面向云存储的属性基双边访问控制方案

李琦[1,2,3]，樊昊源[1]，陈伟[1]，熊金波[4]，韩立东[2]，李瑞[5]

（1.南京邮电大学计算机学院，江苏 南京 210023；2.杭州师范大学浙江省密码技术重点实验室，浙江 杭州 311121；
3.南京邮电大学通达学院，江苏 扬州 225127；4.福建师范大学计算机与网络空间安全学院，福建 福州 350117；
5.西安电子科技大学计算机科学与技术学院，陕西 西安 710071）

摘　要：针对目前云存储中细粒度双边访问控制机制安全模型较弱且外包解密结果缺乏验证的问题，提出了一种面向云存储数据的属性基双边访问控制方案。首先，提出了自适应安全可验证外包双边CP-ABE的形式化定义和安全模型；其次，以此为基础并结合批量可验证技术在合数阶群上设计了双边访问控制方案，支持数据拥有者与数据使用者同时为对方定义访问策略；最后，安全性分析表明，所提方案在自适应安全模型下针对选择明文攻击与选择消息攻击是不可区分的和存在性不可伪造的。实验结果显示，所提方案减轻了用户端的匹配、解密以及验证阶段的计算开销。

关键词：云存储；双边访问控制；自适应安全；批量可验证；外包解密

中图分类号：TN92

文献标志码：A

DOI：10.11959/j.issn.1000−436x.2024062

Attribute-based bilateral access control scheme for cloud storage

LI Qi[1,2,3], FAN Haoyuan[1], CHEN Wei[1], XIONG Jinbo[4], HAN Lidong[2], LI Rui[5]

1. School of Computer Science, Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2. Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China
3. Tongda College of Nanjing University of Posts and Telecommunications, Yangzhou 225127, China
4. College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350117, China
5. The School of Computer Science and Technology, Xidian University, Xi'an 710071, China

Abstract: In the existing cloud storage systems, the fine grained and bilateral access control schemes suffer from weak security model and unverifiable outsourced decryption result. To address this problem, an attribute-based bilateral access control scheme for cloud storage was proposed. Firstly, the formal definition and secure model of adaptively secure and verifiable outsourced bilateral CP-ABE was given. Secondly, combining with the batch verification technology, the attribute based bilateral access control scheme was constructed on the composite order groups, which enabled both the data owner and data user to simultaneously define the access policies for each other. Finally, the security analysis showed that the proposed scheme was indistinguishable and existential unforgeable under adaptive security models against chosen plaintext attacks and chosen message attacks, respectively. The experimental results show that the proposed scheme achieves high performance on the user side, where the computational overhead of matching, decryption, and verification is reduced.

Keywords: cloud storage, bilateral access control, adaptively secure, batch verification, outsourced decryption

收稿日期：2023−10−25；**修回日期**：2024−02−20

通信作者：熊金波，jinbo810@163.com

基金项目：国家自然科学基金资助项目（No.62272102, No.62172320, No.U21A20466）；江苏省高等学校基础科学（自然科学）研究基金资助项目（No.22KJB520029）；浙江省密码技术重点实验室基金资助项目（No.ZCL21015）；南京邮电大学校级自然科学基金资助项目（No.NY222141）

Foundation Items: The National Natural Science Foundation of China (No.62272102, No.62172320, No.U21A20466), The Natural Science Foundation of Jiangsu Higher Education Institutions of China (No.22KJB520029), The Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province (No.ZCL21015), The Natural Science Foundation of Nanjing University of Posts and Telecommunications (No.NY222141)

0　引言

云计算技术的快速发展为数据存储及共享提供了极大的便利。越来越多的公司和个人将数据上传到云服务器进行存储，通过网络随时随地访问自己的数据，同时，数据拥有者（DO, data owner）也可以在云服务提供商（CSP, cloud service provider）的帮助下，指定访问策略来授权其他用户共享数据[1]。随着数据的广泛共享，数据所有权和管理权分离导致的数据安全和隐私泄露问题也得到了学术界和工业界的广泛关注。特别是医疗/个人健康数据，其包含了用户的疾病及诊断信息，一旦泄露将引发巨大的社会风险。

属性基加密（ABE, attribute-based encryption）[2]通过属性来描述用户，为存储在云端的数据提供了安全、灵活、细粒度的一对多共享模式。随后出现的密文策略ABE（CP-ABE, ciphertext-policy ABE）[3]更是为数据拥有者制定访问策略、授权用户访问权限提供了密码学原语。研究人员基于CP-ABE提出了各式各样的访问控制方案[4-11]。

在实际场景下，为帮助数据使用者（DU, data user）筛选目标密文，提升访问控制的效率，还需要考虑对数据拥有者的访问控制，即数据使用者也可以对数据拥有者设置访问策略，满足该访问策略的数据拥有者生成的密文才能被授权数据使用者访问。针对该问题，Damgård等[12]首先提出了访问控制加密（ACE, access control encryption）的概念，这是一种允许细粒度访问控制的新型加密原语，通过被称作“sanitizer”的可信第三方为不同的参与方定义不同的权限，不仅包括允许使用哪些消息，还包括允许发送哪些消息。Kim等[13]给出了任意策略的ACE形式化模型，可以从数字签名方案、谓词加密方案和支持随机功能（单密钥）函数加密方案的组合构建，并进一步对消息发送者的策略进行扩展。Cui等[14]设计了一种面向云-边缘架构的双边访问控制方案，以边缘服务器为“sanitizer”重加密数据，实现消息收发方双边访问控制。Ateniese等[15]提出了ME（matchmaking encryption）的概念，移除了对“sanitizer”的要求，并设计了一种基于身份的双边访问控制方案。Xu等[16]结合ABE首次给出了一种基于属性的双边访问控制模型并给出了具体方案，其中对数据使用者使用了密钥策略ABE（KP-ABE, key-policy ABE）[17]的访问控制模式，对数据拥有者使用了CP-ABE的访问控制模式。随后，Xu等[18]提出了可外包的双边访问控制方案，将大部分的解密计算外包至第三方云端处理，减轻了数据使用者终端的解密开销。Sun等[19]提出了一种面向云辅助物联网健康管理环境的双边访问控制方案。

文献[16,18-19]很好地解决了细粒度双边访问控制以及数据使用者解密开销较大的问题，但是这些方案都是在选择性安全模型下证明的，即在安全游戏中需要事先声明所要挑战的访问策略或属性集合。此外，对于外包解密结果的正确性并没有提供验证手段。本文基于Lewko等[20]方案设计了一种可验证外包解密的双边CP-ABE算法，并结合批量验证技术，提出了一种面向云存储的双边访问控制方案，实现了对数据拥有者和数据使用者的双边访问控制。该方案支持基于线性秘密共享方案（LSSS, linear secret sharing scheme）的访问策略，实现了对同一时间段外包解密密文的批量验证，并在自适应安全模型下证明了自身的安全性。本文的主要贡献如下。

1) 双边访问控制。实现了数据拥有者和使用者之间的双边访问控制，授权机构可分别为数据拥有者和数据使用者的属性集合分配加密密钥和解密密钥。为了正确解密，不仅数据使用者需要满足数据拥有者制定的访问策略，而且数据拥有者也需要满足数据使用者指定的访问策略。

