DOI: 10.19783/j.cnki.pspc.221491

基于区块链和属性基加密的电力数据共享方案

杨小东[1]，廖泽帆[1]，刘 磊[2]，王彩芬[3]

(1.西北师范大学计算机科学与工程学院，甘肃 兰州 730070；2.中电万维信息技术有限责任公司中电万维研究院，甘肃 兰州 730030；3.深圳技术大学大数据与互联网学院，广东 深圳 518118)

摘要：目前电力数据共享方案主要采用属性基加密技术实现一对多的电力数据访问控制，但存在加密效率低和用户属性易被篡改等问题。为了解决这些问题，提出了一种基于区块链和属性基加密的电力数据共享方案。结合属性基加密和对称加密算法，实现了电力数据的机密性和细粒度访问控制。引入在线/离线加密模式，大大提升了数据拥有者的加密性能。利用外包计算技术，降低了数据访问用户的计算负担。将属性集合和电力数据的哈希值上传至区块链，保障用户属性的不可伪造性和解密密文的正确性。分析结果表明，该方案实现了电力数据的安全共享，其加密/解密性能适用于资源受限的电力终端设备。

关键词：电力数据共享；在线/离线加密；属性加密；外包解密；区块链

Power data sharing scheme based on blockchain and attribute-based encryption

YANG Xiaodong[1], LIAO Zefan[1], LIU Lei[2], WANG Caifen[3]

(1. College of Computer Science and Engineering, Northwest Normal University, Lanzhou 730070, China; 2. Institute of China Telecom WanWei, China Telecom WanWei Information Technology Co., Ltd., Lanzhou 730030, China; 3. College of Big Data and Internet, Shenzhen Technology University, Shenzhen 518118, China)

Abstract: Existing data sharing schemes mainly use attribute-based encryption technology to achieve "one-to-many" data access control, but there are problems such as low encryption efficiency and attributes that are easily tampered with. To solve these problems, a blockchain-based ciphertext data sharing scheme is proposed. Combining attribute-based encryption and symmetric encryption algorithms, confidentiality and fine-grained access control of shared data are achieved. The introduction of an on-line/off-line encryption mode greatly improves the encryption performance of the data owner. In addition, it uses outsourcing computing technology to reduce the computing burden of data access users. Attribute sets and Hash values of shared data are uploaded to the blockchain. This ensures the 'unforgeability' of attributes and the correctness of decrypted ciphertext. The analysis shows that this scheme realizes secure data sharing, and its encryption/ decryption efficiency is better than similar schemes. Hence, it is more suitable for resource-constrained smart devices.

This work is supported by the National Natural Science Foundation of China (No. 61662069).

Key words: power data sharing; on-line/off-line encryption; attribute-based encryption; outsourcing decryption; blockchain

0 引言

电力数据具有实时、真实、体量大、颗粒度细等特点，在新冠疫情期间对企业复产复工监测分析、商业景气指数分析、涉疫小区的人员流动及防控等方面发挥了重要支撑作用。然而，全球数据安全事件频出，如何确保电力数据安全已成为各行各业关注的焦点。数据共享技术能有效解决电力数据孤岛问题，促进电力数据流通，充分利用电力数据价值。尽管电力数据共享技术已经成为行业热点，但依然面临着电力数据安全和隐私保护等问题[1-3]。

基于密文策略的属性基加密(ciphertext-policy attribute-based encryption, CP-ABE)是一种适用于电力数据共享的公钥加密技术，只有访问用户的属性集满足电力数据加密采用的访问控制策略时才能解密数据密文[4]。近年来，研究者利用 CP-ABE 的一对多加密和灵活访问控制等特点，提出了一系列面

基金项目：国家自然科学基金项目资助(61662069)；中国博士后科学基金项目资助(2017M610817)

向不同应用场景的数据共享方案[5-7]。文献[8]提出了一种云雾协同的 CP-ABE 方案(下文简称 Chen 方案)，但加密阶段的计算开销较大，未考虑属性篡改和数据丢失等问题。

随着区块链技术日趋成熟，其应用的场景也更加广泛。在不引入第三方中介机构的情况下，区块链具有去中心化、不可篡改、可追溯以及公开透明的特点，一切直接或间接依赖第三方机构的操作与活动，都可以利用区块链得到安全性的提升。区块链本身是一个公开透明的数据账本，它以区块为单位存储数据，区块间首尾相接形成链式结构。如果一个区块的数据发生变化，那么该区块后的数据都会发生变化，这种特性避免了历史数据遭到篡改的可能性[9-12]。因此，区块链技术的上述特点适用于电力系统中的数据共享。

文献[13]利用区块链和 CP-ABE 构造了一种云端数据共享方案，所有上链的数据无法修改。针对车联网中的数据安全和访问控制问题，文献[14]提出了一种基于区块链的车联网数据共享方案。文献[15]设计了一种基于区块链和代理重加密技术的数据共享方案，但访问用户的计算开销较大。文献[16]提出了一种基于区块链的社交网络数据共享方案，但存在属性被恶意篡改等风险。为了抵御属性假冒攻击，文献[17]提出了基于区块链和二叉树的数据共享方案，将属性集合上传至区块链来实现属性的防篡改性。针对跨部门之间的数据共享问题，文献[18]给出了基于区块链的密文数据共享模型，但计算效率较低。此后，与区块链结合的数据共享方案被陆续提出[19-22]。上述大部分方案只考虑了访问用户的计算性能，未考虑数据拥有者的计算负担，在资源受限的数据采集设备中应用时存在一定的局限性。

