DOI: 10.19783/j.cnki.pspc.240771

电力数据多方共享的区块链可搜索加密方案

杨 锐，张瑞婷，翟社平

（西安邮电大学计算机学院，陕西 西安 710121）

摘要：新型电力系统对电力数据的共享提出了更高的要求，但现有电力数据共享方案仍然存在数据安全性不强、用户访问不受限、共享数据难以满足针对性需求等问题。为了解决这些问题，提出了一种可实现电力数据多方共享的区块链可搜索加密方案。结合条件广播代理重加密和公钥可搜索加密，保护了电力数据机密性，同时实现了关键词陷门搜索。代理重加密加入广播机制实现一次加密多用户共享，降低了数据拥有者的计算负担，并通过条件值设定实现细粒度访问控制。设计了加密电力数据多方搜索与共享模型，由区块链存储关键词文件编号索引并执行搜索，保障数据不可篡改且搜索可信。分析结果表明，该方案实现了电力数据的安全搜索与共享，其多用户可控共享适用于数据交换复杂的新型电力系统。

关键词：电力数据共享；可搜索加密；条件广播代理重加密；区块链；新型电力系统

Blockchain searchable encryption scheme for multi-user power data sharing

YANG Rui, ZHANG Ruiting, ZHAI Sheping

(School of Computer Science and Technology, Xi'an University of Posts and Telecommunications, Xi'an 710121, China)

Abstract: The new power system makes higher requirements for power data sharing, but the existing power data sharing schemes still have some problems, such as weak data security, unrestricted user access, and difficulty in meeting specific sharing needs. To solve these problems, a blockchain searchable encryption scheme for multi-user sharing of power data is proposed. By combining conditional broadcast proxy re-encryption and public key searchable encryption, the scheme protects the confidentiality of power data and realizes keyword trapdoor search. The integration of proxy re-encryption with a broadcasting mechanism enables encryption to be needed only once for multi-user sharing, reducing the computing burden of the data owner, and achieving fine-grained access control through conditional value setting. A multi-user search and sharing model of encrypted power data is designed, and a keyword file number is stored and indexed by the blockchain, so as to ensure that the data cannot be tampered with and that the search is reliable. The results show that the scheme realizes secure searching and sharing of power data, and that the multi-user controllable sharing is suitable for the new power system with complex data exchanges.

This work is supported by the Key Research and Development Program of Shaanxi Province (No. 2022GY-038).

Key words: power data sharing; searchable encryption; conditional broadcast proxy re-encryption; blockchain; new power system

0 引言

电力作为现代社会的基石，不仅促进了工业和经济的繁荣，也显著提升了人们的生活水平，成为日常生活中不可或缺的能源[1]。然而，面对当前日趋复杂的电网环境和急剧上升的用电需求，传统电力系统已经不堪重负；加之“双碳”目标的推进，迫切需要构建一个以创新为动力、以数字化和智能化为核心的新型电力系统[2]。与传统的单向电力传输模式不同，新型电力系统在数字化转型过程中，参与主体更多元，如交直流混合电网、微电网、局部直流电网和可控负荷等。同时，大量传感器的应用导致数据量激增，为数据挖掘提供了丰富的素材，也使得人工智能在多个应用场景中的预测分析得到了广泛应用。然而，在众多参与主体间的数据交换

基金项目：陕西省重点研发计划项目资助(2022GY-038)；西安邮电大学研究生创新基金资助(CXJJYL2022036)

中，数据安全问题日益凸显。在数据的流通、使用乃至资产化过程中，数据隐私保护变得尤为重要，一旦发生数据泄露，可能会对国家安全和经济发展造成严重威胁。因此，电网数据作为与国家安全和经济发展紧密相关的资产，其使用必须受到严格限制，以防止信息泄露等安全事件的发生。确保新型电力系统中多方参与者的数据安全，是维护整个系统网络安全的关键任务[3]。

可搜索加密是一种旨在不暴露数据内容的前提下实现数据搜索的技术，在数据共享过程中可以有效提供隐私保护。文献[4]基于非对称密码体制提出公钥可搜索加密方案(public key encryption with keyword search, PEKS)，解决了文献[5]提出的对称可搜索加密方案中仅有共享密钥的用户才可执行关键词搜索的问题。然而，文献[4]的方案需要预先使用数据使用者的公钥加密数据信息，多用户共享必然会增加数据拥有者的计算负担并需要其长期在线响应请求，因此无法满足实际应用的搜索与共享需求。针对 PEKS 实际应用中的多用户搜索需求，已有学者结合其他加密机制提出了不同应用场景下的解决方案，如：文献[6]面向智能交通系统中存在的出行信息被盗用、交通数据被恶意滥用等问题，增加密钥聚合和轻量计算功能，提出了一种新的属性基可搜索加密方案，保障了密钥和数据安全；文献[7]设计了一种支持多关键词查询的航天信息系统云存储数据可搜索加密算法，利用同态线性认证技术实现了多关键词动态查询；针对电子健康记录的安全存储与搜索问题，文献[8]提出了支持用户撤销的可搜索电子健康记录共享方案，使用长度固定的搜索陷门减少了用户开销，并基于变色龙哈希函数生成私钥，避免了未撤销用户频繁更新私钥的问题，从而提升了方案效率。与现有的许多解决方案相似，虽然上述方案允许多数据使用者进行加密搜索，但在实现用户搜索的细粒度控制和数据安全性保护方面仍然可以进一步优化。

文献[9]提出了代理重加密技术，增加中间代理使用重加密密钥转换公钥密文为数据共享提供了新思路。文献[10]将无证书签名与代理重加密结合，提出一种基于云可靠智能电网的实用访问控制的无证书签名代理重加密技术，可以在实现智能电网的数据安全性和身份验证的同时，推动云计算的广泛引用，但是该方案仅考虑数据加密外包，没有考虑智能电网应用中不同参与方的实际搜索需求。文献[11]将代理重加密加入基于身份的可搜索加密算法中，提出一种云环境下可解决搜索权限共享问题的新方案，但是在多用户环境中，数据属主需要为不同数据使用者多次计算重加密密钥，实际应用的计算开销太大。文献[12]提出了一种创新的加密方案，即条件广播代理重加密，这一方案在传统代理重加密的基础上引入了广播机制，允许数据所有者将解密权限下放给多个授权用户，并通过设置特定的条件值，实现在一对多场景中数据的细粒度安全共享。因此，在新型电力系统这种多用户环境中，将 PEKS 与条件代理重加密技术相结合，设计了一种用于电力数据搜索和共享的可搜索加密方案，不仅能够提高 PEKS 在实际应用中的灵活性和适应性，还能更好地满足对数据安全性和共享性的需求。

现有PEKS大多将数据外包给半可信的第三方执行搜索，但是出于经济利益驱使或是节约资源的目的，常有云服务商执行不实搜索甚至恶意窃取或篡改隐私数据。区块链是一个点对点的分布式账本，由哈希链接各个区块组成链表，以共识机制和经济激励共同维护网络安全可信[13]。以区块链取代传统云服务商执行搜索，可以确保数据上链不可篡改，链上搜索操作公开透明、可溯源，从而增强搜索过程中的数据安全性。文献[14]提出一种以患者为中心基于星际文件系统和区块链的电子病历安全存储与高效共享方案，执行以联盟链为中心的跨链电子病历搜索和代理重加密，并使用私有链存储索引降低联盟链存储压力，从而实现电子病历的安全存储与共享。文献[15]提出了一种支持联盟链上关键词密文检索的电子病历双重授权共享方案。为了解决智能病房中可穿戴和监控设备在定期传输数据过程中的数据安全性与访问威胁，文献[16]提出了一种区块链辅助的指定服务器的PEKS，从而实现一对多的安全搜索。面向电力数据应用，文献[17]将区块链与属性基加密技术结合，提出可实现一对多电力数据访问控制的数据共享方案，但是该方案只能将打包数据加密上传，无法执行关键词密文搜索。此外，文献[18-19]基于区块链，分别在交通、医疗等领域结合代理重加密技术设计了加密数据的搜索与共享方案。因此，区块链在不同应用领域为数据的安全搜索与共享提供了可信服务。

为了更好地满足 PEKS 在新型电力系统中的数据安全性和多用户可控共享需求，并解决云服务商不可信问题，本文基于区块链技术，将条件广播代理重加密与 PEKS 结合，提出了一种新型电力系统的数据安全搜索和可控共享方案。该方案基于链上数据难篡改、操作可溯源的特性，设计密文倒排索引存储在联盟链，由智能合约执行可信搜索，分离数据密文与索引从而降低数据泄露风险，主要工作如下：

1) 设计了一种支持新型电力系统多方用户参与的数据搜索与共享方案，结合条件广播代理重加密和传统公钥可搜索加密方案，通过广播机制实现一对多安全加密，设定条件值实现搜索密文可控共享；

2) 设计了一个新型电力系统的多方搜索模型，由可信联盟链取代云服务商提供搜索，将密文与索引分开存储，联盟链共识选举节点轮换担任权威管理者，从而降低中心化管理风险，提升数据安全性；

3) 设计了安全游戏证明搜索所得电力数据密文和关键词搜索陷门的安全性，理论分析证明方案可抵抗合谋攻击、实现多用户环境的细粒度访问控制，实验结果表明方案具有较好的安全性和实用价值。

1 密码学基础知识

1.1 双线性映射

设 G 是素数 p 阶加法循环群，G_{T} 是素数 p 阶乘法循环群。假设映射 $e:G\times G\to G_{\mathrm{T}}$ 为双线性映射，那么 e 需要满足以下性质。

