兼顾隐私保护与结果可验证的点对点能源交易匹配机制

皮冰锋[1,2]，金澈清[1]，钱卫宁[1]，华松[2]，张沈斌[2]
1. 华东师范大学数据科学与工程学院，上海 200062；
2. 天聚地合(苏州)科技股份有限公司，江苏 苏州 215000

摘要
在多边经济调度的推动下，点对点能源交易模式日益受到关注，然而数据隐私泄露和交易监管难题成为制约其发展的关键瓶颈。提出了一种新型的点对点能源交易匹配机制PV-RCI，其在保障隐私保护机制有效性的同时，确保交易匹配结果的可验证性。通过引入可信的监管审计方，并结合同态加密和零知识证明技术，所提机制不仅有效保护了交易过程中的数据隐私，还实现了交易匹配结果的可验证性。所提机制在促进供需双方交易匹配的基础上，降低了交易的社会总成本，为解决能源交易行业的隐私保护和可监管性问题提供了全新的思路。

关键词
点对点；隐私保护；交易匹配；零知识证明

中图分类号：TP309　　文献标志码：A　　doi：10.11959/j.issn.2096-0271.2025041

Peer-to-peer energy transaction matching mechanism balancing privacy-preserving ard result verifiability

PI Bingfeng[1,2], JIN Cheqing[1], QIAN Weining[1], HUA Song[2], ZHANG Shenbin[2]
1. School of Data Science and Engineering, East China Normal University, Shanghai 200062, China
2. Tianju Dihe (Suzhou) Technology Co. , Ltd. , Suzhou 215000, China

Abstract
Under the impetus of multi-bilateral economic dispatch, the peer-to-peer energy trading mode has gained significant attention. However, data privacy breaches and transaction regulatory challenges have emerged as critical barriers to its growth. A new peer-to-peer energy transaction matching mechanism named PV-RCI was proposed, which ensured the effectiveness of privacy-preserving mechanism and the validity of transaction matching mechanism. By incorporating a trusted auditing party and leveraging homomorphic encryption in conjunction with zero-knowledge proof, the proposed mechanism not only safeguarded data privacy but also ensured the verifiability of transaction matching outcomes. On the basis of promoting transaction matching between supply and demand parties, the proposed mechanism significantly reduced the overall social cost of transaction, offering a new approach to addressing privacy-preserving and regulatory issues in the energy trading sector.

Key words
peer-to-peer, privacy-preserving, transaction matching, zero-knowledge proof

0 引言

传统的大规模交易场景，如金融证券[1]、电力能源[2]、数据资源[3]等，通常采用中心化的交易匹配方式及统筹调度机制，需要具备高稳定性的硬件设备及多级容灾备份的软件系统的支撑，以保证系统的可靠性。

为降低中心化交易机制的高信用成本，研究者衍生出了一系列的技术创新，如基于区块链和智能合约的去中心化金融的交易机制[4]、分布式多主体协作的电网模式[5]，以及电力能源和碳排放权的交易匹配方式[6]等。

电力能源交易的日前出清机制会根据参与主体的日前能源申报份额、电网的约束和社会的承受能力集中优化出清。匹配双方的电量和价格相对较隐私，不宜公开。而监管部门希望对交易双方的出清份额进行审核，确保匹配结果满足出清的优化约束及社会治理的要求，因此存在数据隐私保护与监管审计之间的矛盾。

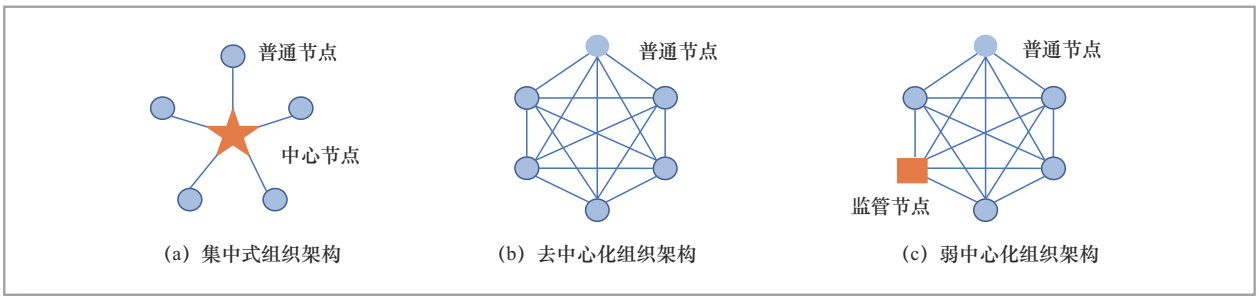
尽管区块链技术为点对点交易提供了信任的框架，但其公开的账本数据存在隐私泄露的风险，而数据加密存储又难以满足监管审计的要求[7]。文献[8]提出的点对点电力交易匹配算法，从理论上证明了其可以实现中心化的电力交易的效果，但交易匹配过程和额度结果验证均采用明文数据传输，存在数据隐私泄露的风险。本文提出了兼顾隐私保护和结果可验证的点对点交易匹配机制 PV-RCI（privacy-preserving and verifiable relaxed consensus innovation），引入可信的监管审计节点[9]，如**图1**所示，运用同态加密技术实现了交易双方的秘密信息共享，采用零知识技术构建交易的可验证证明，在保护数据隐私的基础上实现交易匹配结果的可验证性。本文通过模拟点对点的电力交易匹配的过程，验证了 PV-RCI 的隐私安全提升及匹配结果的可验证性。

本文主要贡献如下。

- 本文提出了一种点对点交易匹配机制，该机制既能有效保护数据隐私安全，又能实现匹配结果的审核验证。
- 本文实现了同态加密和零知识证明的整合应用，将同态加密技术应用于交易双方的秘密信息共享，并借助零知识证明技术构建匹配结果的可验证性证明。
- 本文引入监管审计节点，在保护数据隐私的基础上实现匹配结果的审核验证。

1 相关工作

能源领域日益拓展到多种资源形式，



(a) 集中式组织架构　(b) 去中心化组织架构　(c) 弱中心化组织架构

图1 3种组织架构

包括电力、天然气、氢能源、碳排放和水资源等，能源交易市场的协作方也逐渐增多，形成一个复杂的多边经济调度（multi-bilateral economic dispatch，MBED）及优化问题[10-12]。众多学者已对能源交易进行了深入研究，文献[5]提出的Consensus + Innovation（CI）的共识算法，旨在解决发电节点、负荷节点及储能设备间的协调问题，以实现最优电力调度。文献[8]进一步改进，提出了点对点电力匹配的RCI（relaxed consensus + innovation）共识算法。文献[13]介绍了区块链的去中心化、开放性和透明性等特点，探讨其与分布式能源交易需求的契合性。文献[14]设计了一种基于区块链的绿证与碳联合市场交易机制，利用智能合约促成绿证和碳排放权的交易匹配，实现双边交易和联合市场出清。文献[15]构建了基于虚拟电厂的两阶段交易匹配模型。首先，其以虚拟电厂利益最大化为目标，通过合作博弈确定厂内各单元的功率输出。之后，其依据交易匹配机制逐步调整虚拟电厂的报价，直至交易出清。