为了解决加密效率低下和不支持数据的完整性验证等问题，本文提出了一种基于区块链和云边端协同的电力数据共享方案。该方案利用区块链不可篡改的特性，将用户属性与数据哈希值上链存储，避免了属性遭到篡改并利用哈希值实现解密数据的验证。主要工作如下：

1) 引入在线/离线加密模式，提升了电力数据加密的计算性能。数据拥有者在离线阶段进行电力数据加密的预计算处理；在线阶段利用预计算结果，能在很短的时间内产生电力数据的有效密文。

2) 抵抗属性假冒和用户间的合谋攻击。用户属性集合和系统参数的上链，实现了用户属性的不可篡改性。每个用户的密钥将用户的唯一全局身份与用户属性集合进行绑定，有效阻止了用户间的合谋攻击。

3) 支持密文的外包解密计算。大部分解密计算的工作委托给边缘节点执行，大大降低了数据访问用户的计算负担。

4) 解密密文的完整性验证。电力数据的哈希值存储于区块链，通过验证密文外包解密结果的完整性，保障电力数据共享的正确性。

1 预备知识

令 G 和 G_T 是两个乘法循环群，其阶均是相同的素数 p，其中 g 是 G 的一个生成元。

1.1 双线性映射

一个双线性映射 $e:G\times G\to G_T$ 至少满足如下 3 个性质。

1) 双线性：如果 $x,y\in Z_p^*$，则一定有 $e(g^x,g^y)=e(g,g)^{xy}$。

2) 非退化性：$e(g,g)\neq 1$。

3) 有效性：存在有效的算法计算 $e(g^x,g^y)$。

对于满足上述条件的 (e,G,G_T,p,e) 通常被称为双线性群[15]。

1.2 困难假设问题

q 阶双线性 Diffie-Hellman 幂(q-Bilinear Diffie-Hellman Exponent, q-BDHE)问题：给定一个元组 $(g,g^s,g^d,\cdots,g^{d^q},g^{d^{q+2}},g^{d^{2q}})$，其中 $d,s\in Z_p^*$，区分 $T=e(g,g)^{d^{q+1}s}$ 和一个随机元素 $R\in G_T$。

如果在任意的多项式时间内算法无法以不可忽略的概率解决 q-BDHE 问题，则称 q-BDHE 假设成立[8]。

2 系统模型

本文的电力数据安全共享模型如图 1 所示，涉及 6 个参与方：属性权威机构(attribute authority, AA)、数据拥有者(data owner, DO)、边缘节点(edge node, EN)、云服务器(cloud server, CS)、区块链和数据用户(data user, DU)。

1) AA：主要负责产生系统参数和用户密钥，同时维护区块链网络。

2) DO：主要执行在线/离线加密操作，然后发送电力数据的密文给邻近边缘节点 EN，并将电力数据的哈希值上传至区块链。

3) EN：具有较强的计算和存储能力，主要执行数据访问用户的密文解密外包计算工作。此外，EN 在本地保存短期密文，并将长期密文存储于云服务器。

4) CS：主要存储 EN 转发的长期密文。

5) 区块链：采用基于 Fabric 或以太坊等架构[23]的区块链网络，主要用于存储系统参数、用户属性集合和电力数据的哈希值。

6) DU：首先向 EN 发送密文数据的访问请求，然后验证 EN 返回的半解密密文，最后在本地恢复电力数据。

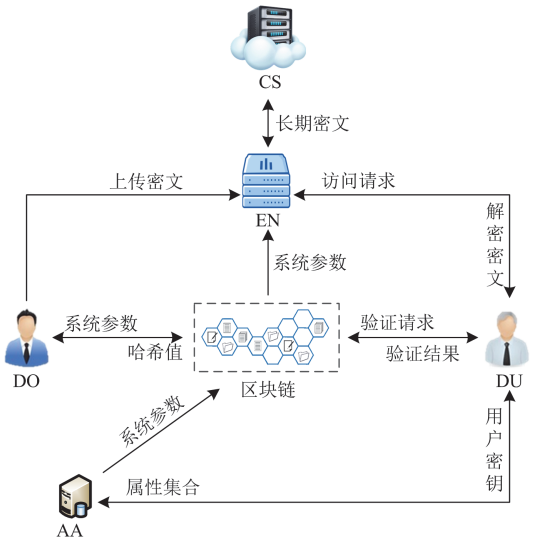

图 1　系统模型

Fig. 1 System model

3　方案构造

基于属性基加密、AES 加密体制和区块链等技术，本节提出了一种云边端协同的电力数据共享方案，由下面 4 个阶段组成。

3.1　系统初始化

给定系统参数 ζ，AA 执行如下操作生成系统参数 PP 和主密钥 MSK。

1) 根据 ζ 生成双线性群 (G,G_T,p,g,e)。

2) 对于属性集合 ATT 中的每个属性 $x\in ATT$，随机选择 $A_x\in G$。

3) 随机选择 $\alpha\in Z_p^*$ 作为主密钥 $MSK=\alpha$，计算 $P_K=e(g,g)^{\alpha}$。

4) 随机选择一个元素 $h\in G$ 和一个安全的哈希函数 $H:\{0,1\}^*\to Z_p^*$。

5) 选择对称加密体制 AES，用 $Enc()$ 和 $Dec()$ 分别表示 AES 的加密算法和解密算法。

6) 上传系统参数

$PP=\{G,G_T,p,g,e,A_x,PK,h,H,Enc,Dec\}$ 至区块链，以供其他用户访问。

3.2　用户注册

当用户加入系统时，从 AA 处获得一个能识别用户的唯一全局身份 $G_{IDu}\in\{0,1\}^*$；然后，AA 根据用户提交的属性集合 $S\subseteq ATT$，生成对应的用户密钥 SK 和转换密钥 TK。AA 具体操作如下：

