基于 CP-ABSE 的农机社会化服务联盟链隐私匹配方案

景 旭[1]，谭 菡[1]，蒋 炎[1]，阮俊虎[2※]

（1. 西北农林科技大学信息工程学院，杨凌 712100；2. 西北农林科技大学经济管理学院，杨凌 712100）

摘 要：针对多个农机社会化服务平台联合，实现跨平台任务匹配中存在的敏感数据泄露和集中式服务器不可信问题，该研究提出了基于密文策略属性基可搜索加密（ciphertext-policy attribute-based searchable encryption，CP-ABSE）的农机社会化服务联盟链隐私匹配方案。该方案基于联盟链构建农机社会化服务联合平台，为多平台数据共享提供去中心化的可信环境；基于 CP-ABSE 技术实现跨平台的任务匹配，支持对任务密文数据的检索以及细粒度的访问控制，保护作业任务发布方和农机手的敏感数据；使用智能合约实现农田作业任务与农机手之间的匹配服务，避免集中式服务器存在的单点故障和恶意违规操作等问题。安全性分析表明，该方案能够保证数据的完整性、机密性以及匹配结果的可信性。基于 Hyperledger Fabric 构建了一个原型系统，测试结果表明，当全局属性数量为 200 时，系统构建和私钥生成的运行时间分别约 8 和 2.5 s，搜索令牌生成与数据加密的计算开销分别为 60 和 80 ms，匹配智能合约平均时延约为 250 ms。该方案破解了农机社会化服务平台间的“数据孤岛”问题，对于促进农机社会化服务的推广具有重要的意义。

关键词：区块链；农机社会化服务；联盟链；隐私匹配；可搜索加密；属性基加密

doi：10.11975/j.issn.1002-6819.202303051

中图分类号：TP309.2；S231 **文献标志码**：A **文章编号**：1002-6819(2023)-11-0047-09

景旭，谭菡，蒋炎，等. 基于 CP-ABSE 的农机社会化服务联盟链隐私匹配方案[J]. 农业工程学报，2023，39(11)：47-55. doi: 10.11975/j.issn.1002-6819.202303051 http://www.tcsae.org

JING Xu, TAN Han, JIANG Yan, et al. CP-ABSE based privacy-preserving match scheme on agricultural machinery socialized service consortium blockchain[J]. Transactions of the Chinese Society of Agricultural Engineering (Transactions of the CSAE), 2023, 39(11): 47-55. (in Chinese with English abstract) doi: 10.11975/j.issn.1002-6819.202303051 http://www.tcsae.org

0 引 言

中国农业生产呈现出“大国小农”、农田碎片化和劳动力缺失等特征，农机社会化服务[1-2]能够解决农户难以承担农机高昂的购买和维护费用的难题，促进小农户和现代农业的有效衔接，有利于实现农业增效、农民增收。基于互联网的农机社会化服务平台[3-4]（以下简称农服平台），如中国农业社会化服务平台、嘀地农机、全国农机化信息服务平台等，汇集了农田作业服务需求和服务资源，打破农户与农机手之间的信息壁垒，提供农事生产服务对接途径。鉴于农业生产的地域性和季节性等特征，部分地区的农机资源会出现冗余或稀缺现象，仅靠本区域内农机调度难以平衡供需关系[5]。多个农服平台联合共享任务和农机手资源，实现农机资源的协调调度[6-7]，能够提高农机作业效率，提升农业全产业链服务能力，增加集约化服务规模效益。但在多平台联合场景中，如果用户的地理位置[8]、任务偏好[9]、农田作业需求等敏感信息以明文形式共享，可能会导致隐私泄露问题，影响农服平台之间合作的积极性。因此，研究农机社会化服务联合平台的隐私匹配具有重要意义。

关于多方联合场景中的隐私匹配，国内外学者开展了广泛的研究。QI 等[10]通过改进局部敏感哈希技术，在保证用户敏感数据隐私的前提下，整合多平台数据，实现了分布式的推荐服务；SOBITHA 等[11]将同态加密技术应用于数据挖掘中，提出了一种个性化推荐方案，但上述两种方案都仅关注用户敏感数据的保护。SHU 等[12-13]使用可搜索加密技术实现任务和工人之间的匹配，保护了被推荐内容和用户双方敏感数据的隐私，但依靠集中式服务器提供数据共享和计算，存在单点故障[14]、易遭受内外部恶意攻击和服务器不可信等问题[15]。牛淑芬等[16-17]将可搜索加密与代理重加密技术应用于多家医院联合场景中，在区块链上实现了电子病历关键字的可靠搜索。GUO 等[18]设计了一个基于智能合约的匹配协议，使用区块链技术在去中心化的联合众包系统中实现了安全任务推荐方案。综上可以看出，现有研究多集中在共享敏感数据前通过加密保证隐私，然而，以密文形式共享数据会削弱数据的可用性[19]，且难以同时保证数据和用户双方的隐私；通过集中式服务器共享数据、提供匹配服务，很难被联盟的各方信任。

区块链[20]作为一个多方共识、不可篡改的分布式账本，由区块链网络中的所有节点共同维护数据，能够在多方联合场景中实现去中心化可信架构；链上智能合约的执行过程对所有节点透明，在给定的输入下，输出结

收稿日期：2023-03-09 修订日期：2023-05-06

基金项目：国家自然科学基金（72271202），陕西省重点研发计划项目（2019ZDLNY07-02-01）

作者简介：景旭，博士，副教授，研究方向为农业信息化、区块链技术、信息系统安全等。Email：jingxu@nwsuaf.edu.cn

※通信作者：阮俊虎，博士，教授，研究方向为数字农业运营管理、农业物联网与区块链技术、农产品电商与物流管理等。Email：rjh@nwsuaf.edu.cn

果稳定；但通过区块链共享密文数据难以实现链上数据的可用性与数据访问权限的设置。密文策略的属性基可搜索加密技术（ciphertext-policy attribute-based searchable encryption，CP-ABSE）[21] 能够保证数据加密条件下的可检索性，实现一对多的细粒度数据共享。

基于联盟链和 CP-ABSE，本文提出一种农机社会化服务联合平台隐私匹配方案。多个农服平台基于联盟链组成去中心化的信息共享平台，各平台将农田作业任务密文和资源调用等信息发布至联盟链中，保证数据的真实性和完整性；通过 CP-ABSE 加密任务数据，保护农户和农机手双方敏感数据的隐私，在各农服平台对合作平台共享的任务数据和农机手的搜索关键字一无所知的情况下，实现任务密文数据检索和细粒度的访问控制；隐私匹配服务转移到智能合约，窃听者无法猜出关键字，可保证搜索返回结果可信。本研究破解了农服平台间的“数据孤岛”问题，能够推动农服平台之间的合作，对于推动农机社会化服务的推广具有重要的意义。

