基于属性基加密的电力市场交易数据隐私保护算法

柳 茜[1]
LIU Qian

摘 要 在电力市场交易数据的隐私保护中，单纯依赖添加数据噪声进行加密的方法受限于隐私预算，难以提供有效的隐私保护，且数据被成功攻击的风险较高。为此，文章提出了基于属性基加密的电力市场交易数据隐私保护算法。在基于电力市场交易数据敏感度添加噪声的全局设置基础上，采用属性基加密方法为数据生成独立的属性密钥，并通过动态更新机制为市场交易参与者分配访问权限，以实现数据的隐私保护。实验结果表明，该算法保护下，电力市场交易数据的被成功攻击概率仅为 0.46%，数据安全性较高，能够提供更加可靠的隐私保护。

关键词 数据隐私保护；交易数据；属性基加密；市场交易数据；电力市场；隐私保护

doi：10.3969/j.issn.1672-9528.2025.11.036

0 引言

如今，电力市场的规模日益增加。如果市场交易过程产生的数据出现泄露，可能导致企业在庞大的电力市场竞争环境中呈现劣势，扰乱市场秩序，阻碍了电力市场的健康发展。因此，避免用户隐私数据泄露，保障数据安全这一问题成为电力市场交易的重要环节之一。然而，由于电力市场的交易数据往往涉及发电、售电、运营商等多方主体，这就意味着交易数据的隐私保护较为困难。在这样的情况下，为了保障电力市场交易数据的安全性，领域内针对数据隐私保护问题展开了热烈讨论。

奚增辉等人[1]提出了基于 Top-K 频繁挖掘的数据隐私保护方法。设置 Top-K，通过频繁挖掘分析数据的内在关联，确定数据的敏感度。结合差分隐私处理，生成数据的私有账本，实现数据的隐私保护。该方法处理的数据出现错误的概率较低。但在实际应用中，该方法容易出现隐私分配不合理的问题，导致数据噪声过多，数据信息出现失真，无法有效抵御外部攻击，隐私保护性能不理想。赵锋等人[2]提出了基于本地差分隐私的数据隐私保护方法。解析原始数据流特征，以此去除数据冗余。通过计算隐私预算，在 Laplace 机制下，为原始数据流添加相应时间尺度的随机噪声，从而保护数据

1. 甘肃中网通讯技术有限公司 甘肃兰州 730000

[57] WANG H F, LIU Q L, PENIN T, et al. Semplore: a scalable IR approach to search the Web of data[J]. Journal of Web semantics, 2009,7(3): 177-188.

[58] DAMLJANOVIC D, AGATONOVIC M, CUNNINGHAM H. Natural language interfaces to ontologies: combining syntactic analysis and ontology-based lookup through the user interaction[C]//The Semantic Web: Research and Applications. Berlin:Springer,2010:106-120.

[59] DAMLJANOVIC D, AGATONOVIC M, CUNNINGHAM H. FREyA: an interactive way of querying linked data using natural language[C]//The Semantic Web: ESWC 2011 Workshops. Berlin: Springer, 2012:125-138.

[60] KLEIN D, MANNING C D. Fast exact inference with a factored model for natural language parsing[C]//NIPS'02: Proceedings of the 16th International Conference on Neural Information Processing Systems.NewYork:ACM,2003:3-10.

[61] D'AQUIN M, MOTTA E.Watson, more than a semantic web search engine[J]. Semantic web, 2011,2(1): 55-63.

[62] DELBRU R, CAMPINAS S, TUMMARELLO G. Searching web data: an entity retrieval and high-performance indexing model[J]. Journal of web semantics, 2012,10: 33-58.

【作者简介】

韩凌（1981—），男，江苏南京人，博士，研究方向：机械、信息检索、人工智能。

（收稿日期：2025-06-15 修回日期：2025-11-05）

的隐私信息。该方法隐私保护下的数据具有良好的可用性。但由于特征复杂度较高，该方法难以解析高维数据流的特征，存在保护漏洞，导致其实际的抗攻击能力有所不足。朱齐亮等人[3]提出了基于k-prototype聚类算法的数据隐私保护方法。采用k-prototype聚类算法，根据数据属性距离进行多类型数据的快速聚类。结合相对熵的计算，建立数据的匿名发布机制，实现敏感数据的隐私保护。该方法能够有效降低数据隐私保护的信息损失率。但该方法设计的数据扰动策略可能较为单一，难以为数据的多维属性添加足够的噪声，导致隐私保护效果不理想，抗攻击能力较差。张愈杰等人[4]提出了基于联邦学习的数据隐私保护方法。在联邦学习的优化下，通过循环交换实现数据聚类。在对噪声分配策略的自适应优化基础上，利用差分隐私算法实现数据的隐私保护。该方法能够适用于非独立同分布的数据集类型。但在算法更新的过程中，攻击者可能会对加密数据进行逆向还原，破解梯度更新机制，导致原始数据产生泄露，抗攻击性能不足，难以实现有效的数据隐私保护。

