文章编号：2096-5125 (2023) 04-0362-08 中图分类号：TM61；TM722 文献标志码：A
DOI：10.19705/j.cnki.issn2096-5125.2023.04.004

基于 Paillier 加密和共识机制的分解协调式算法

周鑫[1]，贺欢[2]，王彬[1*]，祝湘博[2]，孙宏斌[1]
（1. 清华大学电机工程与应用电子技术系，北京市 海淀区 100084；
2. 国网辽宁省电力有限公司鞍山供电公司，辽宁省 鞍山市 114001）

Coordination-decomposition Algorithm Based on Paillier Encryption and Consensus Mechanism

ZHOU Xin[1], HE Huan[2], WANG Bin[1*], ZHU Xiangbo[2], SUN Hongbin[1]
(1. Department of Electrical Engineering, Tsinghua University, Haidian District, Beijing 100084, China;
2. State Grid Anshan Electric Power Company, Anshan 114001, Liaoning Province, China)

Abstract: With the increasing decentralization level of energy systems, coordination-decomposition algorithms start to be broadly applied to solving optimization problems in energy sector. However, coordination-decomposition algorithms require sub-problems to submit coordination variables to the coordination layer, leading to privacy leak risks. Furthermore, there is a trust issue related to the coordination layer. To deal with these problems, Paillier encryption and consensus mechanism are applied to improving the coordination-decomposition algorithm. In each iteration of the coordination-decomposition algorithm, every generator's power output is encrypted into ciphertext that is broadcasted to other generators. One generator selected as the leading node is responsible for computing the total power of all generators using ciphertexts, generating a block consisting of all ciphertexts and computed total power, and broadcasting the block to all generators. All generators will verify the correctness of the block content. Once the block content is verified to be correct, all generators add the block to the ledger and finish current iteration of the coordination-decomposition algorithm. The case analysis results prove that Paillier encryption is able to protect the privacy of all generators in the coordination-decomposition algorithm, and the proposed consensus mechanism is able to prevent the leading node from maliciously tampering with block content, hence establishing trust among generators.

Keywords: energy blockchain; consensus mechanism; Paillier encryption; coordination-decomposition algorithm

摘 要：随着能源系统的去中心化程度不断加深，分解协调式算法开始广泛应用于求解能源领域的优化问题。但是，分解协调式算法需要子优化问题向协调层算法上传协调变量，存在隐私泄露的风险，并且协调层自身还存在着信任问题。为了解决这些问题，引入Paillier加密和区块链共识机制，对分解协调式算法进行改进。在分解协调式算法的每次迭代中，各个发电商的出力通过Paillier加密后以密文的形式广播给其他发电商，某个发电商作为领导节点负责根据密文计算出所有发电商的总出力，并将所有密文和总出力打包生成区块后广播给所有发电商。所有发电商都会对区块内容的正确性进行检查，检查通过后将区块加入到账本中，完成分解协调式算法的本次迭代。算例结果证明了该算法中Paillier加密能够保护各个发电商的隐私，共识机制能够防止领导节点恶意篡改区块内容，在发电商间构建信任。

关键词：能源区块链；共识机制；Paillier加密；分解协调式算法

0 引言

能源系统的规划、调度、交易等领域中通常需要求解优化问题。传统方法采用集中式的优化算法，由中心化机构搜集所有数据并进行求解。但是，随着大量分布式资源的接入，能源系统的去中心化程度正在加深，传统的集中式优化算法难以适应去中心化的能源系统架构。

分解协调式算法是一种分布式优化算法，天然具备去中心化的特点。在分解协调式算法中，原始的优化问题会被分解成多个子优化问题，由协调层负责协调各个子优化问题的解，通过反复迭代求出最优解[1]。目前，分解协调式算法已经在状态估计、模型预测控

基金项目：国家电网有限公司科技项目（5700-202272179A-1-1-ZN）。
Science and Technology Foundation of SGCC (5700-202272179A-1-1-ZN).

制、多能系统联合调度、无功优化等领域中得到了广泛应用[2-5]。但是，分解协调式算法往往需要各个子优化问题向协调层上传协调变量，这些协调变量可能会涉及隐私问题。此外，分解协调式算法还依赖于协调层的可信度，如果协调层执行协调任务时恶意修改数据，将导致分解协调式算法无法得到最优解，甚至无法收敛[6]。因此，有必要寻求新的方法来解决分解协调式算法的隐私与信任问题。

在隐私方面，常用的方法是对数据进行加密以保护隐私，例如信息伪装[7]、同态加密[8]、安全多方计算[9]等。文献[10]针对混合整数二次规划问题，设计了一种基于信息伪装的云端求解算法，对各个分布式资源的隐私数据进行了线性变换，使得云端只能接收到变换后的数据，能够防止隐私被泄露。文献[11]设计了一种能够容许错误的信息伪装方法，可用于隐私数据聚合中。文献[12]采用同态加密技术，利用Paillier加密的密文进行完全隐私保护的电–气协同优化。文献[13]依托安全多方计算技术，设计了一种安全的智能电表数据聚合方法。在这些文献中，使用加密技术保护隐私的效果已经得到了充分验证。