1 关键技术

1.1 CP-ABSE

CP-ABSE 是由密文策略的属性基加密[22] 与可搜索加密技术[23-24] 相结合的密码学技术，能够同时实现一对多的细粒度访问控制和密文数据检索功能，平衡了数据的隐私性和可用性。CP-ABSE 方案[25-26] 中数据所有者可以通过定义密文的访问策略赋予访问者搜索权限，广泛应用于多数据所有者和访问者模型。

1.2 区块链

区块链中集成了分布式数据库、共识机制[27]、P2P 网络、智能合约[28] 和密码学等技术，广泛应用于提供可信服务场景。按照开放程度，区块链可分为公有链、联盟链和私有链。联盟链[29] 网络由成员共同维护，适用于多组织间的数据共享。智能合约本质上是一段运行在区块链上的计算机程序，可以处理较为复杂的业务逻辑。

2 农机社会化服务联合平台隐私匹配方案

2.1 平台架构

农机社会化服务联合平台使用联盟链作为连接各农服平台的枢纽，将相互独立的多个系统组成一个去中心化的联盟。各方能够将农田作业任务共享给合作平台，实现跨平台的农机手资源调用。联合平台主要包括证书授权（certificate authority，CA）中心、农户、农机手、农服平台和联盟链 5 个实体，如图 1 所示。

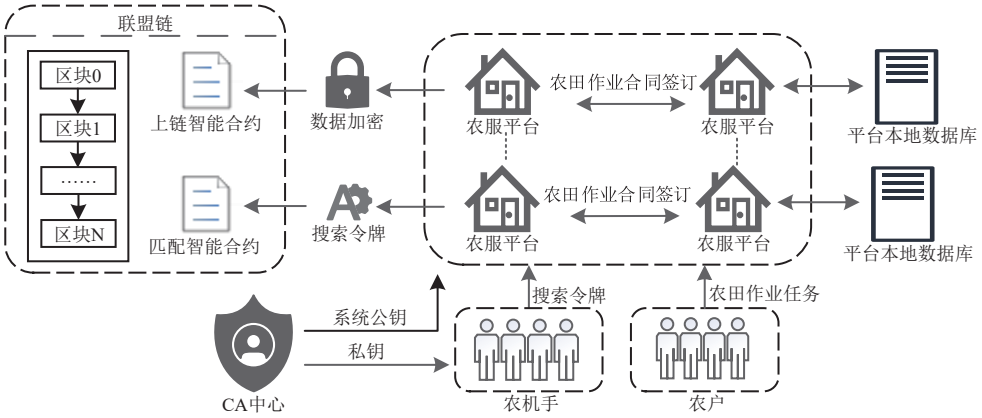


图 1 基于联盟链的农机社会化服务联合平台架构

Fig.1 Agricultural machinery socialization service federated platform architecture based on blockchain

1）CA 中心：全局证书机构，负责生成系统主密钥、系统公钥和农机手私钥。

2）农户：有农田作业需求的用户，通过农服平台在联盟链上发布农田作业任务。

3）农机手：具有闲置农机资源，提供农机服务的农机专业户。农机手使用私钥生成搜索令牌，通过农服平台调用智能合约匹配链上任务。

4）农服平台：农户和农机手对接的平台，是独立的企业或组织，在本地数据库中维护用户和任务的明文数据。主要负责 3 种业务，一是当平台内的农服资源无法满足农田作业任务时，加密任务数据，调用上链智能合约发布至联盟链中；二是接收本平台内农机手提交的搜索令牌，作为参数调用匹配智能合约；三是负责跨平台农田作业合同的签订。

5）联盟链：由农服平台构成联盟链网络，链上智能合约提供任务匹配服务，联盟链账本记录任务信息和平台之间的资源调用数据。

2.2 方案总体设计

在多方联合场景中，集中式服务器难以被各参与方同时信任，因此本方案基于联盟链构建去中心化的联合平台。由智能合约执行任务匹配，可信 CA 中心负责密钥服务。

针对多平台联合场景中敏感共享数据的隐私性和可用性需求，本文基于 CP-ABSE 技术构建匹配方案。将农田作业任务类型和农机手的任务偏好之间的匹配转化为加密关键字和密文索引之间的匹配问题；通过数据所有者和访问者之间细粒度访问控制，实现密文条件下农田作业需求与服务资源之间的匹配。

在农业生产中，农田作业任务具有地域性和大量突发性的特征，而农机手作为农机专业合作社或农机租

赁企业，能够为同区域内多个农田作业任务提供所需的服务资源。本文方案将多个农田作业任务编号以任务集合的形式与任务密文共同存储在联盟链账本中，成功匹配一条任务密文后返回多个任务编号，减少搜索令牌与任务密文的匹配次数，提高匹配智能合约的效率。

