# 基于 CP-ABE 算法的区块链数据访问控制方案

邱云翔[1]，张红霞[2]，曹琪[2]，章建聪[1]，陈兴蜀[2]，金泓键[2]
（1. 华信咨询设计研究院有限公司，浙江 杭州 310000；
2. 四川大学网络空间安全学院，四川 成都 610065）

**摘　要：**与公有链不同，联盟区块链超级账本 Fabric 额外集成了成员管理服务机制，能够提供基于通道层面的数据隔离保护。但这种数据隔离保护机制在通道内同步的仍是明文数据，因此存在一定程度的数据泄露风险。另外，基于通道的数据访问控制在一些细粒度隐私保护场景下也不适用。为了解决上述提及的联盟链超级账本中存在的数据隐私安全问题，提出了一种基于 CP-ABE 算法的区块链数据访问控制方案。结合超级账本中原有的 Fabric-CA 模块，提出的方案在实现用户级细粒度安全访问控制区块链数据的同时，还能够实现对 CP-ABE 方案中用户属性密钥的安全分发。对该方案进行的安全分析表明，该方案实现了 ABE 用户属性私钥安全分发和数据隐私性保护的安全性目标，性能分析部分也说明了所提方案具有良好的可用性。

**关键词：**区块链；超级账本；CP-ABE；数据访问控制
**中图分类号：**TP309.2
**文献标识码：**A
**doi:** 10.11959/j.issn.2096−109x.2020037

# Blockchain data access control scheme based on CP-ABE algorithm

QIU Yunxiang[1], ZHANG Hongxia[2], CAO Qi[2], ZHANG Jiancong[1], CHEN Xingshu[2], JIN Hongjian[2]
1. Huaxin Consulting Co., Ltd., Hangzhou 310000, China
2. College of Cybersecurity, Sichuan University, Chengdu 610065, China

**Abstract:** Different from the public chain, the consortium blockchain Hyperledger Fabric integrates the additional member management service(MSP) mechanism to provide channel-based data isolation protection. However, the data isolation protection mechanism still synchronizes the plaintext data within a channel, so there is a risk of data leakage. Besides, the channel-based data access control mechanism does not apply to some fine-grained privacy protection scenarios. To solve the problems of data privacy and security involved in the consortium chain Hyperledger mentioned above, a blockchain data access control scheme based on the CP-ABE algorithm was proposed. Based on the original existing Fabric-CA module in the Hyperledger, our scheme can realize the secure distribution

**收稿日期：**2019−12−10；**修回日期：**2020−02−07
**通信作者：**章建聪，zhangjc@hxdi.com
**基金项目：**中央高校基本科研业务费基础研究基金（SCU2018D018，SCU2018D022，2019SCU12069）
**Foundation Item:** The Fundamental Research Funds for the Central Universities (SCU2018D018, SCU2018D022, 2019SCU12069)

**论文引用格式：**邱云翔, 张红霞, 曹琪, 等. 基于 CP-ABE 算法的区块链数据访问控制方案[J]. 网络与信息安全学报, 2020, 6(3): 88-98.
QIU Y X, ZHANG H X, CAO Q, et al. Blockchain data access control scheme based on CP-ABE algorithm[J]. Chinese Journal of Network and Information Security, 2020, 6(3): 88-98.

of user attribute keys in the CP-ABE scheme while implementing the fine-grained security access control of blockchain data at the user level. The security analysis shows that the scheme achieves the security goals of ABE user attribute private key security distribution and data privacy protection. The performance analysis also shows that the proposed scheme has good usability.

**Key words:** blockchain, Hyperledger, CP-ABE, data access control

## 1　引言

联盟区块链超级账本[1]（Hyperledger）是 Linux 基金会发起的区块链技术项目，该项目致力于发展跨行业的商用区块链平台技术。区别于人们熟知的公有链，如比特币[2]和以太坊[3-4]等，超级账本技术额外融合了成员管理服务机制[5]，实现了更加适于商用的身份管理、网络隐私、保密以及审查等功能。

传统的区块链网络中，默认情况下整个网络中的数据对每个节点和用户来说都是可见的，这就带来了一定的数据隐私安全隐患：在某些应用场景下，某些敏感的数据并不能以明文方式在整个网络中进行同步。为了解决网络节点数据的透明性带来的安全隐私问题，联盟区块链超级账本增加了对多通道的支持[6]，使同一通道中的节点共同维护一份账本，不同通道中的数据相互隔离。通过这种多通道数据隔离机制，超级账本技术大大增强了数据隐私保护的力度。但在默认情况下，通道中的数据对同一通道中的节点来说仍是完全可见的，因此这种机制仍然存在以下问题。① 数据泄露风险：节点一旦被攻击者攻破，其中的明文数据就会被攻击者全数掌握。② 数据隐私保护粒度过粗：这种基于通道的粗粒度数据隐私保护方式在某些细粒度数据访问控制场景中并不适用。因此，需要一种更加细粒度的数据安全访问控制机制。

基于上述提到的粗粒度数据访问及数据加密问题，在超级账本官方的版本更新中也提出了相应的解决方案，即数据对称加密上链[7]：通过对明文数据进行对称加密然后上链的方式，使只有拥有对称解密密钥的用户才能获取真正的明文数据。这从一定程度上解决了细粒度数据隐私保护的问题。但在实际应用中，为了达到细粒度安全访问控制的需求，该方案要求每份上链数据都需要维护独立的密钥，且需要单独将该密钥分发给访问控制策略中包含的所有接收者。这一过程中涉及大量密钥生成、分发与管理操作，使这一方案并不高效。超级账本官方提出的另一种解决方案是隐私数据机制[8]：通过在授权的组织节点中传递和同步真正的明文数据，非授权的组织节点间传递和同步数据哈希值的做法，该机制可以将数据隐私保护细化到通道中的组织层面，即可以实现通道中某些组织间的私密数据共享，一定程度上解决了本文的问题。但是，在默认情况下，由于在授权的节点之间同步的数据仍是明文数据，这种机制并未根本上解决数据泄露带来的安全性问题。另外，正如上述提到的，隐私数据机制只能将对数据的访问控制细化到组织层面，在一些希望实现基于组织中用户访问控制的场景中，这种机制其实并不能满足本文的需求。