2) 外包解密与批量验证。数据使用者可以指定访问策略在云服务器的协助下筛选目标密文，之后若数据使用者属性集合满足目标密文中的访问策略，云服务器将返回半解密密文，数据使用者经由一次指数运算即可实现最终解密，并且可以对同一个时间段的外包解密计算结果进行批量验证。

3) 自适应安全与计算效率。在自适应安全模型下证明了所提方案的安全性，包括在选择明文攻击下的语义安全和选择消息攻击下的存在性不可伪造。实验结果也表明了所提方案的有效性和实用性。

1　系统模型与形式化定义

1.1　系统模型

系统模型如图1所示，包括4类实体：可信授权机构（TA, trusted authority）、数据拥有者、数据

使用者、云服务提供商。各实体负责的功能及相互之间的交互如下。

1) TA 负责初始化系统参数，包括设置公钥参数和系统主密钥（见①），根据 DO 的属性集合为其设置加密密钥（见②）。

2) DO 为其数据定义访问策略并结合加密密钥进行加密，最终将密文上传至 CSP（见③）；在一般的密钥封装模型下，可以先选定一个对称加密体制利用对称密钥对源数据进行加密，再将该对称密钥视作属性加密体制中的明文来进行加密处理。

3) DU 注册加入系统（见④），生成其公钥和私有解密密钥，随后 TA 根据其属性集合和公钥返回相关外包解密密钥（见⑤），当其需要访问数据时，可以定义一个对目标数据的访问策略并发起访问请求（见⑥），该请求中也包含了 DU 的外包解密密钥。

4) CSP 负责存储密文数据并响应 DU 的访问请求（见⑦），其响应方式是验证该请求中的访问策略是否能匹配数据密文中的加密属性集合，若不通过，则中止；否则，利用请求中包含的 DU 外包解密密钥对目标密文进行外包解密操作，并返回部分解密密文给 DU（见⑧），最终，DU 可以利用其私有解密密钥对部分解密密文进行解密操作，获取最终的明文数据（见⑨）。

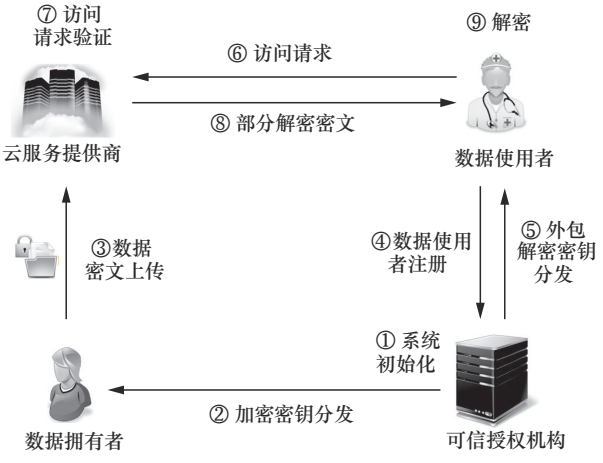


图 1 系统模型

1.2 形式化定义

下面给出可验证外包解密的双边 CP-ABE 的形式化定义。

SETUP $(\lambda,U)\rightarrow(\mathrm{SPK},\mathrm{SMSK})$。该算法输入系统安全参数 λ 和系统属性集合 U，输出系统的公开参数 SPK 和主密钥 SMSK。后续算法默认以 SPK 作为输入。

EKGEN $(\mathrm{SMSK},S_{\mathrm{send}})\rightarrow \mathrm{EK}_{\mathrm{send}}$。该算法输入数据拥有者的属性集合 S_{send} 以及 SMSK，输出 DO 的加密密钥 $\mathrm{EK}_{\mathrm{send}}$。

ENC $(M,\mathrm{EK}_{\mathrm{send}},S'_{\mathrm{send}},\mathbb{A}(\boldsymbol{A},\rho))\rightarrow \mathrm{CT}$。该算法输入消息 M、访问策略 $\mathbb{A}(\boldsymbol{A},\rho)$、DO 的属性子集 $S'_{\mathrm{send}}\subseteq S_{\mathrm{send}}$ 以及 $\mathrm{EK}_{\mathrm{send}}$，输出密文 CT。此外，还将输出 M 的加密密钥 DEK 与外包解密验证组件 V。

DUREG$(u)\rightarrow(\mathrm{PK}_u,\mathrm{SK}_u)$。DU 运行该算法，以其身份 u 作为输入，输出 DU 的公钥 PK_u 以及私有解密密钥 SK_u。PK_u 将会被发送给 TA，而 SK_u 由 DU 自己保管。

DKGEN $(\mathrm{PK}_u,\mathrm{SMSK},S_{\mathrm{rec}})\rightarrow \mathrm{DK}_u$。该算法输入 DU 的属性集合 S_{rec}、PK_u、SMSK，输出 DU 外包解密密钥 DK_u。

VERIFY-EN $(\mathrm{CT},\mathbb{B}(\boldsymbol{B},\pi))\rightarrow\{0,1\}$。该算法输入 DU 制定的访问策略 $\mathbb{B}(\boldsymbol{B},\pi)$ 和 CT，若 CT 中的 S'_{send} 满足 $\mathbb{B}(B,\pi)$，输出 1；否则，输出 0。

SEMI-DEC $(\mathrm{CT},\mathrm{DK}_u)\rightarrow \mathrm{CT}_{\mathrm{semi}}$。该算法输入 CT 和 DK_u，若 S_{rec} 满足 $\mathbb{A}(\boldsymbol{A},\rho)$，则输出部分解密密文 $\mathrm{CT}_{\mathrm{semi}}$，否则，输出 $\perp$。

DUDEC $(\mathrm{CT}_{\mathrm{semi}},\mathrm{SK}_u)\rightarrow M$。该算法输入 $\mathrm{CT}_{\mathrm{semi}}$ 和 SK_u，输出消息 M。

VERIFY$(\{\mathrm{DEK}_k,M_k,\mathrm{CT}_k,V_k\}_{k\in[1,h]})\rightarrow\{0,1\}$。针对密文所处的时间阶段 η，所统计的验证组件 $\{V_k\}_{k\in[1,h]}$ 以及相对应的 $\{\mathrm{DEK}_k,M_k,\mathrm{CT}_k\}_{k\in[1,h]}$，其中 h 表示该时间阶段需要验证的消息总数，进行验证。若所有的 DEK_k 正确，则输出 1；否则，输出 0。

2 威胁模型和安全模型

2.1 威胁模型

TA 为可信实体，诚实地设置公开参数和主密钥，并分别为数据拥有者和数据使用者生成各自需要的密钥；云服务器为恶意的，其试图从各阶段中获取消息的隐私信息，特别地，在外包解密步骤，其试图返回一个错误的外包解密结果来欺骗消息使用者；数据拥有者和数据使用者都是不可信的，数据拥有者试图生成超出其发送权限的密文，而数据使用者试图访问超出其访问权限的密文，他们也可