性质 1(双线性)：$\forall g\in G,\alpha,\beta\in\mathbb{Z}_p^*$，有 $e(g^{\alpha},g^{\beta})=e(g,g)^{\alpha\beta}$。

性质 2(非退化性)：至少存在一个元素 g，使得 $e(g,g)\neq 1$。

性质 3 (可计算性)：$\forall g\in G$，存在与安全常数 ε 相关且可有效计算 $e(g,g)$ 的概率多项式时间算法。

1.2 决策性 n-BDHE 假设

决策性 n-BDHE 假设是基于 (G,G_{T}) 上的决策双线性 DH 指数(bilinear diffie-hellman exponent, BDHE)问题。假设双线性映射 $e:G\times G\to G_{\mathrm{T}}$，$g$ 是 G 的生成元。随机选取 $h\in G,\alpha\in\mathbb{Z}_p^*$，满足 $(g,g_1,g_2,\cdots,g_N,g_{N+2},\cdots,g_{2N},h)\in G^{2N+1},g_i=g^{\alpha^i}$，敌手 $\mathcal{A}$ 随机选取 $Q\in G_{\mathrm{T}}$，并判断 Q 是否与 $e(g,h)^{\alpha^{N+1}}=e(g_{N+1},h)$ 相等。敌手 $\mathcal{A}$ 成功的优势定义为式(1)，如果不存在概率多项式时间内的算法，使敌手 $\mathcal{A}$ 以不可忽略的优势 ε 在 (G,G_{T}) 上解决决策性 n-BDHE 问题，则该假设在 (G,G_{T}) 上成立。

$$Adv_{G,\mathcal{A}}^{\text{n-BDHE}}=\left|\begin{array}{l}\Pr\left[\mathcal{A}(g,g_1,g_2,\cdots,g_N,g_{N+2},\cdots,g_{2N},h,Q)=1\right]-\\ \Pr\left[\mathcal{A}\left(\begin{array}{l}g,g_1,g_2,\cdots,g_N,g_{N+2},\cdots,g_{2N},h,\\ e(g_{N+1},h)\end{array}\right)=1\right]\end{array}\right| \tag{1}$$

2 系统模型

本文的加密电力数据多方搜索与共享模型如图 1 所示，主要包括 5 个参与实体——权威管理者(authority manager, AM)、区块链(blockchain, BC)、数据拥有者(data owner, DO)、数据使用者(data user, DU)和云服务提供者(cloud service provider, CSP)。

1) 权威管理者

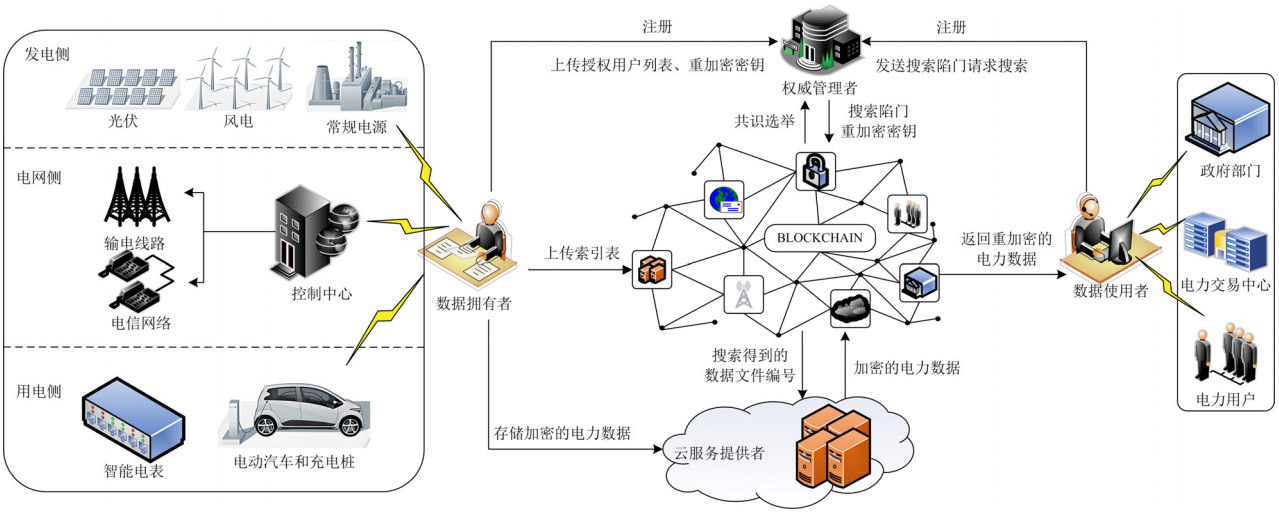

图 1 加密电力数据多方搜索与共享模型图

Fig. 1 Multi-user search and sharing model of encrypted power data

联盟链共识选举可信节点轮换担任 AM 为系统初始化参数。AM 接收来自 DO 的授权用户列表并初步验证 DU 权限，合法则发送搜索陷门给 BC 执行加密数据搜索，否则停止。此外，AM 为 DO 暂时管理重加密密钥，并在 BC 请求时发送密钥。在此过程中，AM 作恶会被撤销并降为普通节点。

2) 区块链

选择可信程度高的联盟链为 BC。DO 上传索引

表到 BC 存储，并为经过 AM 验证的 DU 执行搜索，成功则向 CS 和 AM 分别请求搜索结果对应的电力数据密文和重加密密钥，并为 DU 返回重加密数据；否则停止。在此过程中，BC 无法获知关键词和电力数据密文的任何信息。

3) 数据拥有者

DO 负责加密数据并外包给 CSP。加密的数据包括发电侧的新能源功率数据、发电竞价交易数据等，输电侧的多能源系统调度数据，用电侧的用户行为特征数据、电动车规划数据等。同时，DO 设计关联关键词密文与编号的索引表上传至 BC，并设定共享用户集的人数最大值 N 和授权用户列表，并生成重加密密钥发送给 AM。

4) 数据使用者

政府、营销中心等作为 DU 请求搜索并获取所需的电力数据。DU 使用私钥生成关键词搜索陷门作为搜索请求发送给 AM，接收 BC 返回的重加密搜索结果，解密并获取所需电力数据。

5) 云服务提供者

通常由第三方云服务器担任 CSP。DO 上传初始加密的电力数据到 CSP 存储，并返回 BC 请求的电力数据密文。在此过程中，CSP 无法获知电力数据密文的任何信息。

3　方案与安全模型设计

3.1 方案构建

基于可搜索加密、条件广播代理重加密和区块链等技术，本文设计了一种加密电力数据的多方搜索与共享方案，由以下 8 个阶段组成。假设授权用户集 S 的最多人数为 N，用户使用身份 ID 注册获得序号，即 $S=\{ID_1,\cdots,ID_N\}$，满足条件 dsp 的用户组为 $S'=\{ID_1',\cdots,ID_u'\},u\leqslant N$。

1) 系统初始化

$\mathrm{Setup}(\xi,N)\rightarrow(MSK,PK)$：BC 首先共识选举可信节点担任 AM，输入安全参数 ξ 和授权用户集的人数最大值 N，AM 按照如下步骤计算并输出主私钥 MSK 和系统公钥 PK。

(1) 随机选取 p 阶乘法循环群 G 和 G_{T}，其中 p 是大于 2^{ξ} 的素数，g 是 G 的生成元。定义双线性映射 $e:G\times G\rightarrow G_{\mathrm{T}}$，循环群 $\mathbb{Z}_p^*=\{1,2,\cdots,p-1\}$。

(2) 计算 $g_i=g^{\alpha^i}\in G(i=1,\cdots,N,N+2,\cdots,2N)$，其中随机选取 $\alpha\in_R\mathbb{Z}_p^*$。

(3) 随机选取 $h\in_R G$，定义函数 $\mathcal{F}(x)=hg_1^x$ 和三个目标抗碰撞哈希函数 $\mathcal{H}_1:\{0,1\}^*\rightarrow G$、$\mathcal{H}_2:G_{\mathrm{T}}\rightarrow\{0,1\}^{\log p}$ 和 $\mathcal{H}_3:G_{\mathrm{T}}\rightarrow G$。

(4) 随机选取 $\beta\in_R\mathbb{Z}_p^*$，计算 $y=g^{\beta}$。

(5) 系统内公开主私钥 $MSK=\beta$，系统公钥 $PK=(g,g_1,g_2,\cdots,g_N,g_{N+2},\cdots,g_{2N},\mathcal{F},y,\mathcal{H}_1,\mathcal{H}_2,\mathcal{H}_3)$。

2) 生成用户私钥

$\mathrm{KGen}(MSK,PK,i)\rightarrow sk_i$：用户(DO/DU)执行，输入系统公钥 PK，主私钥 MSK 和在 AM 注册后得到的序号 i，计算私钥为 $sk_i=g_i^{\beta}$，其中 $i\in S$。

3) 加密电力数据并生成关键词密文索引

DO 为授权用户集 S 中满足条件 dsp 的用户组 S' 加密电力数据再外包给 CSP，并为数据密文建立索引表上传到 BC 执行多方可控搜索与共享。假设 DO 拥有的原始电力数据集 $\mathcal{M}$ 中有 n 个数据文件，DO 执行如下步骤得到数据密文和索引。