综上，农机社会化服务联合平台隐私匹配方案主要由系统建立、农机手注册、任务发布、任务匹配和跨平台农田作业等五个阶段构成，如图 2 所示。

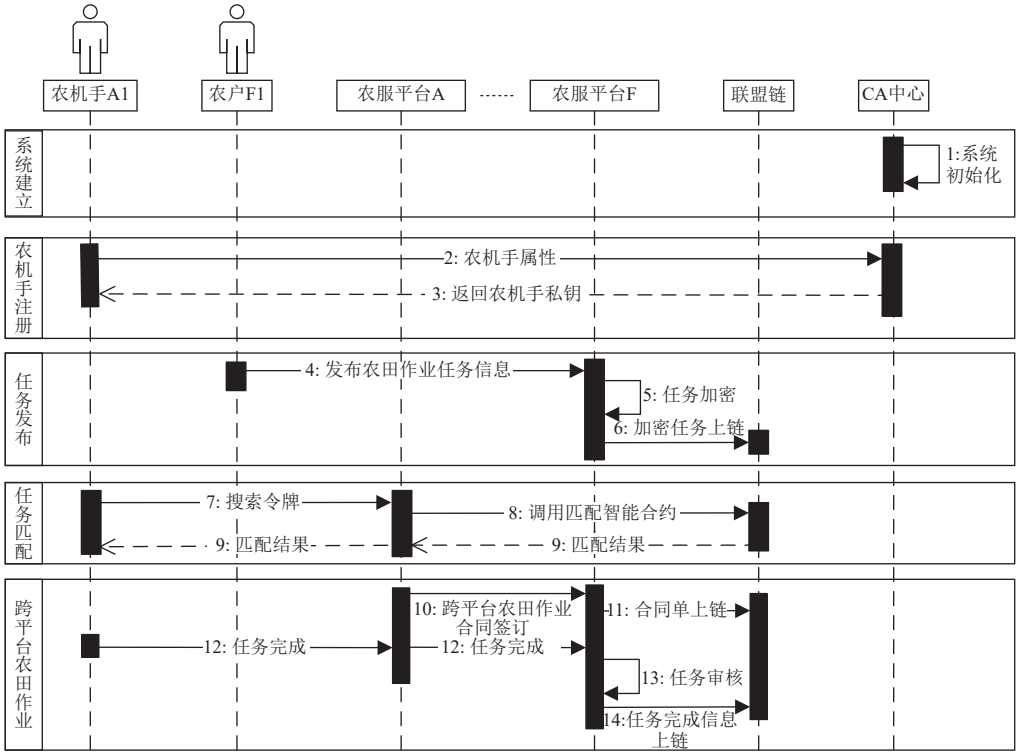


图 2　匹配方案流程

Fig.2　Task matching process

2.3　方案详细流程

农机社会化服务联合平台隐私匹配方案详细流程如下。

2.3.1　系统建立

本阶段分为全局属性设置和系统初始化 2 个步骤。

1）设置全局属性集U

联合平台各方共同设置一个全局属性集$U=\{attr_1, attr_2, \cdots, attr_n\}$，用来规范多平台联合时农机手属性和任务访问权限的设置，n为全局属性集合大小，$attr_i$为U中的一个属性，每个$attr_i$都有两个值v_i和$\neg v_i$，v_i和$\neg v_i$为系统建立阶段生成的随机数，$1\leqslant i\leqslant n$。属性或访问策略中包含属性$attr_i$时，$attr_i=v_i$；否则$attr_i=\neg v_i$。

2）系统初始化

CA中心选取一个安全参数λ，输出系统公钥K_{pub}和系统主密钥K_{pri}。

CA中心首先生成两个阶数为p的乘法循环群G和G_T，g为G的生成元，$e: G\times G\rightarrow G_T$是一个双线性映射，$Z_p$是$p$阶循环群。其次，定义单向哈希函数$H:\{0,1\}^*\rightarrow Z_p$，选取随机数$a, b, c\in Z_p$和随机数集合$\{r_1, r_2, \cdots, r_{2n}\}\in Z_p$、$\{x_1, x_2, \cdots, x_{2n}\}\in G$。最后，计算$u_i=g^{-r_i}$，$y_i=e(x_i, g)$，$K_{pub}=(g, g^a, g^b, g^c, u_i, y_i)$和$K_{pri}=(a, b, c, r_i, x_i)$，其中$1\leqslant i\leqslant 2n$。系统主密钥$K_{pri}$由 CA 中心保管，系统公钥$K_{pub}$公开。

2.3.2　农机手注册

本阶段分为属性和访问策略设置、农机手私钥申请 2 个步骤。

1）农机手属性和任务访问策略设置

设S^{u_r}为农机手u_r的属性集，P^{t_k}为农田作业任务t_k的访问策略。由于农机手属性和任务访问策略采用与门访问结构，S^{u_r}和P^{t_k}均可表示为n比特位的字符串，即$S^{u_r}=\tilde{v}_1^{u_r}\tilde{v}_2^{u_r}\cdots\tilde{v}_n^{u_r}$，$P^{t_k}=\hat{v}_1^{t_k}\hat{v}_2^{t_k}\cdots\hat{v}_n^{t_k}$，$\tilde{v}_i^{u_r}, \hat{v}_i^{t_k}\in U$分别表示$u_r$和$t_k$中的一个属性，与$attr_i$相同，$\tilde{v}_i^{u_r}$和$\hat{v}_i^{t_k}$值为$v_i$或$\neg v_i$。

若$\forall i\in[1, n]$，$\tilde{v}_i^{u_r}\in P^{t_k}$，即$\tilde{v}_i^{u_r}=\hat{v}_i^{t_k}$，则农机手属性$S^{u_r}$满足任务访问策略$P^{t_k}$。

2）农机手私钥申请

农服平台ID_m中的农机手u_r根据属性集S^{u_r}向CA中心申请私钥。CA中心根据S^{u_r}、系统公钥K_{pub}和系统主密钥K_{pri}生成农机手的私钥。

CA 中心计算$K_1^{u_r}=\prod_{i=1}^{n}k_{i,1}$，$K_2^{u_r}=\prod_{i=1}^{n}k_{i,2}$，对于农机手$u_r$的每个属性$\tilde{v}_i^{u_r}$，当$\tilde{v}_i^{u_r}=v_i$时，$k_{i,1}=x_i g^{acr_i}$，$k_{i,2}=y_i=e(x_i, g)$；当$\tilde{v}_i^{u_r}=\neg v_i$时，$k_{i,1}=x_{i+n}g^{acr_{i+n}}$，$k_{i,2}=y_{i+n}=e(x_{i+n}, g)$，其中$1\leqslant i\leqslant n$。然后，计算$K_3^{u_r}=g^{ac}$，农机手私钥$sk_{ID_m}^{u_r}=(K_1^{u_r}, K_2^{u_r}, K_3^{u_r})$。

2.3.3　任务发布

农服平台负责生成任务密文，调用上链智能合约将加密任务发布至联盟链中。

农服平台使用系统公钥K_{pub}加密农田作业任务，设任务编号为t_k，任务访问策略为P^{t_k}，任务类型为关键字w。农

服平台选取随机数$t_1, t_2 \in Z_p$，计算$C_1^{t_k}=g^{ct_1}$，$C_2^{t_k}=g^{a(t_1+t_2)}g^{bH(w)t_1}$和$C_3^{t_k}=g^{t_2}\prod_{i=1}^{n}\hat{u}_i^{t_k}$，对于$P^{t_k}$中的每个属性$\hat{v}_i^{t_k}$，当$\hat{v}_i^{t_k}=v_i$时，$\hat{u}_i^{t_k}=u_i=g^{-r_i}$；当$\hat{v}_i^{t_k}=\neg v_i$时，$\hat{u}_i^{t_k}=u_{i+n}=g^{-r_{i+n}}$。加密后的任务密文为$C_{t_k}=(C_1^{t_k}, C_2^{t_k}, C_3^{t_k})$。