以通过共谋发起上述的攻击。

2.2　安全模型

本文构造了2个安全模型来针对上述可能的攻击，分别是选择明文攻击下的不可区分性（IND-CPA, indistinguishability under a chosen plaintext attack）安全模型和选择消息攻击下的存在性不可伪造（EU-CMA, existential unforgeability under a chosen message attack）安全模型。

2.2.1　IND-CPA 安全模型

IND-CPA安全模型由下述攻击者$\mathcal{A}$和仿真者$\mathcal{B}$交互游戏来定义。

Setup。$\mathcal{B}$运行SETUP算法生成系统公开参数SPK和主密钥SMSK，然后发送SPK给$\mathcal{A}$。

Phase 1。$\mathcal{B}$回应$\mathcal{A}$发起的以下一系列密钥查询。

1) 针对DU的身份u，$\mathcal{B}$运行DUREG算法生成密钥$(\mathrm{PK}_u,\mathrm{SK}_u)$并将其返回给$\mathcal{A}$，同时，$\mathcal{B}$保存$(\mathrm{PK}_u,\mathrm{SK}_u)$，针对同一个身份$u$，$\mathcal{B}$均基于该密钥对来生成相关参数。

2) 针对DU的身份u以及属性集合S_{rec}，$\mathcal{B}$运行DKGEN算法来生成DK_u，若DU的身份u是新加入系统的，$\mathcal{B}$将先生成密钥对$(\mathrm{PK}_u,\mathrm{SK}_u)$再计算并返回$\mathrm{DK}_u$。

Challenge。$\mathcal{A}$提交2个等长的消息m_0和m_1，以及DO的属性集合S_{send}，$\mathcal{B}$随机选择一个比特$b\in\{0,1\}$以及一个访问策略$\mathbb{A}^*(\boldsymbol{A},\rho)$，并调用EKGEN以及ENC算法来生成关于$m_b$挑战密文CT*，最后$\mathcal{B}$返回CT*给$\mathcal{A}$。值得注意的是，在Phase 1询问过的属性集合$S_{\mathrm{rec}}$不能满足挑战的访问策略$\mathbb{A}^*(\boldsymbol{A},\rho)$。

Phase 2。$\mathcal{B}$如同在Phase 1中回应$\mathcal{A}$的查询，对于查询的S_{rec}的限制同Challenge中的一致。

Guess。$\mathcal{A}$输出其对b的猜测b'，若$b'=b$，则$\mathcal{A}$赢得上述游戏。$\mathcal{A}$赢得上述游戏的优势定义为

$$\mathrm{Adv}_{\mathrm{IND\text{-}CPA}}=\left|\Pr[b'=b]-\frac{1}{2}\right|$$

定义1　若在上述安全游戏中，任意多项式时间攻击者$\mathcal{A}$的优势$\mathrm{Adv}_{\mathrm{IND\text{-}CPA}}$都是可忽略的，则称该方案是安全的。

2.2.2　EU-CMA 安全模型

与上述IND-CPA模型类似，EU-CMA安全模型通过攻击者$\mathcal{A}$和仿真者$\mathcal{B}$交互游戏来定义。

SETUP。$\mathcal{B}$如同在IND-CPA模型中一样来设置参数并发送SPK给$\mathcal{A}$。

Query。$\mathcal{B}$可以回应如同在IND-CPA模型中$\mathcal{A}$进行的查询，此外，$\mathcal{A}$还可以重复发起如下的加密查询：$\mathcal{A}$提交一个DO的属性集合S_{send}，消息m，访问策略$\mathbb{A}(\boldsymbol{A},\rho)$，$\mathcal{B}$调用ENC算法返回密文CT。

Forgery。$\mathcal{A}$输出一个关于S^*_{send}的密文CT*，其中，S^*_{send}满足发送者的访问策略$\mathbb{B}^*(\boldsymbol{B},\pi)$，若其满足以下条件，则$\mathcal{A}$赢得该游戏。

1) 所有在加密密钥查询阶段所查询的S_{send}都不能满足$\mathbb{B}^*(\boldsymbol{B},\pi)$。

2) $\mathcal{A}$所返回的密文CT*不能等同于在加密查询阶段获得密文CT，这里的等同意味着2个密文完全相同或者即使不完全相同，但是在同一个域中（例如，同一个消息通过选择不同的随机数加密成完全不同的密文）。

若任何概率多项式时间攻击者$\mathcal{A}$的优势$\mathrm{Adv}_{\mathrm{EU\text{-}CMA}}=\left|\Pr[\mathcal{A}\,\mathrm{wins}]\right|$都是可忽略的，则称该方案是EU-CMA安全的。

3　具体方案

1) 系统初始化

SETUP。随机选择一个阶为合数N（$N=p_1p_2p_3$）的群$\mathbb{G}$，其中p_1,p_2,p_3为3个不同的素数，令$\mathbb{G}_{p_i}$为$\mathbb{G}$的p_i阶子群。定义双线性对$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$，随机选择指数$\alpha,\beta,a,b\in\mathbb{Z}_N$以及一个元素$g\in\mathbb{G}_{p_1}$，对于系统属性集$U$中的每一个属性$i$，选择一个随机指数$s_i\in\mathbb{Z}_N$并计算$T_i=g^{s_i}$。此外，选择哈希函数$H_1:\{0,1\}\times\mathbb{T}\to\mathbb{G}$，$H_2:\{0,1\}^*\times\mathbb{G}_T\to\mathbb{Z}_N$，$H_3:\{0,1\}^*\to\mathbb{G}$，其中$\mathbb{T}$为时间段集合。设置系统公开参数为$\mathrm{SPK}=(\mathbb{G},\mathbb{G}_T,e,g,N,e(g,g)^{\alpha},e(g,g)^{\beta},g^a,g^b,\{T_i\}_{i\in U},H_1,H_2,H_3)$，系统主密钥MSK为$(\alpha,\beta)$以及$\mathbb{G}_{p_3}$的生成元$X_3$。

2) 加密密钥分发

EKGEN。令DO的属性集合为S_{send}，随机选择$q\in\mathbb{Z}_N$，$Q_0,Q_0'\in\mathbb{G}_{p_3}$，对于$S_{\mathrm{send}}$中的每一个属性$i$，随机选择$Q_i\in\mathbb{G}_{p_3}$。DO计算$\mathrm{ek}_1=g^{\beta}g^{bq}Q_0$，$\mathrm{ek}_2=g^qQ_0'$，$\mathrm{ek}_{3,i}=T_i^qQ_i$。得到加密密钥为$\mathrm{EK}_{\mathrm{send}}=(S_{\mathrm{send}},\mathrm{ek}_1,\mathrm{ek}_2,\{\mathrm{ek}_{3,i}\}_{i\in S_{\mathrm{send}}})$。

