支持属性验证与用户撤销的IoMT数据共享方案

李朋祥[1,2,3]，王玥欢[1,2,3]，贾春福[1,2,3]，高敏芬[4]
（1.南开大学密码与网络空间安全学院，天津 300350；2.天津市网络与数据安全技术重点实验室，天津 300350；
3.数据与智能系统安全教育部重点实验室，天津 300350；4.南开大学数学科学学院，天津 300350）

摘 要：为解决诸如医疗物联网（IoMT）场景下敏感数据的访问控制问题，提出了一个基于注册属性加密（RABE）的新型数据访问控制方案VTR-RABE，依托RABE框架，解决传统密文策略属性加密（CP-ABE）方案的密钥托管问题。基于区块链提出了一种半隐私属性验证机制，该机制可以在不泄露用户敏感信息的前提下验证属性的合法性；基于撤销列表实现了支持白盒追踪和全局用户撤销的机制，该机制仅需少量的额外计算开销；此外，设计了外包解密机制，大大减轻解密方的计算压力。最后，通过严格的安全分析和全面的性能评估，证明了VTR-RABE是一种安全、高效且实用的IoMT数据访问控制方案。

关键词：医疗物联网；密文策略属性基加密；注册属性加密；属性验证；可追踪；可撤销
中图分类号：TP390
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2025251

IoMT data sharing scheme supporting attribute verification and user revocation

LI Pengxiang[1,2,3], WANG Yuehuan[1,2,3], JIA Chunfu[1,2,3], GAO Minfen[4]
1. College of Cryptology and Cyber Science, Nankai University, Tianjin 300350, China
2. Tianjin Key Laboratory of Network and Data Security Technology, Tianjin 300350, China
3. Key Laboratory of Data and Intelligent System Security Ministry of Education, Tianjin 300350, China
4. School of Mathematical Sciences, Nankai University, Tianjin 300350, China

Abstract: To address issues such as access control for sensitive data in Internet of medical things (IoMT) scenarios, a novel data access control scheme named VTR-RABE based on registered attribute-based encryption (RABE) was proposed. Building upon the RABE framework, this scheme resolved the key escrow problem inherent in traditional ciphertext-policy attribute-based encryption (CP-ABE) schemes. A semi-private attribute verification mechanism based on blockchain was introduced, which could validate attribute legitimacy without disclosing users' sensitive information. Additionally, a mechanism supporting white-box traceability and global user revocation was implemented via a revocation list, requiring only minimal additional computational overhead. Furthermore, an outsourcing decryption mechanism was designed to significantly reduce the computational burden on the decrypting party. Finally, through rigorous security analysis and performance evaluation, VTR-RABE is demonstrated to be a secure, efficient, and practical data access control solution for IoMT environments.

Keywords: Internet of medical things, ciphertext-policy attribute-based encryption, registration attribute-based encryption, attribute verification, traceability, revocability

收稿日期：2025–10–23；**修回日期：**2025–12–16
通信作者：贾春福，cfjia@nankai.edu.cn
基金项目：国家自然科学基金资助项目（No.62172238）；京津冀自然科学基金合作专项（No.25JJJJC0005）
Foundation Items: The National Natural Science Foundation of China (No.62172238), Beijing-Tianjin-Hebei Natural Science Cooperation Project (No.25JJJJC0005)

0 引言

随着云计算、大数据、物联网等新一代信息与通信技术的迅猛发展，各行业正积极推进数字化转型。在此背景下，医疗健康领域作为数字化转型的重要应用方向，借助医疗物联网（IoMT，Internet of medical things）技术的快速发展，实现了电子病历、实时生理监测数据、医学影像等海量数据在云端与边缘设备间的动态流转。此类数据在云环境中的共享模式，已在众多医疗保健应用场景中展现出重要价值[1-4]。然而，这些数据往往蕴含极高的个人隐私敏感性，将其托管于公共云存储空间会引发严峻的数据隐私与安全问题。密文策略属性加密（CP-ABE，ciphertext-policy attribute-based encryption）[5]技术为实现云端数据安全共享提供了有效解决方案。该技术允许数据所有者自定义访问策略并生成密文，实现了“一对多”的细粒度访问控制。因其能有效保障患者数据在云端共享的安全性，CP-ABE近年来被广泛应用于医疗领域[6-8]。

传统的CP-ABE存在密钥托管问题，即加密系统中需要可信机构长期保存主密钥来为新用户生成私钥，一旦该机构被攻破，则整个系统都会失效，这在大型的IoMT系统中是个致命的缺陷。为解决这个问题，Hohenberger等[9]首次提出了注册属性加密（RABE，registered attribute-based encryption），其私钥生成无需可信机构执行，从根本上解决了密钥托管的问题。随后，一系列基于该框架的改进RABE被提出[10-13]。尽管这些RABE方案解决了密钥托管问题并在性能与表达能力上有所改进，但其应用于IoMT这一特定场景时，仍然有以下问题需要解决。

首先是属性伪造的问题。在RABE中，用户的辅助解密密钥由半可信的密钥策展人聚合生成，这一过程移除了传统CP-ABE中由属性授权机构负责验证用户属性合法性的环节，同时也引入了属性伪造的风险，恶意用户可声称拥有其本不具备的属性。在IoMT系统中，若攻击者成功伪造高权限属性（如声称自己是一名医生），则可非法访问大量敏感医疗数据，从而严重危及整个系统的安全性与隐私性。区块链作为一种去中心化的分布式数据库技术[14]，其固有的高透明和防篡改特性为身份验证系统提供了理想的可信基础。为了解决属性伪造的问题，本文设计了一种基于区块链的半隐私属性验证机制。在该机制中，只有通过验证的属性凭证（而非仅仅是属性名）才会被记录于区块链上，并用于后续的RABE密钥聚合流程。另外在实际场景中，用户用以验证的敏感信息（如执业医师资格证编号）如果被公开，很容易进一步泄露更多隐私身份信息，甚至身份被恶意伪造。本文属性验证机制的核心优势在于，在成功验证属性合法性的同时，有效保障了用户底层敏感信息的隐私性。

其次是私钥泄露问题。在大型IoMT系统中，用户私钥可能因设备丢失而泄露，也可能被恶意用户主动滥用。例如，系统内的医护人员可能出售或出租其私钥，这等同于利用患者隐私信息进行非法牟利。若数据访问控制系统无法有效遏制此类行为，将导致整个系统的安全性形同虚设。为应对这一挑战，一个可靠的IoMT数据访问控制系统必须具备2项核心功能：可追踪性与可撤销性。

可追踪性旨在当发现私钥被滥用时，能够通过分析该私钥精确定位恶意用户的身份。现有追踪机制主要分为2类：白盒追踪[15-17]与黑盒追踪[18-20]。目前，绝大多数白盒追踪方案均采用将用户身份信息（或其编码）直接嵌入用户私钥的策略。当发生私钥滥用事件时，属性授权机构可根据嵌入的信息从滥用私钥中识别出用户身份。黑盒追踪则不关心私钥内部结构，其通过与作为黑盒的盗版解密设备进行交互测试，推断出密钥的身份归属。在传统CP-ABE中，白盒追踪组件通常涉及主密钥，因此执行主体必须是可信机构。然而，在无可信机构的RABE框架下，传统依赖于可信机构的白盒追踪机制难以直接实现。针对此问题，本文创新性地利用RABE中槽位组件与用户辅助解密密钥的内在关联性，设计了一种无需可信机构的原始白盒追踪方案，该方案可以根据用户的原始私钥定位用户身份。

一旦识别出恶意用户，就应该取消其解密权限，这就是CP-ABE的可撤销机制。目前CP-ABE的用户撤销机制也可以分为2类。第一类是直接撤销[21-22]，将所有被撤销用户存放于一张撤销列表中，并将用户身份嵌入私钥中；在进行加密时，加密方将撤销列表嵌入密文中；在解密时，如果解密方的身份在撤销列表中则无法成功解密。另一类是间接撤销[23-24]，间接撤销一般是通过引入撤销管理者执行广播更新机制来实现，在每次撤销时，需要对

未被撤销用户的私钥进行更新。间接撤销的优势是不会显著增大密文体积，但是其难以实现即时撤销，同时需要可信机构定期分发更新密钥，因此难以应用于RABE框架。Li等[25]提出了一种可撤销的RABE方案，然而其方案中的精准撤销机制仅支持单密文模式，在多加密方的场景下难以适用。此外，其系统层面的用户注销机制需由半可信机构生成关键组件，若攻击者与半可信机构合谋，则该注销机制将失效。Wang等[26]提出了一种车联网场景下支持密钥穿刺的RABE方案，其中用户可以穿刺自己泄露的私钥使其失效。该机制虽可实现某种形式的撤销（自我撤销），但无法应对IoMT中最需解决的场景，即系统主动撤销恶意用户的访问权限，以防止其继续滥用私钥。本文在RABE框架中设计了一种直接撤销机制，实现了IoMT场景下恶意用户的系统级即时撤销。

除此之外，高昂的解密计算开销也是实际部署中应该考虑的问题。在IoMT场景中，医疗机构作为频繁的数据访问者，需解密海量患者生理信息，若解密操作本身计算密集，将为其本地计算资源带来沉重负担。外包解密机制[27-28]可将CP-ABE中绝大部分计算密集型解密任务卸载至云服务器等强大计算平台，从而显著减轻终端用户的计算压力。因此，将外包解密技术集成至IoMT数据访问控制方案中，对于保障系统可行性与实用性至关重要。

综上所述，本文以文献[9]提出的RABE框架为基础，提出了一种支持属性验证、白盒追踪、全局撤销和外包解密的IoMT数据共享方案VTR-RABE。本文的主要贡献如下。

1) 基于区块链实现了一种半隐私属性验证机制，解决了RABE框架中的属性伪造漏洞。该机制在高效验证用户属性合法性的同时，无需暴露其原始敏感凭证（如资格证书编号），从而在源头上保护了用户隐私。

2) 在RABE的框架中集成了白盒追踪、用户撤销和外包解密功能。虽然白盒追踪机制仅能对原始格式密钥进行追踪，但其不需要可信第三方持续参与，为RABE中的责任认定提供了可行的解决方案；用户撤销机制实现了基于撤销列表的高效直接撤销，支持系统级即时撤销。与现有文献[25]、文献[26]方案相比，该机制实现了安全的全局用户撤销功能，外包解密机制将绝大部分计算密集型操作转移至云服务器，显著降低了IoMT中数据使用者（如医疗机构）的解密开销，提升了方案的实用性与可扩展性。

3) 给出了VTR-RABE的严格安全性分析，并对方案进行了性能分析和实验验证。结果表明，VTR-RABE是一种适用于实际IoMT环境、安全高效的数据共享方案。

1　预备知识

1.1　合数阶双线性群

合数阶双线性群可由元组$(\mathbb{G},\mathbb{G}_T,e,g,p_1,p_2,p_3)$来描述，其中，$p_1,p_2,p_3$是3个不同的素数，$\mathbb{G},\mathbb{G}_T$是阶为$N=p_1p_2p_3$的乘法循环群，$g$是群$\mathbb{G}$的生成元，双线性映射$e:\mathbb{G}\times\mathbb{G}\to\mathbb{G}_T$具备以下性质。

1)可计算性：e在多项式时间内可被有效计算。

2) 双线性：对于$\forall u,v\in\mathbb{G},a,b\in\mathbb{Z}_N$，有$e\left(u^a,v^b\right)=e\left(u,v\right)^{ab}$。

3)非退化性：$e\left(g,g\right)\neq 1$。

设$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$是阶分别为$p_1,p_2,p_3$的$\mathbb{G}$的子群，$g_1,g_2,g_3$分别是$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$的生成元，则$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$是正交的，即对于$i,k\in[1,3]$，若$i\neq k$，则有$e\left(g_i,g_k\right)=1$。

1.2　子群判定假设

设三素数复合阶双线性群为：$(\mathbb{G},\mathbb{G}_T,e,g,p_1,p_2,p_3)$，$N=p_1p_2p_3$，$\mathcal{G}=(\mathbb{G},\mathbb{G}_T,e,g,N)$，$g_1,g_2,g_3$分别是$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$的生成元。定义分布$\mathcal{D}_0,\mathcal{D}_1$，其中每个分布$\mathcal{D}_b=(D,T_b)$由一组公共组件$D$和一个挑战组件$T_b$组成。如果对于所有概率多项式时间（PPT）敌手$\mathcal{A}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda\in N$，有

$$\left|\Pr\left[\mathcal{A}\left(D,T_0\right)=1\right]-\Pr\left[\mathcal{A}\left(D,T_1\right)=1\right]\right|=\mathrm{negl}(\lambda) \tag{1}$$