农服平台调用上链智能合约将任务密文与对应任务集合T发布至联盟链中，T中包含一个或多个农田作业任务编号，即$T=<t_1, t_2, \cdots, t_k>$。

2.3.4 任务匹配

本阶段分为搜索令牌生成、智能合约执行任务匹配2个步骤。

1）搜索令牌生成

农机手u_r使用系统公钥K_{pub}和私钥$sk_{ID_m}^{u_r}$将任务偏好w'生成搜索令牌。农机手选取随机数$s \in Z_p$，计算$tok_1^{u_r}=(g^a g^{bH(w')})^s$和$tok_2^{u_r}=g^{cs}$，通过私钥计算$T_1^{u_r}=K_1^{u_r}$，$T_2^{u_r}=(K_2^{u_r})^s$，$T_3^{u_r}=(K_3^{u_r})^s$。最终搜索令牌$token_w^{u_r}=(tok_1^{u_r}, tok_2^{u_r}, T_1^{u_r}, T_2^{u_r}, T_3^{u_r})$。

2）智能合约执行任务匹配

农服平台收到农机手提交的搜索令牌$token$后，调用匹配智能合约，判断搜索令牌与任务密文是否匹配。

智能合约计算$\frac{e(C_2, tok_2)}{e(C_1, tok_1)}=\frac{e(C_3, T_3)e(T_1, g)}{T_2}$是否成立。若该等式成立，则搜索令牌与任务密文匹配成功，搜索令牌中的任务偏好与农田作业任务类型相匹配，且农机手的属性满足任务访问策略。搜索令牌与任务密文匹配成功后，智能合约返回任务Key值和文档集合T，否则返回匹配失败。

2.3.5 跨平台农田作业

由于跨平台的农机手资源调用涉及平台间资源整合和收益分配，因此，首先由任务发布平台和接收平台达成一致后签订跨平台农田作业合同。然后，任务发布平台向联盟链提交合同单，任务接收平台验证通过后上链。农机手完成农田作业任务后，通过所在平台将任务完成证明交付给任务发布平台。任务发布平台审核后，将链上合同单中的任务状态变更为已完成。

在匹配方案实际应用中，农机类型和农机手的属性不是固定的，联合平台可周期性的更新。更新流程如下：1）CA中心更新系统公钥和系统主密钥；2）农机手将更新后的属性集合提交给CA中心以更新私钥；3）各农服平台更新链上任务密文。

2.4 数据结构

联盟链账本中链上数据以Key-Value的方式存储。Value值由任务密文$C=<C_1, C_2, C_3>$与对应的任务集合$T=<t_1, t_2, \cdots, t_k>$组成，即Value$=<C, T>$，$T$中包含多个任务编号$t_k$。Key值由农服平台编号$ID_m$与平台发布的链上任务数量$task_n$共同组成，即Key$=ID_m+task_n$。

链上存储的跨平台农田作业合同单中，任务内容的哈希值F_{hash}和任务状态F_{state}作为Value值，即Value$=<F_{hash}, F_{state}>$；Key值由任务发布平台$\overline{ID}_m$、任务接收平台ID_m和双方已达成的交易数量$trade_n$共同组成，Key$=\overline{ID}_m+ID_m+trade_n$。跨平台农田作业合同签订时，任务状态$F_{state}$为未完成状态$F$，任务发布平台在确认任务完成后更改为已完成状态$T$。

2.5 智能合约设计

农机社会化服务联合平台隐私匹配方案中，设置任务上链、匹配等智能合约。智能合约与联盟链账本的交互通过应用程序接口（application programming interface，API）的调用实现，查询操作调用GetState API，上链和更新操作调用PutState API。

2.5.1 任务上链智能合约

农田作业任务具有时效性，若平台内农服资源短缺，将任务加密后调用上链智能合约发布至联盟链，并更新与链上加密任务对应的本地数据库。任务上链流程如图3所示。

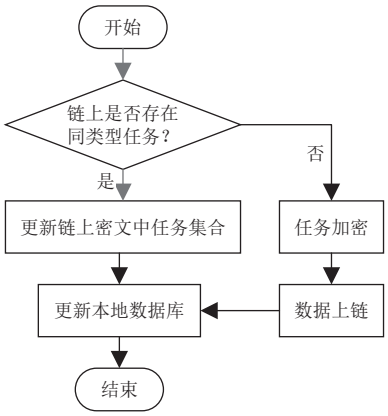


图3 任务上链流程

Fig.3 Task data upload process

在图3中，农服平台在将任务发布至联盟链前，首先检索本地数据库，判断链上是否存在同类型任务密文，即是否存在与待发布任务具有相同关键字和访问策略的链上加密任务，若存在，则更新链上任务集合T；若不存在，则将任务加密后发布至联盟链中。最后，更新本地数据库。

2.5.2 匹配智能合约

农服平台以农机手搜索令牌为参数调用匹配智能合约。匹配智能合约负责搜索令牌与任务密文间的匹配，运行流程如图4所示。

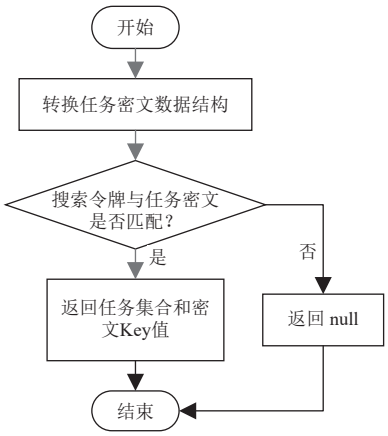


图4 匹配智能合约运行流程

Fig.4 The process of match smart contract

在图 4 中，智能合约从联盟链账本中获取任务密文后，首先将任务密文从 String 类型转换为密文数据结构，然后计算搜索令牌与任务密文是否正确匹配；若匹配，智能合约将任务集合T和任务 Key 值返回给平台，否则返回 null。