3) 数据密文上传

ENC。令DO指定的访问策略为$\mathbb{A}(\boldsymbol{A},\rho)$，$\boldsymbol{A}$为

$\ell \times n$ 矩阵，ρ 将矩阵的每一行 $\boldsymbol{A}_x$ 映射为一个属性 $\rho(x)$，DO 的属性集合为 $S_{\text{send}}' \subseteq S_{\text{send}}$，随机选择向量 $\boldsymbol{y}=(s,y_2,y_3,\cdots,y_n)^{\mathrm{T}} \in \mathbb{Z}_N^{n\times 1}$。对于矩阵的每一行 $\boldsymbol{A}_x$，选择一个随机数 $r_x \in \mathbb{Z}_N$，令 $\text{DEK}=e(g,g)^{\alpha s}$，计算 $C=Me(g,g)^{\alpha s}$，$C'=g^s$，$C_{1,x}=g^{a\boldsymbol{A}_x \boldsymbol{y}}T_{\rho(x)}^{-r_x}$，$D_{1,x}=g^{r_x}$，其中 M 为密钥封装机制中选取的对称密钥，需要用 M 对 DO 的源数据 DATA 进行对称加密得到密文 DATA_M。

DO 随机选择 $q',c \in \mathbb{Z}_N$ 并计算密文组件

$$\begin{aligned} C_2 &= \text{ek}_1 g^{bq'} = g^{\beta} g^{b(q+q')} Q_0 \\ C_3 &= \text{ek}_2 g^{q'} = g^{q+q'} Q_0' \\ C_4 &= g^c \end{aligned} \tag{1}$$

此外，对于当下的时间段 η，计算 $\Gamma=H_1(0\|\eta)$，$Y=H_1(1\|\eta)$，$\tau=H_2(M\|e(g,g)^{\alpha s})$，$V=\Gamma^s Y^{s\tau}$。

令 C_{1-4} 为二进制比特串，即

$$\begin{aligned} C_{1-4} = C \,\|\, C \P\, C_{1,1}\| \cdots \| C_{1,\ell}\| \\ D_{1,1}\| \cdots \| D_{1,\ell}\| C_2\| C_3\| C_4\| V \end{aligned} \tag{2}$$

对于 $S_{\text{send}}' \subseteq S_{\text{send}}$ 中的属性 i'，计算 $C_{4,i'}=\text{ek}_3(T_{i'})^{q'}H_3(C_{1-4})^c$。

最终，DO 将密文 DATA_M、V 以及 CT=$(\mathbb{A}(\boldsymbol{A},\rho),S_{\text{send}}',C,C',\{C_{1,x},D_{1,x}\}_{x\in[\ell]},C_2,C_3,\{C_{4,i'}\}_{i'\in S_{\text{send}}'})$ 上传至云服务器。

4) 使用者注册

DUREG。为一个使用者 u 选择一个随机数 $r \in \mathbb{Z}_N$，并计算 $\text{PK}_u=g^r$，DU 的私有解密密钥为 $\text{SK}_u=r$。

5) 外包解密密钥分发

DKGEN。令 DU 的属性集合为 S_{rec}，TA 随机选择 $t \in \mathbb{Z}_N$，$R_0,R_0' \in \mathbb{G}_{p_3}$，并对于 S_{rec} 中的每一个属性 j，随机选择 $R_j \in \mathbb{G}_{p_3}$。TA 计算 $\text{dk}_1=g^{r\alpha}g^{at}R_0$，$\text{dk}_2=g^tR_0'$，$\text{dk}_{3,i}=T_i{}^tR_i$。

DU 得到其外包解密密钥 DK_u，其中 DK_u=$(S_{\text{rec}},\text{dk}_1,\text{dk}_2,\{\text{dk}_{3,i}\}_{i\in S_{\text{rec}}})$。

6) 访问请求及验证

DU 可以提交外包解密密钥 DK_u 并向云服务器发起访问请求，云服务器接受并执行如下验证操作。

VERIFY-EN。令 DU 指定的访问策略为 $\mathbb{B}(\boldsymbol{B},\pi)$，$\boldsymbol{B}$ 为 $\ell_{\mathbb{B}} \times n_{\mathbb{B}}$ 矩阵，π 将矩阵的每一行 $\boldsymbol{B}_x$ 映射为一个属性 $\pi(x)$，随机选择 $v_2,v_3,\cdots,v_{n_{\mathbb{B}}} \in \mathbb{Z}_N$ 并设置向量 $\boldsymbol{v}=(1,v_2,v_3,\cdots,v_{n_{\mathbb{B}}})^{\mathrm{T}} \in \mathbb{Z}_N^{n_{\mathbb{B}}\times 1}$，计算 $\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\lambda_3,\cdots,\lambda_{n_{\mathbb{B}}})^{\mathrm{T}}=B\boldsymbol{v}$，若 S_{send}' 满足 $\mathbb{B}(\boldsymbol{B},\pi)$ 则令 $I=\{i|i\in[\ell_{\mathbb{B}}],\pi(i)\in S_{\text{send}}'\}$。找到集合 $\{w_i\}_{i\in I}$ 使 $\sum_{i\in I} w_iB_i=(1,0,\cdots,0)$，并验证等式

$$\prod_{i\in I}\left(\frac{e(C_2,g)e(C_{4,i},g)}{e(C_3,g^bT_{\pi(x)})e(C_4,H_3(C_{1-4}))}\right)^{\lambda_i w_i} \overset{?}{=} e(g,g)^{\beta} \tag{3}$$

是否成立，若成立，则输出 1；否则，输出 0。

7) 返回部分解密密文

SEMI-DEC。若 VERIFY-EN 算法输出 1 且 S_{rec} 满足 $\mathbb{A}(\boldsymbol{A},\rho)$，则令 $J=\{j|j\in[\ell],\rho(j)\in S_{\text{rec}}\}$，找到集合 $\{\kappa_j\}_{j\in J}$ 使 $\sum_{j\in J}\kappa_j\boldsymbol{A}_j=(1,0,\cdots,0)$，计算 $\dfrac{e(C',\text{dk}_1)}{\prod_{\rho(j)\in S}\left(e(C_{1,j},\text{dk}_2)e(D_{1,x},\text{dk}_{3,\rho(j)})\right)^{\kappa_j}}=e(g,g)^{\alpha sr}$，并将结果返回给使用者。

8) 使用者解密

DUDEC。DU 用其私有解密密钥 $\text{SK}_u=r$ 计算 $(e(g,g)^{\alpha sr})^{\frac{1}{r}}=e(g,g)^{\alpha s}$ 和 $\dfrac{C}{e(g,g)^{\alpha s}}=M$。最后用 M 对 DATA_M 进行解密得到源数据。

9) 解密结果验证

VERIFY-DEC。针对密文所处的时间阶段 η、所统计的验证组件 $\{V_k\}_{k\in[1,\hbar]}$ 以及相对应的 $\{\text{DEK}_k,M_k,C_k'\}_{k\in[1,\hbar]}$，其中 $\hbar$ 表示该时间阶段所需要验证的消息总数，计算 $\Gamma=H_1(0\|\eta)$，$Y=H_1(1\|\eta)$，$\tau_k=H_2(M_k\|e(g,g)^{\alpha s_k})$，并验证等式 $e\left(\prod_{k=1}^{\hbar}V_k,g\right)\overset{?}{=}e\left(\Gamma,\prod_{k=1}^{\hbar}C_k'\right)e\left(Y,\prod_{k=1}^{\hbar}(C_k')^{\tau_k}\right)$ 是否成立，若成立，则说明这一批次的外包解密结果正确。