1) 随机选择 $z,r,t\in Z_p^*$，设置秘密转换密钥 $UK=z$；

2) 计算 $\beta=H(G_{IDu})$；

3) 对每个属性 $x\in S$，计算 $K_x=(A_x)^{rt\beta}$；

4) 计算 $K_u=g^{\frac{\alpha+z\alpha r}{\beta}}h^{zrt}$，$L_u=g^{zrt}$，$D=g^{\alpha r}h^b$ 和 $E=g^b$；

5) 设置用户密钥 $SK=(K_u,L_u,\{K_x\}_{x\in S},D,E)$；

6) 计算 $K=(K_u)^{1/z}$ 和 $L=(L_u)^{1/z}$，设置用户的转换密钥 $TK=(K,L,\{K_x\}_{x\in S})$；

7) 过安全信道发送 $\{G_{IDu},SK,UK\}$ 给用户；

8) 上传 $\{\beta,TK,S\}$ 至区块链，以供边缘节点 EN 查询使用。

3.3　电力数据上传

DO 访问区块链网络获取系统参数 PP，然后在空闲时间执行离线阶段的预计算操作。对于电力数据 m，DO 执行在线阶段的混合加密操作生成密文数据 CT。

1) 离线阶段

(1) 选择随机数 $s'\in Z_p^*$，计算 $W=(P_K)^{s'}$，$W_0=g^{s'}$ 和 $W_0'=h^{s'}$。

(2) 对于每个属性 $x\in ATT$，选择随机数 $\lambda_x'\in Z_p^*$，计算 $W_x=h^{\lambda_x'}(A_x)^{-s'}$。

2) 在线阶段

(1) 选择一个 AES 加密体制内的对称密钥 K_{ey}，计算 m 的数据密文 $C_f=Enc_{K_{\mathrm{ey}}}(m)$ 和 $\widetilde{C}_f=H(m)$。

(2) 选择一个访问策略 $(\boldsymbol{M},\rho)$，其中 $\boldsymbol{M}$ 是一个 l 行 n 列的矩阵。ρ 是一个将 $\boldsymbol{M}$ 的行号 i 映射到一个属性 x 的单射函数，即 $\rho(i)=x$。

(3) 随机选择 $s\in Z_p^*$ 作为共享秘密值。

(4) 选择随机数 $v_2,\cdots,v_n\in Z_p^*$，设置向量 $\vec{u}=(s,v_2,\cdots,v_n)$。

(5) 对于 $\boldsymbol{M}$ 的每一行 M_i，计算 $\lambda_i=M_i\times(\vec{u})^T$ 作为 s 的秘密共享份额，其中 $i=1,\cdots,n$。

(6) 计算 $C=K_{\mathrm{ey}}\times W$，$c_1=s-s'$，$C_0=W_0$ 和 $C_0'=W_0'$。

(7) 对于行号 $i=1,\cdots,l$，计算 $f_i=\lambda_i-\lambda'_{\rho(i)}$，并设置 $C_i=W_{\rho(i)}$。

(8) 发送 $CT=\{C_f,C_K\}$ 给边缘节点 EN，对称密钥密文 $C_K=\{(\boldsymbol{M},\rho),C,C_0,C'_0,\{f,C_i\}_{i\in[1,l]},c_1\}$。

(9) 上传 $\widetilde{C}_f$ 至区块链，以供访问数据用户 DU 验证密文数据的完整性。

如果 DO 发送的 CT 是短期密文，则边缘节点 EN 在本地存储 CT；否则，EN 转发并存储 CT 在云服务器 CS。

3.4 电力数据共享

收到全局身份为 G_{IDu} 的 DU 所发送的密文 CT 访问请求后，边缘节点 EN 执行如下操作生成 C_K 的半解密密文 $\widetilde{C}_K$。

1) 从区块链网络获取系统参数 PP。

2) 在区块链上查找 G_{IDu} 的 $\{\beta,TK,S\}$，其中转换密钥 $TK=(K,L,\{K_x\}_{x\in S})$。

3) 如果本地不存在 $CT=\{C_f,C_K\}$，则请求 CSP 返回 CT，其中 $C_K=\{(\boldsymbol{M},\rho),C,C_0,C'_0,\{f,C_i\}_{i\in[1,l]},c_1\}$ 为对称密钥密文。

4) 如果 DU 的属性集合 S 不满足访问控制策略 $(\boldsymbol{M},\rho)$，终止流程；否则，执行如下的密文外包解密计算操作。

(1) 令 $I=\{i:\rho(i)=S\}$，计算一组数 $\{w_i\}_{i\in I}$，满足 $\sum_{i\in I}w_i\lambda_i=s$。