上述方法大多基于明文数据传输实现能源的交易匹配，但随着全球数据安全相关法规的不断完善，能源交易中的隐私保护问题逐渐受到广泛关注。文献[16]采用安全多方计算技术构建了一个点对点能源交易框架，为电力产销者和电网运营商提供双向隐私保护，采用区块链解决多方交易的争议。文献[17]提出了基于组合自适应的共识算法实现保护隐私的去中心化交易匹配方式，但双方仍然需要共享部分明文因子。文献[18]提出了两方安全计算架构，在交易匹配过程中，同时使用基于密文的价格计算以及基于智能合约的明文计算，并采用零知识证明验证两个结果的一致性，零知识证明的频繁使用降低了算法的实际效率。

2 点对点电力交易匹配的形式化表示

为构建一个点对点的电力交易匹配市场，系统中所有参与方之间相互协商，基于共识机制优化决策，以高效解决多边经济调度问题。

2.1 节点功率及价格的定义

设交易市场中有n个参与方，i和j是其中的两个参与节点，经过多轮协商确定i与j之间的功率信息为P_{ij}及功率价格为λ_{ij}。采用$n\times n$的矩阵$\boldsymbol{P}$及$\boldsymbol{\Lambda}$分别表示参与节点之间的功率及价格。

$$\boldsymbol{P}=\begin{bmatrix} P_{00} & \cdots & P_{0j} & \cdots & P_{0n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ P_{i0} & \cdots & P_{ij} & \cdots & P_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ P_{n0} & \cdots & P_{nj} & \cdots & P_{nn} \end{bmatrix},$$

$$\boldsymbol{\Lambda}=\begin{bmatrix} \lambda_{00} & \cdots & \lambda_{0j} & \cdots & \lambda_{0n} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \lambda_{i0} & \cdots & \lambda_{ij} & \cdots & \lambda_{in} \\ \vdots & \ddots & \vdots & \ddots & \vdots \\ \lambda_{n0} & \cdots & \lambda_{nj} & \cdots & \lambda_{nn} \end{bmatrix} \quad (1)$$

其中，当$i=j$，或i、j同为发电方、用电方时，$P_{ij}=0$，$\lambda_{ij}=0$，其分别对应矩阵$\boldsymbol{P}$的第i行、矩阵$\boldsymbol{\Lambda}$的第j列值。

节点i的总功率P_i是其与所有相邻节点协商的功率总和，存在着上下限的边界限制。

$$P_i=\sum_{j=0}^{n}P_{ij},\ \underline{P_i}\leqslant P_i\leqslant\overline{P_i},\forall i\in n, \quad (2)$$

其中，$\underline{P_i}$、$\overline{P_i}$分别为节点n的功率下限及上限。

2.2 节点的社会成本

本文引入社会成本的概念以确保能源

交易符合社会可持续发展的要求。发电方式如煤矿、核能等，因环境污染较高，生产成本远高于风力、水力、太阳能等清洁能源。生活、医疗、教育等领域的电力消费可以提高生活的幸福指数，社会成本远低于工业制造等高碳排放、环境污染的领域。本文考虑计算的复杂度，采用二次函数模拟生产成本与消费者效用相关的成本函数。

$$C\left(P_i\right)=\frac{1}{2}a_iP_i^2+b_iP_i+c_i, \tag{3}$$

其中，a_i、b_i及c_i为预设的常数。

2.3 点对点能源交易匹配的形式化表示

能源匹配指能源供应方与需求方进行匹配的过程，要求匹配之后的结果满足电力供需平衡的要求，促成电力交易的成功，并保证社会总成本的最小化，其形式化约束表示如下。

$$\begin{cases}\min\sum_{i=0}^{n}C(P_i)\\ \text{s.t. } P_i\in\left[\underline{P_i},\ \overline{P_i}\right],\ \forall i\in n\\ P_{ij}+P_{ji}=0,\ \forall i,j\in n\\ \lambda_{ij}=\lambda_{ji},\forall i,j\in n\\ P_{ij}\geqslant 0, i\text{ 为发电方}\\ P_{ij}\leqslant 0, i\text{ 为用电方}\end{cases} \tag{4}$$

式（4）中，第一个约束条件是期望达成交易匹配时，所有参与方的社会总成本最小。第二个条件约束了各个节点的总功率，确保其在限定范围之内。第3个条件表示交易双方需要达成能源的供需平衡。第4个约束表示达成交易共识的两者之间保持价格的一致性。最后两个约束条件对节点的角色进行了限定，不能同时为生产者和消费者。

2.4 点对点能源交易匹配的共识算法

RCI共识算法[8]将上述交易匹配的全局最优解分解为每个参与节点的局部最优解，节点之间进行多轮协商，最终达到KKT（Karush-Kuhn-Tucker）条件下的平衡[19]，算法得以收敛。

以参与节点i为例，在第k轮循环中，参与节点i与其他节点j协商后的局部最优解可简化为以下内容。

$$\min C(P_i)-\sum_{j=0}^{n}\lambda_{ij}^kP_{ij}^k \tag{5}$$

根据以下共识过程，协商确定两个节点间的功率P_{ij}及价格λ_{ij}。

2.4.1 节点价格的更新

为达到收敛，节点i与j需要就交易价格达成一致（即$\lambda_{ij}=\lambda_{ji}$），还需要满足能源供需平衡，即$P_{ij}+P_{ji}=0$，本文引入两个因子$\alpha$和$\beta$协调收敛过程如下。

$$\lambda_{ij}^{k+1}=\lambda_{ij}^k-\beta^k\left(\lambda_{ij}^k-\lambda_{ji}^k\right)-\alpha^k\left(P_{ij}^k+P_{ji}^k\right) \tag{6}$$

2.4.2 节点功率的更新

采用拉格朗日松弛函数进一步优化式（5）表示的局部最优解。

$$L_i^{\text{loc}}=C(P_i)-\sum_{j=0}^{n}\lambda_{ij}^kP_{ij}^k+\overline{\mu_i}(P_i-\overline{P_i})-\underline{\mu_i}(P_i-\underline{P_i}) \tag{7}$$

其中，$\overline{\mu_i}$、$\underline{\mu_i}$为拉格朗日乘子。

根据拉格朗日问题的一阶导数求解，本文可以得到以下结果。

$$\begin{cases}C(P_i)-\lambda_{ij}+\overline{\mu_i}-\underline{\mu_i}=0\\ P_i=\dfrac{\lambda_{ij}-\overline{\mu_i}+\underline{\mu_i}-b_i}{a_i}\end{cases} \tag{8}$$

其中，a_i、b_i是节点i的成本函数$C(P_i)$中的因子。

将P_i代入节点i的第k轮迭代更新中，可以表示为以下内容。

$$\tilde{P}_i^k = \frac{\widetilde{\lambda}_{ij}^k - \overline{\mu}_i^k + \underline{\mu}_i^k - b_i}{a_i} \tag{9}$$

其中，$\widetilde{\lambda}_{ij}^k = \sum_{j=0}^{n} f_{ij}^k \lambda_{ij}^k$，记为节点$i$感知的其他所有节点价格的平均值，$f_{ij}^k = \frac{|P_{ij}| + \delta^k}{\sum_{l=0}^{n}(|P_{il}| + \delta^k)}$，$\delta$是持久化因子。