4 安全性证明

4.1 IND-CPA 安全性证明

如果存在一个多项式时间攻击者 $\mathcal{A}$ 以不可忽略的优势攻破本文方案，则可以构造一个仿真者 $\mathcal{B}$ 来攻破文献[20]方案。这里将文献[20]方案和本文的可验证外包解密的双边 CP-ABE 方案分别表示为 Σ_{Fully} 和 Σ_{Ours}。

Setup。$\mathcal{B}$ 向 Σ_{Fully} 提交交互请求，Σ_{Fully} 返回公钥 $\text{SPK}_{\text{Fully}}=(\mathbb{G},\mathbb{G}_T,e,g,N,e(g,g)^{\alpha},g^{a},\{T_i\}_{i\in U})$。然后，$\mathcal{B}$ 随机选择指数 $\beta,b \in \mathbb{Z}_N$，并计算 $e(g,g)^{\beta},g^b$。此外，

再如同真实方案中设置3个哈希函数H_1,H_2,H_3。最终，$\mathcal{B}$为攻击者$\mathcal{A}$返回如下的公开参数。

$$\begin{aligned}&\mathrm{SPK}=(\mathbb{G},\mathbb{G}_T,e,g,N,e(g,g)^{\alpha},\\&e(g,g)^{\beta},g^{a},g^{b},\{T_i\}_{i\in U},H_1,H_2,H_3)\end{aligned}\tag{4}$$

Phase 1过程如下。

EKGEN。令DO的属性集合为S_{send}，针对该查询，$\mathcal{B}$将S_{send}发送给Σ_{Fully}，Σ_{Fully}将其视作用户属性集合返回密钥：$K=g^{\alpha}g^{at}R_0$，$L=g^{t}R_0'$，$K_i=T_i^{t}R_i$。$\mathcal{B}$知晓β，b并计算$\mathrm{ek}_1=g^{\beta}L^{b}$，$\mathrm{ek}_2=L$，$\mathrm{ek}_{3,i}=K_i$。$\mathcal{B}$将$\mathrm{EK}_{\mathrm{send}}$返回给$\mathcal{A}$，其中$\mathrm{EK}_{\mathrm{send}}=\left(S_{\mathrm{send}},\mathrm{ek}_1,\mathrm{ek}_2,\{\mathrm{ek}_{3,i}\}_{i\in S_{\mathrm{send}}}\right)$。

DUREG。为一个使用者u选择一个随机数$r\in\mathbb{Z}_N$，并计算$\mathrm{PK}_u=g^{r}$，DU私有解密密钥为r。针对该DU相关密钥的查询，$\mathcal{B}$在表格中查询关于该DU的密钥，若存在，则直接返回已保存的相关密钥，若该使用者u的身份未在表格，则$\mathcal{B}$为他选择一个随机数$r\in\mathbb{Z}_N$，并计算$\mathrm{PK}_u=g^{r}$，并将$\left(\mathrm{PK}_u,\mathrm{SK}_u\right)$存入表格。

DKGEN。令DU的属性集合为S_{rec}，针对该查询，$\mathcal{B}$将S_{rec}发送给Σ_{Fully}，Σ_{Fully}返回密钥：$K=g^{\alpha}g^{at}R_0$，$L=g^{t}R_0'$，$K_i=T_i^{t}R_i$。$\mathcal{B}$根据使用者u的身份，利用r计算$\mathrm{dk}_1=K^{r}$，$\mathrm{dk}_2=L^{r}$，$\mathrm{dk}_{3,i}=(K_i)^{r}$。$\mathcal{B}$返回$\mathrm{DK}_u=(S_{\mathrm{rec}},\mathrm{dk}_1,\mathrm{dk}_2,\{\mathrm{dk}_{3,i}\}_{i\in S_{\mathrm{rec}}})$给$\mathcal{A}$。

Challenge。$\mathcal{A}$提交m_0、m_1、$\mathbb{A}(\boldsymbol{A},\rho)$以及$S_{\mathrm{send}}$给$\mathcal{B}$，$\mathcal{B}$如phase1中产生$\mathrm{EK}_{\mathrm{send}}$，随后$\mathcal{B}$将$m_0$、$m_1$、$\mathbb{A}(\boldsymbol{A},\rho)$发送给$\Sigma_{\mathrm{Fully}}$，$\Sigma_{\mathrm{Fully}}$随机选择$\kappa\in\{0,1\}$并返回密文$C=m_{\kappa}e(g,g)^{\alpha s}$，$C'=g^{s}$，$D_{1,x}=g^{r_x}$，$C_{1,x}=g^{aA_{x,y}}T_{\rho(x)}^{-r_x}$。此外，$\mathcal{B}$随机选择$q',c\in\mathbb{Z}_N$，计算$C_2=\mathrm{ek}_1g^{bq'}$，$C_3=\mathrm{ek}_2g^{q'}$，$C_4=g^{c}$。对于$S_{\mathrm{send}}$中的属性$i'$，计算$C_{4,i'}=\mathrm{ek}_3(T_{i'})^{q'}H_3(C_{1-4})^{c}$，$\mathcal{B}$随机选择$\kappa'\in\{0,1\}$，计算$\tau=H_2\left(m_{\kappa}\|\left(\dfrac{C}{m_{\kappa'}}\right)\right)$，其余$\Gamma$、$Y$、$V$如真实方案类似计算。$\mathcal{B}$返回密文$\mathrm{CT}=(\mathbb{A}(\boldsymbol{A},\rho),S_{\mathrm{send}},C,C',\{C_{1,x},D_{1,x}\}_{x\in[\ell]},C_2,C_3,\{C_{4,i'}\}_{i'\in S_{\mathrm{send}}})$给$\mathcal{A}$。

Phase 2过程和Phase1类似，只是$\mathcal{A}$不能查询满足$\mathbb{A}(\boldsymbol{A},\rho)$的属性集合。

Guess。$\mathcal{A}$输出它的猜测κ''。

4.2　EU-CMA安全性证明

这里首先给出计算性困难问题。

令$\mathcal{G}$为群生成器，定义如下分布

$$\begin{aligned}&G=(N=p_1p_2p_3,\mathbb{G},\mathbb{G}_T,e)\xleftarrow{R}\mathcal{G},\beta,d\xleftarrow{R}\mathbb{Z}_N\\&g\xleftarrow{R}\mathbb{G}_{p_1},X_2,Y_2,Z_2\xleftarrow{R}\mathbb{G}_{p_2},X_3\xleftarrow{R}\mathbb{G}_{p_3}\\&D=(G,g,g^{\beta}X_2,X_3,g^{d}Y_2,Z_2)\end{aligned}\tag{5}$$

给定D，攻击者需要输出$e(g,g)^{\beta d}$。

$\mathcal{B}$收到实例$D=\left(G,g,g^{\beta}X_2,X_3,g^{d}Y_2,Z_2\right)$，其与攻击者$\mathcal{A}$交互如下。