(1) 为每个数据文件 $m_i\in\mathcal{M}$ 编号 $class_i$，其中 $1\leqslant i\leqslant n$。从 $\mathcal{M}$ 的数据文件中抽取若干关键词 w_j 组成关键词集 $\mathcal{D}ic=\{w_1,\cdots,w_r\}$，其中 $1\leqslant j\leqslant|\mathcal{D}ic|=r$。

(2) 根据数据文件与关键词的关联关系，生成形式为(关键词::{数据文件编号})的明文倒排索引。如关键词 $\{w_1,w_3,w_6,w_8\}$ 包含在编号为 $class_1$ 的数据文件，关键词 $\{w_1,w_2,w_5,w_8,w_9\}$ 包含在编号为 $class_2$ 的数据文件，关键词 $\{w_1,w_2,w_3,w_6,w_7\}$ 包含在编号为 $class_3$ 的数据文件，则索引可类似表示为 $(w_1::\{class_1,class_2,class_3\}),(w_3::\{class_1,class_2\})$。

(3) 由于哈希函数抗碰撞且具有单向性，为了数据文件编号的安全性，计算各文件编号的哈希函数值 $\mathcal{H}_1(class_1),\cdots,\mathcal{H}_1(class_n)$。

(4) $\mathrm{Enc_w}(PK,S,w)\rightarrow c_w$：对于授权用户集 $S=\{ID_1,\cdots,ID_N\}$，随机选取 $\delta\in_R\mathbb{Z}_p^*$，计算关键词集 $\mathcal{D}ic$ 中任意关键词 w_j 的密文为 $c_w=(c_w',c_w'')=\left(\left(\mathcal{H}_1(w)g\right)^{\delta},\left(y\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta}\right)$，其中 $1\leqslant j\leqslant r$。

(5) $\mathrm{Enc}(PK,S,dsp,m)\rightarrow c$：对于满足条件 dsp 的用户，随机选取 $\delta\in_R\mathbb{Z}_p^*$，计算数据集 $\mathcal{M}$ 中任意数据文件 m_i 的密文，如式(2)所示，其中 $1\leqslant i\leqslant n$。

$$c=(\dot{c},\ddot{c},\ddot{c}',\ddot{c}')=\left(m\cdot e(g_1,g_N)^{\delta},g^{\delta},\left(y\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta},\mathcal{F}(dsp)^{\delta}\right)\tag{2}$$

(6) 结合各文件编号的哈希函数值和关键词密文，基于步骤(2)的明文索引得到形式如 $(c_{w_1}::\{\mathcal{H}_1(class_1),\mathcal{H}_1(class_2),\mathcal{H}_1(class_3)\})$ 等的密文倒排索

引，打包 $\mathcal{D}ic$ 中的每个关键词密文索引生成倒排索引表 Tab，并上传到 BC 用于搜索。

(7) 结合各文件编号的哈希函数值和对应编号的数据文件密文，得到形式为 $\{(\mathcal{H}_1(class_1)::c_1),\cdots,(\mathcal{H}_1(class_n)::c_n)\}$ 的数据密文集 $\mathcal{C}$，打包后存储到 CSP。

4) 生成搜索陷门

任意序号为 $j(1\leqslant j\leqslant N, j\neq i)$ 的 DU 执行，选定待查询的关键词集 $\mathcal{W}=\{w_1,\cdots,w_q\},|\mathcal{W}|=q\geqslant 1$。对于 $\mathcal{W}$ 中每个关键词 w_k 的搜索陷门，按如下步骤计算。

(1) $\text{Trapdoor}(PK,sk_j,w)\rightarrow\tau_w$：输入系统公钥 PK，私钥 sk_j，随机选取 $\delta\in_R\mathbb{Z}_p^*$，计算 $\tau_w=(\tau_w',\tau_w'')=((\mathcal{H}_1(w)g)^{\delta},(g\cdot sk_j)^{\delta})$。

(2) DU 最终打包所有搜索陷门得到搜索陷门集 $T_{\mathcal{W}}=\{\tau_{w_1},\cdots,\tau_{w_q}\}$，并发送给 AM 请求搜索。

5) 生成重加密密钥

$\text{ReKGen}(PK,sk_i,dsp,S')\rightarrow rk_{i\rightarrow S'|dsp}$：序号为 i 的 DO 执行，对于授权用户集 S 中满足条件 dsp 的用户组 $S'=\{ID_1',\cdots,ID_u'\}$，按照如下步骤生成数据密文的重加密密钥用于多方可控共享。

(1) 随机选取 $\delta\in_R\mathbb{Z}_p^*,\lambda\in_R G_T$，计算式(3)。

$$\tilde{c}=(\tilde{c}_1,\tilde{c}_2,\tilde{c}_3,\tilde{c}_4)=\left(m\cdot\mathcal{H}_3(\lambda),\lambda\cdot e(g_1,g_N)^{\delta},g^{\delta},\left(y\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta}\right)\tag{3}$$

(2) 随机选取 $\nu\in_R\mathbb{Z}_p^*$，计算重加密密钥 $rk_{i\rightarrow S'|dsp}=(\tilde{r},\tilde{c})=(sk_i\cdot\mathcal{F}(dsp)^{\nu},\tilde{c})$ 并发送给 AM。

6) 执行搜索

$\text{Search}(PK,S,Tab,T_{\mathcal{W}})\rightarrow\mathcal{L}abel/\perp$：BC 执行，接收 AM 验证合格的 DU(序号为 j)发送的搜索陷门集 $T_{\mathcal{W}}=\{\tau_{w_1},\cdots,\tau_{w_q}\}$，按照如下步骤执行搜索。

(1) 初始化搜索结果 $\mathcal{L}abel$ 为 $\varnothing$。

(2) 对于搜索陷门集 $T_{\mathcal{W}}$ 中的每一个关键词搜索陷门 $\tau_{\tilde{w}}$，调用联盟链上部署的智能合约自动遍历倒排索引表 Tab，计算 $\mathcal{H}_2\left(e\left(c_w',\tau_{\tilde{w}}''\cdot\prod_{k\in S,k\neq j}g_{N+1-k+j}\right)\right)\stackrel{?}{=}\mathcal{H}_2(e(\tau_{\tilde{w}}',c_w''))$ 是否成立，不成立则停止搜索输出 $\perp$，说明 DU 数据搜索请求失败，AM 授权验证错误，将被撤销降为普通节点，BC 重新共识选举 AM。

(3) 成立则将该搜索陷门在 Tab 中对应的数据文件编号哈希值并入搜索结果 $\mathcal{L}abel$，重复步骤(2)直到 $\tau_{\tilde{w}}$ 全部计算完成，将 $\mathcal{L}abel$ 发送给 CSP，并向 AM 请求重加密密钥。

7) 搜索结果重加密

$\text{ReEnc}(PK,i,S,dsp,S',rk_{i\rightarrow S'|dsp},c)\rightarrow c_R$：BC 执行，对于 CSP 返回的与搜索结果 $\mathcal{L}abel$ 对应的数据密文集 $\mathcal{C}$ 中的每一个密文 c 以及 AM 发送的重加密密钥 $rk_{i\rightarrow S'|dsp}$，计算 $c_R'=\dot{c}\cdot e\left(\tilde{r}\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},\ddot{c}\right)\Big/e(g_i,\ddot{c})$ 和 $c_R''=\dddot{c}$，得到重加密数据密文 $c_R=(c_R',c_R'',\tilde{c})$，并返回给 DU。

8) 重解密与解密密文

$\text{Dec}_{\text{R}}(PK,sk_j,i,j,S,dsp,S',c_R)\rightarrow m/\perp$：任意搜索成功且满足条件 dsp 的 DU(序号为 j)，对于 BC 返回的重加密数据密文 c_R，计算 $g^{\nu}=\tilde{c}_1\Big/\mathcal{H}_3\left(\tilde{c}_2\cdot e\left(sk_j\cdot\prod_{k\in S',k\neq j}g_{N+1-k+j},\tilde{c}_3\right)\Big/e(g_i,\tilde{c}_4)\right)$，得到原始数据 $m=c_R'/e(g^{\nu},c_R'')$。

$\text{Dec}(PK,sk_i,i,S,dsp,c)\rightarrow m/\perp$：序号为 i 的 DO，对于加密的电力数据密文 c，计算原始数据 $m=\dot{c}\cdot e\left(sk_i\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},\ddot{c}\right)\Big/e(g_i,\dddot{c})$。

3.2 安全模型定义

定义 1：对于任意概率多项式时间的敌手 $\mathcal{A}$，ξ 为安全参数，如果存在一个可忽略的函数 $neg(\xi)$，满足 $Adv_{\text{E},\mathcal{A}}^{\text{IND-CCA}}<neg(\xi)$，那么这个方案 E 在选择密文攻击下具有不可区分性(indistinguishability under chosen ciphertext attack, IND-CCA)，或是语义安全的。

为了证明搜索所得电力数据密文满足 IND-CCA，本文设计敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的安全游戏 1 如下所述。

1) 初始化阶段。$\mathcal{A}$ 在授权用户集 $S=\{1,2,\cdots,N\}$ 下随机选取一个想要攻击的条件 dsp^* 和一个用户组 $U\subseteq S$。

2) 设置阶段。$\mathcal{C}$ 运行 $\text{Setup}(\xi,N)$ 获取主私钥 MSK 和系统公钥 PK，并将 PK 发送给 $\mathcal{A}$。

3) 查询阶段一。敌手 $\mathcal{A}$ 执行如下步骤。

(1) 用户私钥查询 $\text{Extract}(i)$：$\mathcal{C}$ 运行 $\text{KGen}(MSK,PK,i)$ 获取序号为 i 的用户私钥 sk_i，并返回给 $\mathcal{A}$。