基于上述的最优解，本文更新约束节点i与节点j之间的功率P_{ij}。

$$\begin{cases} P_{ij}^{k+1} = \max(0, P_{ij}^k + f_{ij}^k(\tilde{P}_i^k - P_i^k)), & i\text{为发电方} \\ P_{ij}^{k+1} = \min(0, P_{ij}^k + f_{ij}^k(\tilde{P}_i^k - P_i^k)), & i\text{为用电方} \end{cases} \tag{10}$$

2.4.3 节点功率的边界约束

基于节点i的功率边界约束$[\underline{P}_i, \overline{P}_i]$，本文更新式（7）中的拉格朗日乘子$\overline{\mu}_i$及$\underline{\mu}_i$。

$$\begin{cases} \overline{\mu}^{k+1} = \max(0, \overline{\mu}^k + \eta^k(P_i - \overline{P}_i)) \\ \underline{\mu}^{k+1} = \max(0, \underline{\mu}^k + \eta^k(\underline{P}_i - P_i)) \end{cases} \tag{11}$$

2.4.4 迭代收敛的条件

最终根据价格因子λ、功率P及边界约束μ的震荡幅度，判断节点i是否满足停止条件。

$$\begin{cases} |\lambda_{ij}^{k+1} - \lambda_{ij}^k| < \epsilon_\lambda \\ |P_{ij}^{k+1} - P_{ij}^k| < \epsilon_P \\ |\mu_i^{k+1} - \mu_i^k| < \epsilon_\mu \end{cases} \tag{12}$$

当且仅当所有节点都满足停止条件时，共识收敛，交易匹配结束。

3 兼顾隐私保护与结果可验证的点对点能源交易匹配机制

基于上述能源交易匹配的约束及RCI，以及基于明文传输的交易匹配的安全隐患问题，本文提出了一种保护数据隐私且支持交易结果可验证的PV-RCI，如**图2**所示。在RCI的基础上，PV-RCI引入一个可信的审计节点提供加解密服务，使用同态加密[20]及零知识证明[21]，实现了节点之间的密文数据协商及交易匹配，并支持第三方节点对交易匹配结果的监管审查。

支持密文传输的点对点交易匹配的PV-RCI的共识算法详见3.1节，采用同态加密保护数据隐私的过程详见3.2节，基于零知识证明构建的交易匹配结果的正确

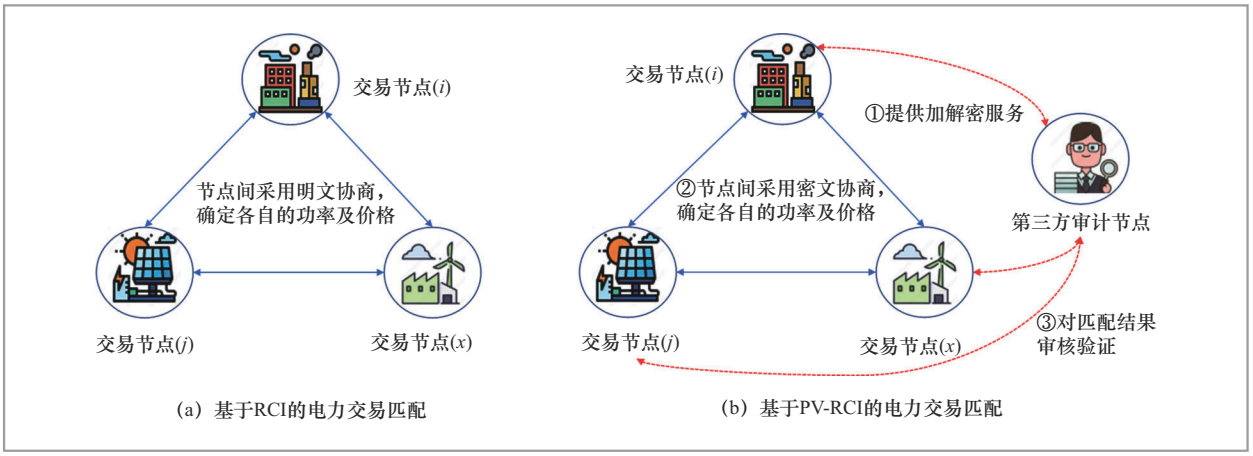


图2 基于明文的RCI以及基于密文的PV-RCI的交易匹配机制

性证明及验证过程详见3.3节。

3.1 基于密文的PV-RCI交易匹配共识算法

基于PV-RCI的共识算法如**图3**所示，为了保护数据隐私，节点i与节点j之间均以密文的方式协商价格及功率。

3.1.1 第三方审计节点的服务内容

第三方审计节点主要为其他交易节点提供以下3种服务。

- 在交易匹配之前，第三方审计节点初始化同态加密所需要的公私钥（pk,sk），并将公钥共享给其他交易节点，用于它们对各自价格、功率信息的加密。
- 在交易匹配过程中，第三方审计节点为其他交易节点解密价格因子。
- 在交易匹配结束后，第三方审计节点解密其他交易节点产生的零知识证明，验证结果的正确性。

3.1.2 节点之间的密文协商

以节点i为例，节点i与节点j间的协商过程如下。

- 算法初始化价格因子λ_{ij}^0及两个节点之间的功率信息P_{ij}^0。
- 节点i从节点j获得其加密后的价格因子$\mathrm{Enc}(\lambda_{ji}^{k+1})$及功率信息$\mathrm{Enc}(P_{ji}^{k+1})$之后，节点$i$采用式（13）所示的同态加密的方式更新自身的价格因子$\mathrm{Enc}(\lambda_{ij}^{k+1})$，之后将叠加了随机数的$\mathrm{Enc}\left(\hat{\lambda}_{ij}^{k+1}\right)$发给第三方解密。

$$\mathrm{Enc}\left(\lambda_{ij}^{k+1}\right)=\lambda_{ij}^{k}-\beta^{k}\left(\lambda_{ij}^{k}-\mathrm{Enc}\left(\lambda_{ji}^{k}\right)\right)-\alpha^{k}\left(P_{ij}^{k}+\mathrm{Enc}\left(P_{ji}^{k}\right)\right) \tag{13}$$

$$\mathrm{Enc}\left(\hat{\lambda}_{ij}^{k+1}\right)=\mathrm{Enc}\left(\lambda_{ij}^{k+1}\right)+r_{ij} \tag{14}$$

其中，r_{ij}为节点i产生的随机数。

- 节点i将第三方解密得到的$\hat{\lambda}_{ij}^{k+1}$去掉随机数，得到自身的价格因子明文λ_{ij}^{k+1}，用于更新计算自身的功率P_{ij}^{k+1}及边界约束μ_{ij}^{k+1}。

