支持数据敏感度分级的属性访问控制方案*

张绮文[1]，袁凌云[1,2]，王孜冉[1]

（1. 云南师范大学　信息学院，云南　昆明　650500；
2. 云南师范大学　民族教育信息化教育部重点实验室，云南　昆明　650500）

摘　要：在大数据时代，数据的多源异构性为数据安全管理带来了严峻挑战，同时基于传统密文策略的属性基加密（CP-ABE）方案中仍然存在用户属性撤销性能低下等问题，面向敏感数据群体，提出一种支持数据敏感度分级的属性访问控制方案。首先，设计数据敏感度分级分类策略，对数据进行精准的敏感度评估和分级，为不同敏感度数据提出了差异化的加密策略；在此基础上，结合变色龙哈希（Chameleon Hash）技术，利用其陷门碰撞特点实现 CP-ABE 加密用户属性的可撤销性，并证明了该方案在一般群模型和随机预言模型下满足 IND-CPA 安全。性能分析与实验结果表明，所提方案提高了数据存储和加密的效率，降低了链上存储负荷，减少了用户属性撤销时的计算成本，极大地提高了数据管理的灵活性和安全性。

关键词：数据分级分类；属性基加密；属性撤销；变色龙哈希；区块链

中图分类号：TP393. 08；TP309　　**文献标识码：**A　　**DOI：**10. 19358/j. issn. 2097 - 1788. 2024. 10. 004

引用格式：张绮文，袁凌云，王孜冉. 支持数据敏感度分级的属性访问控制方案［J］. 网络安全与数据治理，2024，43(10)：20 - 27.

Attribute access control scheme supporting data sensitivity grading

Zhang Qiwen[1]，Yuan Lingyun[1,2]，Wang Ziran[1]

（1. College of Information Science & Technology，Yunnan Normal University，Kunming 650500，China；2. Key Laboratory of Educational Information for Nationalities，Ministry of Education，Yunnan Normal University，Kunming 650500，China）

Abstract：In the era of big data，heterogeneous data from multiple sources brings severe challenges to data security management. At the same time，the attribute-based encryption scheme for traditional ciphertext strategies exhibits poor performance in terms of user attribute revocation. Aiming at these problems，an attribute access control scheme that classifies data sensitivity for sensitive data groups is proposed in the paper. Firstly，we establish a data sensitivity classification and grading strategy. Then，we accurately assess and classify data sensitivity and propose differentiated encryption strategies for data with varying sensitivities. Additionally，we achieve the revocability of CP-ABE encrypted user attributes based on the trapdoor collision feature of chameleon hash algorithm. The scheme is proven to satisfy IND-CPA security under the general group and random oracle models. Furthermore，performance analysis and experimental results show that the proposed scheme can improve the efficiency of data storage and encryption，reduce the burden of blockchain storage and computational costs when user attributes are revoked. As a result，this scheme dramatically improves the flexibility and security of data management.

Key words：data hierarchical classification；attribute-based encryption；attribute revocation；chameleon hashing；blockchain

0　引言

随着数字化技术的迅速发展和广泛应用，数据已成为企业运营的核心要素。然而，在大数据时代下，数据的多源异构性给数据管理带来了新的挑战。数据来源于各种传感器、社交媒体、互联网等多个渠道，其结构、格式和质量的差异给数据整合、处理和分析带来了困难。

*基金项目：国家自然科学基金（62262073）；云南省应用基础研究计划（202101AT070098）；云南省重大科技专项计划（202402AD080002）；云南师范大学“大学生科研训练基金项目”（KX2023019）

与此同时，随着数据流动性的增加，数据的安全性面临着更加严峻的挑战，如何保护数据隐私和确保数据安全成为了亟待解决的重要问题。

在这一背景下，政府加强了数据安全法规的建设，实施了分级管理和国家监管，通过《网络安全法》《数据安全管理办法》和《个人信息保护法（草案）》等法律，强化了数据的分类分级保护，以保障数据的隐私和安全性。尽管我国已经采取了多项措施确保数据安全和隐私保护，但在不同的应用场景中，数据隐私和敏感度的差异性依然显著，这导致了数据价值释放的多样性。在对数据安全性要求较高的场景中，保护数据的隐私和安全是关键；而在其他场合，开放共享和利用数据则是推动创新和发展的重要途径。然而，目前的数据分类和分级机制往往不能很好地适应各种数据特性，存在安全、隐私保护与数据敏感度之间不匹配的问题。因此需要进一步优化现有的机制，以更好地平衡数据的安全性、隐私保护和价值利用。

为了解决上述问题，本文提出一种面向数据敏感度分级的属性访问控制方案，首先，对数据进行敏感度评估和分级，并提出一种差异化的加密策略；其次，基于变色龙哈希（Chameleon Hash）优化基于密文策略的属性基加密（Ciphertext Policy Attribute-Based Encryption，CP-ABE），实现 CP-ABE 加密用户属性的可撤销性，为高敏感数据加密提供一种新的解决方案。