本文针对超级账本 Fabric 目前存在的细粒度数据隐私保护需求，设计了一种基于 CP-ABE 算法的区块链数据访问控制方案，主要贡献如下。

1) 基于 CP-ABE 算法，提出了一种适用于超级账本 Fabric 网络的数据访问控制机制，在保证数据不被泄露的同时能够实现基于用户的最细粒度的数据访问控制。

2) 基于超级账本中已有的 Fabric-CA 模块，实现 CP-ABE 用户属性密钥的动态生成和安全分发等操作。在不影响超级账本原有结构和运行机制的前提下，通过非对称加密算法对用户属性密钥进行加密传输，解决了传统加密方案中广泛存在的密钥分发问题。

## 2　背景技术

### 2.1　区块链和超级账本

#### 2.1.1　区块链和超级账本技术简介

区块链的概念源于比特币[2]，其有效地解决了去中心化分布式场景中节点间的信任问题[9]。从本质上来说，区块链是一种特殊的数据结构，通过结合多种密码学技术和分布式网络技术，区

块链将一个个数据块以链的方式组织起来。同时，区块链使用点对点传输技术和共识机制（如 PoW[10]、PoS[11-12]等），使多个节点之间保存相同的数据内容，并利用这种冗余机制来实现数据的不可篡改性和持久性。区块链网络严格按照“少数服从多数”的机制保证节点间数据的一致性，这意味着攻击者必须控制超过半数的区块链节点（51%攻击[13]）才能实现非法修改或删除已经存在于链上的记录，而这种攻击方式在大规模部署的分布式区块链网络中几乎不可能实现，因此一般认为存储在区块链中的数据是安全的。同时，以以太坊为代表的区块链网络集成了智能合约，使更加复杂和高级的分布式应用得以实现。因为区块链技术的去中心化、上链数据不可篡改、交易内容可追溯以及智能合约实现等特性，学术界和工业界开展了很多的研究工作，目前区块链技术在金融服务、征信和权属管理、资源共享、供应链管理、隐私保护以及公共网络服务等场景中有广泛的应用[14]。

根据系统控制权和交易信息公开与否进行归类[15]，区块链可以分为公有链、私有链和联盟链 3 类。公有链没有任何准入机制，任意节点都可以加入网络中，且信息对整个系统公开，是完全去中心化的点对点系统，如比特币和以太坊等。私有链目前多用于测试场景下，其与普通意义上的数据库并无本质上的区别，只适用于限定的机构之内。联盟链则指的是区块链中设计了特殊的准入机制，交易信息只针对局部进行公开，区块链节点通常需要通过合法的证书才能够发起交易或访问区块链上的内容，这样的设计尤其适合于商业应用场景，在保护商业隐私的同时，能够解决跨机构商业伙伴间的互信问题。

作为联盟区块链的代表技术，超级账本区块链并不是完全去中心化的，而是有若干组织机构共同参与和管理，另外配置一个专用的证书授权机构 Fabric-CA 来处理节点或用户的接入身份权限问题。相比传统公有链技术，超级账本在扩展性和智能合约的功能完善性方面都有了大幅的提升。超级账本支持拜占庭共识协议和基于 Kafka 的崩溃容错共识协议，能够实现快速有效的交易共识。另外，超级账本支持多种常规编程语言智能合约，如 Go、Node.js 和 Java 等。这也意味着在超级账本区块链上部署的智能合约，理论上能够支持任何功能，使超级账本在支撑商业应用时不会受限于编程实现问题。

为了解耦功能，提升扩展性，Fabric 中设计了两种类型的节点：排序节点（Orderer）和对等节点（Peer）。排序节点负责对交易按照规则进行排序并生成区块，可由多个排序节点组成排序集群。排序节点间的共识可采用 PBFT（实用拜占庭容错）算法[16]或基于 Kafka[17]的崩溃容错算法等。对等节点负责验证和同步数据，执行智能合约（Fabric 中又称为链码）等功能。根据节点功能的不同，对等节点又可以分为背书节点、记账节点、主节点、锚节点等，节点身份可基于特定规则切换。功能松耦合、实现模块化保证 Fabric 网络具有良好的扩展性。

#### 2.1.2 Fabric-CA 简介

超级账本区块链网络属于许可链类型，当新用户需要接入网络时，需要从专门的机构获取合法证书，Fabric-CA[18]用于实现这一机构的所有功能。Fabric-CA 由服务器（fabric-ca-server）和客户端（fabric-ca-client）组件组成。它提供 3 个功能：一是注册新用户身份，注册结果将作为用户证书申请的凭据；二是签发证书，即为合法的注册票据生成证书；三是证书更新或撤销，当 Fabric 网络中的用户信息更新时，这一功能将更新对应用户的证书信息。

Fabric-CA 架构如图 1 所示，新用户可通过独立的 Fabric-CA 客户端或集成该客户端的 SDK 程序与 Fabric-CA 服务端交互，其中所有通信都通过 REST API 进行。

#### 2.1.3 超级账本交易流程

典型的超级账本 Fabric 交易流程如图 2 所示。用户在加入超级账本网络之前，可以向 Fabric-CA 注册并获取合法的证书，之后即可使用该证书通过命令行或 Fabric-SDK 与区块链网络交互。超级账本支持多通道机制，每个通道维护着一个独立的区块链账本，区块根据通道 ID 进行分发，通道间数据完全隔离。用户在发起交易时需指定通道 ID（图 2 中的 Channel 1 或 Channel 2），并将交易提案发送给背书节点，背书节点处理请求后，向