则称子群判定假设成立，其中包括3个假设。

假设1　采样$r\in\mathbb{Z}_N$，令$D=(\mathcal{G},g_1,g_3)$，$T_0=g_1^r$，$T_1=(g_1g_2)^r$。

假设2　采样$s_{12},s_{23}\in\mathbb{Z}_N$，令$D=(\mathcal{G},g_1,g_3,\left(g_1g_2\right)^{s_{12}},(g_2g_3)^{s_{23}})$，$T_0=(g_1g_3)^r$，$T_1=g^r$。

假设3　采样$\alpha,s,t_1,t_2,r\in\mathbb{Z}_N$，令$D=(\mathcal{G},g_1,g_2,g_3,g_1^{\alpha}g_2^{t_1},g_1^sg_2^{t_2})$，$T_0=e\left(g_1,g_1\right)^{\alpha s}$，$T_1=e\left(g,g\right)^r$。

1.3　线性秘密共享方案（LSSS）

LSSS是一种访问控制结构，其共享和重构过

程如下。其中，$\boldsymbol{M}$是一个$K \times n$的矩阵，ρ是一个从矩阵行数到属性的单射函数。

1) 共享：设置长度为n的向量$\boldsymbol{y} = (s, y_2, \cdots, y_n)$，其中$y_2, \cdots, y_n \in \mathbb{Z}_p$是随机值，$s \in \mathbb{Z}_p$是秘密值，则属性$\rho(k)$的秘密份额被计算为$\lambda_k = \boldsymbol{M}_k \boldsymbol{y}$，其中向量$\boldsymbol{M}_k$表示矩阵$\boldsymbol{M}$的第$k$行。

2) 重构：设集合S是任意授权属性集，I是关联$\boldsymbol{S}$和访问矩阵$\boldsymbol{M}$的行数索引集合，存在$\{\omega_k\}_{k \in [I]} \subset \mathbb{Z}_p$，使$s = \omega_1 \lambda_1 + \cdots + \omega_{[I]} \lambda_{[I]}$。

1.4 数字签名

数字签名是一种为数字消息提供认证性、完整性和不可否认性的密码原语，其通常包含以下3个算法。

$\mathrm{KeyGen}(1^\lambda)$：输入安全参数$\lambda$，输出一个公私钥对$(\mathrm{pk}, \mathrm{sk})$。

$\mathrm{Sign}(\mathrm{sk}, m)$：输入私钥$sk$和消息$m$，输出一个签名$k$。

$\mathrm{Verify}(\mathrm{pk}, m, k)$：输入公钥pk、消息$m$和签名$k$，输出布尔类型的验证结果。

数字签名的标准安全概念是选择消息攻击下存在性不可伪造（EUF-CMA），其描述为：对于所有的PPT敌手$\mathcal{A}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda \in N$，有

$$\Pr[\mathrm{Verify}(\mathrm{pk}, m^*, k^*), \wedge m^* \in Q | (\mathrm{pk}, \mathrm{sk}) \leftarrow \mathrm{KeyGen}(1^\lambda), k^* \leftarrow A^{\mathrm{Sign}(\mathrm{sk}, \cdot)}(\mathrm{pk})] = \mathrm{negl}(\lambda) \quad (2)$$

2 系统模型与定义

2.1 系统模型

VTR-RABE系统模型如图1所示，包括以下实体。

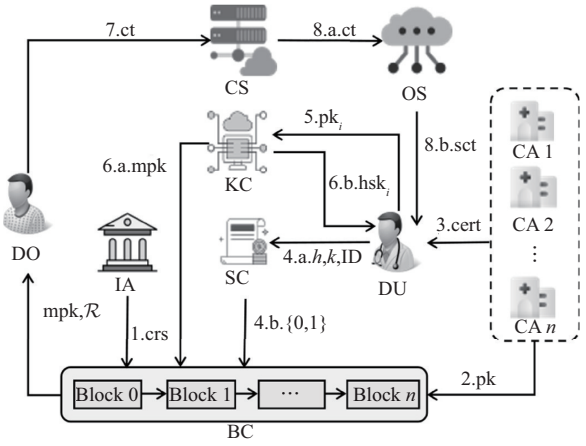

图1 VTR-RABE系统模型

云服务器（CS）：半可信的存储节点，负责存储密文。

数据拥有者（DO）：IoMT中的加密方，负责执行数据加密操作。

数据使用者（DU）：IoMT中的解密方，持有其私钥与辅助解密密钥，并向外包服务器发起解密请求以获取数据。

初始化机构（IA）：完全可信的实体，在系统启动阶段仅负责生成系统公共参数和主密钥，随后退出系统，不参与后续任何操作。

外包服务器（OS）：半可信的实体，在解密过程中为DU承担大部分计算密集型操作。

密钥策展人（KC）：半可信的实体，负责验证用户公钥并执行聚合操作，以生成用于加密的聚合公钥。

凭证机构（CA）：完全可信的实体，仅负责为合法用户颁发属性凭证，不参与密钥生成等后续流程。

区块链（BC）：不可篡改的分布式账本，负责安全地存储系统所需的公共信息。

智能合约（SC）：部署在BC上的自动化程序，负责执行预设的属性验证逻辑，其执行结果被永久记录于链上。

需要强调的是，本方案中的CA对应于现实世界中的权威发证机构，如医院、卫生行政部门或专业资格认证委员会等，其所颁发的凭证是指这些机构签发的数字化身份证明，如电子工作证、数字执业医师资格证等，它们与传统CP-ABE中的属性授权机构不同。属性授权机构必须持有系统主密钥并为用户生成私钥，而CA则完全不参与密钥生成过程，也不需要知晓任何与加密系统相关的密钥信息。凭证的颁发与管理是CA在现实中的固有职能。VTR-RABE的创新之处在于复用了这一现有的、可信的流程，并在此基础上构建了半隐私属性验证机制，而不需要引入额外的专用于加密系统的可信机构。

2.2 算法定义与流程

VTR-RABE的算法定义如下。

1) 初始化

$\mathrm{Setup}(1^\lambda, 1^{|\mathcal{U}|}, 1^L) \rightarrow (\mathrm{crs})$：算法由IA在系统创建之初执行，以安全参数$1^\lambda$、属性空间$\mathcal{U}$的大小以及槽位数量$L$作为输入，输出公共参考字符串crs。

2) 属性验证

$\mathrm{AVSetup}(1^{\lambda}) \rightarrow (\mathrm{pk},\mathrm{sk})$：算法由CA执行，其中pk是凭证签名公钥，sk是凭证签名私钥。

$\mathrm{CerGen}(\mathrm{sk},\mathrm{attr},s) \rightarrow (\mathrm{cert})$：当DU申请凭证时，CA执行此算法，其中attr是需验证的属性，s为CA的全局盐值，算法输出结果cert为数字凭证。

$\mathrm{AttrVer}(h,k,\mathrm{ID},\mathrm{attr},\mathrm{pk}) \rightarrow \{0,1\}$：当DU需要验证属性时，发送隐私保护哈希$h$、签名$k$、DU身份ID、attr以及pk给SC，SC执行此算法输出布尔类型的验证结果。

3) 密钥生成

$\mathrm{KeyGen}(\mathrm{crs},i) \rightarrow (\mathrm{pk}_i,\mathrm{sk}_i)$：算法由槽位索引$i$对应的DU执行，其中，$\mathrm{pk}_i$是索引$i$对应DU的公钥，$\mathrm{sk}_i$是索引$i$对应DU的个人私钥。

$\mathrm{IsValid}(\mathrm{crs},i,\mathrm{pk}_i)$：该算法验证DU上传的$\mathrm{pk}_i$是否合法，防止恶意DU上传混乱格式的公钥以污染主公钥。

$\mathrm{Aggregate}(\mathrm{crs},(\mathrm{pk}_1,S_1),\cdots,(\mathrm{pk}_L,S_L)) \rightarrow (\mathrm{mpk},\mathrm{hsk}_1,\cdots,\mathrm{hsk}_L)$：当每个槽位$i \in [L]$对应的DU都上传了公钥$\mathrm{pk}_i$之后，KC从区块链中查找通过验证的对应属性集$S_i$并执行此聚合算法，生成主公钥mpk以及每个槽位$i \in [L]$对应的辅助解密密钥$\mathrm{hsk}_i$。

4) 数据加密

$\mathrm{Encrypt}(\mathrm{mpk},(\boldsymbol{M},\rho),\mu,\mathcal{R}) \rightarrow \mathrm{ct}$：算法由DO执行，其中，策略矩阵$\boldsymbol{M} \in \mathbb{Z}_N^{K \times n}$，$\rho:[K] \rightarrow \mathcal{U}$是一个将矩阵行数映射到属性域中元素的函数，$\mu$是需要加密的明文，$\mathcal{R} = \{(\mathrm{ID}^{(1)},\mathrm{id}^{(1)}),(\mathrm{ID}^{(2)},\mathrm{id}^{(2)}),\cdots,(\mathrm{ID}^{(r)},\mathrm{id}^{(r)})\}$为撤销列表，最终算法输出密文ct。

5) 数据解密

$\mathrm{OutDec}(\mathrm{hsk}_i,\mathrm{ct},\mathcal{R}) \rightarrow \mathrm{sct}$：当DU发起解密请求，OS执行此算法以承担大部分解密计算开销，最终输出半解密密文sct。

$\mathrm{UserDec}(\mathrm{sk}_i,\mathrm{sct}) \rightarrow \mu$：从OS处接收到sct之后，DU执行此算法解出明文μ。

6) 用户撤销

$\mathrm{Trace}(\mathrm{hsk}_{i'},\mathrm{sk}_{i'},\mathrm{crs}) \rightarrow \mathrm{id}_{i'}$：当系统内察觉到私钥滥用时，KC执行此算法以定位恶意用户的身份。其中，$\mathrm{hsk}_{i'}$为恶意辅助解密密钥，$\mathrm{sk}_{i'}$为恶意私钥，算法最终输出恶意用户的身份$\mathrm{id}_{i'}$。

$\mathrm{Revoke}(\mathrm{id}_{i'},\mathcal{R}) \rightarrow \mathcal{R}'$：锁定到恶意用户身份$\mathrm{id}_{i'}$之后，KC执行此算法对其解密权限进行撤销，算法最终输出更新后的撤销列表$\mathcal{R}'$。

$\mathrm{Update}(\mathrm{ct},\mathrm{mpk},\mathcal{R}') \rightarrow \mathrm{ct}'$：撤销完成之后，为保证方案的前向安全性，DO需要执行此算法对已加密的密文ct执行更新操作，算法输出更新后的密文ct′。

需要说明的是，在本文算法的描述中，为清晰起见，将属性验证过程表述为流程中的第二步。然而，在实际的IoMT系统部署中，属性验证是一个独立于加密操作的前置流程，其唯一的时间约束是必须在KC执行Aggregate算法之前完成。VTR-RABE中各个实体的算法流程如图2所示。

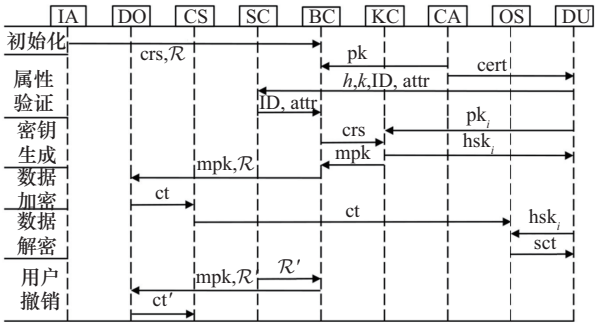

图2　算法流程

2.3　威胁模型与安全模型

本文对系统模型中的实体分别做出以下威胁模型定义。

KC、OS、CS：诚实地执行所有合法请求，但会主动泄露已知信息。因此在VTR-RABE的IND-CPA安全模型中，默认KC、OS和CS是已被腐化的，即其中的所有信息公开。