在信任方面，区块链这种分布式账本技术受到广泛关注[14]。区块链共识机制能够在互不信任的节点间保证账本的一致性。文献[15-16]针对能源领域特点对已有共识机制进行了改进，提出了信用证明共识机制和凸优化证明共识机制。文献[17]将共识机制与分布式优化算法结合起来，保证分布式优化结果的可靠性。文献[18]针对基于交替方向乘子法的最优潮流问题提出了PoOPF（proof of optimal power flow）共识机制，使得网络节点能够对最优潮流问题解的有效性达成一致。文献[19]面向能源系统中的优化问题，利用优化问题难以求解但容易验证的特点设计了PoSo（proof of solution）共识机制。通过引入区块链共识机制，分布式优化算法的信任问题将得以解决。

已有文献大多关注于解决隐私保护问题或使用区块链共识机制构建信任问题，但如何同时解决分解协调式算法中的隐私与信任问题尚未得到充分研究。本文以多个发电商的经济调度模型为例，分析分解协调式算法的隐私与信任问题，并基于已有研究，设计了基于Paillier加密和共识机制的分解协调式算法，既能利用Paillier加密保护各个发电商的隐私，又能通过共识机制在各个发电商之间建立信任，确保协调层计算结果可信。

1 分解协调式算法的隐私与信任问题

1.1 典型分解协调式算法

本文考虑单时间段经济调度模型，以所有发电商的总成本最小为优化目标，并忽略网损、不确定性等约束，如式（1）所示。

$$\begin{cases}\min\limits_{P_i}\sum\limits_{i=1}^{N}C_i(P_i)\\ \text{s.t.}\quad \sum\limits_{i=1}^{N}P_i=D\\ P_{i,\min}\leqslant P_i\leqslant P_{i,\max},i\in\{1,2,\cdots,N\}\end{cases}\tag{1}$$

式中：N为发电商的总个数；P_i为发电商i的出力；$P_{i,\max}$、$P_{i,\min}$为发电商i的出力上下限；D为总负荷；C_i为发电商i的成本函数，满足：

$$C_i(P_i)=a_iP_i^2+b_iP_i\tag{2}$$

式中：a_i、b_i为发电商i的成本函数的二次项和一次项系数。

该经济调度模型可以采用分解协调式算法进行分布式求解。例如，使用原对偶梯度法进行求解的流程如下。

1）初始化$k=0,\lambda^{(k)}=0$。其中，上标k代表第k次迭代；λ代表出清价格。

2）发电商i求解优化问题式（3）得到出力$P_i^{(k+1)}$，并将其上传给协调层。

$$\begin{cases}P_i^{(k+1)}=\arg\min\limits_{P_i}C_i(P_i)-\lambda^{(k)}P_i\\ \text{s.t.}\quad P_{i,\min}\leqslant P_i\leqslant P_{i,\max}\end{cases}\tag{3}$$

3）协调层按式（4）更新出清价格$\lambda^{(k+1)}$，并发送给所有发电商。

$$\lambda^{(k+1)}=\lambda^{(k)}-\alpha\left(\sum_{i=1}^{N}P_i^{(k+1)}-D\right)\tag{4}$$

式中：α为步长参数。

4）如果$|\lambda^{(k+1)}-\lambda^{(k)}|<\epsilon$，其中$\epsilon$为收敛阈值，则停止迭代；否则，令$k\leftarrow k+1$，重新执行步骤2）。

1.2 隐私与信任问题分析

在上述求解算法中，步骤2）要求各个发电商向协调层上传每次迭代后的出力$P_i^{(k+1)}$。这说明，协调层将掌握不同出清价格$\lambda^{(k)}$下各个发电商的出力。根据式（3）可以给出$P_i^{(k+1)}$与$\lambda^{(k)}$之间的关系：

$$P_i^{(k+1)}=\begin{cases}P_{i,\min}, & P_{i,\min}\geqslant\dfrac{\lambda^{(k)}-b_i}{2a_i}\\ \dfrac{\lambda^{(k)}-b_i}{2a_i}, & P_{i,\min}<\dfrac{\lambda^{(k)}-b_i}{2a_i}<P_{i,\max}\\ P_{i,\max}, & P_{i,\max}\leqslant\dfrac{\lambda^{(k)}-b_i}{2a_i}\end{cases}\tag{5}$$