SETUP。除了给定的实例之外，$\mathcal{B}$随机选择$\alpha,a,b\in\mathbb{Z}_N$，计算$e(g,g)^{\alpha},g^{a},g^{b}$，如真实方案中一样计算$T_i=g^{s_i}$并选择哈希函数$H_1,H_2,H_3$。特别地，$\mathcal{B}$计算$e(g,g)^{\beta}=e(g,g^{\beta}X_2)$。最终，$\mathcal{B}$给$\mathcal{A}$发送如下系统公开参数。

$$\begin{aligned}&\mathrm{SPK}=(\mathbb{G},\mathbb{G}_T,e,g,N,e(g,g)^{\alpha},\\&e(g,g)^{\beta},g^{a},g^{b},\{T_i\}_{i\in U},H_1,H_2,H_3)\end{aligned}\tag{6}$$

Phase 1和Phase 2过程如下。

EKGEN。令DO的属性集合为S_{send}，随机选择$q\in\mathbb{Z}_N$，$Q_0,Q_0'\in\mathbb{G}_{p_3}$，对于$S_{\mathrm{send}}$中的每一个属性$i$，随机选择$Q_i\in\mathbb{G}_{p_3}$。计算$\mathrm{ek}_1=g^{\beta}g^{bq}Q_0X_2$，$\mathrm{ek}_2=g^{q}Q_0'$，$\mathrm{ek}_{3,i}=T_i{}^{q}Q_i$。

加密密钥$\mathrm{EK}_{\mathrm{send}}=(S_{\mathrm{send}},\mathrm{ek}_1,\mathrm{ek}_2,\{\mathrm{ek}_{3,i}\}_{i\in S_{\mathrm{send}}})$。

DUREG。如同CPA游戏中一样为使用者u设置$r\in\mathbb{Z}_N$及$\mathrm{PK}_u=g^{r}$。

DKGEN。令DU的属性集合为S_{rec}，由于$\mathcal{B}$知道α和a，因此它如同真实方案一样来计算DU属性密钥为$\mathrm{DK}_u=(S_{\mathrm{rec}},\mathrm{dk}_1,\mathrm{dk}_2,\{\mathrm{dk}_{3,i}\}_{i\in S_{\mathrm{rec}}})$。

加密查询过程如下。

假设消息的访问策略为$\mathbb{A}(\boldsymbol{A},\rho)$，DO的属性集合为$S_{\mathrm{send}}'\subseteq S_{\mathrm{send}}$，令$\mathrm{DEK}=e(g,g)^{\alpha s}$，$\mathcal{B}$如同真实方案一样计算$C=Me(g,g)^{\alpha s}$，$C'=g^{s}$，$C_{1,x}=g^{aA_{x,y}}T_{\rho(x)}^{-r_x}$，$D_{1,x}=g^{r_x}$，$C_2=\mathrm{ek}_1g^{bq'}$，$C_3=\mathrm{ek}_2g^{q'}$，$C_4=g^{c}$。

对于$S_{\mathrm{send}}'\subseteq S_{\mathrm{send}}$中的属性$i'$，$\mathcal{B}$计算$C_{4,i'}=\mathrm{ek}_3(T_{i'})^{q'}H_3(C_{1-4})^{c}$，密文$\mathrm{CT}=(\mathbb{A}(\boldsymbol{A},\rho),S_{\mathrm{send}}',C,C',\{C_{1,x},D_{1,x}\}_{x\in[\ell]},C_2,C_3,\{C_{4,i'}\}_{i'\in S_{\mathrm{send}}'})$。

Forgery。$\mathcal{A}$输出一个关于S_{send}^{*}的密文$\mathrm{CT}^{*}=(\mathbb{A}(\boldsymbol{A},\rho),S_{\mathrm{send}}',C,C',\{C_{1,x},D_{1,x}\}_{x\in[\ell]},C_2,C_3,\{C_{4,i'}\}_{i'\in S_{\mathrm{send}}'})$，其中$S_{\mathrm{send}}^{*}$满足$\mathcal{A}$要挑战的发送者的访问策略$\mathbb{B}^{*}(\boldsymbol{B},\pi)$（可以令$S_{\mathrm{send}}'=S_{\mathrm{send}}^{*}$）。

$\mathcal{B}$设置向量$\boldsymbol{v}=(d,dv_2,dv_3,\cdots,dv_{n_{\mathbb{B}}})^{\mathrm{T}}\in\mathbb{Z}_N^{n_{\mathbb{B}}\times 1}$，其中$v_2,v_3,\cdots,v_{n_{\mathbb{B}}}\in\mathbb{Z}_N$为随机选择的数字，并计算向量$\boldsymbol{\lambda}=(\lambda_1,\lambda_2,\lambda_3,\cdots,\lambda_{n_{\mathbb{B}}})^{\mathrm{T}}=B\boldsymbol{v}$。若$S_{\mathrm{send}}'$满足访问策略$\mathbb{B}^{*}(\boldsymbol{B},\pi)$，则令$I=\{i|i\in[\ell_{\mathbb{B}}],\pi(i)\in S_{\mathrm{send}}'\}$，找到

常数集合$\{w_i\}_{i\in I}$使$\sum_{i\in I}w_iB_i=(1,0,\cdots,0)$，并进行如下计算。

$$T=\prod_{i\in I}\left(\frac{e(C_2,g)e(C_{4,i},g)}{e(C_3,g^bT_{\pi(x)})e(C_4,H_3(C_{1-4}))}\right)^{\lambda_iw_i}=e(g,g)^{\beta d} \tag{7}$$

值得注意的是，由于$\mathcal{B}$不知道d的值，$B\boldsymbol{v}$的值是无法直接计算的，因此可以通过式(8)来计算T的值。

$$T=\prod_{i\in I}\left(\frac{e(C_2,g)e(C_{4,i},g)}{e(C_3,g^bT_{\pi(x)})e(C_4,H_3(C_{1-4}))}\right)^{\lambda_iw_i}=\prod_{i\in I}\left(\frac{e(C_2,g)^{\lambda_iw_i}e(C_{4,i},g)^{\lambda_iw_i}}{e(C_3,g^bT_{\pi(x)})^{\lambda_iw_i}e(C_4,H_3(C_{1-4}))^{\lambda_iw_i}}\right) \tag{8}$$

其中，以$e(C_2,g)^{\lambda_iw_i}$为例来说明如何利用$\mathcal{B}$收到的实例来计算T。

令矩阵$\boldsymbol{B}$中的元素为$B_{i,j}$，令$v_1=1$，有

$$e(C_2,g)^{\lambda_iw_i}=e(C_2,g)^{w_i\sum_jB_{i,j}dv_j}=e(C_2,g)^{dw_i\sum_jB_{i,j}v_j}=e(C_2,g^dY_2)^{w_i\sum_jB_{i,j}v_j} \tag{9}$$

其余的$e(C_{4,i},g)^{\lambda_iw_i}$、$e(C_3,g^bT_{\pi(x)})^{\lambda_iw_i}$以及$e(C_4,H_3(C_{1-4}))^{\lambda_iw_i}$也可以类似进行计算。