(2) 计算

$$\widetilde{C}=C\times(PK)^{c_1},\quad C_{\text{part1}}=e(K,(C_0g^{c_1})^{\beta})$$

$$C_{\text{part2}}=\prod_{i\in I}(e(L^{\beta},C_ih^{f_i}(A_{\rho(i)})^{-c_1})\cdot e(K_{\rho(i)},C_0g^{c_1}))^{w_i}$$

$$C_{\text{part3}}=\frac{e(C_0g^{c_1},D)}{e(E,C'_0h^{c_1})}$$

$$\widetilde{C}_K=\frac{C_{\text{part1}}}{C_{\text{part2}}\times C_{\text{part3}}}$$

(3) 发送半解密密文 $\{\widetilde{C},\widetilde{C}_K\}$ 和 C_f 给 DU。

收到 EN 发送的 $\{\widetilde{C},\widetilde{C}_K,C_f\}$ 后，数据访问用户 DU 执行如下解密操作。

5) 收到 EN 发送的 $\{\widetilde{C},\widetilde{C}_K,C_f\}$ 后，数据访问用户 DU 执行如下解密操作：

(1) 计算 AES 的对称密钥 $Key=\dfrac{\widetilde{C}}{(\widetilde{C}_K)^z}$；

(2) 恢复电力数据 $m=Dec_{K_{ey}}(C_f)$；

(3) 从区块链网络上获取 $\widetilde{C}_f$，并验证 $\widetilde{C}_f=H(m)$ 是否成立，如果成立，说明外包解密密文正确，从而完成电力数据 m 的共享。

4 安全性与性能分析

4.1 正确性分析

1) 转换密钥的正确性

对于用户密钥 $SK=(K_u,L_u,\{K_x\}_{x\in S},D,E)$，这里 $K_u=g^{\frac{\alpha+z\alpha r}{\beta}}h^{zrt}$ 和 $L_u=g^{zrt}$，利用秘密转换密钥 $UK=z$ 计算：

$$K=(K_u)^{1/z}=(g^{\frac{\alpha+z\alpha r}{\beta}}h^{zrt})^{1/z}=g^{\frac{\alpha+z\alpha r}{z\beta}}h^{rt}$$

$$L=(L_u)^{1/z}=(g^{zrt})^{1/z}=g^{rt}$$

2) 密文解密的正确性

对于密文 $CT=\{C_f,C_K\}$，$\beta=H(G_{IDu})$ 和 $C_K=\{(\boldsymbol{M},\rho),C,C_0,C'_0,\{f,C_i\}_{i\in[1,l]},c_1\}$。如果 DU 的属性集合 S 满足 $(\boldsymbol{M},\rho)$，则一定有 $\sum_{i\in I}w_i\lambda_i=s$。于是有第 1 个中间值：

$$\begin{aligned}C_{\text{part1}}&=e(K,(C_0g^{c_1})^{\beta})=e(g^{\frac{\alpha+z\alpha r}{z\beta}}h^{rt},(g^{s'}g^{s-s'})^{\beta})=\\&e(g^{\frac{\alpha+z\alpha r}{z\beta}}h^{rt},g^{s\beta})=e(g^{\frac{\alpha+z\alpha r}{z\beta}},g^{s\beta})e(h^{rt},g^{s\beta})=\\&e(g,g)^{\frac{\alpha s}{z}}e(g,g)^{\alpha rs}e(h,g)^{rts\beta}\end{aligned}\tag{1}$$

由于

$$\begin{aligned}&e(L^{\beta},C_ih^{f_i}(A_{\rho(i)})^{-c_1})e(K_{\rho(i)},C_0g^{c_1})=\\&e((g^{rt})^{\beta},(h^{\lambda'_{\rho(i)}}(A_{\rho(i)})^{-s'})h^{\lambda_i-\lambda'_{\rho(i)}}(A_{\rho(i)})^{-(s-s')})\cdot\\&e((A_{\rho(i)})^{rt\beta},g^{s'}g^{s-s'})=\\&e(g^{rt\beta},h^{\lambda_i}(A_{\rho(i)})^{-s})e((A_{\rho(i)})^{rt\beta},g^{s})=\\&e(g^{rt\beta},h^{\lambda_i})e(g^{rt\beta},(A_{\rho(i)})^{-s})e((A_{\rho(i)})^{rt\beta},g^{s})=\\&e(g,h)^{rt\beta\lambda_i}\end{aligned}\tag{2}$$

因此有第 2 个中间值：

$$\begin{aligned}C_{\text{part2}}&=\prod_{i\in I}(e(L^{\beta},C_ih^{f_i}(A_{\rho(i)})^{-c_1})\cdot e(K_{\rho(i)},C_0g^{c_1}))^{w_i}=\\&\prod_{i\in I}(e(g,h)^{rt\beta\lambda_i})^{w_i}=e(g,h)^{rts\beta}\end{aligned}\tag{3}$$

又因为第 3 个中间值：

$$\begin{aligned}C_{\text{part3}}&=\frac{e(C_0g^{c_1},D)}{e(E,C'_0h^{c_1})}=\frac{e(g^{s'}g^{s-s'},g^{\alpha r}h^{b})}{e(g^{b},h^{s'}h^{s-s'})}=\frac{e(g^{s},g^{\alpha r}h^{b})}{e(g^{b},h^{s})}=\\&\frac{e(g^{s},g^{\alpha r})e(g^{s},h^{b})}{e(g^{b},h^{s})}=e(g^{s},g^{\alpha r})=e(g,g)^{\alpha rs}\end{aligned}\tag{4}$$