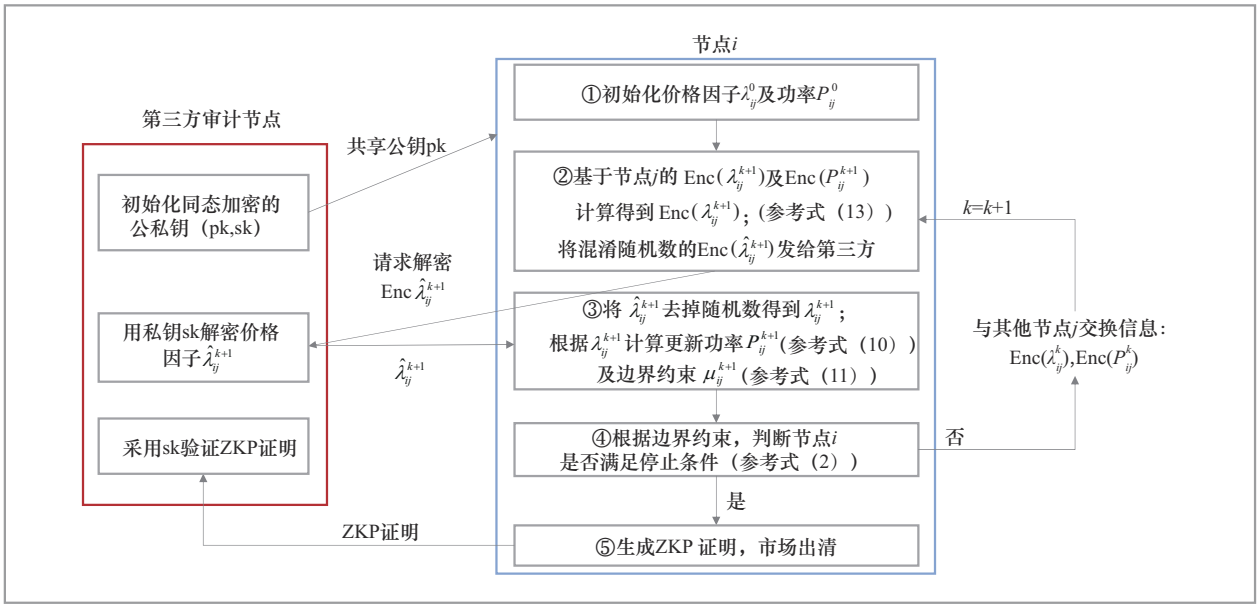


图3 PV-RCI的共识算法

• 算法根据边界约束条件，判断当前节点是否满足停止条件。如果未满足，则采用第三方公钥加密当前的价格因子及功率信息，将密文信息共享给其他节点进行下一轮博弈。

• 当且仅当所有节点都满足停止条件，共识结束，每个节点依据自身的功率信息生成零知识证明，市场出清。

3.2 基于同态加密的秘密信息共享

图 4 描述了两个节点借用第三方审计节点的加解密服务，结合加法同态的算法支持，实现的加密信息共享过程。

3.2.1 基于同态加密的秘密共享的过程

• 节点 j 使用第三方审计节点的公钥 pk，加密其第 k 轮的价格因子 λ_{ji}^{k}、功率 P_{ji}^{k}。

• 节点 j 将加密后的价格因子 $\mathrm{Enc}(\lambda_{ji}^{k}, \mathrm{pk})$ 及功率 $\mathrm{Enc}(P_{ji}^{k}, \mathrm{pk})$ 发送给节点 i。

• 节点 i 获得节点 j 加密后的价格因子及功率信息，采用式（13）所示的同态加密方法，计算得到第 $k+1$ 轮的价格因子密文 $\mathrm{Enc}(\lambda_{ij}^{k+1})$，加上混淆随机数得到 $\mathrm{Enc}(\hat{\lambda}_{ij}^{k+1})$。

• 节点 i 将混淆后的密文 $\mathrm{Enc}(\hat{\lambda}_{ij}^{k+1})$ 发送给第三方节点解密。

• 第三方节点使用其私钥 sk 解密 $\hat{\lambda}_{ij}^{k+1}$，并返回给节点 i。

• 节点 i 将解密的信息去掉随机数，得到新一轮的价格因子 λ_{ij}^{k+1}。

结合第三方的加解密服务及同态加密技术，保障了任意两个节点之间的安全信息传输，同时叠加了随机数混淆价格因子，确保各节点的敏感信息不被泄漏。

3.2.2 基于同态加密的秘密共享的正确性分析

本文引入 Paillier 算法的同态加密机制，主要基于加法同态及标量乘法同态的特性，确保基于式（13）实现的密文价格因子的正确性。

（1）密钥生成

本文随机选择两个大质数 p 和 q，使其满足 $\gcd\left(pq,(p-1)(q-1)\right)=1$，其中，gcd 代表最大公约数。然后计算 $n=pq$ 及 $\lambda=\mathrm{lcm}(p-1,q-1)$，其中 lcm 代表最小公倍

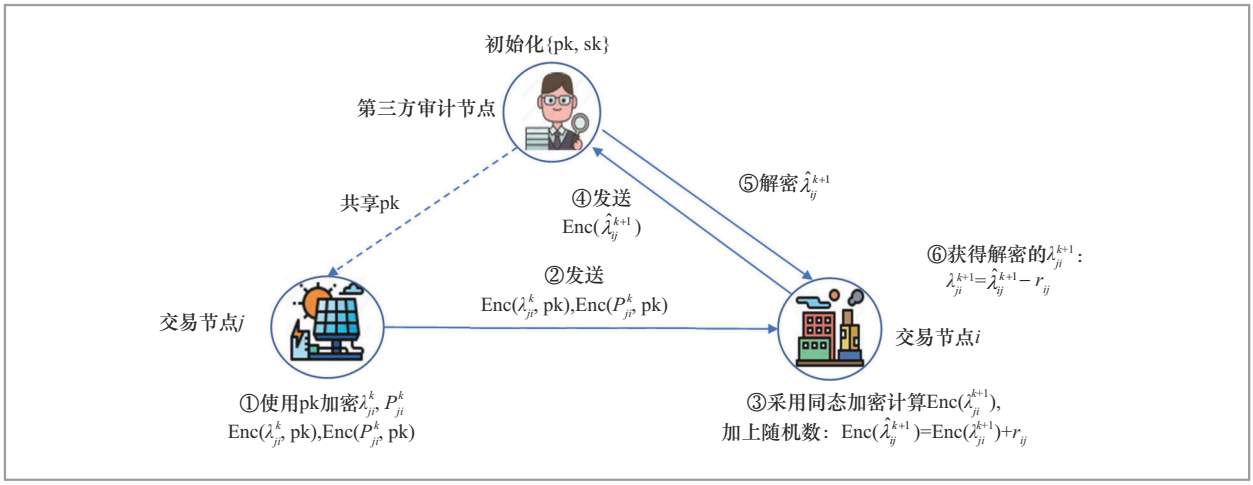


图 4 基于第三方节点的加密共享过程

数。之后随机选择 $g \in Z_{N^2}^*$，计算 g 的逆元 $\mu = L(g^{\lambda} \bmod n^2)^{-1} \bmod n$，其中 $L(x) = \dfrac{x-1}{n}$。

之后分发公钥 $\mathrm{pk} = (n, g)$，保留私钥为 $\mathrm{sk} = (\lambda, \mu)$。

（2）加密算法

本文随机挑选一个 $r \in Z_N$，确保 $\gcd(r, n) = 1$，采用公钥对明文 m 进行加密。

$$\mathrm{Enc}(m, \mathrm{pk}) = g^m \times r^n \bmod n^2 = c \tag{15}$$

（3）解密算法

本文采用私钥对密文 c 进行解密。

$$\mathrm{Dec}(c, \mathrm{sk}) = L(c^{\lambda} \bmod n^2) \times u \bmod n = \frac{L(c^{\lambda} \bmod n^2)}{L(g^{\lambda} \bmod n^2)} \bmod n = m \tag{16}$$