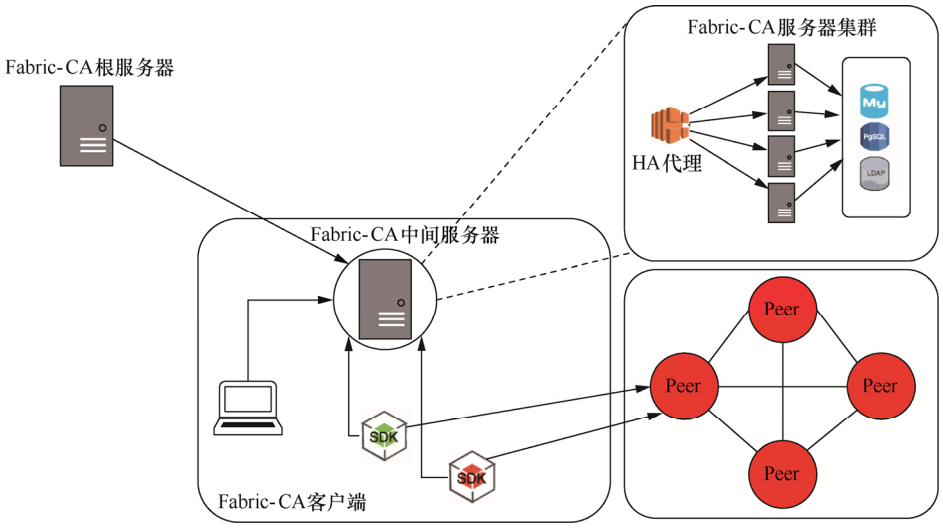



图 1　Fabric-CA 架构
Figure 1　The framework of Fabric-CA

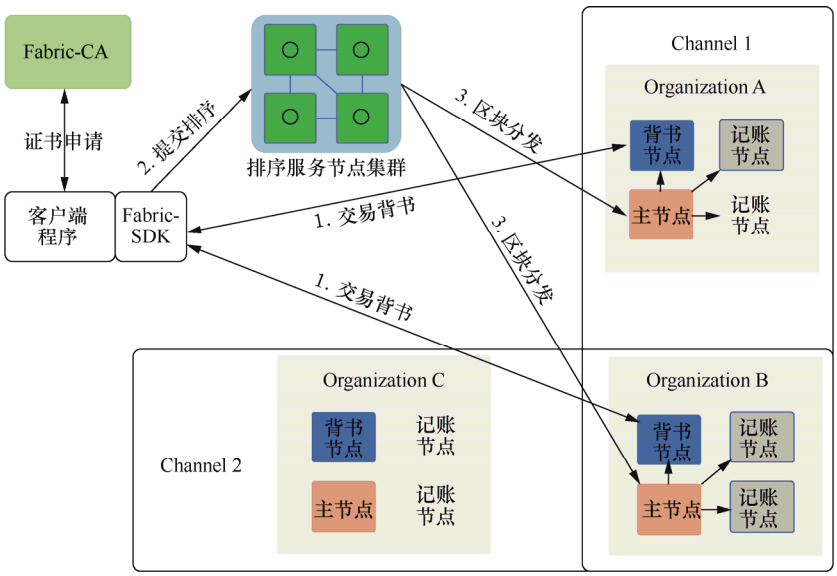



图 2　Fabric 交易流程
Figure 2　The transaction process of Fabric

客户端返回签名后的背书响应（图 2 中 1.）。随后客户端组合来自不同背书节点的背书响应并将最终交易内容发送至排序服务集群进行处理（图 2 中 2.）。在排序完成后，排序节点将根据交易所述通道，将其分发至该通道中的所有主节点，由主节点进行组织内的区块同步。最终收到交易后，各节点验证交易内容和签名，并将合法的交易添加到区块链账本中。

### 2.2　属性基加密技术

属性基加密（ABE，attribute-based encryption）最早由 Goyal 等[19]在 FIBE（fuzzy identity-based encryption）[20]的基础上提出，目的是解决云存储环境中数据的细粒度访问控制问题和大规模用户动态扩展问题[21]。ABE 本质上属于非对称加密技术，但其采用一对多的加密方式。根据解密策略的位置不同，ABE 可以分为密钥策略属性基加密（KP-ABE，key policy attribute-based encryption）[19]和密文策略属性基加密（CP-ABE，ciphertext policy attribute-based encryption）[22]。在 KP-ABE 中，密文的解密策略在密钥生成时被嵌入用户的

私钥中，相关属性则在加密时被嵌入密文中，即访问策略与密钥相关联；在 CP-ABE 中，解密策略在加密时被嵌入密文中，而用户的属性则在密钥生成时被嵌入其私钥中，即访问策略与密文相关联。不论 KP-ABE 还是 CP-ABE，用户都只能在私钥和密文中嵌入的属性集和访问控制策略完全匹配时，才能解密该密文[23]。由于访问控制策略与属性集可能存在一对多的关系，因此 ABE 技术自然地实现了加密访问控制功能。同时根据加密或密钥生成时所指定策略的严格程度，ABE 方案可以灵活地选择密文访问控制机制的粒度。以 CP-ABE 方案为例，通常情况下包含以下 4 种算法。

1) 初始化算法：$(PK,MK) \leftarrow Setup(1^{\lambda})$。

通过传入安全参数 $\lambda$，该算法主要完成方案的初始化过程，生成公开参数 PK 和主密钥 MK。

2) 密钥生成算法：$SK \leftarrow KeyGen(MK,S)$。

通过传入主密钥 MK 和属性集 $S$，该算法为用户生成属性私钥 SK。

3) 加密算法：$CT \leftarrow Encrypt(PK,M,A)$。

通过传入公开参数 PK、明文 $M$ 以及访问结构 $A$，该算法将明文 $M$ 加密成为密文 CT。生成的密文 CT 只能被满足访问结构 $A$ 的用户解密。

4) 解密算法：$M \leftarrow Decrypt(PK,CT,SK)$。

在用户属性私钥 SK 中包含的属性满足密文 CT 包含的访问结构 $A$ 时，通过传入公开参数 PK、密文 CT 和用户私钥 SK，该算法将密文 CT 解密为明文 $M$。

考虑到本文方案的应用需求（即需要由上传数据的用户指定加密数据的用户访问控制列表），将解密策略嵌入密文中的方案 CP-ABE 更适合本文的应用需求。

## 3 方案设计

### 3.1 总体方案框架

针对第 1 节提出的区块链数据访问控制问题，本文提出了一种基于 CP-ABE 算法实现区块链数据访问控制的方案。通过：① 修改原有的用户证书管理机构 Fabric-CA，来实现 CP-ABE 方案初始化以及用户属性私钥的生成和分发；② 将隐私数据通过 CP-ABE 方案加密上链，以实现隐私数据的加密访问控制机制。该方案主要由证书颁发机构 Fabric-CA、区块链网络 Fabric 和客户端 Client 组成，总体方案框架如图 3 所示。