1 相关工作

在传统的公钥密码体系中，使用错误的公钥进行加密会导致接收方无法正确解密，这一问题催生了基于身份的密码学（Identity-Based Cryptograph，IBC）的研究。Shamir 在 1984 年首次提出了基于身份的密码学概念，为解决公钥管理问题提供了新的思路。随后，基于身份的密码学理念得到了进一步的发展和扩展。在此基础上，Sahai 等人[1] 在 2005 年提出了属性基加密（Attribute-Based Encryption，ABE）的初步概念，Goyal 等人[2] 在 2006 年进一步提出了密钥策略的属性基加密（KP-ABE）。而 Bethencourt 等人[3] 在 2007 年提出了加密策略的属性基加密（CP-ABE），这种加密机制允许用户通过属性定义身份，实现了用户间通信无需保存对方公钥的便利。CP-ABE 特别适用于“一对多”云服务共享场景，因此受到了国内外研究界的广泛关注。

然而，在采用 CP-ABE 进行访问控制的多用户系统中，用户身份的变更是一个常见情况。为了确保系统安全，当用户离开系统或其访问权限发生变化时，需要能够即时撤销用户的访问权限，这是 CP-ABE 面临的一个关键挑战，因为传统的 CP-ABE 方案往往不支持用户属性的动态撤销。因此，学术界对 CP-ABE 中的属性撤销问题进行了深入研究。2007 年，Bethencourt 等[3] 提出了 CP-ABE 方案，其中用户的密钥具有有效期，并在过期时需要重新生成，间接完成属性撤销。2011 年，Hur 等人[4] 以对称密钥加密密钥树，从而实现细粒度的属性撤销，但该方案中的属性群密钥适用于整个群体的用户，因此无法防止撤销用户与未被撤销的用户进行共谋攻击。2013 年，Yang 等[5] 提出一种面向云存储的细粒度访问控制方案，针对每个属性生成两个公开参数。在属性撤销时，属性授权机构需要负责更新相应属性的公开参数，并更新用户的解密密钥。这一过程增加了属性授权机构的计算开销，并增加了与用户之间的通信开销。Wang 等人[6] 和 Mao 等人[7] 提出可验证外包计算的属性基加密方案，该方案的密文长度随着访问结构的复杂度而增加。2016 年，Li 等人[8] 提出了一种支持用户撤销的 CP-ABE 方案，但该方案并不支持细粒度的属性撤销。为改进方案不足，Li 等人[9] 利用属性组的概念，再次提出一种具有高效属性撤销的外包加密 CP-ABE 方案，但是该方案存储开销大、解密成本高而且不支持解密外包。2019 年，张文芳等人[10] 提出了一种基于属性权威的 CP-ABE 方案，可以实现属性的直接撤销，该方案依赖于实时在线的属性授权机构实现细粒度的即时属性撤销。但随着时间的推移，撤销列表的长度会不断增加，从而增加存储开销。孙磊等人[11] 提出一种能够支持属性撤销和外包解密的 CP-ABE 方案，但是在密文更新过程中开销较大。2021 年，Tan 等人[12] 实现的支持属性撤销的 CP-ABE 方案面临数据存储和用户细粒度访问控制管理关联性太强的问题。2022 年，雷雪娇等人[13] 提出了一种基于懒惰密文更新的属性变动优化方案，通过某个撤销属性的属性密文集合与撤销属性前的用户密文组做交集，从而缩小需要更新的密文范围并减少密文更新的次数，但还需要避免不必要的密文更新以减少开销。2023 年，Yan 等人[14] 所提出的方案支持策略隐藏和属性撤销，同时实现代理加密和解密，以较低的计算消耗实现了细粒度访问控制。2024 年，许盛伟[15] 等人提出了一种基于角色和属性的零信任访问控制模型研究，实现了访问权限的动态分配，但是其时间开销过大。

显而易见，现有方案主要专注于性能或安全性等单一问题的研究，但在属性级用户撤销的研究中，实现高性能的同时确保高度安全性至关重要。因此，本文采用变色龙哈希技术，设计了一种能够有效撤销用户属性的 CP-ABE 加密方案，以确保属性撤销过程的准确性。此外，本文在计算资源消耗方面进行了优化，以提高系统

的效率和性能。

2　数据敏感度分级

依据《中华人民共和国数据安全法》《数据安全治理实践指南 2.0》和《数据安全治理白皮书 4.0》的分级标准，数据敏感度通常分为四级，最高级别为敏感数据（L4 级），包括诸如个人隐私和商业机密等高度敏感信息；其次是较敏感数据（L3 级），这类信息泄露可能会对社会、组织或个人造成一定程度的影响；低敏感数据（L2 级）包含相对不敏感的信息，其泄露对个人或组织的影响较小；最低级别的数据为不敏感数据（L1 级），这些信息基本上无敏感性，泄露后不会对个人或组织造成明显的影响。此外，不同行业根据自身特点和需求，还会有特定的数据分类标准。