（4）加法同态的特性

对于任意明文 $m_1, m_2 \in Z_N$，其密文表示如下。

$$\begin{cases} c_1 = \mathrm{Enc}(m_1, \mathrm{pk}) = g^{m_1} \times {r_1}^n \bmod n^2 \\ c_2 = \mathrm{Enc}(m_2, \mathrm{pk}) = g^{m_2} \times {r_2}^n \bmod n^2 \end{cases} \tag{17}$$

可以通过密文乘法实现明文的加法。

$$c_1 \times c_2 = \mathrm{Enc}(m_1, \mathrm{pk}) \times \mathrm{Enc}(m_2, \mathrm{pk}) = g^{m_1+m_2}(r_1 r_2)^n \bmod \mathrm{n}^2 = \mathrm{Enc}(m_1 + m_2, \mathrm{pk}) \tag{18}$$

（5）标量乘法同态的特性

对于任意明文 $m \in Z_N$，$k \in N$，可以通过以下方式实现同态性。

$$(c)^k = \mathrm{Enc}(m, \mathrm{pk})^k \bmod n^2 = g^{km} \times r^{kn} \bmod n^2 = \mathrm{Enc}(m \times k, \mathrm{pk}) \tag{19}$$

基于上述加法同态及标量乘法同态的特性，可以确保式（13）基于密文实现的价格因子，经过解密后与式（6）基于明文实现的一致性及正确性。

3.3 基于零知识证明的安全性增强及结果验证

共识算法结束，为了防止单个节点出现作弊行为（如提前结束共识），以及多个节点之间相互串通作弊（如协商超额发电或用电等），需要对每个节点的匹配结果进行审核验证。为保证审核时不泄露各节点的数据隐私，采用零知识证明为每个节点生成核验的 Proof，供第三方节点验证，零知识证明的生成方式如**图 5** 所示。

3.3.1 节点生成零知识证明 Proof

共识结束后，节点 i 接收到其他多个节

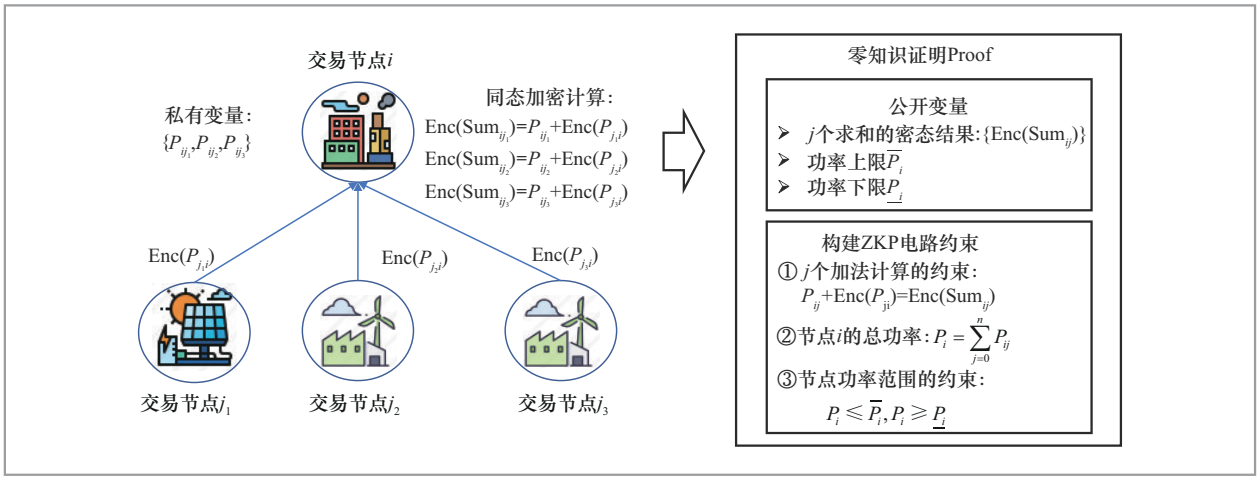


图 5 零知识证明的生成方式

表1 实验样例数据

节点序号	a_n/(元·kW^{-2})	b_n/(元·kW^{-2})	$\underline{P_n}$/kW	$\overline{P_n}$/kW	备注
1	0.067	64	−146	0	用电节点
2	0.075	37	0	1 100	发电节点

点的最终功率信息，将收到的功率密文与自身的功率明文求和，获得密态数据的功率之和；之后将多个密态求和的结果，以及自身的功率上下限作为零知识证明的公开变量。

节点i随后构建3个零知识证明的电路约束，第一个是确保基于密文的同态加法求和计算的正确性；第二个是确保节点总功率计算的正确性；最后一个是约束节点的总功率未超出功率上下限的范围。

3.3.2 第三方节点验证零知识证明

以节点i为例，根据其零知识证明的公开变量，以及它的零知识证明电路约束，第三方审计节点可以验证该节点在密态计算的过程中是否作弊，并可以进一步使用第三方节点的私钥，解密每个密态求和的结果$\mathrm{Enc}\left(\mathrm{Sum}_{ij}\right)$，验证求和的结果是否为0，以此判断节点间交易匹配是否达到了产销平衡。

4 实验及分析

基于上述方案设计开展实验，本文对比基于明文传输的RCI的共识算法和基于加密传输的PV-RCI的共识算法的一致性，同时评估PV-RCI的可行性和安全性。

4.1 实验设定

实验机器为Intel i7-11700 2.50 GHz，8核CPU，100 GB内存，Ubuntu 20.04。采用50个节点（33个用电节点，17个发电节点）进行多次分批实验，部分样例数据见**表1**。本文使用Golang的线程模拟单个交易节点的计算，以Go Channel实现节点之间的密文匹配过程。实验过程采用Gadget-Paillier的同态加密算法库，使用Gnark实现零知识证明的生成和验证。

价格及功率计算过程中的参数设定如下。

$$\alpha^k=\frac{0.01}{k^{0.01}},\beta^k=\frac{0.1}{k^{0.1}},\eta^k=0.005,\delta^k=1 \quad (20)$$

停止参数阈值设定为$\varepsilon_\lambda=0.001$，$\varepsilon_P=0.01$，$\varepsilon_\mu=0.001$。

4.2 实验结果及分析

4.2.1 结果的一致性对比

实验模拟了基于RCI明文传输以及保护隐私的PV-RCI密文传输的两种交易匹配模式，实验结果见**表2**。在这两种交易匹配的模式下，社会总成本的绝对误差为86.69，相对误差不超过0.06%。然而，由于同态加密对数据精确度的影响，在相同

表2 明文与密文共识算法的结果比对

模式	迭代次数/次	用电节点总成本/元	发电节点总成本/元	社会总成本/元
明文RCI	146 130	−438 389.59	259 788.86	−178 600.73
密文PV-RCI	160 099	−438 440.98	259 747.94	−178 687.42

的停止标准上，基于PV-RCI密文传输的迭代次数略多。

图6进一步对比了两种匹配模式下，各个节点相互协商确定的功率信息，可以看出采用两种算法协商的节点功率基本一致。此外，图6也进一步比对了各个节点的真实功率与其功率上下限的差异，可以确定所有节点的真实功率均未超出其上下功率的限制。