BC：在VTR-RABE中可主动泄露任意已知的信息，但存放在BC中的数据不可被篡改，同时部署在BC上的SC作为公开透明的代码段，会诚实执行合法请求。

DU：恶意DU会泄露自身信息、尝试获取任何公开信息，且会与其他恶意DU进行串谋攻击。

本文对VTR-RABE的安全模型定义如下。

1) 选择明文攻击下的不可区分安全（IND-CPA）

首先设置敌手能力：由于VTR-RABE的特殊结构，其解密过程受撤销部分、属性部分、私钥部分3个方面的限制。为了全面评估本文方案的安全性，对于所有槽位索引$i \in [L]$，若不同时满足身份

$\mathrm{id}_i \notin \mathcal{R}$，属性集$S_i$满足挑战密文的访问策略，敌手都可以对其进行腐化查询，即获取其私钥sk_i。

安全模型：本方案的IND-CPA安全性由敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的以下博弈证明。

初始化：挑战者首先运行$\mathrm{Setup}\left(1^{\lambda},1^{|\mathcal{U}|},1^{L}\right)$算法生成公共参考字符串crs；随后初始化，ctr ← 0（记录诚实密钥注册查询次数的计数器）、$\mathcal{F} \leftarrow \varnothing$（记录腐化公钥的集合）、$\mathcal{H} \leftarrow \varnothing$（公钥字典，将公钥pk映射到注册属性集，如果$\mathrm{pk} \notin \mathcal{H}$，则定义$\mathcal{H}[\mathrm{pk}]=\varnothing$）、$\mathcal{R} \leftarrow \left\{\left(\mathrm{ID}^{(1)},\mathrm{id}^{(1)}\right),\cdots,\left(\mathrm{ID}^{(r)},\mathrm{id}^{(r)}\right)\right\}$（初始撤销列表）；随后$\mathcal{C}$将crs发送给$\mathcal{A}$。

挑战前查询：$\mathcal{A}$向$\mathcal{C}$发出以下查询。

密钥生成查询：$\mathcal{A}$指定一个槽位$i \in [L]$。$\mathcal{C}$设置ctr = ctr + 1，运行$\mathrm{KeyGen}(\mathrm{crs},i)$生成$(\mathrm{pk}_{\mathrm{ctr}},\mathrm{sk}_{\mathrm{ctr}})$，并将$(\mathrm{ctr},\mathrm{pk}_{\mathrm{ctr}})$发送给$\mathcal{A}$。随后$\mathcal{C}$将映射$\mathrm{ctr} \to (i,\mathrm{pk}_{\mathrm{ctr}},\mathrm{sk}_{\mathrm{ctr}})$添加到字典$\mathcal{H}$中。

腐化查询：$\mathcal{A}$指定一个索引1≤c≤ctr向$\mathcal{C}$进行腐化查询。$\mathcal{C}$查询元组$\mathcal{H}[c]=(i',\mathrm{pk}',\mathrm{sk}')$，并将sk′发送给$\mathcal{A}$。

挑战：首先$\mathcal{A}$需要提交以下信息。①对于每个槽位$i \in [L]$，$\mathcal{A}$提交三元组$(c_i,S_i,\mathrm{pk}_i^*)$，其中若1≤$c_i$≤ctr，则表明所提交的三元组是第$c_i$次诚实密钥查询的密钥；若$\mathcal{H}[c_i]=\perp$，则表明$\mathrm{pk}_i^*$是由敌手自行生成并提供的公钥；此外，$S_i \subseteq \mathcal{U}$是该槽位注册的属性集。②要挑战的访问策略$P^*=(\boldsymbol{M},\rho)$。③2个等长的消息$\mu_0^*,\mu_1^*$，随后$\mathcal{C}$通过以下回应构建$\mathrm{pk}_i$。

若$1 \leqslant c_i \leqslant \mathrm{ctr}$，$\mathcal{C}$查找$\mathcal{H}[c_i]=(i',\mathrm{pk}',\mathrm{sk}')$。如果$i=i'$，则$\mathcal{C}$设置$\mathrm{pk}_i=\mathrm{pk}'$；如果$\mathcal{A}$此前已经对$c_i$进行过腐化查询，则$\mathcal{C}$将槽位索引$i$添加到集合$\mathcal{F}$中。如果$i \neq i'$，则游戏终止。

若$c_i=\perp$，$\mathcal{C}$运行$\mathrm{IsValid}(\mathrm{crs},i,\mathrm{pk}_i^*)$，若验证通过，则$\mathrm{pk}_i^*$合法，$\mathcal{C}$设置$\mathrm{pk}_i=\mathrm{pk}_i^*$，并将槽位索引$i$添加到集合$\mathcal{F}$中；若验证不通过，则游戏终止。

之后$\mathcal{C}$检查可接受条件如下：对于所有腐化公钥对应的槽位索引$i \in \mathcal{F}$，检查是否存在其属性集S_i满足P^*，且其身份索引$\mathrm{id}_i \notin \mathcal{R}$的槽位。若存在，则游戏终止；若不存在，则$\mathcal{C}$运行$\mathrm{Aggregate}(\mathrm{crs},(\mathrm{pk}_1,S_1),\cdots(\mathrm{pk}_L,S_L))$算法生成主公钥和辅助解密密钥，随后运行$\mathrm{Encrypt}(\mathrm{mpk},(\boldsymbol{M},\rho),\mu_\sigma^*,\mathcal{R})$生成挑战密文$\mathrm{ct}^*$，其中$\sigma=\{0,1\}$。最后$\mathcal{C}$将$\mathrm{ct}^*$发送给$\mathcal{A}$。

挑战后查询：$\mathcal{A}$向$\mathcal{C}$发出以下查询。

腐化查询：$\mathcal{A}$指定一个索引1≤c≤ctr向$\mathcal{C}$进行腐化查询。$\mathcal{C}$查询元组$\mathcal{H}[c]=(i',\mathrm{pk}',\mathrm{sk}')$，并将sk'发送给$\mathcal{A}$。此外，若$\mathcal{A}$在挑战阶段提交了三元组$(c,S,\mathrm{pk}^*)$，则$\mathcal{C}$将槽位索引$i'$添加到集合$\mathcal{F}$中。

猜测：$\mathcal{A}$输出对挑战密文的猜测$b'=\{0,1\}$。

定义1 若PPT敌手$\mathcal{A}$无法以不可忽略的优势攻破上述博弈，则称VTR-RABE是IND-CPA安全的。其中$\mathcal{A}$的优势定义为$\mathrm{Adv}=\left|\Pr[\sigma'=1:\sigma=0]-\Pr[\sigma'=1:\sigma=1]\right|$。

2) 原始白盒可追踪性

本方案的原始白盒可追踪性由敌手$\mathcal{A}$和挑战者$\mathcal{C}$之间的以下博弈证明。

初始化：挑战者首先运行$\mathrm{Setup}\left(1^{\lambda},1^{|\mathcal{U}|},1^{L}\right)$算法生成公共参考字符串crs，初始化idl ← ∅（记录查询的对应id的集合）和skl ← ∅（记录查询的私钥集合）。随后$\mathcal{C}$对于所有$i \in [L]$，执行$\mathrm{KeyGen}(\mathrm{crs},i)$和$\mathrm{Aggregate}(\mathrm{crs},(\mathrm{pk}_i,S_i))$算法生成$\{\mathrm{hsk}_i,\mathrm{sk}_i\}_{i\in[L]}$，并将crs和$\{\mathrm{hsk}_i\}_{i\in[L]}$发送给$\mathcal{A}$。

查询：$\mathcal{A}$向$\mathcal{C}$查询一系列私钥$\{\mathrm{sk}_i\}_{i\in[\mathcal{L}]\subset[L]}$，$\mathcal{C}$将$\{\mathrm{id}_i\}_{i\in[\mathcal{L}]\subset[L]}$加入集合idl中，将$\{\mathrm{sk}_i\}_{i\in[\mathcal{L}]\subset[L]}$加入集合中。

私钥伪造：$\mathcal{A}$输出解密元组$(\mathrm{hsk}_*,\mathrm{sk}_*)$，若$\mathrm{sk}_* \in \mathrm{skl}$且$\mathrm{Trace}(\mathrm{hsk}_*,\mathrm{sk}_*,\mathrm{crs}) \notin \mathrm{idl} \cup \perp$，则$\mathcal{A}$赢得游戏。

定义2 若PPT敌手$\mathcal{A}$无法以不可忽略的优势攻破上述博弈，则称VTR-RABE是原始白盒可追踪的。其中$\mathcal{A}$的优势定义为$\mathrm{Adv}=\Pr[\mathrm{Trace}(\mathrm{hsk}_*,\mathrm{sk}_*,\mathrm{crs}) \notin \mathrm{idl} \cup \perp]$。

3 算法描述

3.1 初始化

$\mathrm{Setup}\left(1^{\lambda},1^{|\mathcal{U}|},1^{L}\right) \to (\mathrm{crs})$：算法根据安全参数$\lambda$选择$(\mathbb{G},\mathbb{G}_T,e,g,p_1,p_2,p_3)$，设$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$是阶分别为$p_1,p_2,p_3$的$\mathbb{G}$的子群，$N=p_1p_2p_3$，$g_1,g_2,g_3$分别是$\mathbb{G}_1,\mathbb{G}_2,\mathbb{G}_3$的生成元，设置群描述$\mathcal{G}=(\mathbb{G},\mathbb{G}_T,e,g,N)$。随后算法随机选择$\alpha,\beta,\theta,b \in \mathbb{Z}_N$，计算$h=g_1^{\beta},v=g_1^{\theta},Z=e\left(g_1,g_1\right)^{\alpha}$。对于每个槽位索引$i \in [L]$，随机选择$t_i,\delta_i,\tau_i,d_i,e_i,\mathrm{id}_i \in \mathbb{Z}_N$，并计算槽位组件：$A_i=$

$(g_1g_3)^{t_i}, B_i = g_1^{\alpha} A_i^{\beta} g_3^{\tau_i}, D_i = h^{\frac{-t_i}{b}} g_3^{d_i}, E_i = (g_1^{\mathrm{id}_i} v)^{t_i} g_3^{e_i}, P_i = (g_1g_3)^{\delta_i}$。对于每个属性$w \in \mathcal{U}$和槽位$i \in [L]$，随机选择$u_{i,w} \in \mathbb{Z}_N$，同时对于每个$j \in [L]$且$j \neq i$，随机选择盲因子$\gamma_{i,j,w} \in \mathbb{Z}_N$，计算属性组件$U_{i,w} = g_1^{u_{i,w}}$，$W_{i,j,w} = A_i^{u_{j,w}} g_3^{\gamma_{i,j,w}}$。最终输出公共参考字符串如下。

$$\mathrm{crs} = (\mathcal{G}, Z, g_1, h, g_1^b, v^b, g_3, \{(\mathrm{id}_i, A_i, B_i, D_i, E_i, P_i)\}_{i \in [L]}, \{(U_{i,w}, W_{i,j,w})\}_{j \neq i, w \in \mathcal{U}})$$

随后IA将crs发送至BC。

3.2　属性验证

$\mathrm{AVSetup}(1^{\lambda}) \rightarrow (\mathrm{pk}, \mathrm{sk})$：算法生成签名公钥pk和签名私钥sk，随机选择全局盐值种子$s \in \{0,1\}^{\lambda}$以及哈希函数：$\mathrm{H}: \{0,1\}^* \rightarrow \{0,1\}^{\lambda}$。随后CA将pk发送至区块链作为验证锚点。

$\mathrm{CerGen}(\mathrm{sk}, \mathrm{attr}, s) \rightarrow (\mathrm{cert})$：当DU申请属性$\mathrm{attr} \in \{0,1\}^{\lambda}$的凭证，算法检查DU是否满足要求，若满足，CA生成唯一凭证编号$\mathrm{num} \in \{0,1\}^{\lambda}$，计算凭证特定盐值$r = \mathrm{H}(s || \mathrm{attr} || \mathrm{num})$，构造隐私保护哈希$h = \mathrm{H}(\mathrm{num} || r)$，生成签名$k = \mathrm{Sign}(\mathrm{sk}, h || \mathrm{ID} || \mathrm{attr})$。最终CA向DU发送数字凭证如下。

$$\mathrm{cert} = (\mathrm{num}, h, k)$$

$\mathrm{AttrVer}(h, k, \mathrm{ID}, \mathrm{attr}, \mathrm{pk}) \rightarrow \{0,1\}$：用户向BC发送$h$,$k$,ID以申请属性验证，SC调用此算法验证签名$\mathrm{Verify}(\mathrm{pk}, h || \mathrm{ID} || \mathrm{attr}, k) = 1$，若验证成功，则可以证明用户ID拥有发证机构认证过的attr属性，随后将此属性加入区块链中对应用户列表的属性集合中。