在分解协调式算法的迭代过程中，协调层会得到发电商i的出力序列$\left\{P_i^{(k+1)}\right\}_{1\leqslant k\leqslant K-1}$与出清价格序列$\left\{\lambda^{(k)}\right\}_{1\leqslant k\leqslant K-1}$，其中$K$为迭代次数。协调层可以将这$K-1$组出力和出清价格代入到式（5）中，通过拟合求出发电商i的成本参数a_i、b_i，从而导致发电商i的隐私被泄露给协调层。值得注意的是，虽然发电商i最后一次迭代得到的最优出力$P_i^{(K+1)}$在一些业务场景下（如自动发电控制）并不会被视为隐私，但是分解协调式算法会给出发电商i的出力序列$\left\{P_i^{(k+1)}\right\}_{1\leqslant k\leqslant K-1}$，而协调层可以通过拟合出力序列$\left\{P_i^{(k+1)}\right\}_{1\leqslant k\leqslant K-1}$得到发电商$i$的隐私成本参数。从隐私保护的角度来看，应当尽量避免发电商将出力$P_i^{(k+1)}$暴露给协调层。

除了隐私问题之外，上述算法的步骤3）还存在着信任问题。出清价格的更新是由协调层按式（4）执行的，如果协调层恶意发送抬高或者压低后的出清价格，各个发电商将无法分辨。因此，各个发电商需要信任协调层严格按照式（4）更新出清价格。在一些场景下，例如小区内的分布式能源交易场景，难以找到具备权威性的协调层让所有发电商都信任。

2 基于Paillier加密的发电商隐私保护算法

在第1.1节的分解协调式算法中，协调层需要收集$P_i^{(k+1)}$来计算$\sum_{i=1}^{N}P_i^{(k+1)}$进而更新出清价格，这会导致各个发电商的隐私泄露给协调层。为了解决隐私问题，本文采用Paillier加密的方法，在不暴露$P_i^{(k+1)}$真实值的前提下，计算得到$\sum_{i=1}^{N}P_i^{(k+1)}$。

2.1 Paillier加密方法

Paillier加密是一种加法同态加密算法，由Paillier在文献[20]中提出。在Paillier加密中，需要生成2个质数p、q，满足条件：

$$\gcd(pq,(p-1)(q-1))=1\tag{6}$$

式中：gcd代表最大公约数。

令$n=pq,\lambda=\mathrm{lcm}(p-1,q-1)$，其中lcm代表最小公倍数。随机选取$g\in\mathbf{Z}_{n^2}^*$，并计算：

$$\mu=\left[L(g^{\lambda}\bmod(n^2))\right]^{-1}\tag{7}$$

式中：

$$L(x)=\frac{x-1}{n}\tag{8}$$

Paillier加密使用公钥(n,g)进行加密，其加密流程如下。

1）选取随机数$r\in\mathbf{Z}_n^*$，满足$0\leqslant r<n$。

2）对明文m进行加密：

$$E(m)=g^m r^n\bmod(n^2)\tag{9}$$

解密则需要使用私钥(λ,μ)。对于密文c，解密得到的明文为

$$D(c)=L(c^{\lambda}\bmod(n^2))\cdot\mu\bmod(n)\tag{10}$$

Paillier加密具有加法同态的特点，满足：

$$E(m_1+m_2\bmod(n))=E(m_1)\cdot E(m_2)\bmod(n^2)\tag{11}$$

即m_1+m_2的密文可以根据m_1、m_2的密文相乘得到。这一点能够用于进行保护隐私的数据求和。

2.2 发电商隐私保护算法

文献[21]使用Paillier加密的方法，在防止各个智能电表数据泄露的情况下，对所有智能电表的数据进行聚合。本文采用类似的方法，利用Paillier加密来计算$\sum_{i=1}^{N}P_i^{(k+1)}$，流程如下。

1）所有发电商和协调层通过协商，共享同一套Paillier加密的公钥(n,g)、私钥(λ,μ)和加密时使用的随机数r。

2）每个发电商生成$N-1$个随机数，并发送给其他发电商。具体来说，发电商i生成随机数s_{ij}，并将s_{ij}发送给发电商$j(j\neq i)$。

3）发电商i根据收到的随机数，按式（12）对出力$P_i^{(k+1)}$进行加密得到密文$\tilde{P}_i^{(k+1)}$，并将$\tilde{P}_i^{(k+1)}$发送给协调层。

$$\tilde{P}_i^{(k+1)}=g^{P_i^{(k+1)}}r^{S_i}\bmod(n^2)\tag{12}$$

式中：

$$S_i=n+\sum_{j=1,j\neq i}^{N}(s_{ij}-s_{ji})\tag{13}$$

4）协调层计算所有密文的乘积：

$$\prod_{i=1}^{N}\tilde{P}_i^{(k+1)}=g^{\sum_{i=1}^{N}P_i^{(k+1)}}r^{Nn}\bmod(n^2)\tag{14}$$

然后按式（10）进行解密得到$\sum_{i=1}^{N}P_i^{(k+1)}$。

在上述流程中，各个发电商仅仅向协调层提供了加密后的出力$\tilde{P}_i^{(k+1)}$。注意式（12）中的加密方法并非标准的Paillier加密，尽管协调层掌握Paillier加密的私