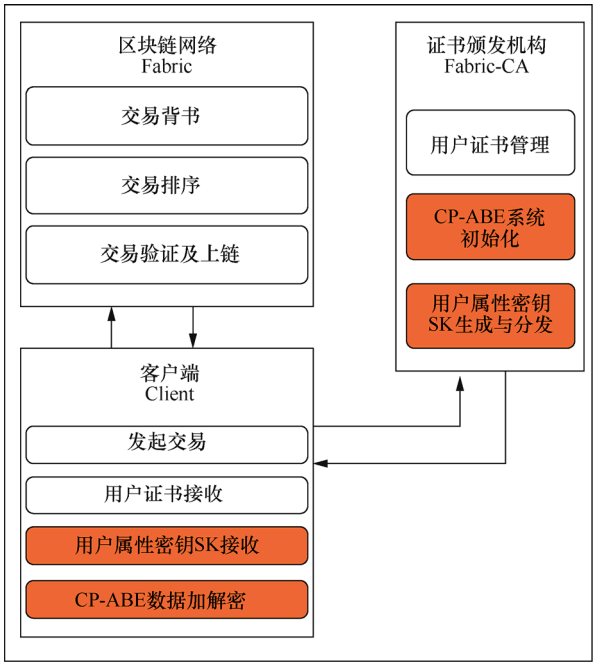



图 3 总体方案框架
Figure 3 The framework of scheme

Fabric-CA 部分：通过利用已有的超级账本 Fabric-CA，该部分主要用于实现以下功能。

1) 用户证书管理：原有区块链网络的用户证书签发与吊销等操作。

2) CP-ABE 系统初始化：主要包含公开参数和主密钥的生成。

3) 用户属性密钥 SK 生成与分发：为某一用户生成并分发特定包含该用户属性的密钥。

其中，用户证书管理为超级账本网络中原有的功能，目前方案中增加了 CP-ABE 系统初始化以及用户属性密钥生成与分发机制。

Fabric 部分：该部分主要实现超级账本网络中原有的功能，包含交易背书、交易排序和交易验证及上链等。在本文方案的实现过程中，该部分主要是将待存储的密文通过背书、排序和节点验证进行上链操作，将密文在整个通道中进行分布式存储。

Client 部分：在原有的超级账本网络中，该部分主要用于实现交易的发起以及用户的证书接

收功能。本文方案在其原有功能之上增加了用户属性密钥 SK 接收和 CP-ABE 数据加解密功能。用户可通过 Client 与 Fabric 网络以及 Fabric-CA 进行交互操作。

### 3.2　CP-ABE 属性集及策略定义

#### 3.2.1　属性定义

CP-ABE 方案中仅拥有满足策略属性的密钥才能对密文进行解密以获取明文数据。由 2.1.3 节可知，超级账本网络中可以包括多个通道（如 Channel1、Channel2 和 Channel3 等），且每个通道中将包含多个组织（如 Org1、Org2 和 Org3 等），每个组织中又将包含多个用户（如 User1、User2 和 User3 等）。作为超级账本区块链网络可划分的最小单位，用户是 CP-ABE 方案属性集中的最细粒度，其固有通道 ID、组织 ID 和用户 ID 这 3 个属性，因此，本文将数据访问控制中属性定义的可选范围如表 1 所示。

表 1　用户属性定义
Table1　Definition of user attribution

| 属性 | 属性值 |
|---|---|
| 通道 ID | Chanel1、Channel2 |
| 组织 ID | Org1、Org2 |
| 用户 ID | User1、User2 |

#### 3.2.2　访问控制策略定义

策略即属性组成的访问结构。由 3.2.1 节可知，本文将属性定义为通道 ID、组织 ID 以及用户 ID 这 3 种，原则上在形成访问控制策略时，可以将这 3 种属性随意组合。例如，在实际的密文生成时，可以将策略 P1 定义为通道 1 组织 1 中的 User1 和通道 2 组织 2 中的全部用户都可以访问，P2 定义为通道 1 组织 1 中的 User1 和通道 1 组织 2 中的全部用户都可以访问。通过将访问控制策略和密文相结合，就可以达到数据访问控制的目的。

由 2.1.3 节可知，超级账本网络的区块分发是按通道 ID 进行分发的，由于通道之间是相互隔离的，即数据区块只能被发往其中一个通道，通常不存在上链数据可以被多个通道同时访问的情况。因而，上述提及的策略 P1 在实际的访问控制中并不存在，即通道 ID 这一属性并不能直接简单地包含在访问控制策略中。但在不考虑通道 ID 属性作为访问策略的选择时，本文将策略定义为仅包含组织 ID 属性或用户 ID 属性中的一个或组合形式，如通道 1 中的某个密文指定策略 P 为（组织 ID = Org2），一旦通道 1 组织 2 中的用户 User1 将获取到的密文泄露给通道 2 组织 2 中的 User2，由于用户 User2 也包含属性 Org2，因此 User2 可以成功解密该密文，从而造成数据泄露问题；再则，当数据拥有者想要使加密密文对 Channel1 中的全部用户都可解密时，在不考虑通道 ID 属性作为访问策略选择时，就需要通过定义多个组织进行与操作，即策略的逻辑相比直接定义策略 P 为（通道 ID = Channel1）更加复杂。因此，为更准确地实现加密数据的数据访问控制，用户策略的指定需在通道层面就开始进行考虑。

为了将可用的访问控制策略更加全面化和具体化地进行展示，如图 4 所示，本文定义了 3 种通用策略：① 特定通道内的所有用户均可解密；② 特定通道内的特定组织中的所有用户均可解密；③ 特定通道内的特定组织中的特定用户可解密。