所以有

$$\widetilde{C}_K=\frac{C_{\text{part1}}}{C_{\text{part2}}\times C_{\text{part3}}}=\frac{e(g,g)^{\frac{\alpha s}{z}}e(g,g)^{\alpha rs}e(h,g)^{rts\beta}}{e(g,h)^{rts\beta}e(g,g)^{\alpha rs}}=e(g,g)^{\frac{\alpha s}{z}} \tag{5}$$

$$\widetilde{C}=C\times(PK)^{c_1}=K_{\text{ey}}\times W\times(PK)^{c_1}=K_{\text{ey}}\times(PK)^{s'}\times(PK)^{s-s'}=K_{\text{ey}}\times e(g,g)^{\alpha s} \tag{6}$$

当收到 EN 返回的半解密密文和密文 $\{\widetilde{C},\widetilde{C}_K,C_f\}$ 后，DU 计算 AES 的对称密钥。

$$\frac{\widetilde{C}}{(\widetilde{C}_K)^z}=\frac{K_{\text{ey}}\times e(g,g)^{\alpha s}}{(e(g,g)^{\frac{\alpha s}{z}})^z}=\frac{K_{\text{ey}}\times e(g,g)^{\alpha s}}{e(g,g)^{\alpha s}}=K_{\text{ey}} \tag{7}$$

然后调用 AES 的解密算法恢复电力数据 $m=Dec_{K_{\text{ey}}}(C_f)$。综上所述，本文方案满足密文解密的正确性。

4.2 安全性证明

定理 1 如果 q-BDHE 假设成立，则本文方案在选择明文攻击安全下满足对称密钥的机密性。

证明：利用归约的思想证明定理 1。本文方案的属性基加密基于 Chen 方案[8]，用于保护对称密钥的机密性。因此，下面证明将本文方案中属性基加密的安全性可归约到 Chen 方案的安全性。如果存在攻击者 $\mathcal{A}$ 能以 ε 的概率攻破本文方案的安全性，则构造一个算法 $\mathcal{F}$ 能以 $\varepsilon/2$ 概率攻破 Chen 方案的安全性。令 $\mathcal{B}$ 是 Chen 方案的挑战者，则 $\mathcal{A}$ 是本文方案的挑战者，$\mathcal{F}$ 充当两个角色：Chen 方案的攻击者和本文方案的挑战者，三者之间关系如图 2 所示。

图 2 攻击者和挑战者之间的关系

Fig. 2 Relationship between attacker and challenger

1) 系统初始化阶段

$\mathcal{A}$ 向 $\mathcal{F}$ 发送一个挑战的访问策略 $(\boldsymbol{M}^*,\rho^*)$，然后 $\mathcal{F}$ 转发其给 $\mathcal{B}$。

2) 系统建立阶段

$\mathcal{F}$ 向 $\mathcal{B}$ 请求 Chen 方案参数 (G,G_T,p,g,e,h,H)，然后选择对称加密体制 AES 的加密算法 $Enc()$ 和解密算法 $Dec()$，最后向 $\mathcal{A}$ 发送系统参数 $PP=\{G,G_T,p,g,e,A_x,PK,h,H,Enc(),Dec()\}$。

3) 密钥询问阶段 1

对于 $\mathcal{A}$ 发送的关于全局身份 G_{IDu} 和属性集合 S 的用户密钥询问，如果 S 不满足 $(\boldsymbol{M}^*,\rho^*)$，则 $\mathcal{F}$ 转发该询问给 $\mathcal{B}$。收到 $\mathcal{B}$ 返回的用户密钥后，$\mathcal{F}$ 转发其给 $\mathcal{A}$。

4) 挑战阶段

$\mathcal{F}$ 转发 $\mathcal{A}$ 发送的两个长度相同的消息 k_0 和 k_1 给 $\mathcal{B}$，获得 $\mathcal{B}$ 返回的 $\{C_\eta^*,C_0^*,C_0^{*'},\{C_i^*\}_{i\in[1,l]}\}$，其中 $\eta\in\{0,1\}$。$\mathcal{F}$ 设置 $c_1^*=0$ 和 $\{f_i^*=0\}_{i\in[1,l]}$，发送挑战密文 $C_K^*=\{(\boldsymbol{M}^*,\rho^*),C_\eta^*,C_0^*,C_0^{*'},\{f_i^*,C_i^*\}_{i\in[1,l]},c_1^*\}$ 给 $\mathcal{A}$。

5) 密钥询问阶段 2

与密钥询问阶段 1 相同。

6) 猜测阶段

$\mathcal{A}$ 输出对 η 的猜测 η'。如果 $\eta=\eta'$，说明 $\{C_\eta^*,C_0^*,C_0^{*'},\{C_i^*\}_{i\in[1,l]}\}$ 是 Chen 方案[8]的一个有效密文，则 $\mathcal{F}$ 能猜测正确的概率是 $\varepsilon+1/2$。如果 $\eta=\eta'$，说明 $\mathcal{B}$ 返回的密文是一组随机数，$\mathcal{F}$ 猜测正确的概率是 $1/2$。因此，$\mathcal{F}$ 能以 $(\varepsilon+1/2)\times1/2+1/2\times1/2-1/2=\varepsilon/2$ 的概率攻破 Chen 方案的安全性。然而，Chen 方案的安全性依赖于 q-BDHE 假设。因此，本文方案在选择明文攻击下满足对称密钥的机密性。