3　算法分析

3.1　正确性分析

农机社会化服务联合平台隐私匹配方案中，农机手任务偏好与任务类型相匹配，且属性满足任务访问策略时，搜索令牌$token$与密文C在匹配阶段的计算如下：

$$\begin{aligned}&\frac{e(C_2,tok_2)}{e(C_1,tok_1)}\\&=\frac{e\left(g^{a(t_1+t_2)}g^{bH(w)t_1},g^{cs}\right)}{e\left(g^{ct_1},(g^{a}g^{bH(w')})^{s}\right)}\\&=\frac{e(g,g)^{acst_1}e(g,g)^{acst_2}e(g,g)^{bcst_1H(w)}}{e(g,g)^{acst_1}e(g,g)^{bcst_1H(w')}}\\&=e(g,g)^{acst_2}\end{aligned}$$

$$\begin{aligned}&\frac{e(C_3,T_3)e(T_1,g)}{T_2}\\&=\frac{e\left(g^{t_2}\prod_{i=1}^{n}g^{-r_i},g^{acs}\right)e\left(\left(\prod_{i=1}^{n}x_ig^{acr_i}\right)^{s},g\right)}{\prod_{i=1}^{n}e(x_i,g)^{s}}\\&=\frac{e(g,g)^{acst_2}\prod_{i=1}^{n}e(g,g)^{-acsr_i}\prod_{i=1}^{n}e(x_i,g)^{s}\prod_{i=1}^{n}e(g,g)^{acsr_i}}{\prod_{i=1}^{n}e(x_i,g)^{s}}\\&=e(g,g)^{acst_2}\end{aligned}$$

可知，等式$\frac{e(C_2,tok_2)}{e(C_1,tok_1)}=\frac{e(C_3,T_3)e(T_1,g)}{T_2}$成立，搜索令牌与密文能够正确匹配。

3.2　安全假设

在许多基于区块链的研究[30-31]中，CA 中心均被假设为可信的，用来保证密钥的安全生成与分发，因此，本文假设 CA 中心是诚实的，会按照协议分发密钥和系统参数，通过安全信道传输数据。

参与构成联盟链的各农服平台通常为较大的企业或组织，理解信誉的重要性，因此假设农服平台是半诚实的，会按照协议的执行，但可能会试图从链上共享密文中推断额外信息。

农机手不会主动泄露自己的私钥。

3.3　安全性分析

1）数据的完整性

农田作业任务密文、跨平台农田作业合同单等存储在联盟链账本中，联盟链分布式数据存储、多方维护、共识确认等特性保证了链上账本中数据不可被篡改，从而保证了数据的完整性。

2）数据的机密性

文献 [21] 中选择关键字攻击游戏证明，如果敌手能够在多项式时间内以不可忽略的优势ε赢得游戏，则挑战者可以在一个多项式时间内以不可忽略的优势解决离散对数 (discrete logarithm，DL) 问题，因此本文使用 CP-ABSE 算法[21]保证了链上密文在选择关键字攻击下具有不可区分性。在 3.2 节的安全假设下，各平台无法从链上共享的密文中获知更多的额外信息，保证了数据的机密性。

3）匹配结果的可信性

本文方案中，搜索令牌由农机手生成，能够与任意平台发布的任务密文匹配；任务匹配通过智能合约以公开透明的方式进行；匹配结果不会存储在联盟链帐本中，避免了被动攻击，因此，匹配结果具有可信性。

4　试验与分析

4.1　测试环境

1）本文在 CPU 型号为 i7-7700HQ 且搭载 Windows10 的设备中进行测试，使用 VMware Workstation 构建 2 核 2 处理器的虚拟机，虚拟机运行内存为 6 GB，硬盘大小为 80 GB。

2）联盟链网络使用 Hyperledger Fabric 2.2 搭建，部署 3 个 orderer 节点为排序节点；部署 peer0.org1.federate.cn、peer1.org1.federate.cn、peer0.org2.federate.cn、peer1.org2.federate.cn 等 4 个 peer 节点充当记账节点，分别属于两个组织 org1 和 org2，每个组织中的 peer0 节点作为锚节点，负责与其他组织共享信息；共识算法选用 raft；状态数据库采用 levelDB；单个区块的最大交易数为 10 笔，最大打包时间间隔为 2 s，最大字节数为 10 MB。

3）CP-ABSE 算法基于密码库 jpbc v2.0.0 (http://gas.dia.unisa.it/projects/jpbc) 实现，使用 Type A 型素数阶椭圆曲线$y^2=x^3+x$。系统公钥、系统主密钥、密文、私钥和搜索令牌的数据结构主要通过Z_r、G_1、G_2和G_T群构造，算法执行过程调用密码库中 powZn 和 mul 等 API。

4）通过区块链基准测试工具 Hyperledger Caplier 测试性能。

4.2　功能测试与对比

1）功能测试

本文基于 CP-ABSE 构造的农机社会化服务联合平台隐私匹配方案功能测试如图 5 所示。

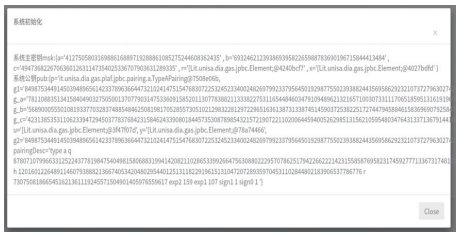
由 CA 中心负责生成的系统主密钥和系统公钥如图 5a 所示。假设农机手属性集S={“甘肃省”，“插秧机”}，农机手向 CA 中心申请属性私钥如图 5b 所示。

以平台 A 在联盟链中发布加密任务为例，设农田作业任务类型w={“小麦除草”}，访问策略P={“陕西省”，“大型割草机”}，任务编号t_k为 277，平台 A 在联盟链中已发布的任务数量为 37 且未上链同类型农田作业任务。平台 A 调用函数 compareToList 检索本地数据库 DB_Task，由于联盟链中账本数据以 Key-Value 的形式存储，此时任务 Key 值为“A38”，Value 值包括农田作业任务密文 C 和任务集合 T，Value={C,“277”}，如图 5c 所示。

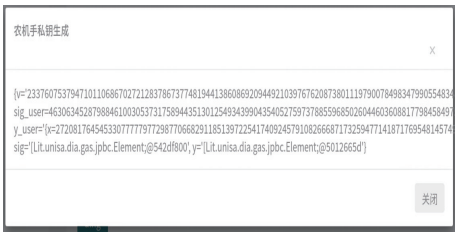
以平台 B 中农机手匹配链上任务为例，假设该农机手任务偏好w'={“小麦除草”}。农机手使用私钥生成搜索令牌 $token$，并发送给所在平台 B，如图 5d 所示。平台 B 将搜索令牌 $token$ 作为参数，调用智能合约 searchcc 匹配链上密文，返回密文 Key 值和任务集合 T，如图 5e 所示。