(2) 重加密密钥查询 $\text{ReExtract}(i,S',dsp)$：$\mathcal{C}$ 使用步骤(1)生成的 sk_i，运行 $\text{ReKGen}(PK,sk_i,dsp,S')$ 获取重加密密钥 $rk_{i\rightarrow S'|dsp}$，并将 $rk_{i\rightarrow S'|dsp}$ 返回给 $\mathcal{A}$。

(3) 电力数据密文重加密查询 ReEncrypt(i,S,dsp,S',c)：$\mathcal{C}$ 使用步骤(2)生成的 $rk_{i\to S'|dsp}$，运行 ReEnc($PK,i,S,dsp,S',rk_{i\to S'|dsp},c$) 获取重加密搜索结果 c_R，并将 c_R 发送给 $\mathcal{A}$。

(4) 电力数据密文解密查询 $\text{Decrypt}_{\text{I}}(i,S,dsp,c)$：$\mathcal{C}$ 使用步骤(1)生成的 sk_i，运行 Dec(PK,sk_i,i,S,dsp,c) 获取原始电力数据 m，并将 m 发送给 $\mathcal{A}$。

(5) 电力数据重加密密文解密查询 $\text{Decrypt}_{\text{II}}(i,j,S,dsp,S',c_R)$：$\mathcal{C}$ 运行 KGen(MSK,PK,j) 获取序号为 j 的用户私钥 sk_j，再运行 $\text{Dec}_{\text{R}}(PK,sk_j,i,j,S,dsp,S',c_R)$ 获取原始电力数据 m，并将 m 发送给 $\mathcal{A}$。

4) 挑战阶段。$\mathcal{A}$ 选定两个长度一致的数据明文 (m_0,m_1)，$\mathcal{C}$ 运行 Enc(PK,U,dsp^*,m_b) 获取目标条件 dsp^* 和目标用户组 U 下明文的加密密文 c^*，其中 $b\in_R\{0,1\}$。

5) 查询阶段二。敌手 $\mathcal{A}$ 继续按照查询阶段一执行，除了以下的查询：

(1) 对于任意 $i\in U$，不可执行用户私钥查询 Extract(i)；

(2) 对于任意 $S',i\in U$ 和 $j\in S'$，不可执行用户私钥查询 Extract(j) 和重加密密钥查询 ReExtract(i,S',dsp^*)；

(3) 对于任意 $i\in U$，不可执行电力数据密文解密查询 $\text{Decrypt}_{\text{I}}(i,U,dsp^*,c^*)$；

(4) 对于任意 $S',i\in U$ 和 $j\in S'$，不可执行用户私钥查询 Extract(j) 和重加密查询 ReEncrypt(i,U,dsp^*,S',c^*)；

(5) 对于任意 S' 和 c_R^*，不可执行电力数据重加密密文解密查询 $\text{Decrypt}_{\text{II}}(i,j,U,dsp^*,S',c_R^*)$，并且 $\text{Dec}_{\text{R}}(PK,sk_j,i,j,U,dsp^*,S',c_R^*)\in\{m_0,m_1\}$，其中 $i\in U,j\in S'$；

6) 猜测阶段。$\mathcal{A}$ 输出猜测 $b'\in\{0,1\}$，如果 $b'=b$，那么敌手 $\mathcal{A}$ 游戏获胜，$\mathcal{A}$ 的获胜优势为 $Adv_{\text{Ec},\mathcal{A}}^{\text{IND-CCA}}=\left|\Pr[b'=b]-1/2\right|$。

如果对于任意概率多项式时间的敌手 $\mathcal{A}$，$Adv_{\text{Ec},\mathcal{A}}^{\text{IND-CCA}}<neg(\xi)$，即 $Adv_{\text{Ec},\mathcal{A}}^{\text{IND-CCA}}$ 可以忽略不计，那么证明本文搜索所得电力数据密文满足 IND-CCA。

定义 2：对于任意概率多项式时间的敌手 $\mathcal{A}$，ξ 为安全参数，如果存在一个可忽略的函数 $neg(\xi)$，满足 $Adv_{\text{E},\mathcal{A}}^{\text{IND-CKA}}<neg(\xi)$，那么这个方案 E 在选择关键词攻击下具有不可区分性(indistinguishability under chosen keyword attack, IND-CKA)，或是语义安全的。

为了证明关键词搜索陷门满足 IND-CKA，本文设计敌手 $\mathcal{A}$ 与挑战者 $\mathcal{C}$ 之间的安全游戏 2 如下。

1) 初始化阶段。$\mathcal{A}$ 在授权用户集 $S=\{1,2,\cdots,N\}$ 下，随机选取一个想要攻击的条件 dsp^* 和一个用户组 $U\subseteq S$。

2) 设置阶段。$\mathcal{C}$ 运行 Setup(ξ,N) 获取主私钥 MSK 和系统公钥 PK，并将 PK 发送给 $\mathcal{A}$。

3) 查询阶段。满足限制条件 $j^*\in U,j\in S,j^*\neq j$ 时，敌手 $\mathcal{A}$ 重复有限次执行如下步骤。

(1) 用户私钥查询 Extract(j)：$\mathcal{C}$ 运行 KGen(MSK,PK,j) 获取序号为 j 的用户私钥 sk_j，并返回给 $\mathcal{A}$；

(2) 搜索陷门查询 Trpd(j,S,w)：$\mathcal{C}$ 使用步骤(1)生成的 sk_j，运行 Trapdoor(PK,sk_j,w) 获取搜索陷门集 τ_w，并将 τ_w 返回给 $\mathcal{A}$。

4) 挑战阶段。$\mathcal{A}$ 选定两个长度一致的关键词 (w_0,w_1)，$\mathcal{C}$ 运行 KGen(MSK,PK,j^*) 获取序号为 j^* 的用户私钥 sk_{j^*}，再运行 Trapdoor(PK,sk_{j^*},w_b) 获取关键词搜索陷门 $\tau_{w_b}^*$，其中 $b\in_R\{0,1\}$。

5) 猜测阶段。$\mathcal{A}$ 输出猜测 $b'\in\{0,1\}$，如果 $b'=b$，那么敌手 $\mathcal{A}$ 游戏获胜，$\mathcal{A}$ 的获胜优势为 $Adv_{\text{E}\tau_w,\mathcal{A}}^{\text{IND-CKA}}=\left|\Pr[b'=b]-1/2\right|$。

如果对于任意概率多项式时间的敌手 $\mathcal{A}$，$Adv_{\text{E}\tau_w,\mathcal{A}}^{\text{IND-CKA}}<neg(\xi)$，即 $Adv_{\text{E}\tau_w,\mathcal{A}}^{\text{IND-CKA}}$ 可以忽略不计，那么证明本文的关键词搜索陷门满足 IND-CKA。

4 安全性与性能分析

4.1 正确性分析

本方案基于授权用户集 S、满足条件 dsp 的用户组 S'、条件 dsp 和原始电力数据 m，对于任意用户 $i\in S,j\in S',S'\subseteq S=\{1,2,\cdots,N\},N\in\mathbb{Z}$，验证正确性如下。

1) 加密的电力数据密文 c 的正确性

$$\dot{c}\cdot e\left(sk_i\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},\ddot{c}\right)\Big/e(g_i,\ddot{c})=\frac{m\cdot e(g_1,g_N)^{\delta}\cdot e\left(g_i^{\beta}\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},g^{\delta}\right)}{e\left(g_i,\left(g^{\beta}\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta}\right)}=\tag{4}$$

$$m\cdot e(g_1,g_N)^{\delta}/e(g,g_{N+1}^{\delta})=m$$

2) 重加密的电力数据密文 c_R 的正确性

$$c'_R/e(g^{v},c''_R)=$$

$$\dot{c}\cdot e\left(\tilde{r}\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},\ddot{c}\right)\Big/e(g_i,\ddot{c})\Big/e(g^{v},\dddot{c})=$$

$$\frac{\dfrac{\dot{c}\cdot e\left(sk_i\cdot\mathcal{F}(dsp)^{v}\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},g^{\delta}\right)}{e(g_i,\ddot{c})}}{e(g^{v},\mathcal{F}(dsp)^{\delta})}= \tag{5}$$

$$\frac{\dfrac{\dot{c}\cdot e\left(sk_i\cdot\prod_{k\in S,k\neq i}g_{N+1-k+i},g^{\delta}\right)}{e(g_i,\ddot{c})}\cdot e(\mathcal{F}(dsp)^{v},g^{\delta})}{e(g^{v},\mathcal{F}(dsp)^{\delta})}=$$

$$m\cdot e(\mathcal{F}(dsp)^{v},g^{\delta})/e(g^{v},\mathcal{F}(dsp)^{\delta})=m$$

3) 搜索陷门与关键词密文匹配的正确性

在 BC 调用智能合约自动执行搜索的过程中，需要逐个匹配搜索陷门与关键词密文是否成立从而获得倒排索引表 Tab 中对应的数据文件编号哈希值，$\mathcal{H}_2\left(e\left(c'_w,\tau''_{\tilde{w}}\cdot\prod_{k\in S,k\neq j}g_{N+1-k+j}\right)\right)\overset{?}{=}\mathcal{H}_2(e(\tau'_{\tilde{w}},c''_w))$ 的验证如下所述。