4.2.2 PV-RCI密文匹配的可靠性验证

本文为了进一步验证PV-RCI密文匹配算法的可靠性，选取单个节点（如第3个节点）进行详细观察。本文在多轮协商迭代过程中，观测其迭代停止指标（$\Delta\lambda, \Delta\bar{\mu}, \Delta\underline{\mu}, \Delta P$）的震荡曲线，如图7（a）所示，可以看出，在经历上下震荡之后，随着多次迭代的进行，所有指标均逐渐趋向于0。图7（b）进一步展示了在共识迭代过程中该节点的功率变化曲线，虽然在开始的几轮，该节点的功率振幅较大，超出了其功率下限，但很快就回到了约束范围以内，逐渐趋于平衡，符合预设的功率范围[-750, 0]。

4.2.3 PV-RCI的可扩展性分析

本文进行分批实验，分别以5个、10个、20个及50个交易节点进行测试，并记录交易匹配过程中的迭代次数、迭代时间，以进行PV-RCI共识算法的可扩展性分析，如图8所示。

随着节点数量的增加，需要进行的迭代次数也会增加。这是因为更多的节点参与共识，意味着更多的点对点之间的信息交互，需要更多的迭代次数以达到共识平衡。

随着迭代次数的增加，迭代时间也呈线性增加。因为每次更新迭代，所有节点都需要对当前状态进行更新评估，进而调整自身的价格因子及功率信息，导致迭代

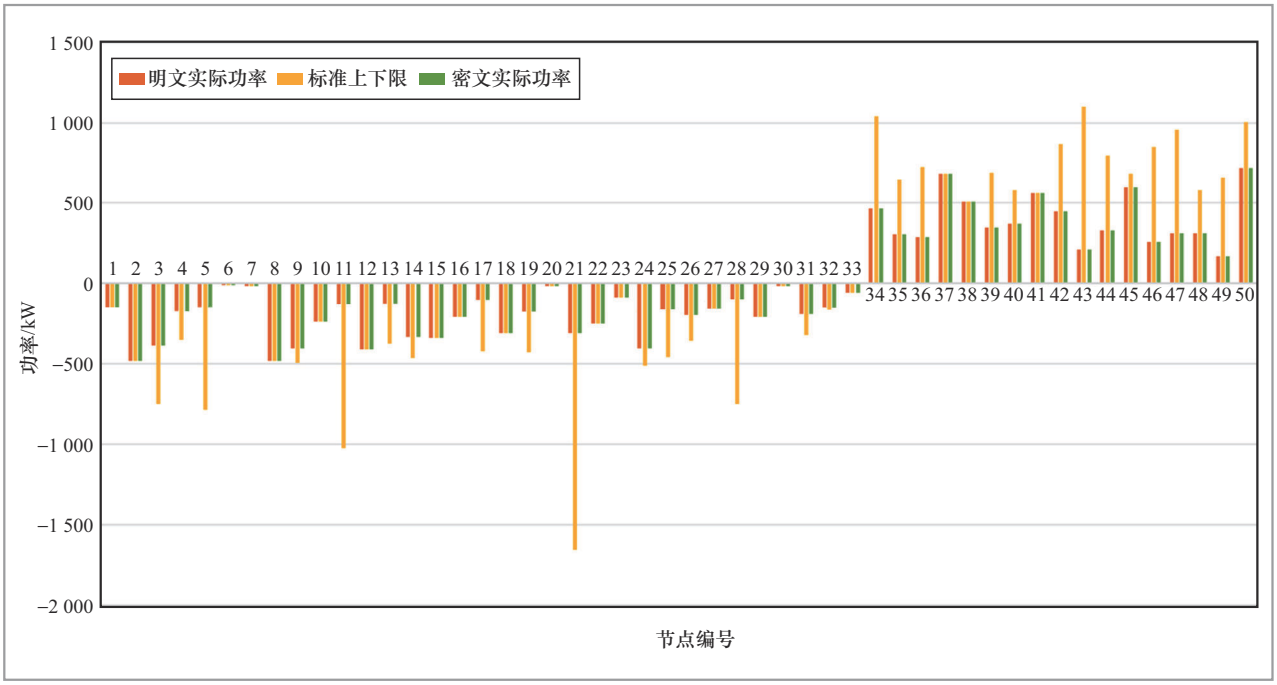


图6 各节点在明文RCI与密文PV-RCI方式下的功率对比

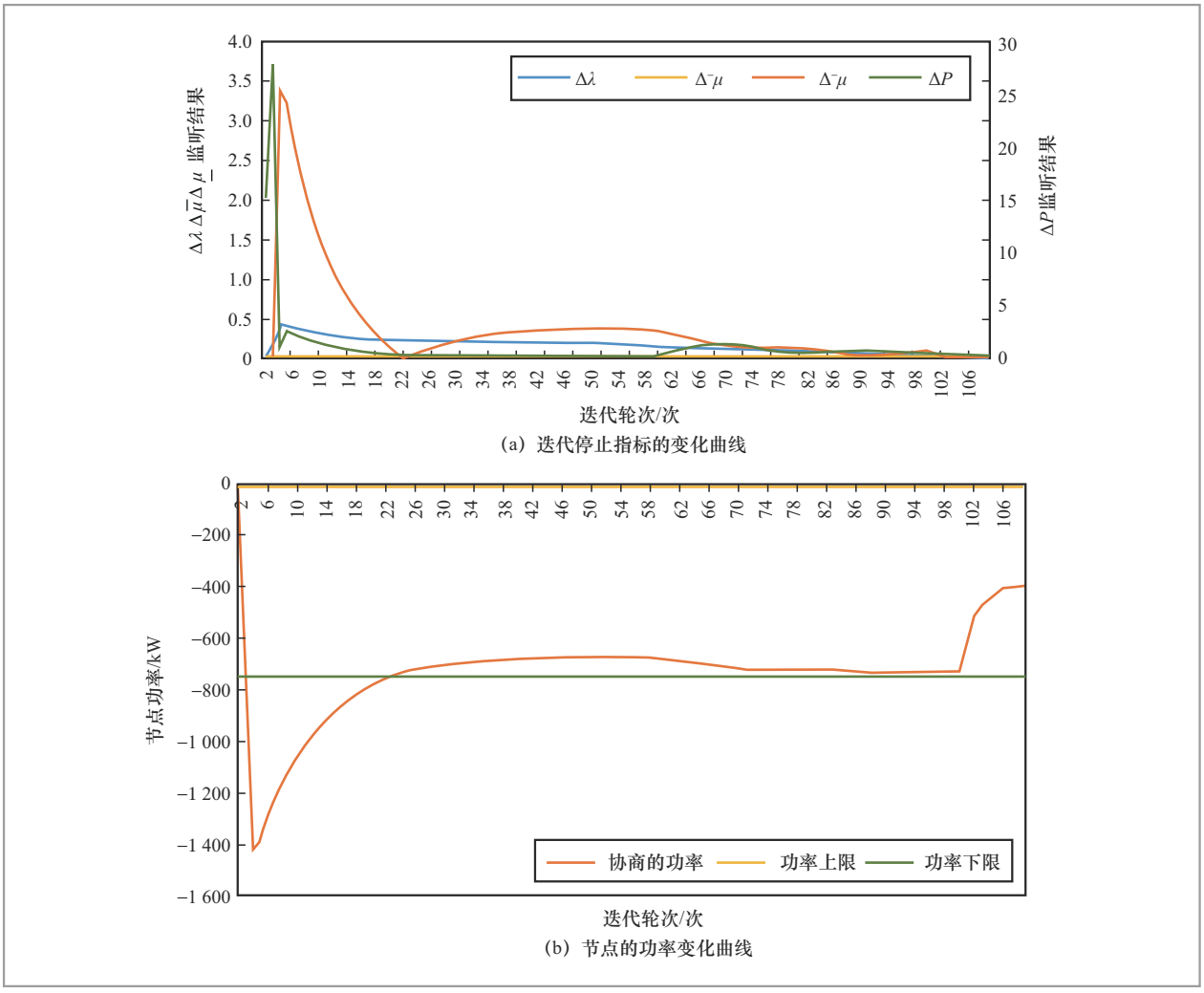


图7 匹配过程中单个节点的详细信息

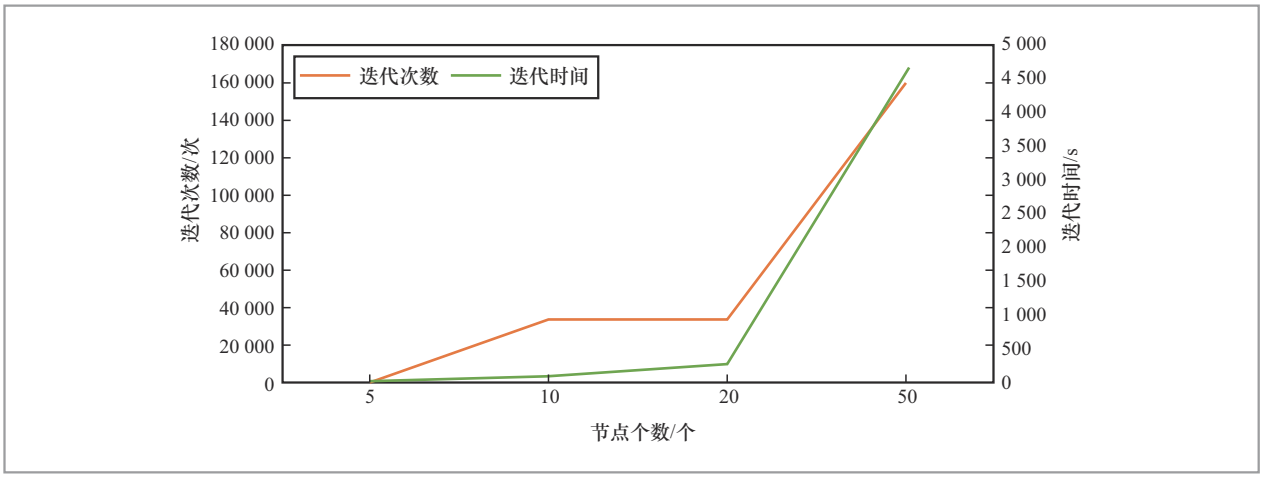


图8 PV-RCI算法的迭代次数与迭代时间分析

时间的延长。后文对迭代的时间进行精细化测试，分析可以优化的地方。

4.2.4 PV-RCI的性能分析

本文开展PV-RCI的4个相关因素的性能测试，以进一步分析PV-RCI匹配算法的耗时情况。

- 基于明文传输的去中心化交易匹配。
- 采用同态加密的去中心化交易匹配。
- 采用同态加密的交易匹配，并生成零知识证明。
- 采用同态加密的交易匹配，生成并验证零知识证明。