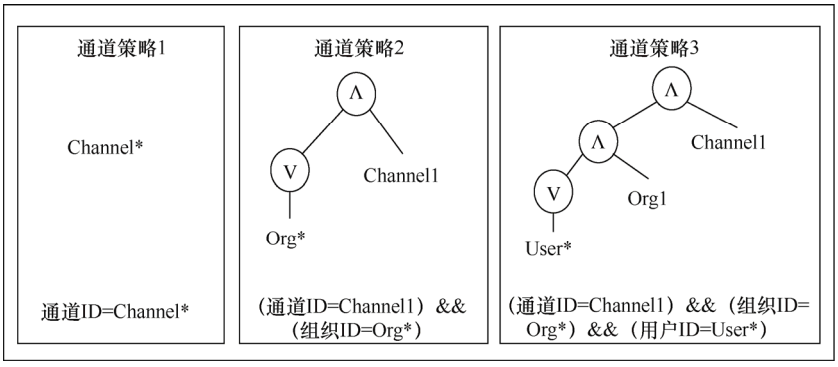



图 4　用户通用策略
Figure 4　User common policy

其中，Channel*、Org*和 User*中符号*表示{*|*∈(1,2,3,4…)}。Channel*指超级账本网络中所有通道组成的集合{Channel1，Channel2…}，Org*指特定通道下的所有组织的集合{Org1, Org2…}，User*指特定的通道下特定的组织中的用户集合{User1，User2…}。

通用策略 1：通道 ID=Channel*，即通道 ID 可以等于{ Channel* }集合中的任意通道，换言之，就是该通道下的所有用户都可对基于该策略加密的密文进行解密从而访问对应明文数据。

通用策略 2：(通道 ID=Channel1)&&(组织 ID=Org*)，即指定了通道 ID 此处只能为 Channel1（但不限于 Channel1，此处仅为具体示例），而组织 ID 可以在 Channel1 的组织集{ Org* }任意选择其中一个，此时该组织下的所有用户都可以对基于该策略加密的密文进行解密从而访问对应明文数据。

通用策略 3：(通道 ID=Channel1)&&(组织 ID=Org1)&&（用户 ID=User*），即指定了通道 ID 此处只能为 Channel1，组织 ID 在此处仅对应 Channel1 中的 Org1（不限于 Org1，仅为示例），而用户 ID 可以在 Channel1 中的 Org1 中形成的用户集{ User* }任意选择。此时，Channel1 中的 Org1 下的某个用户可对基于该策略进行加密的密文解密从而访问对应明文。

用户在将上链数据进行加密时策略指定可直接使用上述 3 种通用策略，仅需将模块中的对应字段改成用户想要指定的字段。除此之外，用户还可以通过将通用策略 2 和通用策略 3 进行组合，实现更细粒度的数据访问控制。

## 4 具体方案与评估

### 4.1 具体方案

基于现有的 Fabric 和 Fabric-CA，可通过在 Fabric-CA 中嵌入 CP-ABE 实现，即相当于 Fabric-CA 作为 CP-ABE 方案中的可信第三方，此时 Fabric-CA 不仅管理着原有 Fabric 网络中用户所需的证书，同时具有 CP-ABE 方案的初始化和用户属性私钥 *SK* 的生成与分发功能。用户通过 Client 实现与 Fabric-CA 和 Fabric 网络的交互，主要包括向 Fabric-CA 登记注册以获得对应的证书和 CP-ABE 方案的用户属性私钥，利用获取到的私钥与用户指定的访问控制策略对明文数据进行加密，再通过交易的形式将密文发送至 Fabric 网络中进行加密数据的上链存储。方案的整体工作流程大致可分为 3 个阶段：密钥生成阶段、数据加密上链阶段和访问控制阶段，包括 Setup、KeyGen、Encrypt、Update、Download 和 Decrypt 这 6 个步骤。为了能够更加客观地展示该方案的具体流程，本文以 User*A* 和 User*B* 之间的交互为例（User*A* 想要将隐私数据加密上链，User*B* 希望能够访问到密文对应的明文），假设 User*A* 通过 Client*A*、User*B* 通过 Client*B* 与 Fabric 网络和 Fabric-CA 进行交互，方案符号说明如表 2 所示，具体的实现细节如图 5 所示。

表 2 方案符号说明

Table2 The description of symbols

| 符号 | 符号定义 |
|---|---|
| SK | 用户对应的 CP-ABE 方案中的属性私钥 |
| MK , PK | CP-ABE 方案中的主密钥和公开参数 |
| $U_{PK}$ , $U_{SK}$ | 原有超级账本网络中用户的公钥和私钥 |
| $U_{cert}$ | 原有超级账本网络中的用户证书 |
| $M$ , CT | 明文数据以及经过加密形成的密文 |

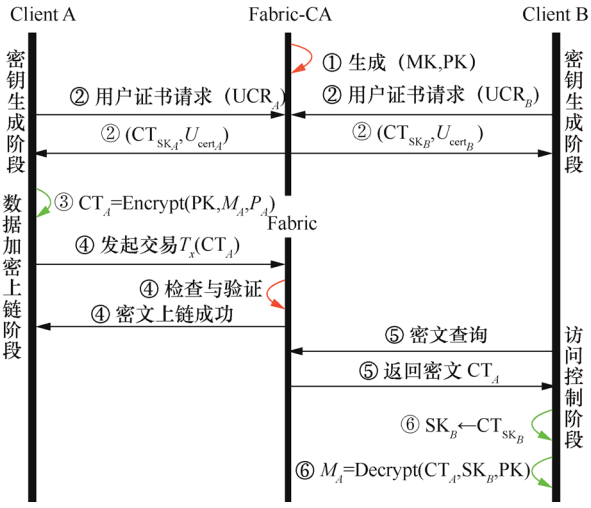



图 5 方案整体工作流程

Figure 5 Overall work flow of the scheme

密钥生成阶段：该阶段主要是用户与 Fabric-CA 的通信阶段，该阶段生成 CP-ABE 方案中的主密钥 MK 和公开参数 PK，并根据用户身份认证阶段发来的用户登记注册请求生成用户证书 Ucert 和用户属性私钥 SK 对应的密文 $CT_{SK}$。