本文主要针对社交媒体范畴的敏感数据，采用北京大学开放研究数据平台提供的 10 万余条知乎用户 JSON 数据[16]。数据包含用户的个人信息和社交互动数据。

为了简化数据分析与处理，将用户姓名与其余数据特征整合成文本数据集，从中随机抽取 1 000 条记录进行研究。在数据敏感度分级方面，为了简化数据管理过程，根据敏感程度将数据分为两个级别：低敏感数据（L1 级和 L2 级）和高敏感数据（L3 级和 L4 级），划分结果如表 1 所示。

表 1　数据敏感度分级表

数据敏感度级别	数据信息
高敏感度	business（业务信息）
	description（描述）
	educations（教育经历）
	employments（就业经历）
	gender（性别）
	locations（地点）
低敏感度	answer_count（回答数量）
	articles_count（文章数量）
	avatar_url（头像链接）
	favorited_count（被收藏数量）
	follower_count（粉丝数量）
	following_count（关注数量）
	headline（头衔）
	name（用户名）
	thanked_count（被感谢数量）
	url_token（URL 标识符）
	user_type（用户类型）
	voteup_count（被点赞数量）

3　数据敏感度分级加密方案

本文基于先前的敏感度分类结果，针对不同敏感级别的数据实施差异化加密。相较于未进行数据敏感度分类的方案，差异化数据加密方案能够显著降低数据加密所需的计算成本，并有效减少区块链存储开销。

3.1　方案设计

初始阶段，通过数据敏感度分析模块，对数据进行深度评估和精准分类，有效区分高敏感度数据和低敏感度数据。针对高敏感度数据，采用基于属性的加密（CP-ABE）技术进行强力加密，实现细致的访问控制，并采用区块链技术，将加密数据存储于区块链上，构建了安全可靠的数据存储和管理框架。此外，对 CP-ABE 技术进行了改进，增加了撤销权限功能，以适应动态变化的数据访问需求。对于低敏感度数据，采用 AES（Advanced Encryption Standard）算法进行加密。在数据传输和存储过程中，AES 算法确保低敏感度数据的机密性，防止未授权访问和数据泄露。在整个数据传输和共享过程中，依据数据的敏感性级别实施定制化的保护措施，尤其是加密后的高敏感度数据，在传输过程中受到严格保护，并存储于区块链上，从而进一步增强数据的安全性。

该方案共涉及五个实体，分别是数据拥有者、数据请求者、认证机构、存储机构和区块链。数据拥有者对数据进行敏感度评估，并根据数据的敏感度等级采用相应的加密策略。对于高敏感度数据，数据拥有者会通过认证机构来注册或获取属性密钥，并将密文和加密后的数据上传至区块链。当数据请求者获取这些数据时，必须先在认证机构注册或提供相应的密钥，满足访问条件后，才能从区块链上获取加密数据。对于低敏感度数据，数据拥有者会通过认证机构注册或获取密钥，并将数据加密后存储在专门的数据存储机构中，同时返回存储位置。数据请求者在请求这些数据时，同样需要先在认证机构注册或提供密钥，然后使用这些密钥从存储机构处获取加密数据。系统架构如图 1 所示。

3.2　面向不同敏感度的数据加密方法

3.2.1　面向低敏感数据的 AES 加密方法

针对低敏感度数据，选择速度快、计算开销小的 AES 算法进行加密。AES 是一种对称加密算法，使用相同的密钥进行加密和解密[17]。在该方案中使用 CBC（Cipher Block Chaining）模式进行加密，该模式通过将前一个密文块与当前明文块进行 XOR 运算来增加加密的随机性和安全性。在加密过程中，首先将消息使用 PKCS7 填充方案进行填充以满足 AES 分组长度的要求。然后随机生

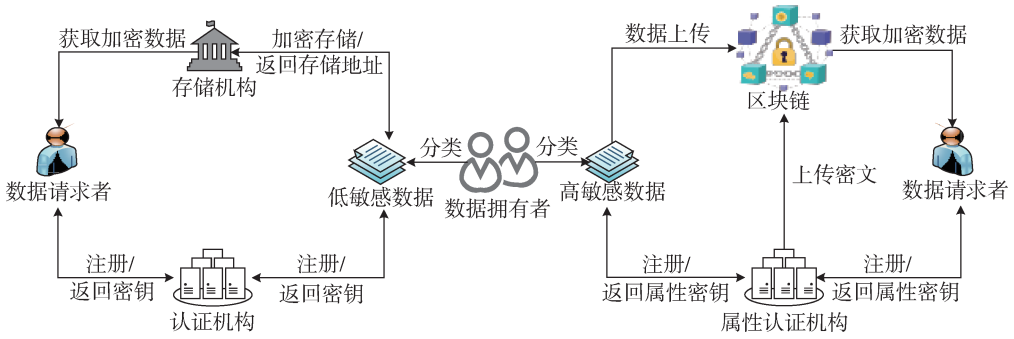

图 1　基于敏感度的数据加密与存储框架图

成一个初始化向量（Initialization Vector，IV），其长度为 AES 分组长度。接着使用密钥和 IV，以及 CBC 模式，通过 AES 加密算法对填充后的消息进行加密。加密算法形式化定义为：