钥，但由于 S_i 的随机性，协调层是无法从密文 $\tilde{P}_i^{(k+1)}$ 反推出明文 $P_i^{(k+1)}$ 的，从而保护了各个发电商的隐私。

3　适应分解协调式算法的能源区块链共识机制

3.1　基本思路

第2章采用Paillier加密解决了分解协调式算法的隐私问题，但是协调层的信任问题尚未解决。区块链作为一种分布式账本技术，具备公开透明、不可篡改等优点，能够在互不信任的主体间构建信任。如果结合Paillier加密，设计一种能源区块链共识机制，就能在保护各个发电商隐私的同时解决信任问题。

文献[18]提出了PoOPF共识机制，与能源系统的分布式优化算法紧密相关，每当分布式优化算法执行完一次迭代后，就生成一个区块，区块中包含各个子优化问题当次迭代的最优解。相比于传统的PoW（proof of work）共识机制，PoOPF并不需要消耗大量的能源去求解复杂的哈希问题，而是要求各个节点执行分布式优化算法，能够很好的适应能源领域的需求。但是，PoOPF共识机制中的区块记录了各个子问题的最优解，对应到本文的模型中，即区块中包含各个发电商的出力 $P_i^{(k+1)}$，这会导致发电商的隐私泄露。

本文尝试对PoOPF共识机制进行改进，区块中不再包含发电商出力的明文 $P_i^{(k+1)}$，而是出力的密文 $\tilde{P}_i^{(k+1)}$，这样将保护各个发电商的隐私。此外，在第2.2节的隐私保护方法中，所有发电商都掌握着解密的私钥，因此，只要所有发电商都公开自身的密文 $\tilde{P}_i^{(k+1)}$，那么任意一个发电商都能独立解密得到 $\sum_{i=1}^{N} P_i^{(k+1)}$。这样，在共识机制中就不再需要协调层进行解密，各个发电商均能进行解密操作，通过共识机制保证解密结果的一致性。

3.2　共识机制设计

本文设计的共识机制整体架构如图1所示，所有发电商都会作为节点参与到共识机制中。分解协调式算法的每次迭代都会从各个发电商中选取1个领导节点。各个发电商将当次迭代的出力的密文 $\tilde{P}_i^{(k+1)}$ 广播给其他发电商，当领导节点收集到所有发电商的密文后，就可以解密得到总出力 $\sum_{i=1}^{N} P_i^{(k+1)}$。领导节点将所有密文以及解密后的总出力打包为1个区块，广播给其他发电商。其他发电商会验证区块所含内容的正确性，当区块通过验证后，各个发电商将区块加入到区块链账本中，并进入分解协调式算法的下一次迭代。

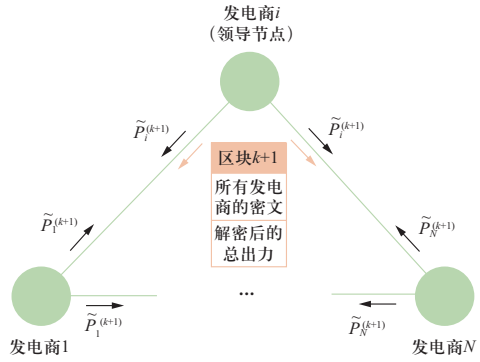

图 1　共识机制整体架构

Fig. 1　Overall architecture of the consensus mechanism

图2展示了共识机制的详细流程，包括初始化、密文广播、区块生成、区块验证、账本更新等步骤。

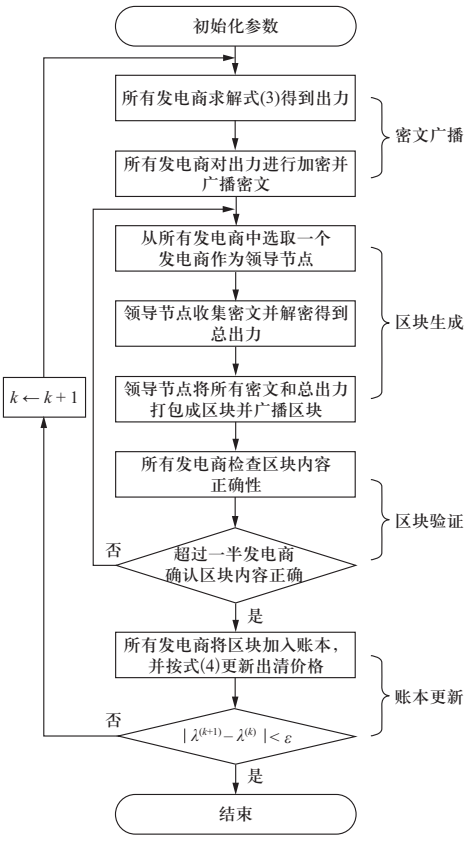

图 2　共识机制流程图

Fig. 2　Flowchart of consensus mechanism

3.2.1　初始化

初始化时所有发电商需要通过协商生成1个初始区块，该初始区块包括所有发电商的数字身份，以及

分解协调算法和Paillier加密的相关参数，例如步长参数α、公钥(n,g)、私钥(λ,μ)和加密时使用的随机数r。

3.2.2 密文广播

初始化完成后，各个发电商开始进入分解协调式算法的迭代中。在第k次迭代时，各个发电商先求解式（3）得到出力$P_i^{(k+1)}$，然后执行第2.2节中的步骤2）和3），得到加密后的出力$\tilde{P}_i^{(k+1)}$，并将密文$\tilde{P}_i^{(k+1)}$广播给其他发电商。