5 性能分析

5.1 特征分析

表1从LSSS访问策略、IND-CPA与EU-CMA攻击下的安全性、双边访问控制、外包解密及可验证等方面将本文方案与文献[16,18-20]方案进行了比较，其中，√表示具备该特征，×表示不具备该特征。由表1可知，本文方案在支持LSSS访问策略和双边访问控制的同时，还实现了自适应安全性、外包解密和可验证。

表1 相关方案的特征比较

方案	LSSS访问策略	IND-CPA	EU-CMA	双边访问控制	外包解密	可验证
文献[16]	√	选择性	选择性	√	×	×
文献[18]	√	选择性	选择性	√	√	×
文献[19]	√	选择性	选择性	√	×	×
文献[20]	√	自适应	×	×	×	×
本文方案	√	自适应	自适应	√	√	√

5.2 计算开销比较

本节将合数阶群上构造的文献[20]方案与本文方案在计算开销方面进行对比。实验在AMD Ryzen 7 5800H with Radeon Graphics CPU @ 3.20 GHz, 32 GB RAM，64位Windows 11操作系统的主机上执行，使用Java编程语言和JPBC库[21]，选取的是JPBC库中Type A1曲线，实验结果取100次测试的平均值。

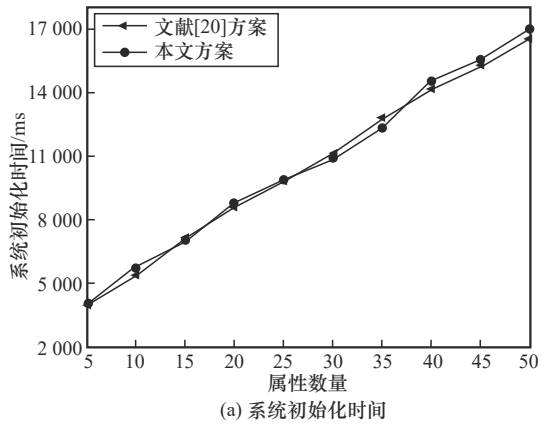
图2给出了2个方案在系统初始化、外包解密密钥生成、密文生成和用户解密等时间对比。图2(a)和图2(b)显示了2个方案的系统初始化时间和外包解密密钥生成时间基本一致，都随着属性数量的增加而增加。图2(c)中，本文方案的密文生成时间要高于文献[20]方案，这是由于本文方案为了支持DU对DO的访问控制，也需要在加密阶段为DO生成一些属性密文以应对DU设置的访问策略。图2(d)显示了用户解密时间，因为本文方案采用了外包解密机制，所以用户解密时间为常数级，与属性数量无关。

图3显示了本文方案在加密密钥生成、解密前验证以及批量密文验证方面的时间。图3(a)与图3(b)分别描绘了在加密密钥生成与解密前验证阶段中的时间与密文数量的线性关系。特别地，解密前验证的计算也由云服务器协助执行，所以在用户端的计算开销可以忽略不计。图3(c)显示了应用批量验证技术之后，可以减轻多个密文验证的时间。

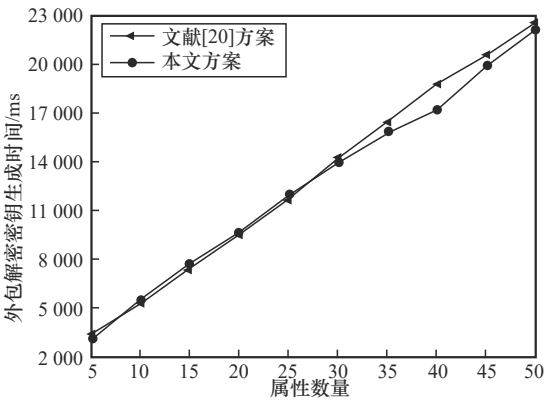
综上所述，与文献[20]方案相比，本文方案额外实现了双边访问控制和批量可验证外包解密，除了在系统初始化、外包解密密钥生成方面的时间与文献[20]方案基本一致外，在用户解密方面的时间要低于文献[20]方案，因此，本文方案是实用且值得采纳的。

6 结束语

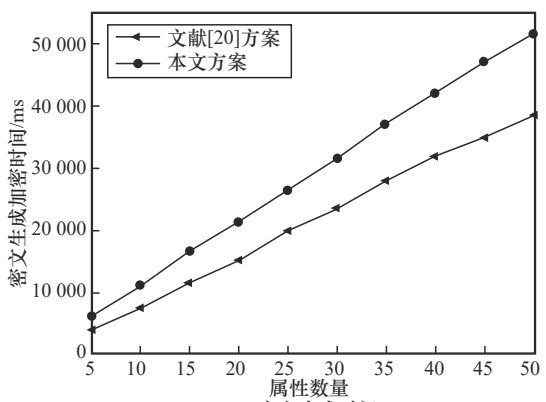
本文将ME、外包解密与自适应安全CP-ABE相结合，提出了自适应安全的可验证外包双边CP-ABE的形式化定义和安全模型，并以此为基础结合批量可验证技术设计了一种面向云存储数据的属性基双边访问控制方案，实现了数据拥有者和数据使用者之间的双边访问控制，解决了传统云存储中细粒度共享机制仅支持单向访问控制的问题。批量可验证和外包解密技术的结合减轻了用户端的匹配、解密以及验证阶段的计算开销。安全性分析和实验结果表明，本文方案是安全有效的。然而，由于本文方案是在合数阶群上构造的，其计算开销相比于素数阶群上构造的方案较大，下一步的工作将考虑在素数阶群上构造自适应安全的双边访问控制方案。