考虑到上述研究人员所提出的数据隐私保护方法并不能有效保障数据的安全性，抗攻击能力不足，无法满足当前电力市场交易环节中，对于交易数据的安全管理需求。为了缓解这一问题，本研究提出了一种基于属性基加密的电力市场交易数据隐私保护算法。

1 基于属性基加密的电力市场交易数据隐私保护算法

1.1 电力市场交易数据隐私保护的全局设置

针对电力市场交易环节中的各个参与者，为其原始数据添加一个基本函数，以此作为客户端发送元组的模板。同时，为了避免密钥泄露问题对数据隐私安全的影响，本研究通过注入噪声的方法为电力市场交易数据引入误差，由此完成数据隐私保护的全局设置。

基于电力市场交易数据的响应需求，建立可编码的基本函数表达式，得到编码形式的电力市场交易数据形式，其公式为[5]：

$$P(x)=\left\{M(x_1),M(x_2),\cdots,M(x_n)\right\} \tag{1}$$

式中：$P(x)$表示原始数据的运算因子编码结构；x表示原始的电力市场交易数据；n表示数据量；M表示基本函数。

将编码结构的电力市场交易数据以元组的形式组合为单独的发送元组[6]。根据发送元组在电力市场交易环节的全局敏感度，为其添加相应的噪声。其中，全局敏感度的量化计算公式为：

$$\Delta f=\max_{P(x)}\left\|f(S_1)-f(S_2)\right\|_1 \tag{2}$$

式中：Δf表示全局敏感度；S_1和S_2表示电力市场交易环节中，两个不同的客户端节点；f表示查询函数。

根据计算所得到的全局敏感度，本研究采用拉普拉斯机制，确定注入噪声大小。这一过程用公式表示为：

$$F(x)=\Delta f+L(\varepsilon) \tag{3}$$

式中：$F(x)$表示注入噪声；L表示拉普拉斯算子；ε表示隐私预算。

完成噪声添加后，对引入了误差干扰的电力市场交易数据进行初始化，得到包含唯一标识符的数据元组，其公式为：

$$K(x)=(x,F,a) \tag{4}$$

式中：$K(x)$表示电力市场交易数据的初始化数据元组；a表示该数据在电力市场交易体系中的唯一标识符。

通过上述步骤，完成电力市场交易数据在隐私保护过程中的全局设置，得到初始化的数据元组。

1.2 基于属性基加密的电力市场交易数据加密

面向初始化的电力市场交易数据元组，为了确保数据在交易共享过程中的隐私安全，本研究采用属性基加密的方法，对其进行数据加密处理。

为电力交易数据元组设置加密的属性域范围，在哈希函数的支持下，生成数据属性基加密的主密钥和公钥。其中，哈希函数的表达式为：

$$H(K)=\left\{0,1\right\}^{*}\rightarrow Z_p \tag{5}$$

式中：H表示哈希函数；Z_p表示设置的属性域范围；*表示乘法循环群。

由此生成属性基加密的主密钥和公钥，分别用公式表示为[7]：

$$Q=(\alpha)^H \tag{6}$$

$$A=(g,\mathrm{e}(g),H)^L \tag{7}$$

式中：Q表示属性基加密的主密钥；α表示安全参数；A表示公钥；g表示生成元；$e(g)$表示生成元之间的线性映射；L表示电力市场交易数据元组的最大位长。

在电力市场交易环节中设置一个中央权威，利用该机构管理不同的数据属性，并根据数据含有的唯一标识符生成相应的属性标记，得到属性基加密的属性密钥[8]。属性密钥的表达式为：

$$m(K)=\left\{x=H(K,\tau)^{v},A,a\right\} \tag{8}$$

式中：$m(K)$表示属性密钥；τ表示随机数；v表示电力市场交易的版本号。

使用生成的属性密钥对电力市场交易数据元组进行加密处理，该过程用公式表示为：

$$c(K)=N(m(K)^{\gamma}\cdot e(g),A) \tag{9}$$

式中：$c(K)$表示属性基加密下的电力市场交易数据；N表示DecryptNode递归算法；γ表示电力市场交易数据传输的节点。

以此作为数据访问策略，在各个客户端节点判断用户的属性是否满足该策略，确定是否执行相应的解密策略。

通过上述步骤，完成基于属性基加密的电力市场交易数据加密处理。

1.3 访问控制下的数据隐私保护

在数据属性基加密的基础上，为了增强数据属性密钥的安全性，设计密钥更新机制。通过这一访问控制策略，实现电力市场交易数据的隐私保护。

以电力市场交易环节的中央权威机构为更新节点，定义数据属性密钥的更新机制 [9]，用公式表示为：

$$V(K)=\left\{m(K)=\frac{v^n}{v}\cdot\frac{v-v^n}{v\tau}\right\} \tag{10}$$

式中：$V(K)$ 表示更新的数据属性密钥。

将不定期动态更新的密钥存储到中央权威机构中进行集中管理，与电力市场交易数据的存储单元分离。利用中央权威机构将更新后的属性密钥发送到未被撤销访问权限的电力市场交易参与者，完成密钥的更新。其中，本研究采用属性域作为参与者的访问权限，用公式表示为：