4.3 安全性分析

1) 数据隐私性

DO 首先使用 AES 的加密算法和对称密钥 K_{ey} 对电力数据 m 进行加密处理，得到数据密文 $C_f=Enc_{K_{\text{ey}}}(m)$；然后利用属性基加密对 K_{ey} 进行加密得到对称密钥密文 C_K。只有属性集合 S 满足访问策略 $(\boldsymbol{M},\rho)$ 的用户才能正确计算出 K_{ey}，之后调用 AES 的解密算法恢复出电力数据 $m=Dec_{K_{\text{ey}}}(C_f)$。定理 1 已证明了对称密钥的安全性，并且 AES 算法是目前公认安全的对称密码体制。因此，本文方案以密文的形式实现了电力数据共享。即本文方案满足电力数据的隐私性。

2) 抗合谋攻击

在用户密钥 SK 中，$K_x=(A_x)^{rt\beta}=(A_x)^{rtH(G_{IDu})}$ 将每个属性 $x\in S$ 与用户的全局身份 G_{IDu} 进行了绑定，使得不同用户的属性组合无法正确地恢复出对称密钥 K_{ey}。因此，本文方案能抵抗用户间的合谋攻击。

3) 抗属性篡改与假冒攻击

在区块链中存储系统参数 PP、用户全局身份 G_{IDu} 的哈希值 $\beta=H(G_{IDu})$、用户的转换密钥 TK 和用户的属性集合 S。利用区块链的不可篡改性，能有效阻止攻击者伪造系统参数和篡改属性，从而可抵抗属性假冒攻击。

4) 数据完整性

DO 将电力数据 m 哈希值 $\widetilde{C}_f = H(m)$ 上传至区块链，哈希函数 H 的单向性确保了攻击者无法从 $\widetilde{C}_f$ 中计算出 m。DU 通过外包计算和解密操作恢复出 m，然后通过验证计算的 $H(m)$ 与区块链链中的 $\widetilde{C}_f$ 是否相等，来判断密文外包解密计算结果的正确性。因此，本文方案能保障电力共享数据的完整性。

5) 51%攻击

目前主流的区块链底层均采用成熟且经过长时间运行的区块链平台，如以太坊、Fabric 以及 FISCO-BCOS 等。51%攻击出现在比特币等依靠 PoW(工作量证明)共识机制的加密货币中，而非 PoW 共识算法则不存在 51%攻击。本文的实验环境基于 FISCO-BCOS 平台搭建，共识算法非 PoW 共识机制，因此不会出现 51%攻击的风险。且长远来看，即便采用了 PoW 共识算法，由于区块链的奖赏机制，诚实工作的收益远高于攻击区块链的收益。因此，51%攻击发生的机率也可以被忽略。

4.4 性能分析

文献[24]评估了密码操作运算的时间开销，结果如表 1 所示。

表 1 密码操作的运行时间

Table 1 Execution time of cryptographic operations

密码操作	符号	运行时间/ms
点乘运算	M	0.001 404
指数运算	E	0.165 217
双线性对运算	P	4.441 043

利用表 1 的执行时间，表 2 和图 3 比较了本文方案与文献[8,14,15,17]方案的计算性能。表 2 仅考虑计算开销比较大的运算操作，用 M，E 和 P 分别表示点乘运算、指数运算和双线性对运算。为了便于描述，假定所有方案选取相同的素数 p 和访问策略 $(\boldsymbol{M}_{l\times n}, \rho)$。

表 2 计算性能对比

Table 2 Comparison of computing performance

方案	DO 加密/ms		DU 解密/ms
	离线阶段	在线阶段	
文献[8]	0	$(1+l)M+(3+2l)E+P=4.9381+0.3318l$	$M+E=0.1666$
文献[14]	0	$(1+2l)M+(2+8l)E+P=4.7729+1.3245l$	$M+E=0.1666$
文献[15]	0	$(1+2l)M+(2+9l)E+P=4.7729+1.4898l$	$(2+5l)M+lE+(1+6l)P=4.4439+26.8185l$
文献[17]	0	$M+(2+2l)E+P=4.7729+0.3304l$	$2M+E+P=4.6091$
本文方案	$lM+(3+2l)\ E=0.4957+0.3318l$	$E=0.165217$	$M+E=0.1666$

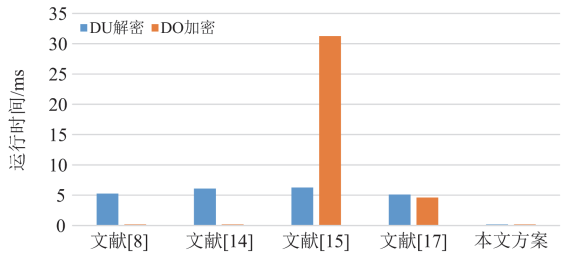

图 3 DO 加密和 DU 解密的计算开销比较

Fig. 3 Comparison of the computational overhead of DO encryption and DU decryption

在图 3 中，选择 $l=1$。在文献[8,14-15,17]中，数据拥有者 DO 的加密开销均与属性个数相关。除了文献[14]，数据用户 DU 的解密开销均与属性个数无关。从表 2 和图 3 可知，本文方案中的 DO 在加密数据时，大部分加密操作的计算任务在离线阶段完成，在线阶段只需执行一次指数运算。此外，DU 在解密数据时将大部分解密计算外包给边缘节点，只需执行一次指数运算和一次点乘运算便可解密密文。与其他方案相比较，本文方案具有较高的加密/解密性能。