等式左侧计算为

$$\mathcal{H}_2\left(e\left(c'_w,\tau''_{\tilde{w}}\cdot\prod_{k\in S,k\neq j}g_{N+1-k+j}\right)\right)=$$

$$\mathcal{H}_2\left(e\left((\mathcal{H}_1(w)g)^{\delta},(g\cdot sk_j)^{\tilde{\delta}}\cdot\prod_{k\in S,k\neq j}g_{N+1-k+j}\right)\right)=$$

$$\mathcal{H}_2\left(e\left((\mathcal{H}_1(w)g)^{\delta},(g\cdot g_j^{\beta})^{\tilde{\delta}}\cdot\prod_{k\in S,k\neq j}g_{N+1-k+j}\right)\right)= \tag{6}$$

$$\mathcal{H}_2\left(e\left(\mathcal{H}_1(w)g,g\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta\tilde{\delta}\beta}\right)$$

等式右侧计算为

$$\mathcal{H}_2(e(\tau'_{\tilde{w}},c''_w))=$$

$$\mathcal{H}_2\left(e\left((\mathcal{H}_1(w)g)^{\tilde{\delta}},\left(y\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta}\right)\right)=$$

$$\mathcal{H}_2\left(e\left((\mathcal{H}_1(w)g)^{\tilde{\delta}},\left(g^{\beta}\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta}\right)\right)= \tag{7}$$

$$\mathcal{H}_2\left(e\left(\mathcal{H}_1(w)g,g\cdot\prod_{k\in S}g_{N+1-k}\right)^{\delta\tilde{\delta}\beta}\right)$$

由以上等式左右两侧计算可知，等式成立。

4.2 安全性证明

1) 搜索所得电力数据密文的安全性

定理 1：如果决策性 n-BDHE 假设成立，$\mathcal{H}_3$ 是目标抗碰撞哈希函数，那么本文方案搜索得到的电力数据密文在随机预言机 *Oracle* 模型下满足 IND-CCA。

证明：假设存在一个敌手 $\mathcal{A}$ 以不可忽略的优势破坏了本文构造的方案，初始化时，$\mathcal{A}$ 选定一个目标条件 dsp^* 和一个用户组 $U\subseteq S$，又构造一个攻破决策性 n-BDHE 问题概率与 $\mathcal{A}$ 相似的模拟者 $\mathcal{S}im$。

$\mathcal{S}im$ 模拟本文方案的安全游戏。首先，给定 $\mathcal{S}im$ 一个系统公钥 PK，并准备三张表格(初始为空)。

表格 1 $\mathcal{SK}_{\text{List}}$：用于记录 Extract($i$) 的查询信息，描述为 (i,sk_i)；

表格 2 $\mathcal{RK}_{\text{List}}$：用于记录 DO(序号为 i)为满足条件 dsp 的用户组 S' 生成的重加密密钥信息，描述为 $(i,S',dsp,rk_{i\to S'|dsp})$；

表格 3 $\mathcal{RE}_{\text{List}}$：用于记录 DO(序号为 i)为满足条件 dsp 的用户组 S' 生成的重加密数据密文信息，描述为 (i,S,S',dsp,c,c_R)。

表格均使用*表示通配符，具体游戏过程如下所述。

(1) 初始化阶段。$\mathcal{S}im$ 选定一个目标条件 dsp^* 和一个目标用户组 $U\subseteq S$。

(2) 设置阶段。$\mathcal{S}im$ 选取一个目标抗碰撞哈希函数 $\mathcal{H}_3$，并将系统公钥 PK 和 $\mathcal{H}_3$ 一起发送给 $\mathcal{A}$。

(3) 查询阶段一。$\mathcal{S}im$ 回答 $\mathcal{A}$ 发出的以下询问。

① Extract(i)：当 $\chi\in U,i\in S'$ 时，如果 $i\in U$ 或表格 $\mathcal{RK}_{\text{List}}$ 中记录了元组 $(\chi,S',dsp^*,*)$，$\mathcal{S}im$ 回答 $\perp$。否则，$\mathcal{S}im$ 转发查询给 *Oracle*，接收 sk_i 回答给 $\mathcal{A}$，并在表格 $\mathcal{SK}_{\text{List}}$ 中记录序号 i 的元组 (i,sk_i)。

② ReExtract(i,S',dsp)：如果表格 $\mathcal{RK}_{\text{List}}$ 中已经记录了元组 $(i,S',dsp,rk_{i\to S'|dsp})$，那么 $\mathcal{S}im$ 将 $rk_{i\to S'|dsp}$ 回复给 $\mathcal{A}$；未记录则按照以下情形处理。

a. 若 $i\notin U$ 或 $dsp\neq dsp^*$，$\mathcal{S}im$ 查询用户 i 的私钥，回答实际为重加密密钥，在表格 $\mathcal{RK}_{\text{List}}$ 中记录元组 $(i,S',dsp,rk_{i\to S'|dsp})$。

b. 若 $i\in U$ 且 $dsp=dsp^*$ 但 $S'\cap\mathcal{SK}_{\text{List}}=\varnothing$，$\mathcal{S}im$ 选取 $r,r'\in_R G$，并回复一个随机的重加密密钥 $rk_{i\to S'|dsp}=(r,Enc'(PK,S',r'))$。再在表格 $\mathcal{RK}_{\text{List}}$ 中记录元组 $(i,S',dsp,rk_{i\to S'|dsp})$。

c. 若 $i \in U$ 且 $dsp = dsp^*$ 且 $S' \cap \mathcal{SK}_{\text{List}} \neq \varnothing$，$\mathcal{Sim}$ 回答 $\perp$。

③ ReEncrypt(i,S,dsp,S',c)：如果表格 $\mathcal{RE}_{\text{List}}$ 已经记录了元组 $(i,S,S',*,c,c_R)$，$\mathcal{Sim}$ 回复 c_R 给 $\mathcal{A}$。未记录则按照以下情形处理。

a. 如果表格 $\mathcal{RK}_{\text{List}}$ 已经记录了元组 $(i,S',dsp,rk_{i\to S'|dsp})$，基于条件 $c \leftarrow Enc(PK,S,dsp,m)$，$\mathcal{Sim}$ 使用重加密密钥生成 c_R，再在表格 $\mathcal{RE}_{\text{List}}$ 中记录元组 $(i,S,S',*,c,c_R)$。

b. 如果表格 $\mathcal{RK}_{\text{List}}$ 没有记录元组 $(i,S',dsp,rk_{i\to S'|dsp})$，那么 $\mathcal{Sim}$ 使用 ReKGen(PK,sk_i,dsp,S') 生成重加密密钥 $rk_{i\to S'|dsp}$，再重加密电力数据密文生成 c_R，最后在表格 $\mathcal{RE}_{\text{List}}$ 中记录元组 $(i,S,S',*,c,c_R)$。

④ Decrypt$_{\text{I}}(i,S,dsp,c)$：如果表格 $\mathcal{SK}_{\text{List}}$ 已经记录了元组 (i,sk_i)，那么使用私钥 sk_i 执行 Dec(PK,sk_i,i,S,dsp,c) 解密获得明文；否则，$\mathcal{Sim}$ 执行 KGen(MSK,PK,i) 生成私钥 sk_i 再解密。

⑤ Decrypt$_{\text{II}}(i,j,S,dsp,S',c_R)$：如果表格 $\mathcal{SK}_{\text{List}}$ 已经记录了元组 (j,sk_j)，那么使用私钥 sk_j 执行 $\text{Dec}_{\text{R}}(PK,sk_j,i,j,S,dsp,S',c_R)$ 重解密获得明文；否则，$\mathcal{Sim}$ 执行 KGen(MSK,PK,j) 生成 sk_j 再解密。

(4) 挑战阶段。$\mathcal{A}$ 选定两个长度一致的数据明文 (m_0,m_1) 发送给 $\mathcal{Sim}$，$\mathcal{Sim}$ 将其转发给挑战者 $\mathcal{C}$。当 $\mathcal{C}$ 返回密文 c^* 时，$\mathcal{Sim}$ 将 c^* 回复给 $\mathcal{A}$。

(5) 查询阶段二。$\mathcal{Sim}$ 回复 $\mathcal{A}$ 类比查询阶段一。

(6) 猜测阶段。$\mathcal{A}$ 输出猜测为 $b' \in \{0,1\}$，$\mathcal{Sim}$ 输出 b'。

在安全游戏中，对于敌手 $\mathcal{A}$ 的攻击模拟者 $\mathcal{Sim}$ 模拟成功，对于随机选择的一个重加密密钥 $rk_{i\to S'|dsp} = (r,c_R)$，必然存在一个值 $\nu' \in \mathbb{Z}_p^*$ 使得 $r = sk_i \cdot \mathcal{F}(dsp)^{\nu'}$。这个问题等价于 c_R 和 $g^{\nu'}$ 一些加密值的不可区分性，由选择明文攻击(chosen plaintext attack, CPA)安全性和目标抗碰撞哈希函数共同决定。因此，如果 $\mathcal{Sim}$ 攻破本文方案的概率不可忽略，那么根据定理 1，$\mathcal{Sim}$ 有不可忽略的优势可以解决决策性 n-BDHE 难题。

2) 关键词搜索陷门的安全性

定理 2：如果决策性 n-BDHE 假设成立，$\mathcal{H}_1$ 是目标抗碰撞哈希函数，那么本文方案的关键词搜索陷门在随机预言机 $\mathcal{O}racle$ 模型下满足 IND-CKA。