3.2.3 区块生成

每次迭代时，都会按照一定的规则从所有发电商中选取1个发电商作为领导节点。这个规则可以是各个发电商轮流成为领导节点，也可以是信用值最高的发电商成为领导节点。

领导节点需要收集各个发电商广播的密文$\tilde{P}_i^{(k+1)}$，并在收集到所有密文后，执行第2.2节中的步骤4）得到解密后的总出力$\sum_{i=1}^{N}P_i^{(k+1)}$。然后，领导节点生成第$k+1$个区块，该区块中包括所有发电商的密文$\left\{\tilde{P}_i^{(k+1)}\right\}_{1\leqslant i\leqslant N}$以及解密后的总出力$\sum_{i=1}^{N}P_i^{(k+1)}$。最后，领导节点将第$k+1$个区块广播给其他发电商。

3.2.4 区块验证

各个发电商收到领导节点广播的第$k+1$个区块后，需要检查区块内容的正确性，防止领导节点恶意篡改区块信息。每个发电商需要检查的内容如下。

1）第$k+1$个区块中包含所有发电商的出力的密文$\tilde{P}_i^{(k+1)}$。每个发电商都会收集到其他发电商广播的密文，如果自身收集的密文与区块中的密文不一致，则说明领导节点恶意篡改了某个发电商的密文。

2）验证第$k+1$个区块中的解密后的总出力$\sum_{i=1}^{N}P_i^{(k+1)}$是正确的。具体方法是验证式（14）是否成立，如果不成立，则说明领导节点恶意篡改了总出力值。

当超过一半的发电商认为区块内容错误时，当前领导节点的信用值降低。此时，需要从剩下的发电商中重新选取1个领导节点，再次执行区块生成和区块验证的步骤。

3.2.5 账本更新

如果超过一半的发电商认为第$k+1$个区块的内容是正确的，各个发电商将第$k+1$个区块加入到本地的账本中，并按照式（4）更新出清价格，然后根据$|\lambda^{(k+1)}-\lambda^{(k)}|<\epsilon$是否得到满足，判断终止迭代或进入下一次迭代。

4 算例分析

4.1 算例参数

本文采用IEEE 30节点网络进行算例分析，该网络中的负荷总功率为$D=283.4$ MW，6个发电商的参数如表1所示。步长参数$\alpha=0.01$美元/MW，收敛阈值$\epsilon=0.001$美元。

表 1 发电商参数

Table 1 Parameters of generators

发电商编号i	a_i /（美元·MW^{-2}）	b_i /（美元·MW^{-1}）	$P_{i,\min}$ /MW	$P_{i,\max}$ /MW
1	0.038	20	0	360.2
2	0.25	20	0	140
3	0.01	40	0	100
4	0.01	40	0	100
5	0.01	40	0	100
6	0.01	40	0	100

4.2 算例结果

使用Paillier加密求解经济调度模型的结果如表2所示。各个发电商出力的明文值与密文值之间相差非常大，从出力的密文值难以反推出出力的明文值，所以Paillier加密能够有效保护各个发电商的隐私。另外，与集中优化结果相比，利用Paillier加密计算得到的明文值的误差均很小，说明基于Paillier加密的方法能够准确求出最优调度结果。

表 2 Paillier加密计算结果

Table 2 Computation results of Paillier encryption

计算结果	明文值	密文值	明文值与集中优化结果之间的误差
发电商1出力/MW	245.55	4.84×10^{1848}	0.008 6
发电商2出力/MW	37.75	3.60×10^{1848}	0.001 3
发电商3出力/MW	0	6.10×10^{1848}	0
发电商4出力/MW	0	4.30×10^{1848}	0
发电商5出力/MW	0	2.94×10^{1848}	0
发电商6出力/MW	0.01	3.89×10^{1848}	0
出清价格/（美元·MW^{-1}）	38.87		0.006 6

图3以发电商1为例，展示了Paillier加密算法的收敛过程。随着迭代次数增加，发电商1的出力明文值

稳定收敛到了最优出力，但是发电商1的出力密文值却在随机振动，且振动方向与明文值的收敛趋势之间没有相关性。这同样表明，Paillier加密算法能够在保护发电商隐私的同时，得出最优的调度结果。