① $\text{Setup}(1^{\lambda}) \rightarrow (\text{MK},\text{PK})$

此阶段和 CP-ABE 方案中的初始化阶段一致。通过输入系统安全参数 $\lambda$，生成 CP-ABE 方案中的主密钥 MK 和公开参数 PK 。

② $\text{KeyGen}(\text{MK},\text{UCR}) \rightarrow (\text{CP}_{\text{SK}},\text{Ucert})$

UCR（user certificate request）即用户证书请求，该请求包含了用户待生成证书对应的公钥 $U_{\text{PK}}$ 和用户的属性 $S$ 。在原超级账本网络中，用户通过 Client 发送 UCR 至 Fabric-CA 申请证书的登记注册，Fabric-CA 对用户的证书请求进行签名生成用户证书 $U_{\text{cert}}$ 并将该证书返回给用户。与原来的 Fabric-CA 不同，在本文的方案中，Fabric-CA 收到该请求时不仅需要生成对应的用户证书 $U_{\text{cert}}$，还需生成 CP-ABE 方案中包含用户属性的用户解密密钥（即 SK ）。为了保障用户属性密钥 SK 的安全性，SK 并不能直接在网络中进行传输。因此，基于原有的 Fabric-CA，本文利用 UCR 中用户证书对应的公钥 $U_{\text{PK}}$ 对新生成的用户属性私钥 SK 进行加密得到密钥对应的密文 $\text{CT}_{\text{SK}}$，仅拥有与用户证书包含的公钥 $U_{\text{PK}}$ 对应的私钥 $U_{\text{SK}}$ 的用户在接收到该 $\text{CT}_{\text{SK}}$ 才能够成功拿到用户属性私钥 SK 。在生成 $\text{CT}_{\text{SK}}$ 后，Fabric-CA 将 $(\text{CT}_{\text{SK}},U_{\text{cert}})$ 返回给用户，待用户继续后续操作。

数据加密上链阶段：该阶段主要是 UserA 与 Fabric 网络交互的阶段，主要是用户 UserA 指定加密策略 $P_A$ 和待上链的明文数据 $M_A$，并对该数据基于策略进行加密得到密文 $\text{CT}_A$，再通过发起交易并将密文作为交易负载的形式即 $\text{Tx}(\text{CT}_A)$ 发送至链上进行密文数据的区块链网络同步。详细步骤如下。

③ $\text{Encrypt}(\text{PK},M_A,P_A) \rightarrow \text{CT}_A$

类似于原始 CP-ABE 方案中的数据加密步骤，UserA 首先通过 Encrypt 算法对指定的明文消息 $M_A$ 在策略 $P_A$ 下，利用 CP-ABE 方案中的公开参数 PK 进行数据的加密得到密文 $\text{CT}_A$；然后该用户向区块链网络发起交易，并将该密文作为交易的负载即交易 $\text{Tx}(\text{CT}_A)$ 发往区块链网络。

④ $\text{Update}(\text{Tx}(\text{CT}_A)) \rightarrow \text{Block}_A$

在接收到 UserA 提交的包含密文数据的交易 $\text{Tx}(\text{CT}_A)$ 后，Fabric 网络首先按照背书策略对 $\text{Tx}(\text{CT}_A)$ 进行背书，主要对交易提案格式、交易提交重复性、交易签名以及交易提交者权限进行验证，进而模拟执行链码生成背书响应并返回到 UserA；在收集到足够的背书响应后，UserA 将密文交易 $\text{Tx}(\text{CT}_A)$ 进一步封装生成 Envelope，并发送至排序节点进行排序；在对交易进行排序打包生成区块 $\text{Block}_A$ 之后，排序节点将区块发送至通道组织进行交易的最终上链验证。组织中记账节点对交易的验证主要包含：① 交易数据的验证，包含交易格式、交易签名以及交易内容是否被篡改的验证；② 链码校验，包含对交易涉及的链码信息是否为空，是否存在违规调用链码的验证；③状态数据的验证，包含对模拟执行时状态数据和提交交易时状态数据一致性的验证。验证成功后将区块 $\text{Block}_A$ 存储到区块链网络同一通道中的各个节点上，完成加密数据的上链存储。需要注意的是，在超级账本对上链交易的背书以及验证过程中，只对交易的格式、签名以及前后状态一致性等进行验证，并未对交易中具体数据的合法性进行验证，即上链数据本身对于超级账本底层来说是透明的，因此可以保证密文数据上链的可行性。

访问控制阶段。该阶段主要是 Fabric 网络与 UserB 之间的交互阶段。在包含密文交易的区块上链之后，整个通道内的全部节点都将对该区块进行同步，UserB 通过客户端请求区块链网络中包含该交易密文的对应信息，得到对应的密文 $\text{CT}_A$。然后利用之前得到的 UserB 属性密钥密文 $\text{CT}_{\text{SK}_B}$，用户首先对 $\text{CT}_{\text{SK}_B}$ 进行解密得到 CP-ABE 方案的用户属性密钥 $\text{SK}_B$，进一步基于 $\text{SK}_B$ 对密文 $\text{CT}_A$ 进行解密，从而得到明文 $M_A$，实现用户级的数据访问控制。详细实现过程如下。

⑤ $\text{Download}(\text{Tx}(\text{CT}_A)) \rightarrow \text{CT}_A$

UserB 通过 clientB 与 Fabric 网络进行交互，请求区块链网络中包含该交易密文的对应信息，从而得到对应的数据密文 $CT_A$。

⑥ $\text{Decrypt}(\text{CT}_A,\text{SK}_B,\text{PK}) \rightarrow M_A$

在密钥产生阶段，为了保证传输用户属性私钥 SK 的安全性，本文将该属性私钥 $\text{SK}_B$ 通过用户原始网络中的公钥 $U_{\text{PK}_B}$ 加密生成 $\text{CT}_{\text{SK}_B}$ 进行传输。在接收到 $\text{CT}_{\text{SK}_B}$ 后，UserB 会对该密文进行解密生成明文属性私钥 $\text{SK}_B$，并在该私钥属性满足