$$C_i = E_k\ (P_i \oplus C_{i-1}) \tag{1}$$

其中，C_i 是第 i 个密文块，E_k 是使用密钥 k 进行的 AES 加密算法，P_i 是第 i 个明文块，C_{i-1} 是前一个密文块或初始化向量。式（1）中，每个密文块的生成都依赖于前一个密文块，因此增加了数据的混淆性。

在解密过程中，首先提取密文中的 IV，然后使用相同的密钥和 IV，以及 CBC 模式，形式化定义解密形式为：

$$P_i = D_k(C_i) \oplus C_{i-1} \tag{2}$$

其中，D_k 是使用密钥 k 进行的 AES 解密算法。解密后得到填充的消息，最后去除填充以还原原始消息。

3.2.2　面向高敏感数据的 CP-ABE 加密方法

鉴于高敏感度数据的需求更为复杂，本文选用 CP-ABE 加密算法对其进行加密。允许基于用户属性实施细致的授权管理，从而提供更加灵活的访问控制，并进一步加强对高敏感数据的保护。下面是 CP－ABE 算法的详细描述：

（1）初始化算法

Setup（λ）→〈msk，PK〉：该算法选择素数阶 p 的群 G_1，G_2，群上的生成元 $g_1 \in G_1$，$g_2 \in G_2$，以及随机整数 α，$\alpha \in \mathbb{Z}_p$。

公钥 pk = g_1，g_2，$e(g_1, g_2)^{\alpha}$，g_1^{α}，g_2^{α}，设置 msk = g_1^{α}，g_2^{α} 为主密钥。公开系统公钥，安全保存系统主密钥。

（2）密钥生成算法

keygen（pk，msk，attributes）→〈key〉：该算法将公钥、主密钥和一组属性 attributes 作为输入。

选择一个随机整数 $t \in \mathbb{Z}_p$。创建私钥为 $K = g^{\alpha} g^{\alpha t}$；$L = g^{t}$；$\forall x \in S$，$\mathrm{SK}_x = h_x^{t}$。返回含主密钥 K、辅助密钥 L、属性密钥 SK_x 和用户属性列表的用户密钥字典 key。

（3）加密算法

encrypt（pk，$\boldsymbol{M}$，$\mathrm{policy}_{\mathrm{str}}$，$\mathrm{CH}_{\mathrm{hash}}$）→〈$D$〉：加密算法以公开密钥 pk、要加密的消息 $\boldsymbol{M}$ 以及属性的变色龙哈希值 $\mathrm{CH}_{\mathrm{hash}}$ 作为输入。另外，基于 LSSS 访问结构将属性和消息 $\boldsymbol{M}$ 关联起来。设 $\boldsymbol{M}$ 是一个 $l \times n$ 阶矩阵。该算法首先选择随机向量 $\boldsymbol{v} = (s, y_2, \cdots, y_n) \in \mathbb{Z}_p^{n}$。这些值将用于共享加密指数 s。$\forall x \in [1, t]$，计算 $\lambda_i = \boldsymbol{v} \cdot \boldsymbol{M}_i$，其中 $\boldsymbol{M}_i$ 是对应于 $\boldsymbol{M}$ 的第 i 行的向量。此外，该算法选择随机 $r_1, \cdots, r_l \in \mathbb{Z}_p$。

密文以 CT =

$$C = \boldsymbol{M} e(g, g)^{\alpha s},\ C' = g^{s},$$
$$(C_1 = g^{a\lambda_1} h_{\rho(1)}^{-r_1},\ D_1 = g^{r_1}),\ \cdots,\ (C_l = g^{a\lambda_l} h_{\rho(l)}^{-r_n},\ D_l = g^{r_l}) \tag{3}$$

的形式发布。此外，密文还包含了原始策略字符串 $\mathrm{policy}_{\mathrm{str}}$、从访问策略中提取的属性列表 p_{list} 和变色龙哈希值 $\mathrm{CH}_{\mathrm{hash}}$。