$$G=\{0\}\in 2^{Z_p} \tag{11}$$

式中：G 表示电力市场交易参与者的授权集合。

在对参与者访问权限的控制下，将可解密的数据属性密钥仅发送到目标的参与者节点上，使外界节点无法进行数据访问，实现电力市场交易数据的隐私保护。

通过上述，完成基于属性基加密的电力市场交易数据隐私保护算法的研究设计。

2 算例测试

2.1 电力市场交易数据

为验证本文算法在实践应用中的数据隐私保护性能，参照真实的电力市场交易体系，开展数据隐私保护性能测试实验。

所依托的电力市场环境的累计交易电量达到 $2.633\,86\times10^{11}$ kWh 以上，平均交易额达到 365.22 元 /MWh，为大型的电力市场交易体系。该电力市场的交易环境采用了云服务的数据部署模式，如图 1 所示。

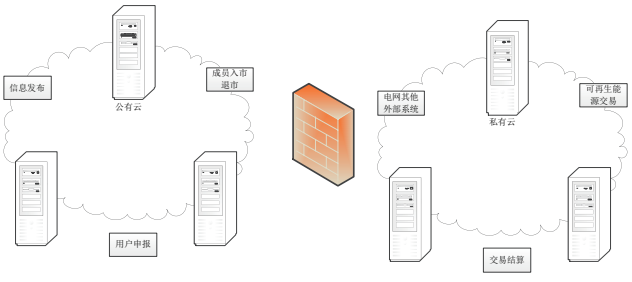

图 1 电力市场交易数据的云服务部署模式

如图 1 所示，该电力市场将发电商、运营商以及其他参与主体部署为互联网访问交易服务集群的形式。这种部署形式通过在第三方的公用云服务节点公开交易政策以及结果等信息，从而实现了隐私数据和公开数据的有效隔离。基于这种数据部署模式，本次实验针对其中的私有云服务集群上的电力市场交易数据，进行了数据隐私保护的实践测试。通过数据爬取技术，成功获取了如表 1 所示的实验数据。

表 1 电力市场交易数据

数据类型	数据量
电能量交易数据	15 815
辅助服务交易数据	19 611
容量交易数据	9 119
绿色电力交易数据	8 915

针对上述数据，本次实验特别采用了分布式拒绝服务（DDoS）等多种攻击模式，对已经实施了隐私保护措施的电力市场交易数据进行了全面的攻击测试。通过这种方式，旨在深入检验和评估这些数据在面对各种潜在威胁时的隐私保护性能，以确保其在实际应用中的安全性和可靠性。

2.2 算例实践与性能分析

面向爬取得到的实验数据，随机选取 1 000 条电力市场交易数据作为测试对象，测试本文算法的数据隐私保护性能。为更直观地评估本文算法的数据隐私保护性能，本次测试采用基于 Top-K 频繁挖掘和 k-prototype 聚类算法的两种数据隐私保护方法作为对比，在相同环境下对不同方法进行测试，以分析本文算法的性能水平。

采用 Hyperledger Fabric 作为工具完成各数据隐私保护方法的部署实现，并使其在 docker 沙箱中运行，确保各方法的数据隐私保护方案能够正确实施。针对选取的 1 000 条电力市场交易数据实验对象，评估各方法在面向不同大小数据时，所生成密钥的尺寸大小，结果如图 2 所示。

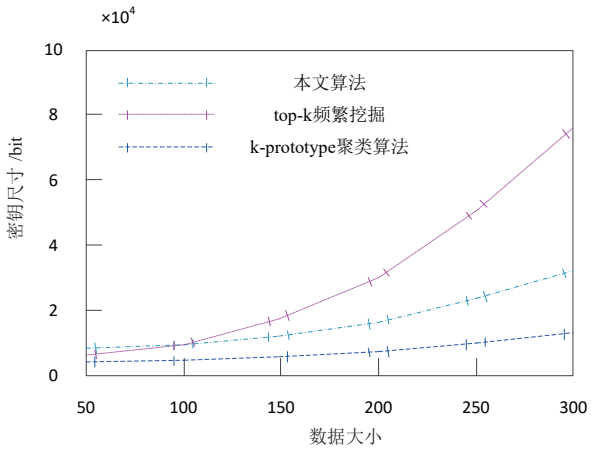

图 2 各方法数据加密的密钥尺寸对比

从图 2 可以看出，随着数据增大，本文算法能够自适应地更新密钥尺寸大小，以确保密钥的安全性。而基于 Top-K 频繁挖掘的数据隐私保护方法的密钥尺寸增大比例过大，这导致数据隐私保护过程的计算开销较大，基于 k-prototype 聚类算法的方法的增大比例则过小，难以为数据提供足够复杂的密钥。综合可见，本文算法隐私保护下的数据密钥尺寸更加合理。