$CT_A$ 中包含的策略 $P_A$ 时，利用 $SK_B$ 对 $CT_A$ 进行解密得到加密数据对应的明文 $M_A$，实现常规情况下 UserA 和 UserB 间基于 CP-ABE 方案实现的区块链数据访问控制。

### 4.2 安全性分析

该方案的安全性分析主要包括用户属性私钥 SK 的安全分发和数据隐私性保证，具体如下。

（1）用户属性私钥 SK 的安全分发

首先，作为原始超级账本中的模块，Fabric-CA 是完全可信的，从而保证了主密钥 MK 和 PK 的初始化生成阶段可信、对用户属性的审核可信、用户属性私钥 SK 生成过程可信。但是，由于 Fabric-CA 没有原生的密钥分发机制，因此本文方案中采用了基于用户证书请求中包含的公钥 $U_{PK}$ 加密 SK 生成 $CT_{SK}$，再将 $CT_{SK}$ 分发至对应用户的机制，进而保证了用户属性私钥 SK 的传输安全性。因为每个用户在发起用户证书请求 UCR 时，用户会将其公钥 $U_{PK}$ 放入对应的 UCR 中，Fabric-CA 在接收到该证书请求后会动态生成用户属性私钥 SK，再通过 UCR 中包含的 $U_{PK}$ 对 SK 进行加密，此时只有拥有与该公钥 $U_{PK}$ 对应的私钥 $U_{SK}$ 的用户才能成功解密 $CT_{SK}$，进而取得 SK。而其他用户，即使拿到 $CT_{SK}$ 也无法对其解密，达到窃取用户属性私钥 SK 的目的。

（2）数据隐私性保证

数据所有者对明文数据进行 CP-ABE 方案加密进而上链，故在整个 Fabric 网络中仅对该数据密文可见。此外，如前所述，Fabric-CA 完全可信，有关密钥产生对应阶段可信。数据所有者直接通过指定策略 P 对该数据的访问权限进行限制，仅包含满足策略 P 属性的用户才能对该数据进行解密进而访问，不满足该策略 P 对应的解密属性私钥无法解密该密文，进而保证了数据隐私性。

### 4.3 性能分析

本节主要针对方案的实现性能进行分析。实验环境使用 Oracle VM VirtualBox 安装的 Ubuntu16.04 LTS 虚拟机，并分配了 4 GB 内存和 1 个核心处理器。在对性能指标进行选择时，考虑到本文方案并未对原有超级账本网络的交易流程进行改动，只是将原来区块链网络中上链的明文数据替换成了经 CP-ABE 加密后的密文数据，这种改动对于底层的交易流程来说是透明的，不会影响到超级账本网络原本的运行效率。因此，只需针对 CP-ABE 方案的性能指标进行测量，本节主要对文献[22]实现的 CP-ABE 方案进行用户属性私钥生成时间和加解密时间的测量。

在本文设计的方案中，CP-ABE 方案涉及的属性私钥最多包含 3 个属性：通道 ID、组织 ID 以及用户 ID。由文献[19]可知，私钥产生时间随包含属性个数的增加呈线性增长趋势，在本文方案中考虑属性最多为 3 个的前提下，经过测量得出私钥产生时间在 0.031 5 s 左右。同时考虑到在实际的超级账本交易过程中，单个区块最大能够容纳 10 MB 的数据，因此将实验中最大的数据大小设置为 10 MB。由图 6 显示，随着需加解密数据大小的增加，对应的加解密时间都在以线性的趋势增加。在数据大小为最大即 10 MB 时，此时加密的时间在 0.08 s 左右，解密的时间在 0.065 s 左右。

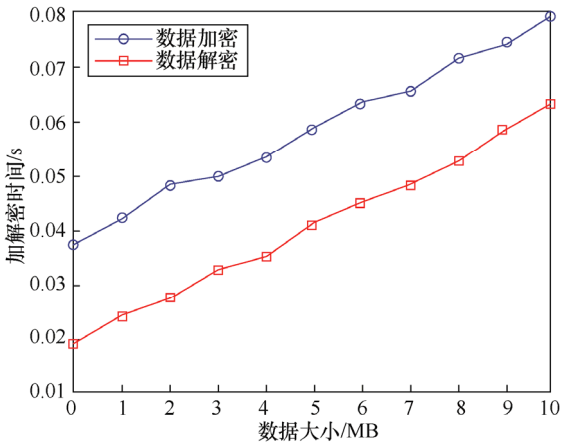



图 6 数据大小对加解密时间的影响

Figure 6 Impact of data size on encryption and decryption time

通过对用户属性私钥生成时间和需加解密数据大小对加解密时间的影响进行测量，发现这两个操作实现的时间都是在可接受的范围增量内，因此，在原有超级账本网络运行机制上实现的基于 CP-ABE 算法的区块链数据访问控制机制具有良好的可行性。

### 4.4 方案的对比分析

本节将提出的方案与目前已有的超级账本官方解决方案进行比较，分别从用户级访问控制粒度、数据隐私性、密钥安全分发以及加/解密密钥

表 3　安全性和性能对比
Table3　The comparison of safety and performance

| 方案 | 类型 | 用户级访问控制粒度 | 数据隐私性 | 密钥安全分发 | 加/解密密钥管理简易性 |
|---|---|---|---|---|---|
| 方案[7] | 对称加密 | √ | √ | × | × |
| 方案[8] | 哈希同步 | × | × | — | — |
| 本文方案 | 属性基加密 | √ | √ | √ | √ |

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

管理简易进行对比。其中，用户级访问控制粒度说明该方案是否支持对超级账本网络最细访问控制粒度即用户级别的访问控制功能；数据隐私性代表该方案是否对上链数据的隐私性进行保障；密钥安全分发说明该方案是否保证了密钥的安全分发特性；加/解密密钥管理简易性代表在保证加密密文安全性的前提下用户是否不需要管理维护多个加/解密密钥，即是否能够摆脱“一密一钥”的复杂操作。

如表 3 所示，本文方案相比同类方案，不仅可以保证上链数据隐私性、支持基于用户级别的最细访问控制粒度，还在保证密钥安全分发的前提下简化了加/解密密钥的管理工作，因此更加适用于超级账本网络的上链数据访问控制实现。