3.3　密钥生成

$\mathrm{KeyGen}(\mathrm{crs}, i) \rightarrow (\mathrm{pk}_i, \mathrm{sk}_i)$：算法随机选择$r_i \in \mathbb{Z}_N$，计算$T_i = g_1^{r_i}, Q_i = P_i^{r_i}, R_i = g_3^{r_i}$。对于每个$j \neq i$，计算交叉项$V_{j,i} = A_j^{r_i}$。生成公钥$\mathrm{pk}_i$和私钥$\mathrm{sk}_i$如下。

$$\mathrm{pk}_i = (T_i, Q_i, R_i, \{V_{j,i}\}_{j \neq i}), \mathrm{sk}_i = r_i$$

随后，DU将pk_i发送给KC，并秘密保存sk_i。

$\mathrm{IsValid}(\mathrm{crs}, i, \mathrm{pk}_i)$：算法首先确认$\mathrm{pk}_i$中的所有组件均为群$\mathbb{G}$中的元素。如果是，则检查式(3)是否成立。

$$e(g_3, T_i) = 1 = e(g_1, R_i), e(T_i, P_i) = e(g_1, Q_i), e(R_i, P_i) = e(g_3, Q_i) \tag{3}$$

随后对于每个$j \neq i$，检查式(4)是否成立 。

$$e(g_1, V_{j,i}) = e(T_i, A_j), e(g_3, V_{j,i}) = e(R_i, A_j) \tag{4}$$

如果以上所有检查都通过，则算法返回1，否则返回0。需要注意的是，对于每个槽位$i \in [L]$，D_i,E_i组件由于不必参与下一步的密钥聚合，因此不必参与检查。

$\mathrm{Aggregate}(\mathrm{crs}, (\mathrm{pk}_1, S_1), \cdots, (\mathrm{pk}_L, S_L)) \rightarrow (\mathrm{mpk}, \mathrm{hsk}_1, \cdots, \mathrm{hsk}_L)$：算法计算属性无关公钥$\hat{T}$，以及对于每个$i \in [L]$，计算属性无关槽位私钥$\hat{V}_i$，即

$$\hat{T} = \prod_{j \in [L]} T_j, \hat{V}_i = \prod_{j \neq i} V_{i,j} \tag{5}$$

对于每个属性$w \in \mathcal{U}$，计算属性相关公钥$\hat{U}_w$，对于每个属性$w \in \mathcal{U}$和每个槽位$i \in [L]$，计算属性相关槽位私钥，即

$$\hat{U}_w = \prod_{j \in [L]: w \notin S_j} U_{j,w}, \hat{W}_{i,w} = \prod_{j \neq i: w \notin S_j} W_{i,j,w} \tag{6}$$

最后，算法输出主公钥mpk以及特定槽位对应的辅助解密密钥hsk_i如下。

$$\mathrm{mpk} = \left(\mathcal{G}, Z, g_1, h, g_1^b, v^b, \hat{T}, \{\hat{U}_w\}_{w \in \mathcal{U}}\right), \mathrm{hsk}_i = \left(\mathrm{mpk}, i, \mathrm{id}_i, S_i, A_i, B_i, D_i, E_i, \hat{V}_i, \{\hat{W}_{i,w}\}_{w \in \mathcal{U}}\right)$$

随后KC将mpk发送至BC，将hsk_i依次发送给特定DU。

3.4　数据加密

$\mathrm{Encrypt}(\mathrm{mpk}, (\boldsymbol{M}, \rho), \mu, \mathcal{R}) \rightarrow \mathrm{ct}$：DU首先随机选择$s, s^{(1)}, s^{(2)}, s^{(3)}, s_1, \cdots, s_r \in \mathbb{Z}_N$，其中，$s = s^{(1)} + s^{(2)} + s^{(3)}, s^{(3)} = s_1 + \cdots s_r$，计算$C_1 = \mu Z^s, C_2 = g_1^s$，对于每个$f \in [r]$，计算$C_{3,f} = h^{s_f}, C_{4,f} = (g_1^{b \cdot \mathrm{id}^{(f)}} v^b)^{s_f}$。随机选择$y_2, \cdots, y_n \in \mathbb{Z}_N$，生成向量$\boldsymbol{y} = \{s^{(2)}, y_2, y_3, ..., y_n\}^{\mathrm{T}}$，对于每个$k \in [K]$计算$C_{5,k} = h^{\boldsymbol{M}_k \boldsymbol{y}} \hat{U}_{\rho(k)}^{-s}$，其中$\boldsymbol{M}_k$是$\boldsymbol{M}$的第$k$行；最后计算$C_6 = h^{s^{(1)}} \hat{T}^{-s}$，生成密文如下。

$$\mathrm{ct} = ((\boldsymbol{M}, \rho), C_1, C_2, \{C_{3,f}, C_{4,f}\}_{f \in [r]}, \{C_{5,k}\}_{k \in [K]}, C_6)$$

随后DO将ct发送至CS。

3.5　数据解密

$\mathrm{OutDec}(\mathrm{hsk}, \mathrm{ct}, \mathcal{R}) \rightarrow \mathrm{sct}$：设$I = \{k | \rho(k) \in S_i\}$是满足访问策略$(\boldsymbol{M}, \rho)$属性集的索引集合，则存在$\{w_k\}_{k \in I}$使$w_1 \boldsymbol{M}_1 + \cdots + w_k \boldsymbol{M}_k = (1, 0, \cdots, 0)$，其中$\boldsymbol{M}_k$是矩阵$\boldsymbol{M}$的第$k$行。若DU满足属性要求，则OS可进行如下计算。

$$\mu_1 = \frac{C_1}{e\left(C_2,B_i\right)} e\left(C_6,A_i\right) e\left(C_2,\hat{V}_i\right) \prod_{k \in I} \left(e\left(C_{5,k},A_i\right) \cdot e\left(C_2,\hat{W}_{i,\rho(k)}\right)\right)^{w_k} \prod_{f \in [r]} \left(e\left(C_{3,f},E_i\right) e\left(C_{4,f},D_i\right)\right)^{\frac{1}{\mathrm{id}_i - \mathrm{id}^{(f)}}} \tag{7}$$

$$\mu_2 = e\left(C_2,A_i\right) \tag{8}$$

随后 OS 将半解密密文 $\mathrm{sct} = (\mu_1,\mu_2)$ 发送给 DU。

$\mathrm{UserDec}(\mathrm{sk}_i,\mathrm{sct}) \rightarrow \mu$：DU 接受到 sct 后执行如下计算。

$$\mu = \mu_1 \mu_2^{r_i} \tag{9}$$

3.6 用户撤销

$\mathrm{Trace}(\mathrm{hsk}_{i'},\mathrm{sk}_{i'},\mathrm{crs}) \rightarrow \mathrm{id}_{i'}$：VTR-RABE 的追踪算法要求输入的 $\mathrm{hsk}_{i'}$ 是标准格式的原始私钥。算法首先确认是否 $A_{i'},D_{i'},E_{i'} \in \mathbb{G}$，如果是，则检查式(10)是否成立。

$$e\left(\hat{T},A_{i'}\right) = e\left(g_1,A_{i'}^{\mathrm{sk}_{i'}} \hat{V}_{i'}\right) \tag{10}$$

若检查不通过，则算法返回 $\perp$。若检查通过，则证明 $\mathrm{sk}_{i'}$ 与 $\mathrm{hsk}_{i'}$ 是关联的，随后检查式(11)是否成立。

$$e\left(g_1^b,D_{i'}\right) e\left(A_{i'},h\right) = 1, e\left(g_1^{b \cdot \mathrm{id}_{i'}} v^b,A_{i'}\right) = e\left(E_{i'},g_1^b\right) \tag{11}$$

若检查不通过，则说明是 $\mathrm{id}_{i'}$ 是伪造组件，则需要查找 crs 中对应槽位组件的信息，以获取恶意用户的真实身份索引 $\mathrm{id}_{i'}$。若检查通过，则证明泄露辅助解密密钥 $\mathrm{hsk}_{i'}$ 中的身份组件 $D_{i'},E_{i'}$ 与身份索引 $\mathrm{id}_{i'}$ 相关联，因此可得恶意用户的身份索引 $\mathrm{id}_{i'}$。

$\mathrm{Revoke}(\mathrm{id}_{i'},\mathcal{R}) \rightarrow \mathcal{R}'$：SC 接收到恶意身份 $\mathrm{id}_{i'}$ 后，更新撤销列表 $\mathcal{R}$ 为

$$\mathcal{R}' = R \cup \left\{ \left(\mathrm{ID}^{(r+1)},\mathrm{id}^{(r+1)}\right) = \left(\mathrm{ID}_{i'},\mathrm{id}_{i'}\right)\right\} \tag{12}$$

随后 SC 将更新后的撤销列表 $\mathcal{R}'$ 存放于区块链中。

$\mathrm{Update}(\mathrm{ct},\mathrm{mpk},\mathcal{R}') \rightarrow \mathrm{ct}'$：撤销列表更新之后，DO 需要更新密文。算法首先随机选择 $s_{r+1} \in \mathbb{Z}_N$，计算 $s^{(3)\prime} = s^{(3)} + s_{r+1}$；对于撤销组件，新增 $C_{3,r+1} = h^{s_{r+1}}$，$C_{4,r+1} = (g_1^{b \cdot \mathrm{id}^{(r+1)}} v^b)^{s_{r+1}}$，并更新数据密文组件 $C_1' = C_1 Z^{s_{r+1}}$。最终生成更新后的密文如下。

$$\mathrm{ct}' = \left((\boldsymbol{M},\rho),C_1',C_2,\left\{C_{3,f},C_{4,f}\right\}_{f \in [r+1]},\left\{C_{5,k}\right\}_{k \in [K]},C_6\right)$$

需要说明的是，本文重点描述了基于 Hohenberger 等[9]提出的 slot-RABE 方案的功能性改进，对于其拓展的多层标准 RABE 方案，VTR-RABE 按照文献[9]中的聚合方法可以直接兼容。

4 正确性验证

设

$$d_{\mathrm{attr}} = \prod_{k \in I} \left(e\left(C_{5,k},A_i\right) e\left(C_2,\hat{W}_{i,\rho(k)}\right)\right)^{w_k} \tag{13}$$

可知

$$e\left(C_{5,k},A_i\right) = e\left(h^{\boldsymbol{M}_k \boldsymbol{y}} \hat{U}_{\rho(k)}^{-s},(g_1 g_3)^{t_i}\right) = e\left(h,g_1\right)^{t_i \boldsymbol{M}_k \boldsymbol{y}} \prod_{j \in [L]:\rho(k) \notin S_j} e\left(g_1,g_1\right)^{-t_i s u_{j,\rho(k)}},$$

$$e\left(C_2,\hat{W}_{i,\rho(k)}\right) = \prod_{j \in [L] \setminus \{i\}:\rho(k) \notin S_j} e\left(g_1^s,W_{i,j,\rho(k)}\right) = \prod_{j \in [L] \setminus \{i\}:\rho(k) \notin S_j} e\left(g_1,g_1\right)^{t_i s u_{j,\rho(k)}}$$

由于 $\rho(k) \in S_i$，可得

$$\prod_{j \in [L]:\rho(k) \notin S_j} e\left(g_1,g_1\right)^{-t_i s u_{j,\rho(k)}} = \prod_{j \in [L] \setminus \{i\}:\rho(k) \notin S_j} e\left(g_1,g_1\right)^{-t_i s u_{j,\rho(k)}}$$

因此可得

$$e\left(C_{5,k},A_i\right) e\left(C_2,\hat{W}_{i,\rho(k)}\right) = e\left(h,g_1\right)^{t_i \boldsymbol{M}_k \boldsymbol{y}},$$

$$d_{\mathrm{attr}} = \prod_{k \in I} e\left(h,g_1\right)^{t_i w_k \boldsymbol{M}_k \boldsymbol{y}} = e\left(h,g_1\right)^{t_i s^{(2)}}$$

设

$$d_{\mathrm{revo}} = \prod_{f \in [r]} \left(e\left(C_{3,f},E_i\right) e\left(C_{4,f},D_i\right)\right)^{\frac{1}{\mathrm{id}_i - \mathrm{id}^{(f)}}} \tag{14}$$