利用全部的实验数据，针对各方法隐私保护下的数据安全性能进行测试。采用 DDoS 等攻击模式进行数据入侵，并统计各方法保护下，数据被成功攻击的次数，结果如图 3 所示。

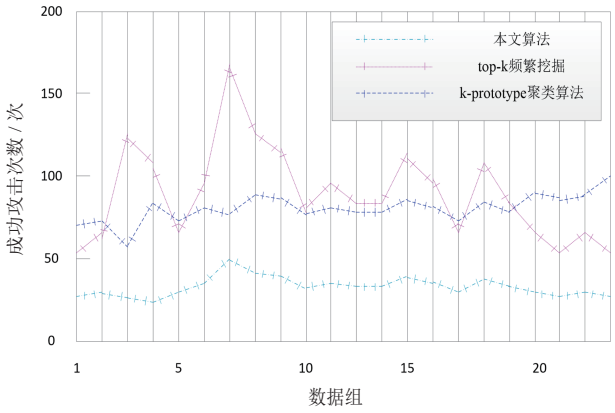

图 3 各方法数据隐私保护性能对比

从图 3 可以看出，与其他两种方法相比，本文算法保护下的电力市场交易数据被成功攻击的次数明显更少，平均每组数据的成功攻击概率仅为 0.47%，数据的安全性较优，表明本文算法对于电力市场交易数据的安全保护性能更高。

3 结语

本研究所提出的基于属性基加密技术的电力市场交易数据隐私保护算法，是在对原始数据进行初始化的全局设置之后，进一步采用属性基加密算法对数据信息进行加密处理。通过这种方式，数据在未被成功解密的情况下，外部的参与者是无法获取到真实的数据信息的。此外，结合密钥的动态更新机制，本算法能够对电力市场交易参与各方的访问权限进行有效控制，从而确保了电力市场交易数据的隐私性得到了有效的保护。基于本文所提出的算法所提供的数据隐私保护机制，能够确保电力市场参与者的核心利益不受侵害。通过这种方式，电力市场参与者的商业机密得到了安全保障，从而有助于提高企业自身的市场竞争力。进一步地，这种数据隐私保护机制有助于维护电力市场交易环节的公平竞争环境，确保所有参与者在公平的条件下进行交易，从而促进了整个电力市场的健康发展。

参考文献：

[1] 奚增辉，王卫斌，屈志坚，等 . top-k 频繁挖掘下电力敏感数据差分隐私保护 [J]. 电子设计工程，2025, 33 (10): 112-115.

[2] 赵锋，范淞，赵艳琦，等 . 基于本地差分隐私的可穿戴医疗设备流数据隐私保护方法 [J]. 信息网络安全，2025, 25 (5): 700-712.

[3] 朱齐亮，余雪婷 . k-prototype 聚类算法和相对熵下敏感数据重发布隐私安全保护 [J]. 吉林大学学报 (工学版), 2025, 55 (3): 1009-1014.

[4] 张愈杰，龙士工，张珺铭，等 . 非独立同分布数据下联邦学习的隐私保护算法 [J]. 计算机工程与设计，2025, 46 (4): 1047-1055.

[5] 孙政霞，吴春颖 . 基于 CiteSpace 的国内数据隐私保护可视化分析 [J]. 现代信息科技，2025, 9 (7): 173-178.

[6] 胡宇涵，杨高，蔡红叶，等 . 三维分布式无线智能系统数据传输路径隐私保护方案 [J]. 信息网络安全，2025, 25 (4): 536-549.

[7] 徐建，陈恺强，潘丽涛 . 云计算环境下电子信息工程数据隐私保护机制研究 [J]. 网络安全和信息化，2025(3): 141-143.

[8] 张岩杰，张恩利，常任琪，等 . 人工智能技术在体育教学应用中的学生数据隐私保护研究 [J]. 体育科技文献通报，2025, 33 (2): 291-294.

[9] 王天阳，李晓会，陈洪洋 . 参与式感知设备多维数据的个性化差分隐私保护方案 [J]. 计算机工程与科学，2024, 46 (11): 1997-2006.

【作者简介】

柳茜（1983—），女，甘肃兰州人，本科，中级工程师，研究方向：电子工程，email:chenj197009@163.com。

（收稿日期：2025-06-16 修回日期：2025-11-05）