（4）解密算法

decrypt（pk，sk，CT，CH）→〈$\boldsymbol{M}$〉：在解密过程中，以密文 CT、私钥 sk 及 CH 作为输入。首先验证输入的变色龙哈希值是否与密文中的变色龙哈希值 $\mathrm{CH}_{\mathrm{hash}}$ 匹配。假设 s 满足访问结构，并且 $I \subset \{1, 2, \cdots, l\}$ 被定义为 $I \subset \{i: \rho(i) \in S\}$。然后，设 $\det \{w_i \in \mathbb{Z}_p\}_{i \in I}$ 是一组常数，使得如果 $\{\lambda_i\}$ 是根据 $\boldsymbol{M}$ 的任何秘密 s 生成的有效份额，则 $\sum_{i \in I} w_i \lambda_i = s$。值得注意的是，可能由不同的方式来选择 w_i 值以满足这一条件。

解密算法首先计算

$$e(C', K) / \left(\prod_{i \in I} (e(C_i, L) e(D_i, K_{\rho(i)}))^{w_i}\right) =$$
$$e(g,g)^{\alpha s} e(g,g)^{\alpha s t} / \left(\prod_{i \in I} e(g,g)^{t \alpha \lambda_i w_i}\right) = e(g,g)^{\alpha s} \tag{4}$$

然后，解密算法可以从 C 中除去这个值，得到消息 $\boldsymbol{M}$。

3.3　基于变色龙哈希的可撤销 CP-ABE

变色龙哈希[18]是一种特殊的哈希函数，具有抗碰撞陷门的特性。对于两个不同的哈希值，存在一个特殊的

陷门值，使得通过将这个陷门值与某个消息连接后再进行哈希运算，可以得到相同的哈希值。这种抗碰撞陷门的存在增强了变色龙哈希函数的安全性，使得攻击者难以伪造具有相同哈希值的消息。在基于密文策略的属性基加密（CP-ABE）中应用变色龙哈希技术时，可以为每个用户分配一个唯一的变色龙哈希值，该变色龙哈希值与用户的属性相关联。当用户的属性需要撤销时，可以通过改变变色龙哈希值，而不是直接撤销密钥，从而实现属性撤销。下面是变色龙哈希算法的详细描述：

（1）getSecretKey（）：该算法用于获取私钥，随机选取一个 1 ~ q 之间的大素数。q 通过调用函数 get_ large_ prime_ length（length）生成。

（2）getPublicKey（g，sk）：该算法执行快速幂运算来计算公钥 pk = g^{sk} mod p。其中，p 是通过一个循环得到的。具体过程如下：

随机选择一个偶数 d，然后计算 $p = q \times d + 1$。检查 p 是否为素数，如果是，则终止过程；如果不是，则继续选择下一个偶数 d，直到找到一个满足条件的 p。

g 是通过函数 getGenerator（result）生成的生成元。函数中传入的参数 result 是由函数 primeFactorization（length）生成的，是一个二维列表用于存储素数因子分解的结果。

该过程的安全性可规约到离散对数的困难性问题，从而确保了私钥 sk 不能轻易被计算出来，而公钥 pk 可以被公开使用。

（3）treateMSG(msg)：该算法将属性处理为整数。

（4）ChameleonHash（pk，g，m，r）：该算法通过公钥 pk、生成元 g、属性 m 及随机数 r 计算哈希值 CH = quickPower（g，m，p）· quickPower（PK，r，p）mod p。分别对生成元 g 和公钥 pk 进行了快速幂运算，其中 g 是用于表示消息的底数，pk 是用于表示随机数的底数。这两个运算得到了消息 m 和随机数 r 对应的哈希值。接着，将这两个哈希值相乘，并再次对给定的模数取模，得到了最终的变色龙哈希值 CH。

（5）Forge(sk，m_1，r_1，m_2)：该算法用于计算变色龙哈希的攻击，即给定两个不同的消息 m_1，m_2，sk 以及原始消息 m_1 生成变色龙哈希时所用的随机数 r_1，计算出一个随机数 r_2 使其和改变后的消息 m_2 一起计算变色龙哈希时，能得到与原始消息 m_1 相同的哈希值。

$$x,\ y,\ \gcd = \text{exgcd}(\text{sk}) \tag{5}$$

$$r_2 = x \times (m_1 - m_2 + \text{sk} \times r_1) \bmod q \tag{6}$$

首先通过扩展欧几里得算法计算出私钥 sk 和模数 q 的乘法逆元 x，然后根据变色龙哈希的攻击原理，利用 x 计算出 r_2。

当用户属性撤销时，涉及两种情况，一种是用户属性撤销后，不满足访问策略不具有访问权限。在这种情况下，直接采用新的属性生成新的变色龙哈希值，即通过 ChameleonHash 计算出新的属性的变色龙哈希值。另一种是用户属性撤销后，仍然满足访问策略具有访问权限，在这种情况下，利用变色龙哈希的哈希碰撞算法，即首先通过 Forge 计算出随机数 r_2，利用 r_2 通过 ChameleonHash 在属性信息与原来不同的情况下计算出与原来一致的变色龙哈希值。属性撤销算法见算法 1。