可知

$$e\left(C_{3,f},E_i\right) = e\left(h^{s_f},(g_1^{\mathrm{id}_i} v)^{t_i} g_3^{e_i}\right) = e\left(h,g_1\right)^{\mathrm{id}_i t_i s_f} e\left(h,v\right)^{t_i s_f},$$

$$e\left(C_{4,f},D_i\right) = e\left((g_1^{b \cdot \mathrm{id}^{(f)}} v^b)^{s_f},h^{\frac{-t_i}{b}} g_3^{d_i}\right) = e\left(h,g_1\right)^{-\mathrm{id}^{(f)} t_i s_f} e\left(h,v\right)^{-t_i s_f}$$

因此可得

$$d_{\mathrm{revo}} = \prod_{f \in [r]} e\left(h,g_1\right)^{t_i \frac{(\mathrm{id}_i - \mathrm{id}^{(f)}) s_f}{\mathrm{id}_i - \mathrm{id}^{(f)}}} = e\left(h,g_1\right)^{t_i s^{(3)}}$$

设

$$d_{\text{slot}} = e\left(C_6,A_i\right)e\left(C_2,\hat{V}_i\right) \tag{15}$$

可知

$$e\left(C_6,A_i\right) = e\left(h^{s^{(1)}}\hat{T}^{-s},(g_1g_3)^{t_i}\right) = e\left(h,g_1\right)^{t_is^{(1)}}\prod_{j\in[L]}e\left(T_j,A_i\right)^{-s},$$

$$e\left(C_2,\hat{V}_i\right) = \prod_{j\neq i}e\left(g_1,V_{i,j}\right)^{s}$$

对于所有的$j \neq i$，$e\left(T_j,A_i\right) = e\left(g_1,V_{i,j}\right)$，可得

$$d_{\text{slot}} = e\left(h,g_1\right)^{t_is^{(1)}}\prod_{j\in[L]}e\left(T_j,A_i\right)^{-s}\prod_{j\neq i}e\left(g_1,V_{i,j}\right)^{s} = e\left(h,g_1\right)^{t_is^{(1)}}e\left(g_1,g_1\right)^{-r_it_is}$$

因此

$$\mu_1 = \frac{C_1}{e\left(C_2,B_i\right)}d_{\text{attr}}d_{\text{revo}}d_{\text{slot}} = \frac{\mu e\left(g_1,g_1\right)^{\alpha s}e\left(h,g_1\right)^{t_is}e\left(g_1,g_1\right)^{-r_it_is}}{e\left(g_1,g_1\right)^{\alpha s}e\left(h,g_1\right)^{t_is}} = \mu e\left(g_1,g_1\right)^{-r_it_is}$$

又因为$\mu_2 = e\left(C_2,A_i\right) = e\left(g_1,g_1\right)^{t_is}$，则最终可得

$$\mu_1\mu_2^{r_i} = \mu e\left(g_1,g_1\right)^{-r_it_is}e\left(g_1,g_1\right)^{r_it_is} = \mu$$

5　安全性分析

5.1　IND-CPA 安全

定理 1　若子群判定假设成立，则不存在PPT敌手$\mathcal{A}$能够以不可忽略的优势攻破VTR-RABE。

证明　假设VTR-RABE的IND-CPA安全可以被攻破，PPT敌手$\mathcal{A}$可以在多项式时间内攻破本文方案，$\mathcal{C}$是可以模拟方案算法的挑战者。本文的证明遵循双系统方法[29]，按照如下思路进行：首先将原方案修改成安全模型定义的游戏模式，随后将挑战密文从正常密文修改成半功能密文，再依次将每个槽位的相关参数从正常切换成半功能。双系统方法的要求是：正常槽位对应的密钥可以解密正常密文和半功能密文；半功能槽位对应的密钥可以解密正常密文，无法解密半功能密文。因此在最后，可以合理地根据子群判定假设将半功能挑战密文修改成随机值，即敌手$\mathcal{A}$对于分辨挑战密文没有任何优势。下面是指定的半功能密文和半功能槽位的结构。

半功能密文：表达式为

$$\text{ct}' = \left((\boldsymbol{M},\rho),C_1,C_2g_2^{\zeta_2},\left\{C_{3,f},C_{4,f}g_2^{\zeta_{4,f}}\right\}_{f\in[r]},\left\{C_{5,k}g_2^{\zeta_{5,k}}\right\}_{k\in[K]},C_6g_2^{\zeta_6}\right) \tag{16}$$

其中，$\zeta_2,\zeta_{4,f},\zeta_{5,k},\zeta_6 \in \mathbb{Z}_N$。

半功能槽位：在crs中，对每个$i \in [L]$只修改槽位组件参数，表达式为

$$A_i = \left(g_1g_3\right)^{t_i},B_i = g_1^{\alpha}A_i^{\beta}\left(g_2g_3\right)^{\tau_i},D_i = g_1^{\frac{-\beta t_i}{b}}\left(g_2g_3\right)^{d_i},E_i = \left(g_1^{\text{id}_i}v\right)^{t_i},P_i = g^{\delta_i} \tag{17}$$

对于$\mathcal{A}$提交的挑战密文μ_σ^*，定义如下混合游戏序列。

1) $\text{Hyb}_{\text{real}}^{(\sigma)}$：$\text{Hyb}_{\text{real}}^{(\sigma)}$按照2.3节中定义的IND-CPA安全模型，由真实方案生成。

2) $\text{Hyb}_1^{(\sigma)}$：$\text{Hyb}_1^{(\sigma)}$与$\text{Hyb}_{\text{real}}^{(\sigma)}$相比仅仅调整参数生成方式，具体修改如下。

初始化：$\mathcal{C}$随机选择$s \in \mathbb{Z}_N$，随后对于每个$i \in [L]$，$\mathcal{C}$将P_i的生成方式修改为

$$P_i = \left(g_1^sg_3\right)^{\delta_i} \tag{18}$$

挑战：$\mathcal{C}$随机选择$\lambda^{(1)},\lambda^{(2)},\lambda^{(3)},\lambda_1,\cdots,\lambda_r \in \mathbb{Z}_N$，其中$\lambda^{(1)}+\lambda^{(2)}+\lambda^{(3)} = 1,\lambda^{(3)} = \lambda_1+\cdots\lambda_r$，然后随机选择$y_2,\cdots,y_n \in \mathbb{Z}_N$，生成向量$\boldsymbol{y}' = \{1,y_2,y_3,\cdots,y_n\}^{\text{T}}$。对于每个$f \in [r]$，修改$C_{3,f}$和$C_{4,f}$的生成方式为

$$C_{3,f} = \left(g_1^s\right)^{\beta\lambda_f},C_{4,f} = \left(g_1^s\right)^{b\cdot\text{id}^{(f)}\lambda_f+\theta b\lambda_f} \tag{19}$$

对于每个$k \in [K]$，修改$C_{5,k}$的生成方式为

$$C_{5,k} = \left(g_1^s\right)^{\beta\boldsymbol{M}_k\boldsymbol{y}'}\prod_{i\in[L]:\rho(k)\notin S_i}\left(g_1^s\right)^{u_{i,\rho(k)}} \tag{20}$$

修改C_6的生成方式为

$$C_6 = \left(g_1^s\right)^{\beta}\left(\prod_{i\in[L]}\frac{R_i}{Q_i^{\delta_i^{-1}}}\right) \tag{21}$$

显而易见的是，由于s和δ_i都是随机值，因此$\mathcal{A}$无法区分$\text{Hyb}_1^{(\sigma)}$与$\text{Hyb}_{\text{real}}^{(\sigma)}$中的$P_i$组件，其余每个修改的组件从数学上与原组件不可区分，因此可知，对于多项式敌手$\mathcal{A}$与$\sigma' = \{0,1\}$，存在一个可忽略的函数$\text{negl}(\cdot)$，使对于所有的$\lambda \in \mathbb{N}$，有

$$\left|\Pr\left[\text{Hyb}_{\text{real}}^{(\sigma)}(\mathcal{A}) = 1\right] - \Pr\left[\text{Hyb}_1^{(\sigma)}(\mathcal{A}) = 1\right]\right| = \text{negl}(\lambda) \tag{22}$$

3) $\text{Hyb}_{2,0}^{(\sigma)}$：$\text{Hyb}_{2,0}^{(\sigma)}$将正常密文转换为半功能密文，可以使用正常密钥解密，具体修改如下。

初始化：对于每个$i \in [L]$，$\mathcal{C}$将P_i的生成方式修改为

$$P_i = \left(\left(g_1 g_2 \right)^s g_3 \right)^{\delta_i} \tag{23}$$

挑战：修改C_2, C_6的生成方式为

$$C_2 = \left(g_1 g_2 \right)^s, C_6 = \left(\left(g_1 g_2 \right)^s \right)^{\beta} \left(\prod_{i \in [L]} \frac{R_i}{Q_i^{\delta_i^{-1}}} \right) \tag{24}$$

对于每个$f \in [r]$，修改$C_{3,f}$和$C_{4,f}$的生成方式为

$$C_{3,f} = \left(\left(g_1 g_2 \right)^s \right)^{\beta \lambda_f}, C_{4,f} = \left(\left(g_1 g_2 \right)^s \right)^{b \cdot \mathrm{id}^{(f)} \lambda_f + \theta b \lambda_f} \tag{25}$$

对于每个$k \in [K]$，修改$C_{5,k}$的生成方式为

$$C_{5,k} = \left(\left(g_1 g_2 \right)^s \right)^{\beta \boldsymbol{M}_k \boldsymbol{y}'} \prod_{i \in [L]: \rho(k) \notin S_i} \left(\left(g_1 g_2 \right)^s \right)^{u_{i,\rho(k)}} \tag{26}$$

简单来说，将g_2元素嵌入上述组件中以形成半功能密钥，由于合数阶群的正交性质，密文中所有含有g_2的部分在使用正常密钥解密时都可以被消除，不会影响正常解密。若子群判定假设中的假设1成立，对于多项式敌手$\mathcal{A}$与$\sigma' = \{0,1\}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda \in N$，有

$$\left| \Pr\left[\mathrm{Hyb}_1^{(\sigma)}(\mathcal{A}) = 1 \right] - \Pr\left[\mathrm{Hyb}_{2,0}^{(\sigma)}(\mathcal{A}) = 1 \right] \right| = \mathrm{negl}(\lambda) \tag{27}$$

4) $\mathrm{Hyb}_{2,l}^{(\sigma)}$：$\mathrm{Hyb}_{2,l}^{(\sigma)}$与$\mathrm{Hyb}_{2,l-1}^{(\sigma)}$相比，将第$l$个槽位改成了半功能槽位，具体修改如下。

初始化：对于$l \in [L]$，$\mathcal{C}$将B_l, D_l的生成方式修改为

$$B_l = g_1^{\alpha} A_l^{\beta} \left(g_2 g_3 \right)^{\tau_l}, D_l = g_1^{\frac{-\beta t_l}{b}} \left(g_2 g_3 \right)^{d_l} \tag{28}$$

这一步的目的是逐步将正常槽位转换为半功能槽位，依然是将g_2元素嵌入上述组件中。半功能密文与半功能槽位生成的半功能私钥中都含有g_2元素，因此将会导致解密失败。现在将这一步的修改分为2个部分讨论：关于B_l的修改，本方案沿用RABE中安全分析的修改方式，若RABE的证明方法是正确的，可以认为$\mathcal{A}$无法分辨$\mathrm{Hyb}_{2,l}^{(\sigma)}$与$\mathrm{Hyb}_{2,l-1}^{(\sigma)}$中的$B_l$组件；若子群判定假设中的假设2成立，$\mathcal{A}$无法分辨$\mathrm{Hyb}_{2,l}^{(\sigma)}$与$\mathrm{Hyb}_{2,l-1}^{(\sigma)}$中的$D_l$组件。综上所述，若RABE是安全的，且子群判定假设中的假设2成立，则对于多项式敌手$\mathcal{A}$与$\sigma' = \{0,1\}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda \in N$，有

$$\left| \Pr\left[\mathrm{Hyb}_{2,l-1}^{(\sigma)}(\mathcal{A}) = 1 \right] - \Pr\left[\mathrm{Hyb}_{2,l}^{(\sigma)}(\mathcal{A}) = 1 \right] \right| = \mathrm{negl}(\lambda) \tag{29}$$