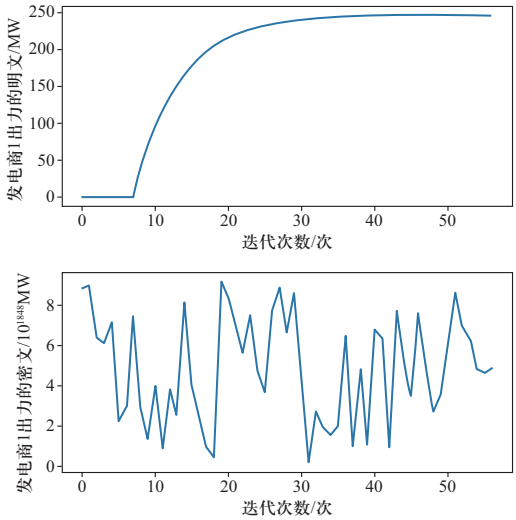

图 3　发电商1每次迭代的出力明文值与密文值

Fig. 3　Plaintexts and ciphertexts of generator 1's output power in each iteration

表3比较了Paillier加密算法、集中优化算法和分解协调式算法的性能。在迭代次数方面，Paillier加密算法与分解协调式算法完全相同，因为Paillier加密算法实际上是将分解协调式算法的协调层算法通过加密的方式进行计算，并不会改变分解协调式算法的迭代次数。在总计算时间方面，集中优化算法和分解协调式算法花费的时间均较少，而Paillier加密算法的总计算时间明显更多。这是因为Paillier加密算法每次迭代都涉及发电商出力的加密和解密操作，导致总计算时间增加。也就是说，Paillier加密算法以增加总计算时间为代价保护了所有发电商的隐私。在通信量方面，分解协调式算法只需要各个发电商与协调层通信，其通信量比较低，而Paillier加密算法还需要所有发电商两两之间发送随机数进行加密，这会增加Paillier加密算法的通信量。

表 3　与其他算法的性能比较

Table 3　Performance comparison with other algorithms

性能指标	Paillier加密算法	集中优化算法	分解协调式算法
迭代次数/次	56		56
总计算时间/s	14.54	0.027	0.11
通信量	中等		低

4.3　共识机制分析

本文提出的共识机制在每次执行分解协调式算法的迭代时都会生成1个区块，各个区块的生成时间如图4所示。每个区块的生成时间为0.22~0.32 s，能够满足实际应用的需求。由于本文采用的经济调度模型比较简单，每次迭代中各个发电商求解子优化问题耗时较少，区块生成时间主要由Paillier加密和解密的耗时决定。如果将本文提出的共识机制应用于更复杂的优化算法，子优化问题的求解时间将会增加，从而导致区块生成时间增加。

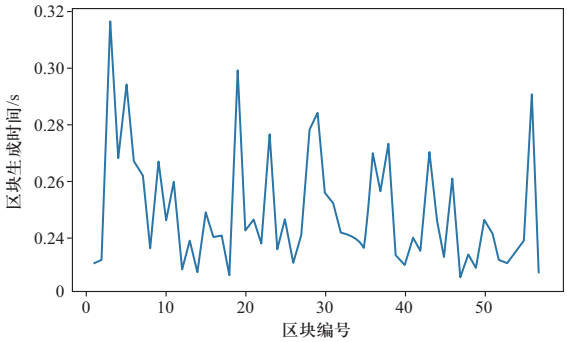

图 4　迭代过程中各个区块的生成时间

Fig. 4　Block generation time in each iteration

图5以第10个区块为例，展示了区块中包含的内容。6个发电商在当次迭代的出力密文以及领导节点解密得到的总出力都包含在了区块中。当区块10被加入到账本中后，表明所有发电商对该区块中记录的出力值达成了一致，分解协调式算法当次迭代的结果作为存证记录到了区块链中。

区块10
区块9哈希值
当前区块哈希值
发电商1出力密文：9.28×10^{1848}
发电商2出力密文：8.91×10^{1848}
发电商3出力密文：6.47×10^{1848}
发电商4出力密文：1.99×10^{1848}
发电商5出力密文：4.91×10^{1848}
发电商6出力密文：3.28×10^{1848}
解密后的总出力：107.66

图 5　区块10内容展示

Fig. 5　Illustration of block 10's content

图6展示了本文提出的共识机制如何防止领导节点在打包区块时篡改区块内容。假设领导节点篡改了区块10中的发电商2出力密文以及解密后的总出力，

当其他发电商收到此区块后，一方面会发现区块10中的发电商2出力密文与发电商2广播给自己的出力密文不一致，另一方面会发现式（14）并不成立，所以领导节点对区块10的篡改将会被各个发电商检测出来。这种检查机制将促使所有发电商在担任领导节点时尽可能诚实地执行打包操作，在互不信任的发电商之间建立起了信任。