算法 1：AttributeRevocation

```
输入：pk，sk，a，b，p，q，g，rand1，CH，x
输出：newCH
if access_ policy_ satisfied 满足 do
        x，y，gcd = exgcd（sk，q）
        rand2 = x * （m1 - m2 + sk * r1）% q
        while b > 0 满足 do
            if b % 2 =1 满足 do
                result1 = result1 * g % p
            g = g * g % p
            b > > = 1
        while rand2 > 0 满足 do
            if r % 2 =1 满足 do
                result2 = result2 * pk % p
            pk = pk * pk % p
            rand2 > > = 1
        newCH = result1 * result2% p
else
        newCH = quickPower（g，b，p）* quickPower
（pk，rand1，p）% p
End if
```

当用户进行解密时，解密算法会先对比传入的变色龙哈希值与原有密文中的哈希值是否一致，若一致则成功解密，若不一致则解密失败。

综上所述，变色龙哈希算法为 CP-ABE 提供了一种有效的属性撤销机制。通过为每个用户分配唯一的变色龙哈希值，并根据用户的属性信息动态更新这些哈希值，可以实现对用户访问权限的灵活管理。这种基于哈希函数的属性撤销方法不仅可以有效地降低密钥管理的复杂度，还能够保护用户的隐私，防止密钥泄露或者滥用。

3.4 安全性分析

本方案的安全性证明主要基于定理 1 及定理 2 的安全模型。

定理 1 若 q-parallel BDHE 假设[19]成立，那么，不

存在多项式时间内对手可以选择性地攻破本方案。挑战矩阵的大小为 $l^* \times n^*$，其中 l^*，$n^* \leqslant q$。

证明：假设在选择性安全博弈中，对手 A 对本方案有不可忽略的优势 $\varepsilon = \mathrm{Adv}_A$。此外，假设它选择了一个挑战矩阵 $\boldsymbol{M}^*$，其中两个维度都至多为 q。下面将建立一个模拟器来解决 q-parallel BDHE 问题。

定理 2 在一般群模型和随机预言模型下通过挑战者与攻击者之间的博弈游戏来描述该方案的安全模型能达到 IND－CPA 安全。游戏规则如下：

参数设置：挑战者 S 执行 Setup（λ），生成主密钥 $\mathrm{msk} = g_1^{\alpha}$，$g_2^{\alpha}$ 和公开密钥 $\mathrm{pk} = g_1$，g_2，$e(g_1, g_2)^{\alpha}$，g_1^{α}，g_2^{α}，并将 pk 传递给攻击者 A。

密钥查询阶段 1：攻击者 A 提交一系列属性集合给 S，通过 keygen（pk，msk，attributes）获得对应的私钥 sk 字典 key。

挑战阶段：攻击者 A 提交两个等长消息 M_0、M_1 和一个访问控制策略给 S。S 随机选择 $b \in \{0, 1\}$，并根据访问控制策略加密消息 M_b，生成密文 CT^* 并将其发送给 A。

密钥查询阶段 2：攻击者 A 再次随机提交一系列属性集合给 S，值得注意的是本次所提交的是不满足访问策略的属性集合。

猜测阶段：A 输出值 $b' \in \{0, 1\}$ 作为对 b 的猜测。若 $b = b'$，则认为 A 赢得了游戏。定义 A 在该游戏中的优势为 $\varepsilon = \left| \Pr[b = b'] - \frac{1}{2} \right|$。本文方案在一般群模型和随机预言模型下，在任意多项式时间内 A 的优势 ε 是可忽略的，即 A 几乎不可能赢得游戏的胜利，则称本文方案在一般群模型和随机预言模型下是抗选择明文攻击（IND－CPA）安全的。

4 实验评估

4.1 实验设置

本节将分别从不同属性数量下的性能对比以及所提出方案与相关方案的性能对比两个方面进行分析。模拟实验的详细设置如表 2 所示。

表 2 实验环境配置

名称	配置信息
操作系统	Ubuntu 18.04
开发语言	Python3.6
框架	Charm-crypto 0.5
CPU	11th Gen Intel（R）Core（TM）i5－1135G7 @2.40 GHz
内存	4 GB

4.2 实验结果分析

4.2.1 不同属性数量下的时间开销对比

本研究方案测试了在不同属性个数下生成密钥、加密和解密操作的平均耗时变化情况，实验结果如图 2 所示。

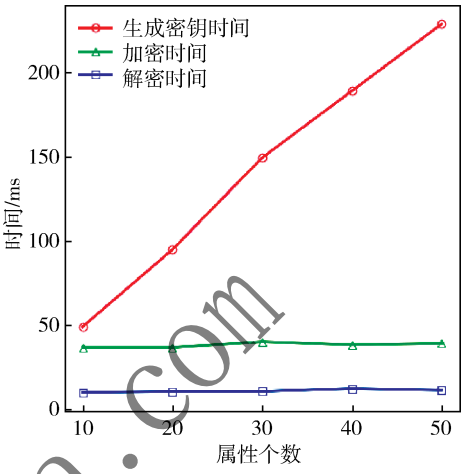

图 2 不同属性个数计算开销对比

由图 2 可知，随着属性个数的增加，生成密钥所需时间略有上升，而加密时间和解密时间相对稳定。由于随着属性个数增加，生成密钥需要处理更多数据或进行更复杂的计算，从而导致耗时略微增加。然而，加密操作和解密操作相对于生成密钥操作更为简单，因此受属性个数增加的影响较小，其耗时表现相对稳定。综合而言，本文方案在处理不同属性个数时，尽管生成密钥的耗时略有增加，但整体性能表现仍然可观，且加解密操作表现良好。