证明：假设存在一个敌手 $\mathcal{A}$ 以不可忽略的优势破坏了本文构造的方案，初始化时，$\mathcal{A}$ 选定一个目标条件 dsp^* 和一个用户组 $U \subseteq S$，又构造一个攻破决策性 n-BDHE 问题概率与 $\mathcal{A}$ 相似的模拟者 $\mathcal{Sim}$。

$\mathcal{Sim}$ 模拟本文方案的安全游戏。首先，给定 $\mathcal{Sim}$ 一个系统公钥 PK，并准备两张表格(初始为空)。

表格 1 $\mathcal{SK}_{\text{List}}$：用于记录 Extract$(i)$ 的查询信息，描述为 (i,sk_i)；

表格 2 $\mathcal{TW}_{\text{List}}$：用于记录 Trpd$(j,S,w)$ 的查询信息，描述为 (sk_j,τ_w)。

表格均使用*表示通配符，具体游戏过程如下所述。

(1) 初始化阶段。$\mathcal{Sim}$ 选定一个目标条件 dsp^* 和一个目标用户组 $U \subseteq S$。

(2) 设置阶段。$\mathcal{Sim}$ 选取一个目标抗碰撞哈希函数 $\mathcal{H}_1$，并将系统公钥 PK 和 $\mathcal{H}_1$ 一起发送给 $\mathcal{A}$。

(3) 查询阶段。$\mathcal{Sim}$ 回答 $\mathcal{A}$ 发出的以下询问：

① Extract(j)：如果 $j \in U$，$\mathcal{Sim}$ 回答 $\perp$；否则，$\mathcal{Sim}$ 转发查询给 $\mathcal{O}racle$，回复接收到的 sk_j 给 $\mathcal{A}$，并在表格 $\mathcal{SK}_{\text{List}}$ 中记录序号 j 的元组 (j,sk_j)。

② Trpd(j,S,w)：如果表格 $\mathcal{TW}_{\text{List}}$ 已经记录了元组 (sk_j,τ_w)，那么 $\mathcal{Sim}$ 将 τ_w 回复给 $\mathcal{A}$；未记录则按照以下情形处理。

a. 如果表格 $\mathcal{SK}_{\text{List}}$ 已经记录了元组 (j,sk_j)，那么 $\mathcal{Sim}$ 执行 Trapdoor(PK,sk_j,w) 生成 τ_w，并在表格 $\mathcal{TW}_{\text{List}}$ 中记录元组 (sk_j,τ_w)。

b. 如果表格 $\mathcal{SK}_{\text{List}}$ 没有记录元组 (j,sk_j)，那么 $\mathcal{Sim}$ 执行 KGen$\left(MSK,PK,j\right)$ 生成 sk_j 后再生成 τ_w，并在表格 $\mathcal{TW}_{\text{List}}$ 中记录元组 (sk_j,τ_w)。

(4) 挑战阶段。$\mathcal{A}$ 选定两个长度一致的关键词 (w_0,w_1) 发送给 $\mathcal{Sim}$，$\mathcal{Sim}$ 将其转发给挑战者 $\mathcal{C}$。当 $\mathcal{C}$ 返回密文 τ_w^* 时，$\mathcal{Sim}$ 将 τ_w^* 回复给 $\mathcal{A}$。

(5) 猜测阶段。$\mathcal{A}$ 输出猜测为 $b' \in \{0,1\}$，$\mathcal{Sim}$ 输出 b'。

在安全游戏中，对于敌手 $\mathcal{A}$ 的攻击模拟者 $\mathcal{Sim}$ 模拟成功，对于随机选择的一个关键词搜索陷门 $\tau_w = (\tau_w',\tau_w'') = ((\mathcal{H}_1(w)g)^{\delta},(g\cdot sk_j)^{\delta})$，必然存在一个值 $\delta \in_R \mathbb{Z}_p^*$ 使得 $(\mathcal{H}_1(w)g)^{\delta} = (\mathcal{H}_1(w)g)^{\delta^*}$ 且 $(g\cdot sk_j)^{\delta} = (g\cdot sk_{j^*})^{\delta^*}$ 的概率极低，其中 $\delta^* \in_R \mathbb{Z}_q^*$。因此，如果 $\mathcal{Sim}$ 攻破本文方案的概率不可忽略，那么根据定理 2，$\mathcal{Sim}$ 有不可忽略的优势可以解决决策性 n-BDHE 难题。

4.3 安全性分析

1) 数据隐私性

本文方案是将 PEKS 与条件广播代理重加密技术结合，从而实现电力数据密文的多方搜索与共享。DO 首先设定授权用户集 S 和条件 dsp，并为满足条件 dsp 的用户组 $S' \subseteq S$ 加密原始电力数据 m，得到数据密文 $c \leftarrow \mathrm{Enc}(PK, S, dsp, m)$；再使用基于自己的序号 i 生成的私钥 sk_i 为用户组 S' 生成重加密密钥 $rk_{i \to S'|dsp} \leftarrow \mathrm{ReKGen}(PK, sk_i, dsp, S')$。只有满足条件 dsp 的 DU 才可以正确计算出重加密后的电力数据密文 $c_R \leftarrow \mathrm{ReEnc}(PK, i, S, dsp, S', rk_{i \to S'|dsp}, c)$，之后使用基于自己的序号 j 生成的私钥 sk_j 执行重解密获得原始电力数据 $m \leftarrow \mathrm{Dec_R}(PK, sk_j, i, j, S, dsp, S', c_R)$。定理 1 已证明了电力数据密文的安全性，并且 PEKS 是目前已知安全的非对称密码体制可搜索加密。因此，本文方案以密文形式实现了多方数据安全共享，满足电力数据的隐私性。

2) 抗合谋攻击

在电力数据的搜索和共享过程中，存在权威管理者与恶意用户勾结窃取数据所有者隐私数据的风险。在本文方案中，数据所有者将敏感数据加密后存储在云服务提供商处，确保数据存储安全；将关键词-文件编号的索引密文上传到区块链，利用区块链的不可篡改性保护索引的安全；为满足条件的授权用户生成重加密密钥，并将其发送给由联盟链共识机制选举节点轮换担任的权威管理者，从而降低单一代理作恶的风险。当数据使用者请求搜索时，权威管理者负责验证其授权，只有验证通过且搜索成功联盟链才执行重加密操作，以确保在整个搜索过程中，权威管理者无法获取到明文数据或用户私钥的任何信息。由于搜索和重加密由联盟链执行，一旦此过程失败，权威管理者作恶就会被发现并降为普通节点，增加了其作恶成本，从而在一定程度上抑制了其与恶意用户勾结的动机。此外，通过联盟链的节点轮换机制，降低了单一管理者持续作恶的可能性，并减少了由于单点故障导致的风险。以上措施有效防止了权威管理者与恶意用户之间的不当合作，从而确保电力数据的安全搜索与共享。

3) 多用户环境的细粒度访问控制

通常电力数据中包含有敏感数据，不同企业机构或个人对于数据的需求不同，因此多方用户环境中数据的搜索与共享必须实现细粒度访问控制。本文方案中，每个用户会在权威管理者注册并获得唯一的序号，再根据序号生成私钥；数据拥有者预先设定授权用户集和条件值，只为满足条件的用户组生成重加密密钥及重加密电力数据，并且只有满足条件的数据使用者才可以使用自己的私钥重解密电力数据密文，成功获取原始电力数据，从而实现了数据用户的细粒度访问控制。

4.4 性能分析

1) 功能性分析

由表 1 的方案功能比较可知，文献[10]将无证书签名技术与代理重加密结合，实现了电力数据的加密共享，无法实现密文关键词搜索和多用户细粒度控制。文献[17]虽然将属性基加密与对称加密算法结合，实现了电力数据密文的共享和细粒度访问控制，但是仍然无法实现关键词密文搜索，从而满足用户的针对性数据需求，并且方案只能满足选择明文攻击下的不可区分性(indistinguishability under chosen plaintext attack, IND-CPA)安全。文献[20]进一步结合基于属性的可搜索加密，提出适用于电网系统的电力数据保护加密方案，但是方案由传统云服务器提供不可信的搜索服务，存在数据安全隐患。本文与文献[21]类似，结合条件广播代理重加密改进传统 PEKS 并使用区块链执行可信搜索，但是该方案没有明确的应用环境，难以贴合电力数据的应用场景。与其他方案相比，本文方案结合区块链提供可信搜索，在确保电力数据机密性的基础上进一步满足多用户环境的细粒度可控共享，更加适用于复杂参与方的新型电力系统应用环境。

表 1 功能比较

Table 1 Function comparison

方案	多用户细粒度控制	区块链	可搜索加密	攻击安全性	电力数据共享
文献[10]	×	√	×	IND-CCA	√
文献[17]	√	√	×	IND-CPA	√
文献[20]	√	×	√	IND-CCA	√
文献[21]	√	√	√	IND-CCA	×
本文	√	√	√	IND-CCA	√

2) 计算成本分析

本文方案搭建的实验环境为 12th Gen Intel(R) Core(TM) i7-12700H 2.30 GHz，使用 Vmware 虚拟机安装 Ubuntu 系统，基于开源项目 Hyperledger Fabric 设计联盟链仿真环境，构建了一个新型电力系统的加密电力数据多用户搜索与共享方案[22]。基于 JAVA 语言使用 jPBC 密码库仿真，并将本方案和其他方案进行对比，仿真实验选择椭圆曲线

type = A (方程为 $y^2 = (x^3 + x) \bmod p$)，双线性群通过实例化库中的 Pairing 对象实现，群元素调用库中 getZr(·), getG1(·) 等方法随机产生，选择哈希函数 SHA-1，根据本文方案设计调用库中函数实现相应功能。