方案功能比较如表 3 所示。由表 3 可知，文献[8]仅使用外包计算提升了效率，无法确保数据完整性与属性的防篡改。文献[14]尽管引入区块链技术，但并未实现防属性篡改。文献[15,17]也存在类似问题，在方案的功能上有所欠缺。而本文方案采用了区块链和密文外包解密计算技术，能在提高计算效率的同时防止属性的恶意篡改和保障数据的完整性。与其他方案相比较，本文方案在确保数据安全性的前提下能满足电力数据共享的高效性，更适用于资源受限的电力终端设备(如智能电表等)。

表 3 功能比较

Table 3 Comparison of functions

方案	区块链	外包计算	防属性篡改	数据完整性
文献[8]	×	√	×	×
文献[14]	√	√	×	√
文献[15]	√	×	×	×
文献[17]	√	×	√	√
本文方案	√	√	√	√

注：√和×分别表示满足或不满足该功能。

本文搭建区块链的实验环境为 Intel(R) Xeon(R) Gold 6133 2.50 GHz，Ubuntu Server 22.04 LTS 64 位，区块链底层平台选用 FISCO-BCOS 3.1.0。实验模拟生成了 1000~5000 条用户属性数据，将用户数据打包后上链存储，测试打包上链以及从区块链回传数据的时间，具体测试结果如图 4 和图 5 所示。

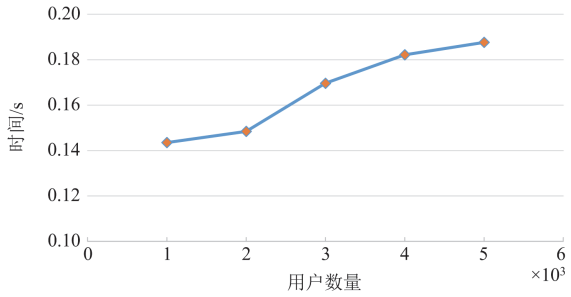

图 4 用户数据上传时间

Fig. 4 User data upload time

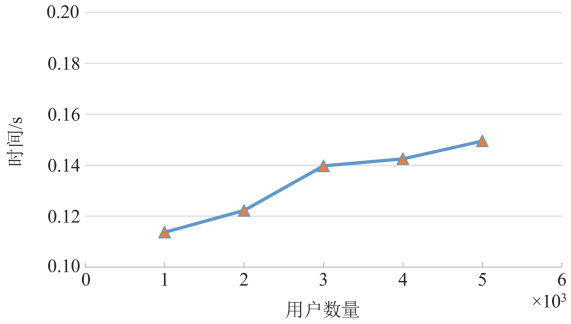

图 5 回传用户数据时间

Fig. 5 Time to return user data

由图 4 与图 5 可知，随着用户数量不断增多，上链时间会小幅增加，效率略有降低，但用户的数量增长更为显著，以小幅的效率降低来换取较大的用户扩增是可以接受的。回传用户数据的时间略低于上传数据的时间，原因在于上传用户数据时区块链平台需要运行共识算法向节点公开数据。区块链平台所选择的不同共识算法会对时间产生不同程度的影响。

5　结论

基于区块链和云边端协同技术，本文提出了一种高效的电力数据共享方案。通过在线/离线加密模式和外包计算机制，大大降低了数据拥有者和数据访问用户的计算负担。利用区块链的不可伪造性等特点，实现了属性的防篡改性和解密密文的完整性验证。然而，该方案依赖于一个可信的属性授权机构颁发用户密钥，存在单点失效和权限过大等问题。因此，下一步的工作是设计基于区块链和多属性授权机构的电力数据共享方案。

参考文献

[1] 张瑶, 王傲寒, 张宏. 中国智能电网发展综述[J]. 电力系统保护与控制, 2021, 49(5): 180-187.
ZHANG Yao, WANG Aohan, ZHANG Hong. Overview of smart grid development in China[J]. Power System Protection and Control, 2021, 49(5): 180-187.

[2] 朱炳铨, 郭逸豪, 郭创新, 等. 信息失效威胁下的电力信息物理系统安全评估与防御研究综述[J]. 电力系统保护与控制, 2021, 49(1): 178-187.
ZHU Bingquan, GUO Yihao, GUO Chuangxin, et al. A survey of the security assessment and security defense of a cyber physical power system under cyber failure threat[J]. Power System Protection and Control, 2021, 49(1): 178-187.

[3] 郑楷洪, 杨劲锋, 王鑫, 等. 用电量数据的可视化研究综述[J]. 电力系统保护与控制, 2022, 50(9): 179-187.
ZHENG Kaihong, YANG Jingfeng, WANG Xin, et al. Overview of visualization research on electricity consumption data[J]. Power System Protection and Control, 2022, 50(9): 179-187.

[4] GOYAL V, PANDEY O, SAHAI A, et al. Attribute-based encryption for fine-grained access control of encrypted data[C] // Proceedings of the 13th ACM Conference on Computer and Communications Security, 2006: 89-98.

[5] SONG Haina, HAN Xinyu, LÜ Jie, et al. MPLDS: An integration of CP-ABE and local differential privacy for achieving multiple privacy levels data sharing[J]. Peer-to-Peer Networking and Applications, 2022, 15(1): 369-385.

[6] QAISAR Z H, ALMOTIRI S H, AL GHAMDI M A, et al. A scalable and efficient multi-agent architecture for malware protection in data sharing over mobile cloud[J]. IEEE Access, 2021, 9: 76248-76259.