平台 B 中农机手接取平台 A 发布的农田作业任务，

通过 Hyperledger explorer 显示的跨平台农田作业合同单如图 5f 所示。

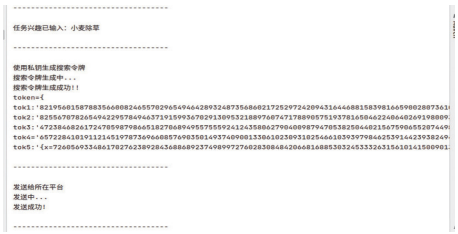


a. 系统主密钥和系统公钥生成
a. Master key and public key generation

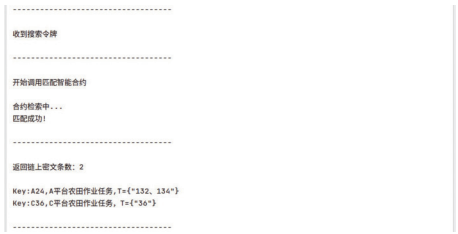


b. 农机手私钥生成
b. Agricultural mechanic private key generation

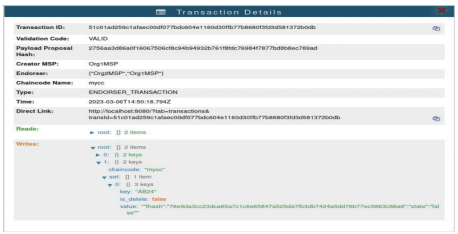
c. 数据加密并上链
c. Data encryption and upload



d. 搜索陷门生成
d. Token generation



e. 链上匹配
e. Match on blockchain



f. 跨平台农田作业合同单
f. Cross-platform agricultural task contract

图 5 功能测试
Fig.5 Function test

表 1 功能性对比

Table 1 The comparison of performance

方案 Scheme	方法 Method	区块链 Blockchain	不依赖代理加密 Independent of proxy re-encryption	细粒度访问控制 Fine-grained access control	密文搜索 Ciphertext searchable	多平台 Multi-platform federate
方案 1 Scheme1[10]	局部敏感哈希	×	√	–	×	√
方案 2 Scheme2[14]	多密钥全同态加密算法	√	–	×	×	–
方案 3 Scheme3[15]	可搜索加密	√	√	×	√	×
方案 4 Scheme4[18]	可搜索加密+代理重加密	√	×	×	√	√
本文方案 Scheme in this study	CP-ABSE	√	√	√	√	√

注：“√”文献方案支持此特性，“×”文献方案不支持此特性，“–”文献方案中无相应的特性要求。

Note: “√” This feature is supported by the literature scheme, “×” This feature is not supported by the literature scheme, “–” There is no corresponding feature requirement in the literature scheme.

由表 1 可以看出，方案 1[10] 和方案 2[14] 无法实现密文数据搜索功能，方案 2[14]、方案 3[15] 和方案 4[18] 均不能实现细粒度的访问控制，且方案 4[18] 需要依靠代理进行密文的安全转换。表 1 中文献所提方案均满足多方数据共享场景中对敏感数据的隐私保护需求，通过与以上方案对比，表明本文方案在功能性上具有一定的优势。

4.3 性能测试

本节对算法各阶段进行数值模拟实验，通过改变全局属性的数量来分析算法的效率，全局属性数量分别取值 50、100、150、200，测试包括本地性能测试和链上性能测试两个部分。

1）本地性能测试

本地性能测试的实验结果取算法运行 50 次的平均值，如图 6 所示。

由图 6a 可以看出，系统构建算法和私钥生成算法的运行时间与全局属性数量线性相关。当全局属性数量为 50 时，系统构建算法和私钥生成算法运行时间分别约 1.2 和 0.6 s，满足业务简单的联合平台的应用需求；当全局属性数量为 200 时，系统构建算法和私钥生成算法运行时间分别约 8 和 2.5 s，基本满足业务相对复杂的联合平台的应用需求。

2）功能对比

本文方案与文献[10,14-15,18] 的功能性对比如表 1 所示。

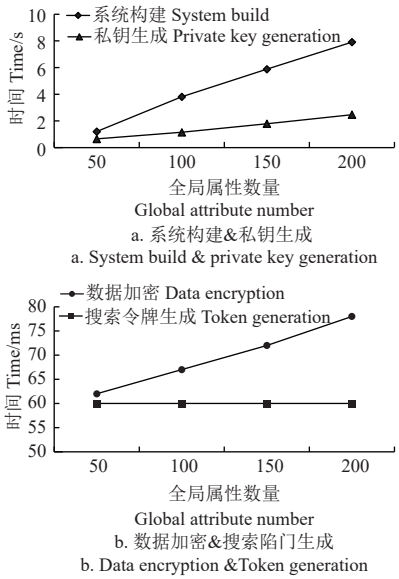


图 6　本地性能测试

Fig.6　Local performance test

由图 6b 可以看出，当全局属性数量发生变化时，搜索令牌生成算法的计算开销基本稳定在 60 ms 左右，数据加密算法的计算时间分布在 60～80 ms 区间内，两种算法运行时间较低，满足联合平台中任务发布和农机手生成搜索令牌两种运行次数较多的业务需求。

2）链上性能测试

链上性能测试中将交易总量设置为 5 000，以平均时延作为性能评估指标，取 5 次测试的平均值。实验结果表明匹配智能合约的平均时延约为 250 ms，不会随着全局属性个数的增加而改变。因为 CP-ABSE 算法生成的密文长度恒定，匹配智能合约的计算过程与全局属性数量无关。

5　结　论

本文基于联盟链构造了农机社会化服务联合平台，使用 CP-ABSE 技术设计并实现了联合平台中保护隐私的匹配方案。本方案使用智能合约提供任务匹配服务，保证匹配结果的可信性；基于 CP-ABSE 实现任务发布方和农机手双方敏感数据加密条件下的可搜索性，农户可以自主设置访问策略，达到细粒度的访问控制。

安全性分析表明，本方案可以保证区块链账本中敏感共享数据在选择关键字攻击下的不可区分性，保证了数据完整性和机密性。基于 Hyperledger Fabric 构建了农机社会化服务联合平台原型系统，功能测试结果表明，该方案能够实现数据加密情况下，区块链中安全、准确和细粒度的跨平台匹配；性能测试结果表明，算法的运行效率基本满足联合平台的应用需求。

本文基于 CP-ABSE 技术提出的隐私匹配方案在农机社会化服务联合平台中具有可行性和有效性，满足数据隐私性、完整性和可信性的需求以及平台的性能要求，但在改进和优化方面仍然存在一些可行的技术点，如多关键字搜索、可追责性等。多关键字搜索可提高搜索的准确性和效率，提升用户的搜索体验，具有更高的实用性；可追责 CP-ABSE 能够增强联合平台对私钥泄露问题的监测和追踪能力。