5) $\mathrm{Hyb}_{\mathrm{rand}}^{(\sigma)}$：$\mathrm{Hyb}_{\mathrm{rand}}^{(\sigma)}$与$\mathrm{Hyb}_{2,L}^{(\sigma)}$相比，仅需将密文中的$C_1$组件替换为$\mathbb{G}_T$中的随机元素即可。根据双系统方法，当半功能槽位转换完毕之后，C_1可以替换成同类型的随机元素。即：若子群判定假设中的假设3成立，对于多项式敌手$\mathcal{A}$与$\sigma' = \{0,1\}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda \in N$，有

$$\left| \Pr\left[\mathrm{Hyb}_{2,l}^{(\sigma)}(\mathcal{A}) = 1 \right] - \Pr\left[\mathrm{Hyb}_{\mathrm{rand}}^{(\sigma)}(\mathcal{A}) = 1 \right] \right| = \mathrm{negl}(\lambda) \tag{30}$$

此时，$\mathcal{A}$无法从完全独立于挑战明文μ_σ^*的C_1组件中获取任何明文信息，即：对于多项式敌手$\mathcal{A}$与$\sigma' = \{0,1\}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda \in N$，有

$$\left| \Pr[\sigma' = 1 : \sigma = 0] - \Pr[\sigma' = 1 : \sigma = 1] \right| = \mathrm{negl}(\lambda) \tag{31}$$

证毕。

5.2 撤销机制安全性

1) 撤销伪造

定理2 若VTR-RABE是IND-CPA安全的，则VTR-RABE不可被伪造撤销组件。

证明 VTR-RABE的不可撤销伪造由敌手$\mathcal{A}$与挑战者$\mathcal{C}$之间的安全游戏证明。假设$\mathcal{A}$可以伪造撤销组件，$\mathcal{C}$可以向一个VTR-RABE加密预言机$\mathcal{O}$进行查询，其以攻破VTR-RABE的IND-CPA安全为目标。

首先，$\mathcal{C}$向$\mathcal{O}$申请注册一个槽位i，并向合法密文ct发起挑战，其中，S_i满足密文ct的访问策略需求，且$(\mathrm{ID}_i, \mathrm{id}_i) \in \mathcal{R}$。随后$\mathcal{C}$在区块链中查询到crs，将其发送给$\mathcal{A}$，并要求$\mathcal{A}$针对$\mathrm{id}_i$伪造可绕过撤销解密的私钥组件。若$\mathcal{A}$成功伪造了撤销组件$(\mathrm{id}_i, D_i', E_i')$，则$\mathcal{C}$以$\mathrm{hsk}_i' = \left(\mathrm{mpk}, i, \mathrm{id}_i, S_i, A_i, B_i, D_i', E_i', \hat{V}_i, \left\{ \hat{W}_{i,w} \right\}_{w \in \mathcal{U}} \right)$与$\mathrm{sk}_i = r_i$为输入，执行算法$\mathrm{OutDec}(\mathrm{hsk}_i', \mathrm{ct}, \mathcal{R})$和$\mathrm{UserDec}(\mathrm{sk}_i, \mathrm{sct})$，即可成功解密ct，此时$\mathcal{A}$伪造撤销组件的优势直接转化为$\mathcal{C}$攻破VTR-RABE的IND-CPA安全性的优势。证毕。

2) 前向和后向安全性

定理3 若VTR-RABE是IND-CPA安全的，则VTR-RABE的撤销机制满足前向和后向安全性。

证明　撤销机制的前向和后向安全性由敌手$\mathcal{A}$与挑战者$\mathcal{C}$之间的安全游戏证明。假设$\mathcal{A}$可以攻破撤销机制的前向和后向安全性，$\mathcal{C}$可以向一个VTR-RABE加密预言机$\mathcal{O}$进行查询，其以攻破VTR-RABE的IND-CPA安全为目标。

初始化、查询阶段：$\mathcal{C}$调用$\mathcal{O}$的初始化、属性验证以及私钥生成阶段算法分别与$\mathcal{A}$进行正常交互。

挑战阶段：$\mathcal{A}$提交撤销前的撤销列表$\mathcal{R}$、被撤销的用户集合$\left\{\left(\mathrm{ID}^{(1)},\mathrm{id}^{(1)}\right),\cdots\left(\mathrm{ID}^{(x)},\mathrm{id}^{(x)}\right)\right\}$，要挑战的访问策略$P^*=(\boldsymbol{M},\rho)$以及2个等长的消息$\mu_0^*,\mu_1^*$，其中要求不在撤销列表$\mathcal{R}$中的用户属性集不可满足访问策略需求。随后$\mathcal{C}$计算撤销后的撤销列表$\mathcal{R}'=\mathcal{R}\cup\left\{\left(\mathrm{ID}^{(1)},\mathrm{id}^{(1)}\right),\cdots\left(\mathrm{ID}^{(x)},\mathrm{id}^{(x)}\right)\right\}$，同时对于$\sigma\in\{0,1\}$，执行$\mathrm{Encrypt}(\mathrm{mpk},(\boldsymbol{M},\rho),\mu_\sigma^*,\mathcal{R}')$生成挑战密文$\mathrm{ct}^*$。

猜测阶段：$\mathcal{A}$输出对σ的猜测$\sigma'\in\{0,1\}$，$\mathcal{C}$将σ'作为对$\mathcal{O}$的挑战密文的猜测。

前向安全性：撤销发生之后，DO会根据新的撤销列表添加此次被撤销的DU的密文分量。此外，更新密文之后，原密文将被删除。此时任意用户无法分辨执行Update算法和直接执行Encrypt算法得到的挑战密文。因此根据安全游戏，$\mathcal{A}$攻破撤销机制前向安全性的优势直接转化为$\mathcal{C}$攻破VTR-RABE的IND-CPA安全性的优势。即：若VTR-RABE是IND-CPA安全的，则撤销机制满足前向安全性。

后向安全性：由于撤销前后用户的私钥不会发生任何更新，因此以更新后的$\mathcal{R}'$为输入计算出的挑战密文和直接初始化撤销列表$\mathcal{R}'$为输入计算出的挑战密文在任意用户视角下无法区分。根据安全游戏，$\mathcal{A}$攻破撤销机制后向安全性的优势直接转化为$\mathcal{C}$攻破VTR-RABE的IND-CPA安全性的优势。即：若VTR-RABE是IND-CPA安全的，则撤销机制满足后向安全性。证毕。

5.3　原始白盒可追踪性

定理4　若VTR-RABE是IND-CPA安全的，则VTR-RABE是原始白盒可追踪的。

证明　原始白盒可追踪性由敌手$\mathcal{A}$与挑战者$\mathcal{C}$之间的安全游戏证明。假设$\mathcal{A}$可以攻破原始白盒可追踪性，$\mathcal{C}$可以向一个VTR-RABE加密预言机$\mathcal{O}$进行查询，以攻破VTR-RABE的IND-CPA安全为目标。

初始化：$\mathcal{C}$初始化$\mathrm{idl}\leftarrow\varnothing$和$\mathrm{skl}\leftarrow\varnothing$，调用$\mathcal{O}$的初始化、属性验证以及私钥生成阶段算法分别与$\mathcal{A}$进行正常交互，生成$\{\mathrm{hsk}_i,\mathrm{sk}_i\}_{i\in[L]}$，并将crs和$\{\mathrm{hsk}_i\}_{i\in[L]}$发送给$\mathcal{A}$。

查询：$\mathcal{A}$向$\mathcal{C}$查询一系列私钥$\{\mathrm{sk}_i\}_{i\in[\mathcal{L}]\subset[L]}$，$\mathcal{C}$将$\{\mathrm{id}_i\}_{i\in[\mathcal{L}]\subset[L]}$加入集合idl中，将$\{\mathrm{sk}_i\}_{i\in[\mathcal{L}]\subset[L]}$加入集合skl中。

私钥伪造：$\mathcal{A}$输出一个解密元组$(\mathrm{hsk}_*,\mathrm{sk}_*)$，$\mathcal{C}$将$(\mathrm{hsk}_*,\mathrm{sk}_*)$作为对$\mathcal{O}$攻击私钥。

由于本文的原始白盒可追踪性安全模型要求敌手$\mathcal{A}$提交的私钥是标准格式的私钥，因此若$\mathrm{sk}_*\in\mathrm{skl}$且$\mathrm{Trace}\left(\mathrm{hsk}_*\right)\notin\mathrm{idl}\cup\perp$，则证明$\mathrm{sk}_*$与$\mathrm{hsk}_*$分属于不同的用户，这实际上是一种串谋攻击方式，因此若$\mathcal{A}$输出的解密元组$(\mathrm{hsk}_*,\mathrm{sk}_*)$可以进行正常解密，则$\mathcal{C}$也可以通过串谋攻击攻破VTR-RABE的IND-CPA安全。

值得一提的是，即使VTR-RABE无法追踪非原始密钥，其在IoMT数据共享场景下仍具有显著作用。对于更为普遍的单个内部人员直接共享或出售其私钥的情况（而非多恶意用户构建的高级解密器），VTR-RABE可以快速追踪到恶意用户的身份，并予以撤销或警告。证毕。

5.4　属性验证机制安全性

威胁模型设定：攻击者可以从区块链和恶意用户处获取信息，即可获得恶意用户的凭证集合$\mathrm{malicertlist}=\{\mathrm{cert}_1,\mathrm{cert}_2,\cdots,\mathrm{cert}_t\}$，同时也可以观察到正常用户的验证信息$h^*,k^*,\mathrm{ID}^*$。

属性验证机制安全性由敌手$\mathcal{A}$和模拟器$\mathcal{C}$之间的攻防游戏证明，分别分析隐私保护性和验证可靠性。

定理5　隐私保护性。假设所采用的哈希函数H是单向的，则对于任何PPT敌手$\mathcal{A}$，其成功从公开的验证信息h^*,k^*,ID^*中恢复出用户敏感凭证编号num^*的优势是可忽略的。其中哈希函数的单向性为：对于所有的PPT敌手$\mathcal{A}$，存在一个可忽略的函数$\mathrm{negl}(\cdot)$，使对于所有的$\lambda\in\mathbb{N}$，有

$$\Pr\left[\mathcal{A}(y)=x:y\leftarrow H(x)\right]=\mathrm{negl}(\lambda)\tag{32}$$

证明　假设存在一个PPT敌手$\mathcal{A}$能够以不可忽略的优势从h^*,k^*,ID^*中恢复出num^*，那么可以构

造一个模拟器$\mathcal{C}$，旨在破解哈希函数H的单向性。$\mathcal{C}$接收到一个单向函数挑战$y \leftarrow H(x)$后，设置$y = h^*$，如果$\mathcal{A}$成功输出了num^*，则$\mathcal{C}$计算$r^* = H(s^* \| \text{attr}^* \| \text{num}^*)$，得出$x = \text{num}^* \| r^*$，即成功破解了$H$的单向性；此时$\mathcal{A}$的优势直接转化为$\mathcal{C}$破解单向性的优势，与$H$的单向性假设矛盾。证毕。

定理6 验证可靠性，假设所采用的数字签名方案满足EUF-CMA安全，则对于任何PPT敌手$\mathcal{A}$，其成功伪造恶意用户ID′一个关于新属性attr′的有效验证信息（即签名k'）的优势是可忽略的。

同样通过归约来证明。假设存在一个PPT敌手$\mathcal{A}$能够以不可忽略的优势伪造一个有效的属性验证申请，即针对一个新的三元组$(h',\text{ID}',\text{attr}')$（此前未被签名过）产生一个有效的签名$k'$。可以构造一个模拟器$\mathcal{C}$，旨在破解签名方案的EUF-CMA安全性。$\mathcal{C}$拥有对签名预言机$\text{Sign}(\text{sk},\cdot)$的访问权限，但其不知道签名私钥sk。$\mathcal{C}$为$\mathcal{A}$模拟整个系统的运行环境。当$\mathcal{A}$要对某个属性$(h_i,\text{ID}_i,\text{attr}_i)$进行签名时，$\mathcal{C}$将其转发给自身的签名预言机并将返回的签名$k_i = \text{Sign}(\text{sk},h_i \| \text{ID}_i \| \text{attr}_i)$交给$\mathcal{A}$。最终，如果$\mathcal{A}$输出一个关于新元组$(h',\text{ID}',\text{attr}')$的有效伪造$k'$，则$\mathcal{C}$即可输出$k'$作为其对签名方案的伪造。因此，$\mathcal{A}$的成功优势直接转化为$\mathcal{C}$攻破EUF-CMA安全的优势。证毕。