4.2.2 不同方案的时间开销对比

此外，在限定属性个数的条件下，将现有方案与本文方案进行比较，由图 3 可知，在密钥生成过程中，本文方案的耗时略高于方案 2[14]，这是由于密钥生成计算开销与属性个数相关联。在加密阶段，由于本文加密时采用了类似于 LSSS 的存取结构，本文方案的耗时均低于其余三种方案。在解密阶段，本文方案的耗时高于方案 2，但低于方案 1[3] 和方案 3[20]，这是因为方案 2 采用了代理解密，导致解密时间稳定在 1.5 ms。在属性撤销阶段，方案 1 通过定义用户密钥的有效期，在过期时重新生成，间接完成属性撤销，其撤销时间不做参考，同时本文方案仅通过更新变色龙哈希值来实现属性撤销，计算时间远低于其余两方案。综合比较之下，尽管在密钥生成时间和解密时间方面，本文方案略高于方案 2，但在加密时间尤其是属性撤销的时间上表现出显著的优势。同时，本文方案采用了数据敏感度分级，在加密前面向

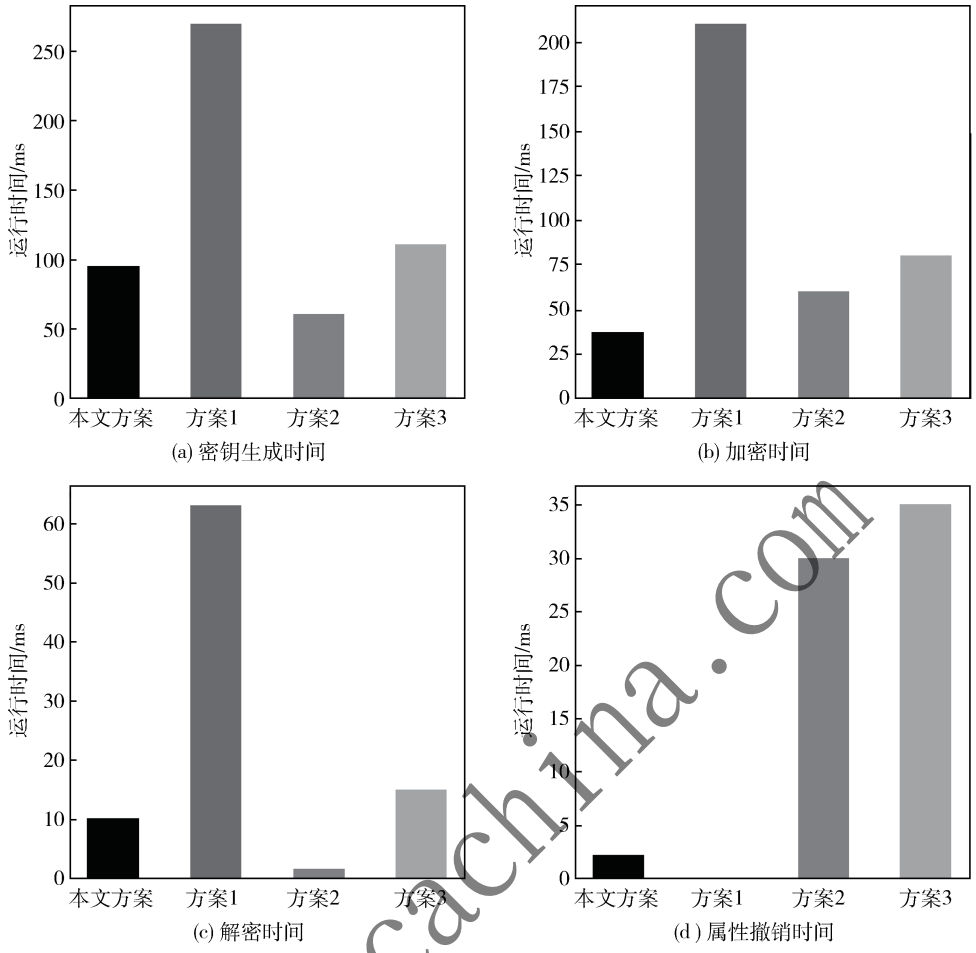

图 3　不同方案计算开销对比

数据的敏感度对数据进行针对性处理，从而节省了数据的存储开销。这一结果进一步验证了本文方案在设计上的合理性和优越性。

5　结束语

本文提出了一种基于区块链的数据分级策略，结合支持用户属性撤销的 CP-ABE 方案，旨在应对数据管理中常见的挑战，如数据存储冗余、数据加密效率低以及数据易泄露和篡改等问题。所提方案通过对数据进行敏感度分级，并采用差异化的加密算法进行保护，从而提升了数据存储和加密的效率，降低了计算成本和区块链的存储需求。同时，引入变色龙哈希技术实现了用户属性的有效撤销，增强了数据管理的灵活性和安全性。下一步将深入研究基于区块链的数据分级策略，探索其在数据管理领域的更多应用场景，同时优化共识算法和加密技术以提高系统性能和稳定性，并研究高效的用户属性撤销机制，探索一种更有效的身份和权限管理方法。

参考文献

[1] SAHAI A, WATERS B. Fuzzy identity-based encryption [C]// 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2005: 457 – 473.

[2] GOYAL V, PANDEY O, SAHAI A, etal. Attribute-based encryption for fine-grained access control of encrypted data [C]// 13th ACM Conference on Computer and Communicatons Security. New York: ACM, 2006: 89 – 98.

[3] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption [C]//2007 IEEE Symposium on Security and Privacy. New Jersey: IEEE, 2007: 321 – 334.

[4] HUR J, DONG K N. Attribute-based access control with efficient revocation in data outsourcing systems [J]. IEEE Transactions on Parallel and Distributed Systems, 2011, 22 (7): 1214 – 1221.

[5] YANG K, JIA X H, REN K L. Attribute-based fine-grained access control with efficient revocation in cloud storage systems [C]//8th ACM SIGSAC Symposium on Information, Computer and Communications Security, New York, USA, 2013: 523 – 528.

[6] WANG H, HE D, SHEN J, et al. Verifiable outsourced ciphertext-policy attribute-based encryption in cloud computing [J].

Soft Computing, 2017, 21: 7325 – 7335.