## 5　结束语

本文分析了目前超级账本区块链网络中存在的数据明文存储以及数据访问控制机制粗粒度问题，提出了一种基于 CP-ABE 算法的区块链数据访问控制方案，实现了基于用户属性的细粒度访问控制目标。同时，为了解决密钥分发问题，本文基于超级账本区块链中原有的 Fabric-CA 模块，通过添加对 CP-ABE 算法密钥（包括系统初始化和用户属性私钥）的生成支持，进一步利用非对称加密算法实现了用户属性私钥的安全分发。最后，对本文所提方案的安全性分析验证了该方案的设计达到了用户属性私钥安全分发和数据隐私保护的安全性目标，实现了超级账本区块链网络中隐私数据的细粒度访问控制功能。性能分析部分也表明了本文方案的可用性。同时通过与已有类似方案进行对比，进一步说明了本文设计方案对超级账本网络的上链数据访问控制实现的适用性。

## 参考文献：


[1] ANDROULAKI E, BARGER A, BORTNIKOV V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains[C]//European Conference on Computer Systems, 2018 : 1-15.

[2] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[R]. 2008.

[3] WOOD G. Ethereum: a secure decentralised generalised transaction ledger[R]. 2014.

[4] 闫莺, 郑凯, 郭众鑫. 以太坊技术详解与实战[M]. 北京: 机械工业出版社, 2018.
YAN Y, ZHENG K, GUO Z X. Ethereum technical details and actual combat[M]. Beijing: China Machine Press, 2018.

[5] 陈剑雄, 张董朱. 深度探索区块链 Hyperledger 技术与应用[M]. 北京: 机械工业出版社, 2018 .
CHEN J X, ZHANG D Z. In-depth exploration of blockchain hyperledger technology and application[M]. BeiJing: China Machine Press, 2018.

[6] Channels. Hyperledger fabric channels[EB].

[7] Enccc_example. 2019 Hyperledger fabric enccc_example[EB].

[8] Private data. 2019 Hyperledger fabric private data[EB].

[9] 沈鑫, 裴庆祺, 刘雪峰. 区块链技术综述[J]. 网络与信息安全学报, 2016, 2(11): 11-20.
SHEN X, PEI Q Q, LIU X F. Survey of block chain[J].Chinese Journal of Network and Information Security, 2016, 2(11): 11-20.

[10] JAKOBSSON M, JUELS A. Proofs of work and bread pudding protocols. in secure information networks: communications and multimedia security[C]//IFIP TC6/TC11 Joint Working Conference on Communications and Multimedia Security (CMS '99).1999.

[11] VASIN P. Blackcoin’s proof-of-stake protocol v2[EB].

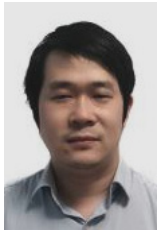
[12] KING S, NADAL S. PPCoin: peer-to-peer crypto-currency with proof-of-stake[J]. Self-published Paper, 2012(8): 19.

[13] YE C. Analysis of security in blockchain: case study in 51%-attack detecting[C]//2018 5th International Conference on Dependable Systems and Their Applications (DSA). 2018.

[14] 章峰, 史博轩, 蒋文保. 区块链关键技术及应用研究综述[J]. 网络与信息安全学报, 2018, 4(4): 26-33.
ZHANG F, SHI B X, JIANG W B. Review of key technology and its application of blockchain[J]. Chinese Journal of Network and

Information Security, 2018, 4(4):26-33.
[15] 中国信息通信研究院. 区块链白皮书[R]. 2018.
China Academy of Information and Communication Technology. White paper of blockchain[R]. 2018.
[16] SUKHWANI H, MARTINEZ J M, CHANG X, et al. Performance modeling of PBFT consensus process for permissioned blockchain network (Hyperledger Fabric)[C]//Symposium on Reliable Distributed Systems. 2017: 253-255.
[17] KREPS J, NARKHEDE N, RAO J. Kafka: a distributed messaging system for log processing[C]//The NetDB. 2011 (11): 1-7.
[18] Certificate Authorities. 2019 Hyperledger fabric certificate authorities[EB].
[19] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C]// Symposium on Computer and Communications Security. 2006: 89-98.
[20] BOLDYREVA A, GOYAL V, KUMAR V, et al. Identity-based encryption with efficient revocation[C]// Symposium on Computer and Communications Security. 2008: 417-426.
[21] 林素青. 支持访问更新的可验证外包属性加密方案[J]. 网络与信息安全学报, 2019, 5(1): 41-53.
LIN S Q. Verifiable outsourced attribute-based encryption with access update[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 41-53.
[22] BETHENCOURT J, SAHAI A, WATERS B. Ciphertext-policy attribute-based encryption[C]//IEEE symposium on security and privacy (SP'07). 2007.
[23] 张兴兰, 崔遥. 基于群签名的属性加密方案[J]. 网络与信息安全学报, 2019, 5(1): 19-25.
ZHANG X L, CU Y. Attribute-based encryption schema with group signatures[J]. Chinese Journal of Network and Information Security, 2019, 5(1): 19-25.

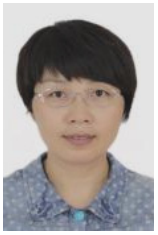
[作者简介]



**邱云翔**（1988− ），男，贵州六枝人，硕士，华信咨询设计研究院有限公司工程师，主要研究方向为信息安全、数据安全。

**张红霞**（1996− ），女，河北邢台人，四川大学硕士生，主要研究方向为区块链安全及应用、网络行为分析。

**曹琪**（1996− ），女，四川广安人，四川大学硕士生，主要研究方向为区块链安全及应用、网络行为分析。



**章建聪**（1975− ），女，浙江金华人，硕士，华信咨询设计研究院有限公司高级工程师，主要研究方向为数据通信、信息安全。

**陈兴蜀**（1968− ），女，贵州六枝人，博士，四川大学教授、博士生导师，主要研究方向为云计算与大数据安全、可信计算与信息保障。

**金泓键**（1996− ），男，重庆人，四川大学硕士生，主要研究方向为区块链安全及应用、大数据分析。