5.5 外包解密机制安全性

在VTR-RABE中，将由KC生成的hsk作为外包解密密钥发送给OS，而用户保留sk。由于hsk是由半可信的KC公开生成的，其本身不包含任何敏感信息，属于可公开的密钥组件。因此，将其提供给OS并不会泄露任何额外信息以降低系统安全性。基于此，若VTR-RABE方案本身是IND-CPA安全的，则其外包解密机制在该安全模型下同样是安全的。外包解密过程的安全性可直接归约于原方案的安全性。

6 分析与实验

6.1 功能分析

VTR-RABE与各个方案的功能对比如表1所示。由表1可知，VTR-RABE是目前唯一一个支持属性验证、白盒追踪、全局撤销和外包解密的RABE方案，是一个功能更加完备的IoMT数据共享方案。

表1 VTR-RABE与各个方案的功能对比

	基于注册	属性验证	可追踪	可撤销	外包解密
文献[9]	√	×	×	×	×
文献[13]	√	×	×	×	×
文献[15]	×	×	×	√	×
文献[17]	×	×	√	√	×
文献[25]	√	×	×	√	×
文献[26]	√	×	√	√	√
VTR-RABE	√	√	√	√	√

6.2 性能分析

为全面评估VTR-RABE的性能表现，本文选取了3个最具代表性的相关工作作为基准进行对比分析，分别是Hohenberger等[9]提出的基础RABE方案（记为RABE）、Li等[25]提出的支持精准撤销的RABE方案（记为RRABE）和Wang等[26]提出的支持密钥穿刺的RABE方案（记为PR-ABE），旨在通过理论分析，综合展示VTR-RABE在计算开销与通信开销等方面的性能表现。本文在分析过程中仅标识最大量级的计算和存储开销，分析过程中需要用到的符号定义如表2所示。

表2 符号定义

符号	含义
$\|U\|$	系统属性个数
$\|L\|$	系统设定槽位个数
$\|M\|$	加密所需属性个数
$\|I\|$	解密所需属性个数
$\|V\|$	最大可穿刺次数
$\|X\|$	密钥已被穿刺次数
$\|R\|$	撤销列表中元素个数
E	群G中的指数运算
E_T	群G_T中的指数运算
P	双线性对运算
$\|G\|$	群G中的一个元素大小
$\|G_T\|$	群G_T中的一个元素大小

1) 计算开销对比

各个方案的计算开销对比如表3所示。表3中列出的“撤销”操作开销，已综合考虑了追踪、撤销、密文更新及密钥更新等相关步骤的总成本。由于各个方案的私钥验证计算开销都是$|L|P$，私钥聚合步骤都仅有乘法运算，因此这2个步骤未在表

中展示。由表3可知，尽管VTR-RABE在公共参考字符串中集成了撤销组件，但其初始化阶段的计算开销与基础的RABE相比，并未出现显著（量级上）的增长。与PR-ABE类似，由于在加密与解密算法中引入了额外功能组件（VTR-RABE需处理撤销列表，PR-ABE需处理穿刺组件），其本地计算开销相较于基础的RABE方案有所增加。然而，VTR-RABE与PR-ABE均支持外包解密，能将绝大部分计算密集型解密任务转移至外包服务器。因此，与DU的本地计算开销对比，VTR-RABE和PR-ABE相较于不支持外包解密的RABE和RRABE方案，具有压倒性优势。RRABE实现了2种撤销机制，其计算开销均与系统用户数线性相关。相比于RRABE和PR-ABE，VTR-RABE的撤销操作仅需极低的、常数级别的计算开销，显著优于RRABE和PR-ABE。

2) 存储开销对比

各个方案的存储开销对比如表4所示。VTR-RABE的公共参考字符串、私钥、主公钥以及辅助解密密钥的大小与RABE方案相比均保持了同一量级，未因新增功能而引入显著额外开销。在密文尺寸方面，由于VTR-RABE将撤销列表嵌入密文中，其存储开销相对于RABE和RRABE有所提高，但作为实现安全的系统级用户撤销的RABE方案，这是可接受的代价。

6.3　实验对比

为了评估VTR-RABE的性能，本文对比了VTR-RABE与RABE、RRABE、PR-ABE密码算法的计算开销，并测试了所采用区块链算法的计算开销，每个实验进行50轮，取平均值作为最终的实验结果。密码学实验使用基于配对的Java密码学库（JPBC）中的A类椭圆曲线实现，其中，VTR-RABE、RABE和RRABE使用到的三素数合数阶群中的每个素数子群，以及PR-ABE使用到的素数阶群的群阶都为128位。除此之外，本文使用Remix IDE平台模拟以太坊区块链以测试智能合约算法的性能，主要关注gas消耗量以及估算的实际价格成本。价格成本计算公式为：总费用= gas用量×gas单价（Gwei）×Gwei比率（ETH）× ETH单价，其中，Gwei比率固定（1 Gwei = 10^{-9} ETH），设定常规场景下gas单价（1 gas = 30 Gwei）和ETH单价（1 ETH = $3 000）。实验平台为：Apple M1芯片，内存为16 GB，系统为macOS Monterey。

以U和L为变量，各个方案的初始化计算开销分别如图3和图4所示。由图3和图4可以看出，VTR-RABE在初始化阶段的计算开销与RABE相差不大，这表明在槽位组件中嵌入用户身份信息所带来的额外开销是可接受的；PR-ABE因其基于计算效率更高的素数阶群构建，故在此阶段展现出更优的性能。

表3　　**计算开销对比**

方案	初始化	私钥生成	加密	外包解密	用户解密	追踪	撤销
RABE	$\|L\|^2\|U\|E$	$\|L\|E$	$2\|M\|E$	—	$2\|I\|P + \|I\|E_T$	—	—
RRABE	$\|L\|^2\|U\|E$	$\|L\|E$	$2\|M\|E$	—	$2\|I\|P + \|I\|E_T$	—	$\|L\|E$
PR-ABE	$\|L\|^2\|U\|E$	$(\|V\|+\|L\|+3\|X\|)E$	$2\|M\|E + 2\|V\|E$	$\|V\|\|X\|E$	E	$3P$	$2\|V\|E$
VTR-RABE	$\|L\|^2\|U\|E$	$\|L\|E$	$2\|M\|E + 3\|R\|E$	$2\|I\|P + \|I\|E_T + 2\|R\|P + \|R\|E_T$	E_T	$3P$	$3E + E_T$

表4　　**存储开销对比**

方案	公共参考字符串	私钥	主公钥	辅助解密密钥	密文
RABE	$\|L\|^2\|U\|\|G\|$	0	$\|U\|\|G\|$	$\|U\|\|G\|$	$\|M\|\|G\|$
RRABE	$\|L\|^2\|U\|\|G\|$	0	$\|U\|\|G\|$	$\|U\|\|G\|$	$\|M\|\|G\|$
PR-ABE	$\|L\|^2\|U\|\|G\|$	$3\|X\|E$	$\|U\|\|G\|+\|V\|\|G\|$	$\|U\|\|G\|$	$\|M\|\|G\|+\|V\|\|G\|$
VTR-RABE	$\|L\|^2\|U\|\|G\|$	0	$\|U\|\|G\|$	$\|U\|\|G\|$	$\|M\|\|G\|+2\|R\|\|G\|$

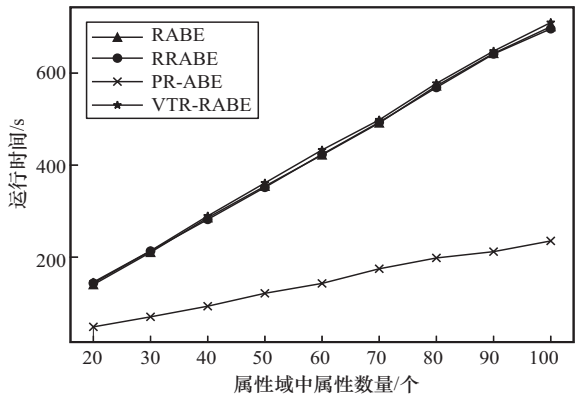

图 3 初始化计算开销（变量为 U）

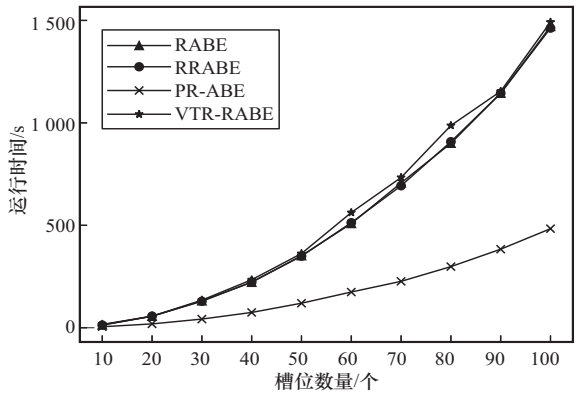

图 4 初始化计算开销（变量为 L）

私钥生成阶段计算开销如图 5 所示。设定 PR-ABE 的最大可穿刺次数为 50，PR-ABE 因需生成与最大可穿刺次数相关的密钥组件，其开销显著高于其他方案；VTR-RABE、RABE 及 RRABE 的私钥生成逻辑相似，故开销相近。

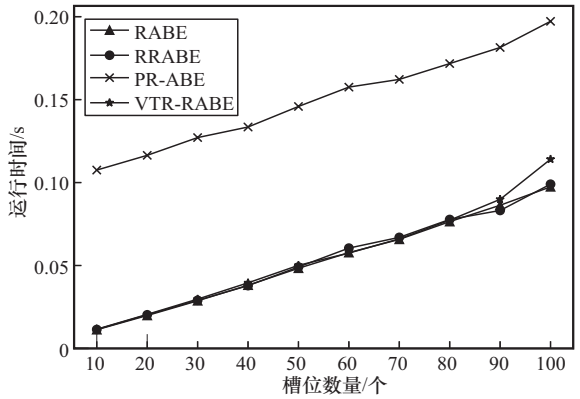

图 5 私钥生成计算开销

加密阶段的计算开销如图 6 所示。设定 VTR-RABE 的撤销列表长度为 20，为支持高级功能（VTR-RABE 的撤销列表与 PR-ABE 的穿刺组件），两者均引入了额外的计算开销，因此其加密耗时高于基础的 RABE 方案。

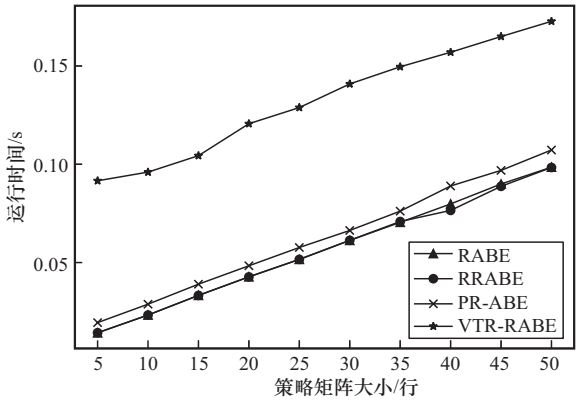

图 6 加密计算开销

用户自身的解密计算开销如图 7 所示。得益于外包解密机制，VTR-RABE 与 PR-ABE 将绝大部分计算转移至服务器端，使用户本地的解密开销降至极低的常数级别。

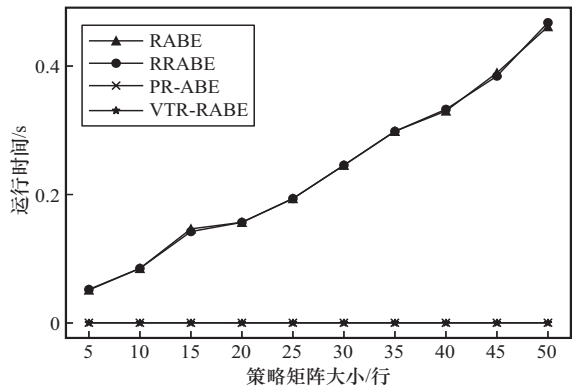

图 7 解密计算开销

以 L、撤销密文数量及撤销用户数量为变量时，各方案的撤销操作总开销分别如图 8、图 9 和图 10 所示，包含追踪、撤销、私钥更新以及密文更新等所有相关步骤，其中 RRABE 实现了 2 种撤销机制（RRABE.a 为精准撤销，RRABE.b 为用户注销）。由图 8 可知，VTR-RABE 与 PR-ABE 的撤销计算开销与 L 线性无关，优势明显；由图 9 可知，RRABE.a 与 VTR-RABE 的撤销计算开销随更新的密文数量增长而增长，但 VTR-RABE 相比于 RRABE. a 增长速度更加缓慢；由图 10 可知，RRABE.b 的撤销计算开销随着单次撤销用户数量的增长而降低，RRABE.a、PR-ABE 和 VTR-RABE