测试结果如图9所示，可以看出基于同态加密的迭代过程最耗时，而生成和验证零知识证明的时间都很小。图10进一步细化了基于同态加密的迭代过程，发现加密和解密操作最耗时。为提升同态加密的效率，后期可以采用基于SIMD的打包加密技术[22]进行加速。相比于文献[18]，本方案中零知识证明的生成和验证时间相对较短，因为只需要在共识结束之后生成零知识证明并验证，无须在每轮迭代过程中进行。生成零知识证明的时间大约为0.42 s，证明文件的大小为128 KB，第三方验证时间仅需3 ms。

4.2.5 第三方审计节点的安全性分析

每个节点在请求第三方解密价格因子时，叠加了自定义的随机数，因此第三方无法通过解密获得真实的价格因子。第三方节点无法获得也不会存储任何价格因子或功率明文，即使被攻击，攻击者也无法获得其他节点的敏感数据。在每轮迭代中，价格因子都会被节点产生的新的随机数混淆，即使攻击者从第三方获得某轮的解密数据，也无法推导出之前的信息，保障了历史数据的隐私安全。

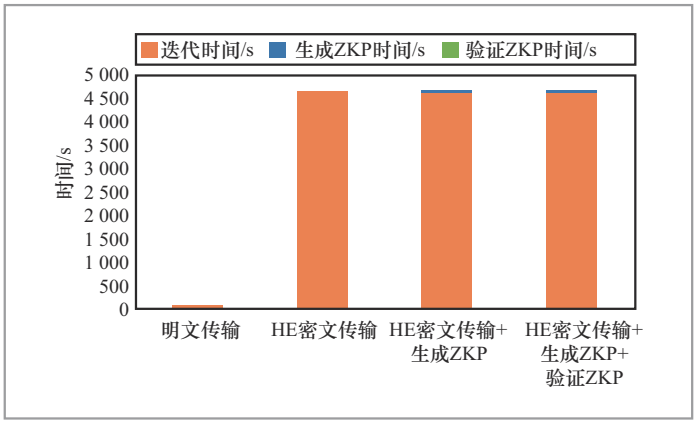


图9 各因素的耗时分析

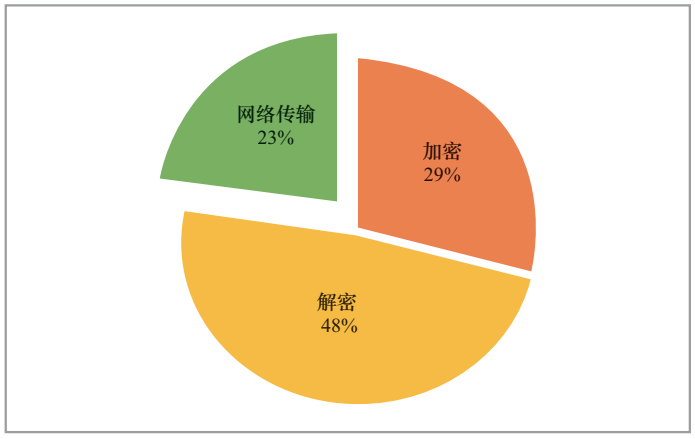


图10 同态加密的性能分析

5 结束语

针对电力能源领域，本文提出了一种兼顾隐私保护和结果可验证的点对点交易匹配机制PV-RCI，其确保了交易匹配过程中的数据隐私安全，同时也实现了交易匹配结果的可验证性。本文采用同态加密技术，实现了发电节点与用电节点间的安全通信，确保了交易数据的机密性。此外，

本文引入了零知识证明机制，用于构造交易匹配结果的证明文件，增强了交易的透明度。系统设计中引入了一个可信的第三方审计节点，该机构不仅作为信任代理，为其他参与方提供加解密服务，还担任监管角色，以确保交易匹配结果的正确性。考虑社会成本函数，本系统促进了能源市场对绿色清洁能源的生产和使用，有效降低了电力交易的社会总成本。PV-RCI交易匹配的共识机制不仅对能源领域日益增长的数据安全和隐私保护起到了推动作用，也可以对数据交易、金融证券等领域的交易匹配需求提供新的解决方案和启示。未来研究可以进一步强化交易匹配过程的验证机制，加强共识算法的可扩展性，并探索更高效的同态加密算法，以提升系统性能。

参考文献：

[1] 谢平，邹传伟，刘海二. 互联网金融的基础理论[J]. 金融研究，2015(8)：1-12.
XIE P，ZOU C W，LIU H E. The fundamental theory of Internet finance[J]. Journal of Financial Research，2015(8)：1-12.