本文的加密电力数据多用户搜索与共享方案是结合条件广播代理重加密技术改进传统公钥关键词密文搜索方案，参考文献[21]的实验设计方案，分组多次测量电力数据加密、重加密密钥生成、关键词搜索陷门生成、联盟链搜索、重加密搜索结果和解密恢复原始电力数据 6 个阶段的时间，从而多方面评估本文方案的电力数据加密、搜索与共享的时间成本，结果如图 2 所示。

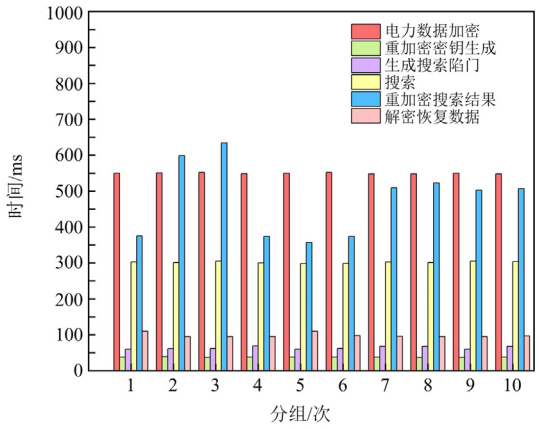

图 2 本文方案不同阶段测试时间

Fig. 2 Test time of different stages of the scheme in this paper

由图 2 可知，本文方案为搜索成功且可共享数据的授权用户执行电力数据密文重加密的时间成本较大，方案其余阶段的时间开销相对稳定，但是整体时间消耗仍在用户可以接受的范围。

本文方案的重要设计之一解决了传统 PEKS 方案难以支持多用户参与的搜索与共享的问题，即由联盟链执行关键词陷门搜索，并对成功搜索获得的密文结果执行重加密，最后将重加密的电力数据返回给授权用户，从而完成电力数据的安全搜索与可信共享。因此，为验证方案可适应新型电力系统多用户环境下的复杂数据交换，本文增加测试不同用户数量对于搜索与重加密的时间开销影响，如图 3 所示。

分析图 3 可知，虽然权威管理者预先验证用户是否授权，减少了无效的搜索开销，但是关键词陷门搜索的时间仍然随用户数量增加而增加。联盟链重加密电力数据密文虽然相比其余阶段时间开销更大，但是用户数量增加出现恶意用户的可能性会提升，这样搜索失败的概率就会增加，而重加密只有授权用户搜索成功才会执行，因此一旦搜索失败重加密电力数据密文的时间开销反而减少。

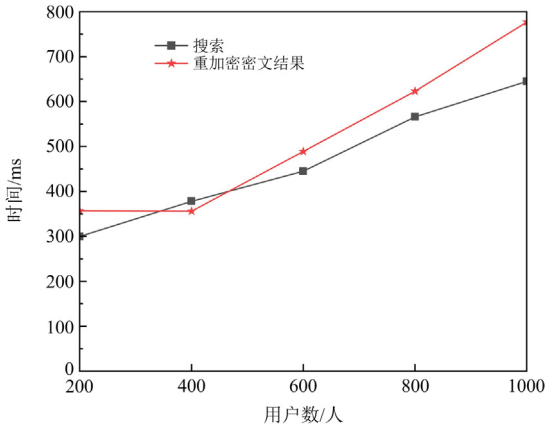

图 3 不同用户数的搜索与重加密时间变化结果

Fig. 3 Results of search and re-encryption time changes for different user numbers

本文方案是结合条件广播代理重加密技术改进传统 PEKS，旨在实现加密电力数据的安全搜索与共享。文献[23]针对跨医院病例数据难以共享的问题，提出了一种区块链上基于可搜索加密的电子病历数据共享方案，分别使用可搜索加密和代理重加密技术实现联盟链上的关键词安全搜索与患者的电子病历数据共享。文献[24]将具有相等性测试的公钥加密与代理重加密结合，基于区块链提出一种轻量级数据搜索与共享方案，解决了车载社交网络中车辆数据的隐私泄露与不安全问题。文献[25]同样针对电子医疗系统中加密的个人医疗记录阻碍了医生对于信息的有效搜索问题，设计了一种安全实用的代理可搜索重加密方案。以上三个方案均为基于区块链的加密数据搜索与共享方案，给出了详细的方案设计和各阶段的时间开销结果。为了测试本文提出的可搜索加密方案的性能，本文将不同方案的原始数据加密时间、关键词陷门生成时间和密文数据搜索时间分别进行分析对比，得到实验结果如图 4—图 6 所示。

由图 4 可知，随着文件数量增加，各方案的数据加密时间都在增加，但是整体时间消耗仍在用户可接受的范围内，并且加密过程由数据拥有者完成，不影响电力数据的搜索与共享性能。其中，文献[25]

的时间开销最大，其余方案的时间增加相对平稳。通过分析原方案设计可知，文献[25]在加密过程中多次使用除法和幂乘运算，这样在文件数量不断增加时，必然会大幅度增加计算开销和时间成本；而本文方案在内的其余 3 个方案多使用乘法和幂乘运算，因此时间开销增加相对平缓。特别地，文献[24]在加密过程中多使用异或、或等逻辑运算，因此在这几个对比方案中加密时间最短。

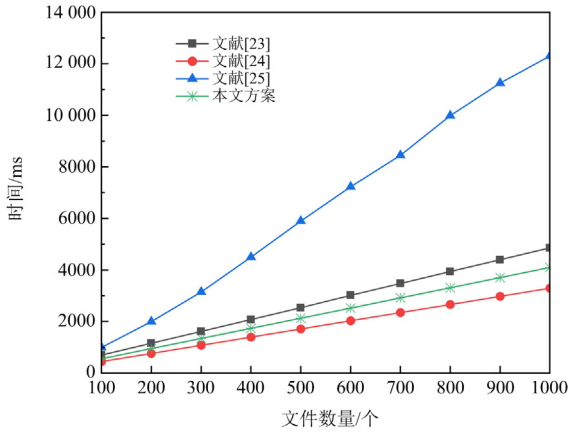

图 4 不同文件数量的数据加密时间

Fig. 4 Data encryption time of different file numbers

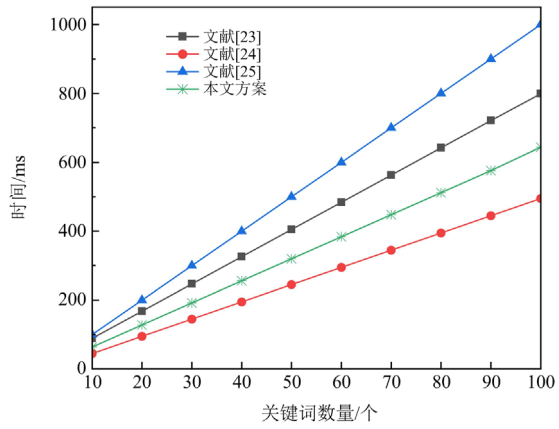

图 5 不同关键词数量的陷门生成时间

Fig. 5 Trapdoor generation time of different keyword quantities

根据图 5 可知，本文方案的关键词陷门生成时间随关键词数量增加呈现线性增加，但是与其他 3 个方案相比，仍具有一定的使用价值。文献[25]的时间开销相比最高，主要是陷门生成过程中多次使用除法和幂乘运算，文献[23]也是除法运算增加了时间开销；文献[24]使用乘法运算极大地降低了时间损耗，而本文方案虽然使用幂乘在一定程度上增加了时间开销，但是实际时间消耗仍在用户可接受的范围。此外，陷门生成过程主要由请求电力数据的用户完成，对链上搜索和数据共享的影响可以忽略。

由图 6 可以直观地看出，本文对比的 4 个方案的密文搜索时间都随文件数量增加呈现上升趋势，但是搜索时间在实际应用中都是可以接受的。综合以上 3 个阶段的测试对比，在电力数据的实际搜索与多方共享过程中，本文方案的时间开销在用户可以承受的范围内，并且在随机预言机模型下，方案具有数据隐私性和安全性，在新型电力系统的复杂应用环境下具有实用价值。

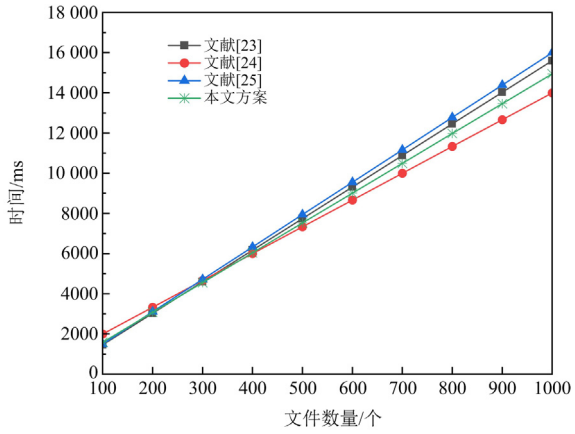

图 6 不同文件数量的密文搜索时间

Fig. 6 Ciphertext search time of different file numbers

5 结论

基于区块链技术，本文结合条件广播代理重加密改进传统 PEKS，设计了一种新型电力系统中加密电力数据的多用户安全搜索与共享方案。通过动态轮换的权威管理者验证用户权限、智能合约自动执行搜索和联盟链为授权用户重加密搜索结果，多方面共同保证了新型电力系统中数据的搜索安全性与多参与方共享可控，同时在一定程度上降低了搜索复杂度和数据拥有者的计算负担。然而，该方案将加密的关键词与文件编号索引上传到联盟链存储用于执行搜索，存在数据量过大、密文索引过多导致的区块链存储负担过重等问题。因此，下一步可以考虑如何优化该方案中区块链的索引存储，降低区块链上存储负担。

参考文献

[1] 裴林, 黄成, 杨啸, 等. 考虑隐私保护和去中心化的分布式能源交易模式研究[J]. 电力系统保护与控制, 2024, 52(2): 143-154.