［参　考　文　献］

[1] 耿鹏鹏，檀竹平，罗必良. “挤出”抑或“吸纳”：农机服务如何影响农业劳动力转移[J]. 华中农业大学学报（社会科学版），2022，160(4)：24-37.
GENG Pengpeng, CHAN Zhuping, LUO Biliang. “Squeezing out” or “Absorption”: How agricultural machinery services affect the transfer of agricultural labor[J]. Journal of Huazhong Agricultural University (Social Sciences Edition), 2022, 160(4): 24-37. (in Chinese with English abstract)

[2] 纪月清，王许沁，陆五一，等. 农业劳动力特征、土地细碎化与农机社会化服务[J]. 农业现代化研究，2016，37(5)：910-916.
JI Yueqing, WANG Xuqin, LU Wuyi, et al. The characteristics of rural labors, land fragmentation, and agricultural machinery services[J]. Research of Agricultural Modernization, 2016, 37(5): 910-916. (in Chinese with English abstract)

[3] 赵春江，李瑾，冯献. 面向 2035 年智慧农业发展战略研究[J]. 中国工程科学，2021，23(4)：1-9.
ZHAO Chunjiang, LI Jin, FENG Xian. Development strategy of smart agriculture for 2035 in China[J]. Strategic Study of CAE, 2021, 23(4): 1-9. (in Chinese with English abstract)

[4] 李忠旭，庄健. 互联网使用、非农就业与农机社会化服务——基于 CLDS 数据的经验分析[J]. 农林经济管理学报，2021，20(2)：166-175.
LI Zhongxu, ZHUANG Jian. Internet usage, non-agriculture and agricultural machinery socialized services: Empirical analysis vased on data from CLDS[J]. Journal of Agro-Forestry Economics and Management, 2021, 20(2): 166-175. (in Chinese with English abstract)

[5] 杨昊天，王良民，刘路， 等. 基于区块链的农机跨区域调度模型构建与应用[J]. 农业工程学报，2022，38(11)：31-40.
Yang Haotian, Wang Liangmin, Liu Lu, et al. Model construction and application of agricultural machinery cross-region scheduling based on blockchain[J]. Transactions of the Chinese Society of Agricultural Engineering (Transactions of the CSAE), 2022, 38(11): 31-40. (in Chinese with English abstract)

[6] 张帆，罗锡文，张智刚等. 基于改进多父辈遗传算法的农机调度优化方法 [J]. 农业工程学报，2021，37（9）：192-198.
Zhang Fan, Luo Xiwen, Zhang Zhigang, et al. Agricultural machinery scheduling optimization method based on improved multi-parents genetic algorithm[J]. Transactions of the Chinese Society of Agricultural Engineering (Transactions of the CSAE), 2021, 37(9): 192-198. (in Chinese with English abstract)

[7] 张璠，滕桂法，苑迎春，等. 农机跨区作业紧急调配算法适宜性选择[J]. 农业工程学报，2018，34(5)：47-53.
Zhang Fan, Teng Guifa, Yuan Yingchun, et al. Suitability selection of emergency scheduling and allocating algorithm of

agricultural machinery[J]. Transactions of the Chinese Society of Agricultural Engineering (Transactions of the CSAE), 2018, 34(5): 47-53. (in Chinese with English abstract)

[8] 彭滔，钟文韬，王国军，等. 移动社交网络中面向隐私保护的精确好友匹配[J]. 通信学报，2022，43(11)：90-103.
PENG Tao, ZHONG Wentao, WANG Guojun, et al. Privacy-preserving precise profile matching in mobile social network[J]. Journal on Communications, 2022, 43(11): 90-103. (in Chinese with English abstract)

[9] SHU J, JIA X. Secure task recommendation in crowdsourcing[C]// 2016 IEEE Global Communications Conference (GLOBECOM). Washington: IEEE, 2016: 1-6.

[10] QI L, WANG X, XU X, et al. Privacy-aware cross-platform service recommendation based on enhanced locality-sensitive hashing[J]. IEEE Transactions on Network Science and Engineering, 2020, 8(2): 1145-1153.

[11] SOBITHA A S, SHUNMUGANATHAN K L. Role of agent technology in web usage mining: homomorphic encryption based recommendation for e-commerce applications[J]. Wireless Personal Communications, 2016, 87(2): 499-512.

[12] SHU J, JIA X, YANG K, et al. Privacy-preserving task recommendation services for crowdsourcing[J]. IEEE Transactions on Services Computing, 2018, 14(1): 235-247.

[13] YIN H, XIONG Y, DENG T, et al. A privacy-preserving and identity-based personalized recommendation scheme for encrypted tasks in crowdsourcing[J]. IEEE Access, 2019, 7: 138857-138871.

[14] 刘雪娇，王慧敏，夏莹杰，等. 具有隐私保护的车联网空间众包任务分配方法[J]. 浙江大学学报（工学版），2022，56(7)：1267-1275.
LIU Xuejiao, WANG Huimin, XIA Yingjie, et al. Task allocation method for Internet of vehicles spatial crowdsourcing with privacy[J]. Journal of Zhejiang University (Engineering Science), 2022, 56(7): 1267-1275. (in Chinese with English abstract)

[15] WU Y, TANG S, ZHAO B, et al. BPTM: Blockchain-based privacy-preserving task matching in crowdsourcing[J]. IEEE Access, 2019, 7: 45605-45617.

[16] 牛淑芬，陈俐霞，李文婷，等. 基于区块链的电子病历数据共享方案[J]. 自动化学报，2022，48(8)：2028-2038.
NIU Shufen, CHEN Lixia, LI Wenting, et al. Electronic medical record data sharing scheme based on blockchain[J]. Acta Automatica Sinica, 2022, 48(8): 2028-2038. (in Chinese with English abstract)

[17] 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 on Communications, 2020, 41(8): 204-214. (in Chinese with English abstract)

[18] GUO Y, XIE H, MIAO Y, et al. Fedcrowd: A federated and privacy-preserving crowdsourcing platform on blockchain[J]. IEEE Transactions on Services Computing, 2020, 15(4): 2060-2073.

[19] 景旭，蒋炎. 集群式农产品供应链区块链密文策略可验多部门监管方案[J]. 农业工程学报，2023，39(3)：227-236.
JING Xu, JIANG Yan. Multi-department supervision scheme of the verifiable blockchain ciphertext policy for cluster agricultural supply chain[J]. Transactions of the Chinese Society of Agricultural Engineering (Transactions of the CSAE), 2023, 39(3): 227-236. (in Chinese with English abstract)

[20] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Decentralized Business Review, 2008: 21260.