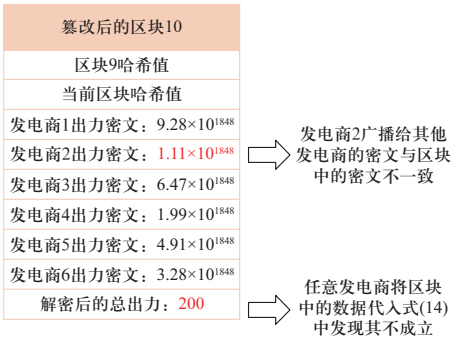

图 6 区块正确性检查

Fig. 6 Correctness check of blocks

表4将本文提出的共识机制与PoW和PoOPF共识机制进行了比较。

1）耗能量：PoW共识机制需要求解复杂的哈希问题，消耗大量能源，而PoOPF和本文提出的共识机制则只需要求解对应的优化问题，耗能量较低。

2）区块生成间隔：PoW共识机制生成新的区块需要求解哈希问题，花费时间较长；PoOPF共识机制生成新的区块需要等待所有子优化问题求解完毕，花费时间较短；本文提出的共识机制不但需要等待所有发电商求解子优化问题，还涉及发电商出力的加密和解密，其区块生成间隔要比PoOPF共识机制长一些。

3）区块大小：PoW共识机制中区块包含的交易数目并不是固定的；PoOPF共识机制中区块包含每个子优化问题的解，其大小与子优化问题个数有关；本文提出的共识机制包含各个发电商出力的密文值，区块大小与发电商个数有关。

4）区块内容：PoW和PoOPF共识机制中区块包含的内容都是明文记录的，所有区块链节点都可以接触到，而本文提出的共识机制中区块只包含加密后的发电商出力，不会导致各个发电商隐私被泄露。

5）通用程度：PoW共识机制是一种通用的共识机制，能够适用于所有场景；PoOPF共识机制是针对能源领域中的分布式优化算法设计的；本文提出的共识机制则进一步限定了分布式优化算法的范围，即该分布式优化算法是一种分解协调式算法，且协调层的算法必须属于Paillier加密支持的计算类型。

表 4 与其他共识机制的比较

Table 4 Comparison with other consensus mechanisms

指标	PoW	PoOPF	本文提出的共识机制
耗能量	高	低	低
区块生成间隔	长	短	中
区块大小	随机	由子优化问题个数决定	由发电商个数决定
区块内容	明文	明文	密文
通用程度	可应用于所有场景	专门为分布式优化算法设计	专门为协调层采用Paillier加密的分解协调式算法设计

5 结论

本文分析了分解协调式算法的隐私与信任问题，提出了基于Paillier加密和共识机制的分解协调式算法，能够同时解决其隐私与信任问题。在分解协调式算法的每次迭代中，各个发电商的出力通过Paillier加密变为密文，某个发电商作为领导节点根据密文计算得到总出力，并生成区块。生成区块内容的正确性将会被其他发电商检查，防止领导节点恶意篡改区块内容。IEEE 30节点算例表明本文提出的方法能够保护发电商的隐私数据不被泄露，并且能够检测出领导节点的恶意篡改行为，解决了信任问题。但是本文采用的经济调度模型比较简单，协调层只需要计算所有发电商的总出力。在处理更加复杂的模型时，协调层的计算任务将更为复杂，Paillier加密不一定能够保证通过密文计算出协调结果，需要研究安全多方计算等更加通用的方法。

参考文献

[1] BOYD S, PARIKH N, CHU E, et al. Distributed optimization and statistical learning via the alternating direction method of multipliers[J]. Foundations and Trends® in Machine Learning, 2011, 3(1): 1-122.

[2] 张佳楠，袁启海，余建明，等. 基于联络线扩展区域分解协调的分布式并行状态估计[J]. 电力系统自动化，2019，43(4)：166-173.
ZHANG Jianan, YUAN Qihai, YU Jianming, et al. Distributed parallel state estimation based on decomposition and coordination of tie-line extended area[J]. Automation of