PEI Lin, HUANG Cheng, YANG Xiao, et al. A distributed energy trading model considering privacy protection and decentralization[J]. Power System Protection and Control, 2024, 52(2): 143-154.

[2] 凡航, 徐葳, 范晓昱, 等. 隐私计算在新型电力系统中的应用分析与展望[J]. 电力系统自动化, 2023, 47(19): 187-199.
FAN Hang, XU Wei, FAN Xiaoyu, et al. Application analysis and prospect of privacy-preserving computation in new power systems[J]. Automation of Electric Power Systems, 2023, 47(19): 187-199.

[3] 王增平, 林一峰, 王彤, 等. 电力系统继电保护与安全控制面临的挑战与应对措施[J]. 电力系统保护与控制, 2023, 51(6): 10-20.
WANG Zengping, LIN Yifeng, WANG Tong, et al. Challenges and countermeasures to power system relay protection and safety control[J]. Power System Protection and Control, 2023, 51(6): 10-20.

[4] BONEH D, DI CRESCENZO G, OSTROVSKY R, et al. Public key encryption with keyword search[C] // Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques, May 2-6, 2004, Interlaken, Switzerland: 506-522.

[5] SONG D, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C] // Proceeding 2000 IEEE Symposium on Security and Privacy, S&P 2000, May 14-17, 2000, Berkeley, CA, USA: 44-55.

[6] 牛淑芬, 戈鹏, 董润园, 等. 智能交通系统中具有隐私保护性的属性基可搜索加密方案[J/OL]. 电子与信息学报: 1-10[2024-05-19]. http://kns.cnki.net/kcms/detail/11.4494.tn.20240401.1457.016.html.
NIU Shufen, GE Peng, DONG Runyuan, et al. Privacy preseving attribute based searchable encryption scheme in intelligent transportation system[J/OL]. Journal of Electronics and Information: 1-10[2024-05-19]. http://kns.cnki.net/kcms/detail/11.4494.tn.20240401.1457.016.html.

[7] 刘雄飞, 于志远, 包钊源, 等. 基于航天信息系统云平台的可授权数据安全共享研究[J]. 上海航天(中英文), 2023, 40(4): 46-53, 87.
LIU Xiongfei, YU Zhiyuan, BAO Zhaoyuan, et al. An efficient authorized data security sharing method based on aerospace information system cloud platform[J]. Shanghai Aerospace (Chinese & English), 2023, 40(4): 46-53, 87.

[8] 王政, 王经纬, 殷新春. 支持用户撤销的可搜索电子健康记录共享方案[J]. 计算机应用, 2024, 44(2): 504-511.
WANG Zheng, WANG Jingwei, YIN Xinchun. Searchable electronic health record sharing scheme with user revocation[J]. Journal of Computer Applications, 2024, 44(2): 504-511.

[9] BLAZE M, BLEUMER G, STRAUSS M. Divertible protocols and atomic proxy cryptography[C] // International Conference on the Theory and Application of Cryptographic Techniques, 1998, Berlin, Germany: 127-144.

[10] AHENE E, DAI Junfeng, FENG Hao, et al. A certificateless signcryption with proxy re-encryption for practical access control in cloud-based reliable smart grid[J]. Telecommunication Systems, 2019, 70: 491-510.

[11] 朱敏惠, 陈燕俐, 胡媛媛. 支持代理重加密的基于身份可搜索加密方案[J]. 计算机工程, 2019, 45(1): 129-135, 140.
ZHU Minhui, CHEN Yanli, HU Yuanyuan. Identity-based searchable encryption scheme supporting proxy re-encryption[J]. Computer Engineering, 2019, 45(1): 129-135, 140.

[12] CHU Chengkang, WENG Jian, CHOW S S, et al. Conditional proxy broadcast re-encryption[C] // Information Security and Privacy: 14th Australasian Conference, July 1-3, 2009, Brisbane, Australia: 327-342.

[13] 陈嘉莉, 马自强, 兰亚杰, 等. 基于区块链技术的医疗信息共享研究综述[J/OL]. 计算机应用研究: 1-14[2024-05-20]. https://doi.org/10.19734/j.issn.1001-3695.2023.12.0620.
CHEN Jiali, MA Ziqiang, LAN Yajie, et al. Overview of medical information sharing based on blockchain technology[J/OL]. Computer Application Research: 1-14 [2024-05-20]. https://doi.org/10.19734/j.issn.1001-3695.2023.12.0620.

[14] 杜晓玉, 刘帅起, 韩志杰, 等. 以患者为中心基于IPFS和区块链的医疗信息共享方案[J/OL]. 计算机应用: 1-16[2024-05-20]. http://kns.cnki.net/kcms/detail/51.1307.TP.20240311.1044.008.html.
DU Xiaoyu, LIU Shuaiqi, HAN Zhijie, et al. Patient-centric medical information sharing scheme based on IPFS and blockchain[J/OL]. Computer Application: 1-16[2024-05-20]. http://kns.cnki.net/kcms/detail/51.1307.TP.20240311.1044.008.html.

[15] 马雪, 潘恒, 姚中原, 等. 基于联盟链的可搜索电子病历双重授权共享方案[J]. 应用科学学报, 2023, 41(5): 881-895.
MA Xue, PAN Heng, YAO Zhongyuan, et al. Dual

authorization sharing scheme of searchable electronic medical data based on consortium blockchain[J]. Journal of Applied Sciences, 2023, 41(5): 881-895.

[16] YU Hongtao, LIU Suhui, CHEN Liquan, et al. Blockchain-enabled one-to-many searchable encryption supporting designated server and multi-keywords for cloud-IoMT[J]. Journal of Systems Architecture, 2024, 149: 103103.

[17] 杨小东, 廖泽帆, 刘磊, 等. 基于区块链和属性基加密的电力数据共享方案[J]. 电力系统保护与控制, 2023, 51(13): 169-176.
YANG Xiaodong, LIAO Zefan, LIU Lei, et al. Power data sharing scheme based on blockchain and attribute-based encryption[J]. Power System Protection and Control, 2023, 51(13): 169-176.

[18] YEH L Y, SHEN N X, HWANG R H. Blockchain-based privacy-preserving and sustainable data query service over 5G-VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(9): 15909-15921.

[19] 牛淑芬, 于斐, 陈俐霞, 等. 加密电子病历数据共享方案[J]. 计算机工程与科学, 2022, 44(9): 1610-1619.
NIU Shufen, YU Fei, CHEN Lixia, et al. A data sharing scheme for encrypted electronic health record[J]. Computer Engineering and Science, 2022, 44(9): 1610-1619.

[20] ZHANG Xun, MU Dejun, ZHAO Jinxiong. Attribute-based keyword search encryption for power data protection[J]. High-Confidence Computing, 2023, 3(2): 100-115.

[21] 翟社平, 张瑞婷, 杨锐, 等. 多用户环境的区块链可搜索加密方案[J/OL]. 西安电子科技大学学报, 1-18[2024-05-30]. https://doi.org/10.19665/j.issn1001-2400.20240205.
ZHAI Sheping, ZHANG Ruiting, YANG Rui, et al. Blockchain searchable encryption scheme for multi-user environment[J/OL]. Journal of Xi'an University of Electronic Science and Technology: 1-18[2024-05-30]. https://doi.org/10.19665/j.issn1001-2400.20240205.

[22] 翟社平, 童彤, 白喜芳. 基于区块链的属性代理重加密数据共享方案[J]. 计算机工程与应用, 2023, 59(8): 270-279.
ZHAI Sheping, TONG Tong, BAI Xifang. Blockchain-based attribute proxy re-encryption data sharing scheme[J]. Computer Engineering and Applications, 2023, 59(8): 270-279.

[23] 牛淑芬, 刘文科, 陈俐霞, 等. 基于联盟链的可搜索加密电子病历数据共享方案[J]. 通信学报, 2020, 41(8): 204-214.
NIU Shufen, LIU Wenke, CHEN Lixia, et al. Electronic medical record data sharing scheme based on searchable encryption via consortium blockchain[J]. Journal of Communications, 2020, 41(8): 204-214.

[24] ZHOU Yuanjian, CAO Zhenfu, DONG Xiaolei, et al. BLDSS: a blockchain-based lightweight searchable data sharing scheme in vehicular social networks[J]. IEEE Internet of Things Journal, 2022, 10(9): 7974-7992.

[25] XUE Linlin. DSAS: a secure data sharing and authorized searchable framework for e-healthcare system[J]. IEEE Access, 2022, 10: 30779-30791.

收稿日期：2024-06-19； 修回日期：2024-08-14

作者简介：

杨 锐(1976—)，女，硕士，讲师，研究方向为区块链；E-mail: yangrui@xupt.edu.cn

张瑞婷(2000—)，女，通信作者，硕士研究生，研究方向为区块链、数据隐私保护；E-mail: 18691729079@163.com

翟社平(1971—)，男，博士，教授，研究方向为区块链、知识图谱。E-mail: zhaisheping@xupt.edu.cn

(编辑 姜新丽)