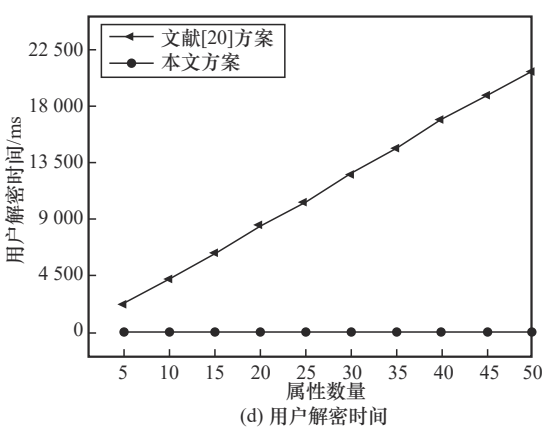
(a) 系统初始化时间



(b) 外包解密密钥生成时间

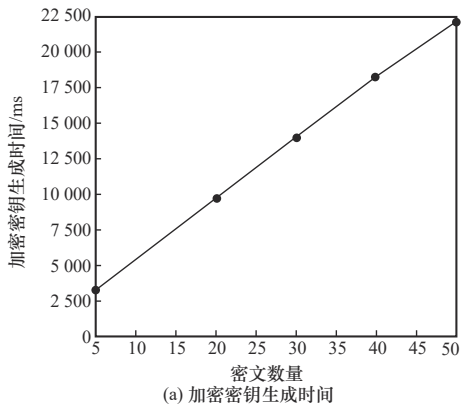


(c) 密文生成时间

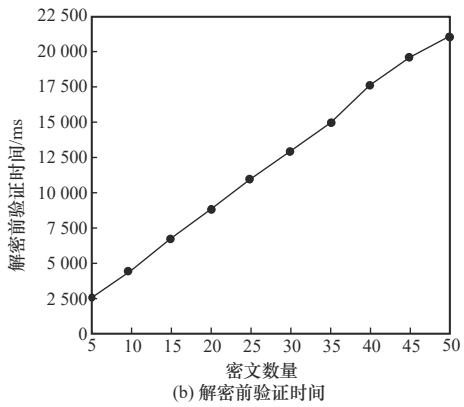


(d) 用户解密时间

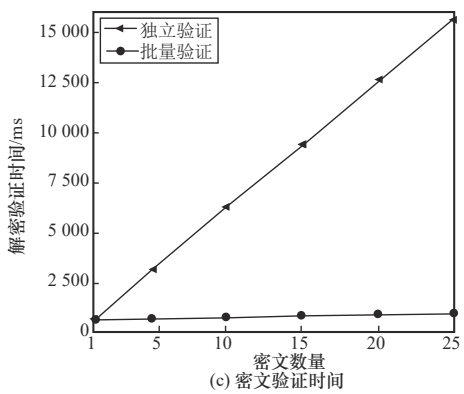
图2　在系统初始化、外包解密密钥生成、密文生成和用户解密等方面的时间对比



(a) 加密密钥生成时间



(b) 解密前验证时间



(c) 密文验证时间

图3　本文方案在加密密钥生成、解密前验证以及解密验证方面的时间

参考文献:

[1] ZHANG Y H, DENG R H, XU S M, et al. Attribute-based encryption for cloud computing access control: a survey[J]. ACM Computing Surveys, 2021, 53(4): 1-41.

[2] SAHAI A, WATERS B. Fuzzy identity-based encryption[C]//Advances in Cryptology. Berlin: Springer, 2005: 457-473.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//Proceedings of the 2007 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2007: 321-334.

[4] YU S C, WANG C, REN K, et al. Achieving secure, scalable, and fine-grained data access control in cloud computing[C]//Proceedings of IEEE INFOCOM. Piscataway: IEEE Press, 2010: 1-9.

[5] 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.
ZHANG J W, MA J F, MA Z, 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.

[6] 郭丽峰, 邢晓敏, 郭慧. 云存储中高效可追踪可撤销的属性基加密方案[J]. 密码学报, 2023, 10(1): 131-145.
GUO L F, XING X M, GUO H. An efficient traceable and revocable attribute-based encryption scheme in cloud storage[J]. Journal of Cryptologic Research, 2023, 10(1): 131-145.

[7] 宁建廷, 黄欣沂, 魏立斐, 等. 支持恶意用户追踪的属性基云数据共享方案[J]. 计算机学报, 2022, 45(7): 1431-1445.
NING J T, HUANG X Y, WEI L F, et al. Tracing malicious insider in attribute-based cloud data sharing[J]. Chinese Journal of Computers, 2022, 45(7): 1431-1445.

[8] 罗王平, 冯朝胜, 邹莉萍, 等. 一种支持快速加密的基于属性加密方案[J]. 软件学报, 2020, 31(12): 3923-3936.
LUO W P, FENG C S, ZOU L P, et al. Attribute-based encryption scheme with fast encryption[J]. Journal of Software, 2020, 31(12): 3923-3936.

[9] 冯涛, 陈李秋, 方君丽, 等. 基于本地化差分隐私和属性基可搜索加密的区块链数据共享方案[J]. 通信学报, 2023, 44(5): 224-233.
FENG T, CHEN L Q, FANG J L, et al. Blockchain data sharing scheme based on localized difference privacy and attribute-based searchable encryption[J]. Journal on Communications, 2023, 44(5): 224-233.

[10] MIAO Y B, TONG Q Y, CHOO K K R, et al. Secure online/offline data sharing framework for cloud-assisted industrial Internet of things[J]. IEEE Internet of Things Journal, 2019, 6(5): 8681-8691.

[11] NING J T, CAO Z F, DONG X L, et al. Auditable $\sigma $-time outsourced attribute-based encryption for access control in cloud computing[J]. IEEE Transactions on Information Forensics and Security, 2018, 13(1): 94-105.

[12] DAMGÅRD I, HAAGH H, ORLANDI C. Access control encryption: enforcing information flow with cryptography[C]//Theory of Cryptography Conference. Berlin: Springer, 2016: 547-576.

[13] KIM S, WU D J. Access control encryption for general policies from standard assumptions[J]. IACR Cryptology EPrint Archive, 2017, 2017: 467.

[14] CUI J, LI B, ZHONG H, et al. A practical and efficient bidirectional access control scheme for cloud-edge data sharing[J]. IEEE Transactions on Parallel and Distributed Systems, 2022, 33(2): 476-488.

[15] ATENIESE G, FRANCATI D, NUÑEZ D, et al. Match me if you can: matchmaking encryption and its applications[J]. Journal of Cryptology, 2021, 34(3): 16.

[16] XU S M, NING J T, LI Y J, et al. Match in my way: fine-grained bilateral access control for secure cloud-fog computing[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(2): 1064-1077.

[17] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]//Proceedings of the 13th ACM Conference on Computer and Communications Security. New York: ACM Press, 2006: 89-98.

[18] XU S M, NING J T, HUANG X Y, et al. Server-aided bilateral access control for secure data sharing with dynamic user groups[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 4746-4761.

[19] SUN J F, YUAN Y, TANG M J, et al. Privacy-preserving bilateral fine-grained access control for cloud-enabled industrial IoT healthcare[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6483-6493.

[20] LEWKO A, OKAMOTO T, SAHAI A, et al. Fully secure functional encryption: attribute-based encryption and (hierarchical) inner product encryption[C]//Advances in Cryptology. Berlin: Springer, 2010: 62-91.

[21] CARO A D, IOVINO V. jPBC: Java pairing based cryptography[C]//Proceedings of the 2011 IEEE Symposium on Computers and Communications (ISCC). Piscataway: IEEE Press, 2011: 850-855.

[作者简介]

李琦（1989– ），男，江苏淮安人，博士，南京邮电大学副教授，主要研究方向为属性基密码学、访问控制、物联网安全等。

樊昊源（2000– ），男，山西晋城人，南京邮电大学硕士生，主要研究方向为属性基密码学。

陈伟（1979– ），男，江苏淮安人，博士，南京邮电大学教授，主要研究方向为网络安全、人工智能安全等。

熊金波（1981– ），男，湖南益阳人，博士，福建师范大学教授、博士生导师，主要研究方向为安全深度学习、数据安全与隐私保护。

韩立东（1982– ），男，山东济南人，博士，杭州师范大学副教授，主要研究方向为公钥密码学、云计算安全、网络安全等。

李瑞（1983– ），男，陕西西安人，博士，西安电子科技大学教授，主要研究方向为智能感知、物联网与智能化系统等。