Electric Power Systems, 2019, 43(4): 166-173 (in Chinese).
[3] 叶林，路朋，赵永宁，等. 含风电电力系统有功功率模型预测控制方法综述[J]. 中国电机工程学报，2021，41(18)：6181-6197.
YE Lin, LU Peng, ZHAO Yongning, et al. Review of model predictive control for power system with large-scale wind power grid-connected[J]. Proceedings of the CSEE, 2021, 41(18): 6181-6197 (in Chinese).
[4] 张雨曼，刘学智，严正，等. 光伏–储能–热电联产综合能源系统分解协调优化运行研究[J]. 电工技术学报，2020，35(11)：2372-2386.
ZHANG Yuman, LIU Xuezhi, YAN Zheng, et al. Decomposition-coordination based optimization for PV-BESS-CHP integrated energy systems[J]. Transactions of China Electrotechnical Society, 2020, 35(11): 2372-2386 (in Chinese).
[5] 罗天，汪可友，李国杰，等. 基于拉格朗日对偶松弛的多区域柔性直流互联电网无功优化[J]. 电力系统自动化，2019，43(11)：68-76.
LUO Tian, WANG Keyou, LI Guojie, et al. Reactive power optimization in multi-area VSC-HVDC interconnected power grids based on Lagrangian dual relaxation[J]. Automation of Electric Power Systems, 2019, 43(11): 68-76 (in Chinese).
[6] CHEN Sijie, SHEN Zeyu, ZHANG Ling, et al. A trusted energy trading framework by marrying blockchain and optimization[J]. Advances in Applied Energy, 2021, 2: 100029.
[7] XIN S J, GUO Q L, WANG J H, et al. Information masking theory for data protection in future cloud-based energy management[J]. IEEE Transactions on Smart Grid, 2018, 9(6): 5664-5676.
[8] ALEXANDRU A B, GATSIS K, SHOUKRY Y, et al. Cloud-based quadratic optimization with partially homomorphic encryption[J]. IEEE Transactions on Automatic Control, 2021, 66(5): 2357-2364.
[9] EVANS D, KOLESNIKOV V, ROSULEK M. A pragmatic introduction to secure multi-party computation[J]. Foundations and Trends® in Privacy and Security, 2018, 2(2-3): 70-246.
[10] TIAN Nianfeng, GUO Qinglai, SUN Hongbin. Privacy preservation method for MIQP-based energy management problem: a cloud-edge framework[J]. Electric Power Systems Research, 2021, 190: 106850.
[11] KNIRSCH F, EIBL G, ENGEL D. Error-resilient masking approaches for privacy preserving data aggregation[J]. IEEE Transactions on Smart Grid, 2018, 9(4): 3351-3361.
[12] 高晗，李正烁. 具有完全隐私保护的电–气综合能源系统分布式协同算法[J/OL]. 电力系统自动化，2022：1-15. (2022-08-18). https://kns.cnki.net/kcms/detail/32.1180.TP.20220818.0918.004.html.
[13] MUSTAFA M A, CLEEMPUT S, ALY A, et al. A secure and privacy-preserving protocol for smart metering operational data collection[J]. IEEE Transactions on Smart Grid, 2019, 10(6): 6481-6490.
[14] 颜拥，陈星莺，文福拴，等. 从能源互联网到能源区块链：基本概念与研究框架[J]. 电力系统自动化，2022，46(2)：1-14.
YAN Y, CHEN X Y, WEN F S, et al. From energy Internet to energy blockchain: basic concept and research framework[J]. Automation of Electric Power Systems, 2022, 46(2): 1-14 (in Chinese).
[15] 平健，严正，陈思捷，等. 基于区块链的分布式能源交易市场信用风险管理方法[J]. 中国电机工程学报，2019，39(24)：7137-7145.
PING Jian, YAN Zheng, CHEN Sijie, et al. Credit risk management in distributed energy resource transactions based on blockchain[J]. Proceedings of the CSEE, 2019, 39(24): 7137-7145 (in Chinese).
[16] 平健，陈思捷，严正. 适用于电力系统凸优化场景的能源区块链底层技术[J]. 中国电机工程学报，2020，40(1)：108-116.
PING Jian, CHEN Sijie, YAN Zheng. A novel energy blockchain technology for convex optimization scenarios in power system[J]. Proceedings of the CSEE, 2020, 40(1): 108-116 (in Chinese).
[17] 张玲，陈思捷，严正，等. 基于区块链共识机制的多区域最优潮流分布式算法[J]. 中国电机工程学报，2020，40(20)：6433-6441.
ZHANG Ling, CHEN Sijie, YAN Zheng, et al. Multi-regional optimal power flow distributed algorithm based on blockchain consensus mechanism[J]. Proceedings of the CSEE, 2020, 40(20): 6433-6441 (in Chinese).
[18] MAGDA F, COSTAS M, MANOLIS V. Decentralized blockchain-based consensus for optimal power flow solutions[J]. Applied Energy, 2021, 283: 116100.
[19] CHEN S J, MI H N, PING J, et al. A blockchain consensus mechanism that uses proof of solution to optimize energy dispatch and trading[J]. Nature Energy, 2022, 7(6): 495-502.
[20] PAILLIER P. Public-key cryptosystems based on composite degree residuosity classes[C]//Advances in Cryptology — EUROCRYPT'99. Berlin, Heidelberg: Springer Berlin Heidelberg, 2007: 223-238.
[21] ERKIN Z, TSUDIK G. Private computation of spatial and temporal power consumption with smart meters[C]// Proceedings of the 10th International Conference on Applied Cryptography and Network Security. New York: ACM, 2012: 561-577.

收稿日期：2023-04-04；修回日期：2023-04-23。

作者简介：


周鑫

周鑫（1997），男，博士研究生，研究方向为保护隐私的能源系统多主体可信协同优化，E-mail：zx-scott@foxmail.com。

王彬（1984），男，博士，副研究员，研究方向为智能电网和能源互联网能量管理与运行调控。通信作者，E-mail：wb1984@tsinghua.edu.cn。

孙宏斌（1969），男，博士，教授，研究方向为电力系统调度与控制、智能电网。

（责任编辑　张宇）