[7] MAO X P, LAI J Z, MEI Q X, et al. Generic and efficient constructions of attribute-based encryption with verifiable outsourced decryption [J]. IEEE Transactions on dependable and Secure computing, 2015, 13 (5): 533 – 546.

[8] LI J G, YAO W, ZHANG Y C, et al. Flexible and fine-grained attribute-based data storage in cloud computing [J]. IEEE Transactions on Services Computing, 2016, 10 (5): 785 – 796.

[9] LI J G, YAO W, HAN J G, et al. User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage [J]. IEEE Systems Journal, 2017, 12 (2): 1767 – 1777.

[10] 张文芳, 陈桢, 刘旭东, 等. 支持细粒度属性直接撤销的CP-ABE方案 [J]. 软件学报, 2019, 30 (9): 2760 – 2771.

[11] 孙磊, 赵志远, 王建华, 等. 云存储环境下支持属性撤销的属性基加密方案 [J]. 通信学报, 2019, 40 (5): 47 – 56.

[12] TAN L, YU K P, SHI N, et al. Towards secure and privacy-preserving data sharing for COVID-19 medical records: a blockchain-empowered approach [J]. IEEE Transactions on Network Science and Engineering, 2021, 9 (1): 271 – 281.

[13] 雷雪娇, 王银龙, 努尔买买提·黑力力. 基于懒惰模式密文更新的CP-ABE属性变动方案 [J]. 计算机科学, 2022, 49 (10): 327 – 334.

[14] YAN L, GE L, WANG Z, et al. Access control scheme based on blockchain and attribute-based searchable encryption in cloud environment [J]. Journal of Cloud Computing, 2023, 12 (1): 61.

[15] 许盛伟, 田宇, 邓烨, 等. 基于角色和属性的零信任访问控制模型研究 [J]. 信息安全研究, 2024, 10 (3): 241 – 247.

[16] 北京大学开放研究数据平台. 10W + 知乎用户数据集 [DB/OL]. [2024 – 04 – 15]. https://doi.org/10.18170/DVN/XLRXFR.

[17] 秦志光. 密码算法的现状和发展研究 [J]. 计算机应用, 2004, 24 (2): 1 – 4.

[18] 周坚, 金瑜, 何亨, 等. 基于嵌套Merkle Hash tree区块链的云数据动态审计模型 [J]. 计算机应用, 2019, 39 (12): 3575 – 3583.

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

[20] 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 Computing, 2019, 18 (4): 1667 – 1680.

(收稿日期: 2024 – 07 – 15)

作者简介:

张绮文 (2003 –), 女, 本科, 主要研究方向: 访问控制、区块链。

袁凌云 (1980 –), 通信作者, 女, 博士, 教授, 主要研究方向: 物联网安全、区块链、传感器网络。E-mail: blues520@sina.com。

王孜冉 (2003 –), 男, 本科, 主要研究方向: 密码学。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部