[21] GUO W F, DONG X L, CAO Z F, et al. Efficient attribute-based searchable encryption on cloud storage[J]. Journal of Physics: Conference Series, 2018, 1087(5): 052001.

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

[23] SONG D X, WAGNER D, PERRIG A. Practical techniques for searches on encrypted data[C]// Proceeding 2000 IEEE Symposium on Security and Privacy. Berkeley: IEEE Press, 2000: 44-55.

[24] 杜瑞忠，谭艾伦，田俊峰. 基于区块链的公钥可搜索加密方案[J]. 通信学报，2020，41(4)：114-122.
DU Ruizhong, TAN Ailun, TIAN Junfeng. Public key searchable encryption scheme based on blockchain[J]. Journal on Communications, 2020, 41(4): 114-122. (in Chinese with English abstract)

[25] 杨旸，林柏钢，马懋德. 具有细粒度访问控制的隐藏关键词可搜索加密方案[J]. 通信学报，2013，34(S1)：92-100.
YANG Yang, LIN Bogang, MA Maode. Secure hidden keyword searchable encryption scheme with fine-grained and flexible access control[J]. Journal on Communications, 2013, 34(S1): 92-100. (in Chinese with English abstract)

[26] WANG Q, ZHU Y, LUO X. Multi-user searchable encryption with coarser-grained access control without key sharing[C]// 2014 International Conference on Cloud Computing and Big Data. Wuhan: IEEE, 2014: 119-125.

[27] 谢晴晴，董凡. 轻量级区块链技术综述[J]. 软件学报，2023，34(1)：33-49.
XIE Qingqing, DONG Fan. Survey on lightweight blockchain technology[J]. Journal of Software, 2023, 34(1): 33-49. (in Chinese with English abstract)

[28] Szabo N. Smart contracts: building blocks for digital markets[J]. EXTROPY:The Journal of Transhumanist Thought, 1996, 18(2): 28.

[29] 刘敖迪，杜学绘，王娜，等. 区块链技术及其在信息安全领域的研究进展[J]. 软件学报，2018，29(7)：2092-2115.
LIU Aodi, DU Xuehui, WANHG Na, et al. Research progress of blockchain technology and its application in information security[J]. Journal of Software, 2018, 29(7): 2092-2115. (in Chinese with English abstract)

[30] 赵子军，应作斌，杨钊，等. 结合区块链和车辆社交网络的车队成员推荐[J]. 西安电子科技大学学报，2020，47(5)：

122-129.
ZHAO Zijun, YING Zhuobin, YANG Zhao, et al. Recommendation of platoon members by combining the blockchain and vehicular social network[J]. Journal of Xidian University, 2020, 47(5): 122-129. (in Chinese with English abstract)

[31] 张磊，郑志勇，袁勇. 基于区块链的电子医疗病历可控共享模型[J]. 自动化学报，2021，47(9)：2143-2153.
ZHANG Lei, ZHENG Zhiyong, YUAN Yong. A Controllable sharing model for electronic health records based on blockchain[J]. Acta Automatica Sinica, 2021, 47(9): 2143-2153. (in Chinese with English abstract)

CP-ABSE based privacy-preserving match scheme on agricultural machinery socialized service consortium blockchain

JING Xu[1], TAN Han[1], JIANG Yan[1], RUAN Junhu[2※]

(1. *College of Information Engineering*, *Northwest A&F University*, *Yangling* 712100, *China*;　2. *College of Economics & Management*, *Northwest A&F University*, *Yangling* 712100, *China*)

Abstract: The purchase and maintenance of agricultural machinery can be one of the most formidable challenges for smallholder farmers in recent years. The agricultural machinery socialization services can effectively improve the quality of agricultural production through integration and redistribution of farm machinery resources. However, the traditional agricultural machinery socialization systems tend to confine the resources within their respective individual systems. The participation of tasks and workers was limited in the matching processes of other systems. Thus, a federated platform is necessary to combine the different agricultural machinery services in order to facilitate the development of agricultural modernization by sharing the resources for cross-platform matching. But, the implementation of the federated platform can cause significant security concerns. For example, there is a potential risk of sensitive information leakage, when the data is shared across different platforms, resulting in serious privacy violations. Additionally, the centralized servers responsible for the task-matching services cannot always return accurate predicts. Therefore, it is crucial to explore safe and reliable privacy matching in the federated platform. In this study, a privacy-preserving matching scheme was introduced using CP-ABSE. The farming tasks were matched to the optimal farm mechanics. The blockchain was then employed as the underlying platform to establish the federation of agricultural machinery service platforms. The blockchain ledger was selected to record the task information of each platform and the transferring data of cross-platform, in order to avoid tampered data. Furthermore, each agricultural machinery service maintained the autonomy to access and then utilize the potential resources from other cooperation platforms. CP-ABSE technology was used to ensure the confidentiality of sensitive data in both tasks and farmers. As such, an accurate matching was achieved under ciphertext conditions. The matching farming tasks and agricultural mechanics were transformed into a task access control and keyword-based search. Specifically, the matching between farming task types and mechanics' interests could be transformed to the match between encrypted keywords and ciphertext indexes by the matching scheme. The fine-grained access control between multiple data owners and users was taken as the matching between farming operation requirements and farm services available from mechanics. Simultaneously, the service code was deployed onto the smart contracts. Different agricultural machinery service platforms published the encrypted task requirements on the blockchain using upload smart contracts. Smart contracts were then matched to perform the secure task-matching services. This approach replaced the need for a centralized server, such as the single points of failure and tampering with the match data. The security analysis showed that the matching scheme was achieved in the integrity and confidentiality of sensitive data that was shared with other cooperative platforms. Additionally, the ciphertext of tasks stored on the blockchain ledger possessed indistinguishability, which could resist the selective plaintext attacks. Finally, a prototype test system was constructed using Hyperledger Fabric, in order to verify the effectiveness of the matching scheme. The average latency of the matching smart was contracted around 250 ms, indicating that the operation efficiency of the algorithm fully met the basic application requirements of the federated platform. The scheme can be expected to effectively achieve the security of sensitive data and cross-platform task matching in the federation platforms of agricultural machinery service.

Keywords: blockchain; agricultural machinery socialization service; consortium blockchain; privacy matching; searchable encryption; attribute-based encryption