[2] 王继业，孟坤，曹军威，等. 能源互联网信息技术研究综述[J]. 计算机研究与发展，2015，52(5)：1109-1126.
WANG J Y，MENG K，CAO J W，et al. Information technology for energy Internet：a survey[J]. Journal of Computer Research and Development，2015，52(5)：1109-1126.

[3] 王旭，倪宏，韩锐. 基于拍卖的数据中心资源匹配算法[J]. 计算机与现代化，2018(10)：114-121.
WANG X，NI H，HAN R. Auction-based resource match algorithm in data centers[J]. Computer and Modernization，2018(10)：114-121.

[4] 邓钇敏，司世景，王健宗，等. 去中心化金融的交易机制综述[J]. 大数据，2022，8(4)：67-84.
DENG Y M，SI S J，WANG J Z，et al. Exchange mechanism for decentralized finance：a survey[J]. Big Data Research，2022，8(4)：67-84.

[5] HUG G，KAR S，WU C Y. Consensus innovations approach for distributed multiagent coordination in a microgrid[J]. IEEE Transactions on Smart Grid，2015，6(4)：1893-1903.

[6] 曾慧，王美艳，李涛，等. 基于P2P的碳市场交易模型及电碳联合出清方法[J]. 电力需求侧管理，2024，26(3)：95-100.
ZENG H，WANG M Y，LI T，et al. P2P-based carbon market trading model and electri-city-carbon joint clearing method[J]. Elec-tric Power Demand Side Management，2024，26(3)：95-100.

[7] 祝烈煌，董慧，沈蒙. 区块链交易数据隐私保护机制[J]. 大数据，2018，4(1)：46-56.
ZHU L H，DONG H，SHEN M. Privacy protection mechanism for blockchain transaction data[J]. Big Data，2018，4(1)：46-56.

[8] SORIN E，BOBO L，PINSON P. Consensus-based approach to peer-to-peer electricity markets with product differentiation[J]. IEEE Transactions on Power Systems，2018，34(2)：994-1004.

[9] 金澈清，张召，潘斌. 区块链：面向新一代互联网的基础设施[J]. 新疆师范大学学报：哲学社会科学版，2020，41(5)：103-113.
JIN C Q，ZHANG Z，PAN B. Blockchain：Infrastructure for the new generation of the Internet[J]. Journal of Xinjiang Normal University：Philosophy and Social Sciences Edition，2020，41(5)：103-113.

[10] LI H，WANG Z，CHEN G，et al. Distributed robust algorithm for economic dispatch in smart grids over general unbalanced directed networks[J]. IEEE Transactions on Industrial Informatics，

2019, 16(7): 4322-4332.

[11] DUAN Y, HE X, ZHAO Y. Distributed algorithm based on consensus control strategy for dynamic economic dispatch problem[J]. International Journal of Electrical Power & Energy Systems, 2021, 129: 106833.

[12] YAN Y, CHEN Z, VARADHARAJAN V, et al. Distributed consensus-based economic dispatch in power grids using the paillier cryptosystem[J]. IEEE Transactions on Smart Grid, 2021, 12(4): 3493-3502.

[13] 王蓓蓓, 李雅超, 赵盛楠, 等. 基于区块链的分布式能源交易关键技术[J]. 电力系统自动化, 2019, 43(14): 53-64.
WANG B B, LI Y C, ZHAO S N, et al. Key technologies of distributed energy trading based on blockchain[J]. Automation of Electric Power Systems, 2019, 43(14): 53-64.

[14] 冯昌森, 谢方锐, 文福拴, 等. 基于智能合约的绿证和碳联合交易市场的设计与实现[J]. 电力系统自动化, 2021, 45(23): 1-11.
FENG C S, XIE F R, WEN F S, et al. Design and implementation of a green certificate and carbon joint trading market based on smart contracts[J]. Automation of Electric Power Systems, 2021, 45(23): 1-11.

[15] CHU T, AN X, ZHANG W, et al. Multiple virtual power plants transaction matching strategy based on alliance blockchain[J]. Sustainability, 2023, 15(8): 6939.

[16] ZHOU X, WANG B, GUO Q, et al. Bidirectional privacy-preserving network-constrained peer-to-peer energy trading based on secure multiparty computation and blockchain[J]. IEEE Transactions on Power Systems, 2023, 39(1): 602-613.

[17] 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 L, HUANG C, YANG X, et al. Research on distributed energy trading patterns considering privacy protection and decentralization[J]. Power System Protection and Control, 2024, 52(2): 143-154.

[18] LI Z, XU H, ZHAI F, et al. A privacy-preserving, two-party, secure computation mechanism for consensus-based peer-to-peer energy trading in the smart grid[J]. Sensors, 2022, 22(22): 9020.

[19] SINHA A, SOUN T, DEB K. Using karush-kuhn-tucker proximity measure for solving bilevel optimization problems[J]. Swarm and Evolutionary Computation, 2019, 44: 496-510.

[20] 杨亚涛, 赵阳, 张卷美, 等. 同态密码理论与应用进展[J]. 电子与信息学报, 2021, 43(2): 475-487.
YANG Y T, ZHAO Y, ZHANG J M, et al. Advances in homomorphic cryptography theory and applications[J]. Journal of Electronics and Information Technology, 2021, 43(2): 475-487.

[21] 李威翰, 张宗洋, 周子博, 等. 简洁非交互零知识证明综述[J]. 密码学报, 2022, 9(3): 379-447.
LI W H, ZHANG Z Y, ZHOU Z B, et al. Survey on succinct non-interactive zero-knowledge proofs[J]. Journal of Cryptography, 2022, 9(3): 379-447.

[22] HUANG Z, LU W, HONG C, et al. Cheetah: lean and fast secure two-party deep neural network inference[C]//Proceedings of the 31st USENIX Security Symposium (USENIX Security 22). Boston: USENIX, 2022: 809-826.

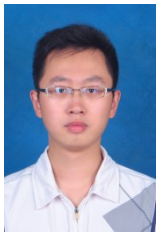
作者简介

皮冰锋（1982– ），女，华东师范大学数据科学与工程学院博士生，天聚地和（苏州）科技股份有限公司数字创新主管，主要研究方向为大数据、区块链、隐私计算等。

金澈清（1977– ），男，博士，华东师范大学数据科学与工程学院教授，主要研究方向为区块链、数据流管理等。

钱卫宁（1976– ），男，博士，华东师范大学数据科学与工程学院教授、博士生导师，主要研究方向为大数据管理、可扩展事务处理等。

华松（1987– ），男，天聚地和（苏州）科技股份有限公司高级研发工程师，主要研究方向为区块链、分布式计算等。



张沈斌（1984– ），男，天聚地和（苏州）科技股份有限公司高级研发工程师，主要研究方向为区块链、隐私计算等。

收稿日期: 2024-08-19

通信作者: 皮冰锋,19688624@qq.com