[7] ZHANG Zhijun, REN Xiaojun. Data security sharing method based on CP-ABE and blockchain[J]. Journal of Intelligent & Fuzzy Systems, 2021, 40(2): 2193-2203.

[8] 陈家豪, 殷新春. 基于云雾计算的可追踪可撤销密文策略属性基加密方案[J]. 计算机应用, 2021, 41(6): 1611-1620.
CHEN Jiahao, YIN Xinchun. Traceable and revocable ciphertext-policy attribute-based encryption scheme based on cloud-fog computing[J]. Journal of Computer Applications, 2021, 41(6): 1611-1620.

[9] 王胜寒, 郭创新, 冯斌, 等. 区块链技术在电力系统中的应用: 前景与思路[J]. 电力系统自动化, 2020, 44(11): 10-24.

WANG Shenghan, GUO Chuangxin, FENG Bin, et al. Application of blockchain technology in power systems: prospects and ideas[J]. Automation of Electric Power Systems, 2020, 44(11): 10-24.

[10] DU Haorui, CHEN Jianhua, LIN Fei, et al. A lightweight blockchain-based public-key authenticated encryption with multi-keyword search for cloud computing[J]. Security and Communication Networks, 2022: 1-11.

[11] 邵奇峰, 金澈清, 张召, 等. 区块链技术:架构及进展[J]. 计算机学报, 2018, 41(5): 969-988.
SHAO Qifeng, JIN Cheqing, ZHANG Zhao, et al. Blockchain: architecture and research progress[J]. Chinese Journal of Computers, 2018, 41(5): 969-988.

[12] ESPOSITO C, FICCO M, GUPTA B B. Blockchain-based authentication and authorization for smart city applications[J]. Information Processing & Management, 2021, 58(2).

[13] ZUO Yuting, KANG Zhaozhe, XU Jian, et al. BCAS: a blockchain-based ciphertext-policy attribute-based encryption scheme for cloud data security sharing[J]. International Journal of Distributed Sensor Networks, 2021, 17(3): 1-16.

[14] 杨颜博, 张嘉伟, 马建峰. 一种使用区块链保护车联网数据隐私的方法[J]. 西安电子科技大学学报, 2021, 48(3): 21-30.
YANG Yanbo, ZHANG Jiawei, MA Jianfeng. Method for using the blockchain to protect data privacy of IoV[J]. Journal of Xidian University, 2021, 48(3): 21-30.

[15] 李雪莲, 张夏川, 高军涛, 等. 支持属性和代理重加密的区块链数据共享方案[J]. 西安电子科技大学学报, 2022, 49(1): 1-16.
LI Xuelian, ZHANG Xiachuan, GAO Juntao, et al. Blockchain data sharing scheme supporting attribute and proxy re-encryption[J]. Journal of Xidian University, 2022, 49(1): 1-16.

[16] FAN Kai, PAN Qiang, ZHANG Kuan, et al. A secure and verifiable data sharing scheme based on blockchain in vehicular social networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5826-5835.

[17] 曾辉祥, 习宁, 谢晴晴, 等. 抗属性篡改的去中心化密文数据安全共享[J]. 西安电子科技大学学报, 2022, 49(2): 135-145.
ZENG Huixiang, XI Ning, XIE Qingqing, et al. Decentralized ciphertext sharing based on blockchain[J]. Journal of Xidian University, 2022, 49(2): 135-145.

[18] 尚松超, 陈勃翰, 颜光伟, 等. 基于区块链的数据共享访问控制模型[J]. 通信技术, 2021, 54(12): 2666-2673.
SHANG Songchao, CHEN Bohan, YAN Guangwei, et al. Model for data sharing and access control based on blockchain[J]. Communications Technology, 2021, 54(12): 2666-2673.

[19] WINSTER S G, KUMAR A S, RAMESH R. User centric block-level attribute based encryption in cloud using blockchains[J]. Computer Systems Science and Engineering, 2022, 42(2): 605-618.

[20] ZHANG Leyou, ZHANG Tianshuai, WU Qing, et al. Secure decentralized attribute-based sharing of personal health records with blockchain[J]. IEEE Internet of Things Journal, 2022.

[21] XIANG Xinyin, ZHAO Xingwen. Blockchain-assisted searchable attribute-based encryption for e-health systems[J]. Journal of Systems Architecture, 2022, 124: 102417.

[22] EZHIL A V, INDRA G K, KULOTHUNGAN K. Auditable attribute-based data access control using blockchain in cloud storage[J]. The Journal of Supercomputing, 2022, 78(8): 10772-10798.

[23] JYOTHILAKSHMI K B, ROBINS V, MAHESH A S. A comparative analysis between hyperledger fabric and ethereum in medical sector: a systematic review[J]. Sustainable Communication Networks and Application, 2022: 67-86.

[24] DOHARE I, SINGH K, AHMADIAN A, et al. Certificateless aggregated signcryption scheme for cloud-fog centric industry 4.0[J]. IEEE Transactions on Industrial Informatics, 2022, 18(9): 6349-6357.

收稿日期：2022-09-18；　　修回日期：2022-12-31

作者简介：

杨小东(1981—)，男，通信作者，博士，教授，硕士生导师，研究方向为密码学与大数据安全；E-mail: y200888@平共处163.com

廖泽帆(1997—)，男，硕士研究生，研究方向为电力系统数据安全；E-mail: lzf0097@163.com

刘　磊(1982—)，男，本科，研究方向为数据隐私保护。E-mail: 18919312217@189.cn

(编辑　魏小丽)