的撤销计算开销则与撤销用户数量正相关，但VTR-RABE不仅在三者中增速最慢，与RRABE.b相比，在单次撤销用户数量小于7时，VTR-RABE的撤销效率都要优于RRABE.b。

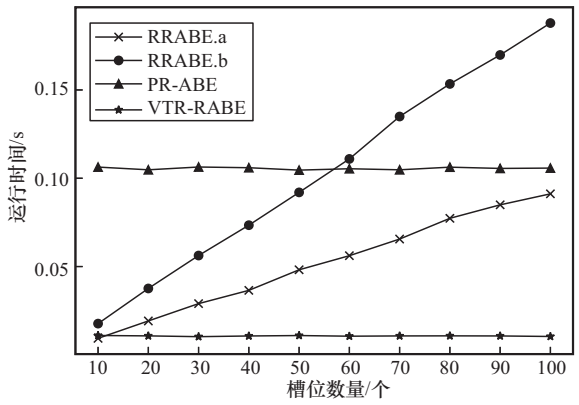

图8　撤销计算开销（变量为L）

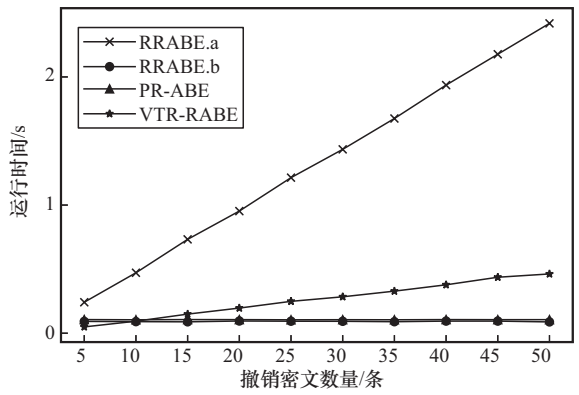

图9　撤销计算开销（变量为撤销密文数量）

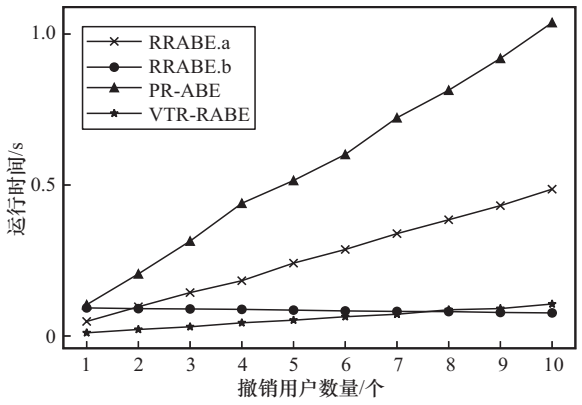

图10　撤销计算开销（变量为撤销用户数量）

链上用户信息操作开销如图11所示，其中的添加操作包括对用户每个属性进行验证以及将其存储到列表。由图11可知，添加和查询操作的计算开销都与该用户拥有的属性数量正相关，当用户属性数量为50时，添加此用户的操作需要消耗1.62×10^6 gas，而查询该用户仅需1.77×10^5 gas。在实际IoMT应用场景下，假设每个医生平均拥有10个属性，系统内含有100个医生时，存储所有用户信息的成本约为3.68×10^7 gas。按照常规网络拥堵程度，所有医生信息的整体存储价格成本约为$3 312。对于一个医疗系统来说，这个成本是完全可接受的。

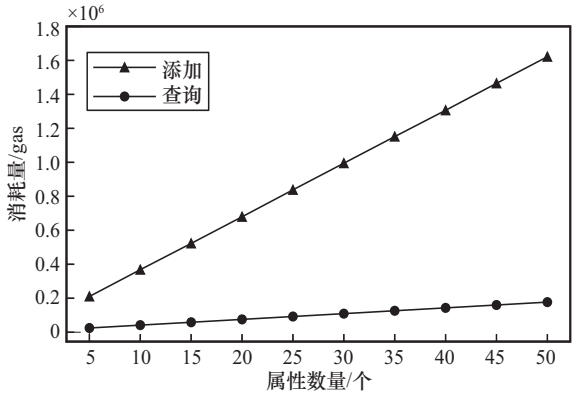

图11　链上用户信息操作开销

7　结束语

本文面向IoMT等数据敏感性较强的场景下数据安全共享的迫切需求，针对现有RABE方案在实际部署中的功能性缺陷，提出了一种兼具高安全性与实用性的新型RABE方案——VTR-RABE。首先，针对RABE框架中属性验证环节缺失所引发的属性伪造风险，创新性地基于区块链与智能合约技术设计了半隐私属性验证机制，从源头确保了用户只能为其真实合法拥有的属性集申请密钥。其次，为应对私钥滥用威胁，提出了RABE框架下的原始白盒追踪方案，并实现了高效的系统级即时撤销机制，使系统能够在发现恶意行为后快速定位责任主体并立即剥夺其访问权限。此外，为缓解IoMT终端设备的计算压力，实现了外包解密功能，将最耗时的双线性对计算转移至云服务器。在安全性方面，通过严格的形式化安全证明，证实了VTR-RABE满足IND-CPA安全，验证了撤销、追踪、属性验证和外包计算的安全性。在性能方面，理论与实验分析表明，VTR-RABE以可接受的计算与存储开销为代价，实现了功能性的全面增强，最终达成安全、效率与功能性的良好平衡，充分证明了其在实际IoMT环境中应用的巨大潜力。

参考文献：

[1] BAO Z J, HE D B, WANG H Q, et al. A group signature scheme with selective linkability and traceability for blockchain-based data sharing systems in E-health services[J]. IEEE Internet of Things Journal, 2023, 10(23): 21115-21128.

[2] XU G, FAN X Y, XU S Y, et al. Anonymity-enhanced sequential multi-signer ring signature for secure medical data sharing in IoMT[J]. IEEE Transactions on Information Forensics and Security, 2025, 20: 5647-5662.

[3] 谢晴晴, 宋亮晴, 冯霞. 面向医疗数据分享的轻量级且安全的搜索方案[J]. 通信学报, 2024, 45(11): 206-222.
XIE Q Q, SONG L Q, FENG X. Lightweight and secure search scheme for medical data sharing[J]. Journal on Communications, 2024, 45(11): 206-222.

[4] 俞惠芳, 李磊. 基于椭圆曲线签密的跨链医疗数据共享方案[J]. 通信学报, 2024, 45(12): 57-66.
YU H F, LI L. Cross-chain medical data sharing scheme based on elliptic curve signcryption[J]. Journal on Communications, 2024, 45(12): 57-66.

[5] 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 Press, 2007: 321-334.

[6] LIU X, WEI Z Y, LI G X, et al. An enhanced traceable access control scheme based on multi-authority CP-ABE for cloud-assisted e-health system[J]. Computer Networks, 2024, 254: 110766.

[7] ZHAO J, ZHANG K, GONG J Q, et al. Lavida: large-universe, verifiable, and dynamic fine-grained access control for E-health cloud[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 2732-2745.

[8] WANG Y S, ZHOU J, CAO Z F, et al. MuEOC: efficient SGX-based multi-key homomorphic outsourcing computation for E-health system[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(3): 2103-2118.

[9] HOHENBERGER S, LU G, WATERS B, et al. Registered attribute-based encryption[C]//Advances in Cryptology – EUROCRYPT 2023. Berlin: Springer, 2023: 511-542.

[10] ZHU Z Q, ZHANG K, GONG J Q, et al. Registered ABE via predicate encodings[C]//Advances in Cryptology – ASIACRYPT 2023. Berlin: Springer, 2023: 66-97.

[11] ATTRAPADUNG N, TOMIDA J. A modular approach to registered ABE for unbounded predicates[C]// Advances in cryptology - CRYPTO 2024. Berlin: Springer, 2024: 280-316.

[12] GARG R, LU G, WATERS B, et al. Reducing the CRS size in registered ABE systems[C]// Advances in cryptology - CRYPTO 2024. Berlin: Springer, 2024: 143-177.

[13] LU G, WATERS B, WU D J. Multi-authority registered attribute-based encryption[C]// Advances in cryptology - EUROCRYPT 2025. Berlin: Springer, 2025: 3-33.

[14] TAHERPOUR A, WANG X D. A high-throughput and secure coded blockchain for IoT[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(4): 3561-3579.

[15] LI Q, XIA B, HUANG H P, et al. TRAC: traceable and revocable access control scheme for mHealth in 5G-enabled IIoT[J]. IEEE Transactions on Industrial Informatics, 2022, 18(5): 3437-3448.

[16] MA R N, ZHANG L Y, WU Q, et al. BE-TRDSS: blockchain-enabled secure and efficient traceable-revocable data-sharing scheme in industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics, 2023, 19(11): 10821-10830.

[17] MENG F, CHENG L X. TSR-ABE: traceable and server-aided revocable ciphertext-policy attribute-based encryption under static assumptions[J]. IEEE Transactions on Information Forensics and Security, 2024, 20: 955-967.

[18] NING J T, CAO Z F, DONG X L, et al. Traceable CP-ABE with short ciphertexts: how to catch people selling decryption devices on eBay efficiently[C]//Computer Security – ESORICS 2016. Berlin: Springer, 2016: 551-569.

[19] LUO F C, AL-KUWARI S. Generic construction of black-box traceable attribute-based encryption[J]. IEEE Transactions on Cloud Computing, 2023, 11(1): 942-955.

[20] FAN K, LI W H, BAI Y H, et al. EIV-BT-ABE: efficient attribute-based encryption with black-box traceability based on encrypted identity vector[J]. IEEE Internet of Things Journal, 2024, 11(9): 15229-15240.

[21] 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.

[22] ZHANG L Y, LI X M, WU Q, et al. Blockchain-aided anonymous traceable and revocable access control scheme with dynamic policy updating for the cloud IoT[J]. IEEE Internet of Things Journal, 2024, 11(1): 526-542.

[23] ZHOU J, CAO Z F, DONG X L, et al. TR-MABE: White-box traceable and revocable multi-authority attribute-based encryption and its applications to multi-level privacy-preserving e-healthcare cloud computing systems[C]//Proceedings of the 2015 IEEE Conference on Computer Communications (INFOCOM). Piscataway: IEEE Press, 2015: 2398-2406.

[24] HUANG X, XIONG H, CHEN J H, et al. Efficient revocable storage attribute-based encryption with arithmetic span programs in cloud-assisted Internet of things[J]. IEEE Transactions on Cloud Computing, 2023, 11(2): 1273-1285.

[25] LI J G, CHEN S B, LU Y, et al. Revocable registered attribute-based encryption with user deregistration[J]. IEEE Internet of Things Jour-

nal, 2025, 12(15): 31526-31535.

[26] WANG C H, MING Y, LIU H, et al. Puncturable registered ABE for vehicular social networks: enhancing security and practicality[J]. IEEE Transactions on Dependable and Secure Computing, 2025, 22(6): 5998-6011.

[27] LAI J Z, DENG R H, GUAN C W, et al. Attribute-based encryption with verifiable outsourced decryption[J]. IEEE Transactions on Information Forensics and Security, 2013, 8(8): 1343-1354.

[28] ZHANG L Y, YOU W T, MU Y. Secure outsourced attribute-based sharing framework for lightweight devices in smart health systems[J]. IEEE Transactions on Services Computing, 2022, 15(5): 3019-3030.

[29] WATERS B. Dual system encryption: realizing fully secure IBE and HIBE under simple assumptions[C]//Advances in Cryptology - CRYPTO 2009. Berlin: Springer, 2009: 619-636.

[作者简介]

李朋祥（1998– ），男，河南商丘人，南开大学博士生，主要研究方向为密码学应用、属性加密、访问控制。

王玥欢（2002– ），女，黑龙江哈尔滨人，南开大学硕士生，主要研究方向为密码学应用、属性加密、云安全。

贾春福（1966– ），男，河北文安人，博士，南开大学教授、博士生导师，主要研究方向为网络与信息安全、可信计算、恶意代码分析、密码学及应用等。

高敏芬（1968– ），女，天津人，南开大学高级工程师，主要研究方向为可证明安全、密码分析、密码学及应用等。