隐藏访问策略的高效CP-ABE方案[J]. 计算机研究与发展, 2019, 56(10): 2151–2159. doi: 10.7544/issn1000-1239.2019.20190343.
WANG Yue and FAN Kai. Effective CP-ABE with hidden access policy[J]. *Journal of Computer Research and Development*, 2019, 56(10): 2151–2159. doi: 10.7544/issn1000-1239.2019.20190343.

[11] ZHANG Yinghui, ZHENG Dong, and DENG R H. Security and privacy in smart health: Efficient policy-hiding attribute-based access control[J]. *IEEE Internet of Things Journal*, 2018, 5(3): 2130–2145. doi: 10.1109/JIOT.2018.2825289.

[12] LAI Junzuo, DENG R H, and LI Yingjiu. Expressive CP-ABE with partially hidden access structures[C]. Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, Seoul, Korea, 2012: 18–19. doi: 10.1145/2414456.2414465.

[13] HUR J. Attribute-based secure data sharing with hidden policies in smart grid[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2013, 24(11): 2171–2180. doi: 10.1109/TPDS.2012.61.

[14] MICHALEVSKY Y and JOYE M. Decentralized policy-hiding ABE with receiver privacy[C]. The 23rd European Symposium on Research in Computer Security, Barcelona, Spain, 2018: 548–567. doi: 10.1007/978-3-319-98989-1_27.

[15] QIAN Huiling, LI Jiguo, and ZHANG Yichen. Privacy-preserving decentralized ciphertext-policy attribute-based encryption with fully hidden access structure[C]. The 15th International Conference on Information and Communications Security, Beijing, China, 2013: 363–372. doi: 10.1007/978-3-319-02726-5_26.

[16] HAN Jinguang, SUSILO W, MU Yi, *et al*. Privacy-preserving decentralized key-policy attribute-based encryption[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2012, 23(11): 2150–2162. doi: 10.1109/TPDS.2012.50.

[17] GE Aijun, ZHANG Jiang, ZHANG Rui, *et al*. Security analysis of a privacy-preserving decentralized key-policy attribute-based encryption scheme[J]. *IEEE Transactions on Parallel and Distributed Systems*, 2013, 24(11): 2319–2321. doi: 10.1109/TPDS.2012.328.

[18] HAN Jinguang, SUSILO W, MU Yi, *et al*. Improving privacy and security in decentralized ciphertext-policy attribute-based encryption[J]. *IEEE Transactions on Information Forensics and Security*, 2015, 10(3): 665–678. doi: 10.1109/TIFS.2014.2382297.

[19] WANG Minqian, ZHANG Zhenfeng, and CHEN Cheng. Security analysis of a privacy-preserving decentralized ciphertext-policy attribute-based encryption scheme[J]. *Concurrency and Computation:Practice and Experience*, 2016, 28(4): 1237–1245. doi: 10.1002/cpe.3623.

[20] CATALANO D and FIORE D. Vector commitments and their applications[C]. The 16th International Conference on Practice and Theory in Public-Key Cryptography, Nara, Japan, 2013: 55–72. doi: 10.1007/978-3-642-36362-7_5.

张志强：男，博士生，研究方向为应用密码学、隐私保护.
朱友文：男，教授，研究方向为应用密码学、人工智能安全、隐私保护.
王　箭：男，教授，研究方向为应用密码学、系统安全、隐私保护.
张玉书：男，教授，研究方向为多媒体安全与人工智能、区块链与物联网安全、云计算与大数据安全等.

责任编辑：余　蓉