文章编号:1003－6199(2025)01－0007－05 DOI:10.16339/j.cnki.jsjsyzdh.202501002

基于混合加密的电力网络数据安全与隐私保护算法研究

汪林†

(国电南瑞科技股份有限公司,江苏 南京 211106)

摘 要:为缩短电力网络数据加解密时间,提出了基于混合加密的电力网络数据安全与隐私保护算法。将电力网络数据转换为时间数据序列并进行预处理,通过隐私偏序拓扑分类,建立隐私数据多视图聚类。采用高级加密标准(AES)算法加密电力网络隐私数据,使用椭圆曲线密码学(ECC)公钥加密AES会话密钥,结合Hash函数计算散列值,生成数据安全验证签名。通过混合加密实现电力网络数据安全与隐私保护。实验结果表明,所提算法的数据加解密时间仅为430 ms,能够有效提高电力网络数据安全与隐私保护的实时性。

关键词:混合加密;椭圆曲线密码学;高级加密标准;电网数据;隐私保护

中图分类号:TP399 **文献标识码**:A

Research on Data Security and Privacy Protection Algorithms for Power Network Based on Hybrid Encryption

WANG lin†

(NARI Technology Co., Ltd., Nanjing, Jiangsu 211106, China)

Abstract: To shorten the encryption and decryption time of power network data, a hybrid encryption based power network data security and privacy protection algorithm is proposed. Convert power network data into time series and preprocess, and establish multi view clustering of private data through privacy partial order topology classification. Using advanced encryption standard (AES) algorithm to encrypt power network privacy data, using elliptic curve cryptography (ECC) public key to encrypt AES session key, combined with Hash function to calculate hash value, and generate data security verification signature. Implementing data security and privacy protection in power networks through hybrid encryption. The experimental results show that the data encryption and decryption time of the proposed algorithm is only 430 ms, which can effectively improve the real-time security and privacy protection of power network data.

Key words: mixed encryption; elliptic curve cryptography; advanced encryption standard; grid data; privacy protection

电力网络的发展离不开高速、双向的通信网络[1]。通过集成的电力网络,与控制技术、传感技术等先进的技术相结合,加强电网用户与供应商之间的联系,从而形成更加完善的电网安全运行策略。当前分布式电网中接入的可再生能源、智能终端设备越来越多,流通在用户和企业之间的数据流也在增大。这种背景下,数据隐私安全问题受到广泛关注,一旦电力网络数据出现泄漏,很容易直接暴露用户的隐私信息[2]。因此,各种数据安全和隐私保护技术涌现出来,以期促进智能电网的发展。

收稿日期:2023－08－24

作者简介:汪林(1981—),男,江苏扬州人,本科,研究方向:数字平台与通信领域网络智能化运维,人工智能与网络安全多模态认知与生成式智能,电力行业信息与数据。

† **通信联系人**,E-mail: gaoxiaqi199936rfa@163.com

文献[3]依托于区块链技术搭建数据隐私保护平台，并在平台中引入国密算法，在对电力数据进行加密、解密的过程中，可以保证数据的安全性，从而达到保护隐私数据的目的。但通过性能测试可知，该算法的执行效率较低。文献[4]运用随机森林算法处理隐私数据，预测出数据每种属性的敏感度，并通过 k 均值聚类算法将原始数据聚类为多个子数据集，按照每个聚类集合的数据敏感程度，给出不同程度的数据隐匿处理方案，实现数据安全和隐私保护。实验结果表明，该算法可用性较差。文献[5]提出将待处理数据放到可监管的联盟链上，利用决策线性加密算法对原始数据进行加密，并通过非交互式零知识证明算法实现访问用户身份验证，向符合安全要求的用户发送密钥，经过解密处理获取所需的数据。理论分析和模拟实验都证明了这种方法的安全性较低。

考虑到现有的数据安全与隐私保护算法无法满足电网数据处理要求，对此，本研究结合椭圆曲线密码学算法与高级加密标准算法，设计了基于混合加密算法的新型保护算法。在保证数据安全性的同时，提升数据隐私保护执行效率。

1 设计基于混合加密的电力网络数据安全与隐私保护算法

1.1 电力网络数据序列预处理

由于电力网络每日产生的数据量极大，为了便于对这部分数据进行安全隐私保护，按照数据采集时间，构建电力网络数据时间混沌序列[6]。对此序列中的位矩阵进行置乱、替代，从而预处理初始序列。具体处理过程如图 1 所示。

由图 1 可知，将原始电力网络数据时间序列按照 64 位字节数为一组的形式完成划分，并以任意一组 64 位明文数据纹理，将其分为左区和右区两个分部，左区直接进行置换和逆置换运算，右区则是在完成密钥位数扩展后，结合模拟密钥，实现 48 位异或运算和 32 位异或运算，将运算结果与左区数据结合起来，同时进行置换运算。在迭代结束后，得到电力网络数据混沌序列预处理结果。

1.2 建立隐私数据多视图聚类方案

不同的电力网络数据表现出的敏感性存在差异，在数据安全与隐私保护过程中，可以给出对应的个性化保护算法，以便取得更加有效的保护结果。实际操作过程中，先获取预处理后的数据序列中每个数据的属性，并计算属性隐私程度，以此来确定电力网络数据的敏感性。根据隐私数据排序敏感性[7]，完成隐私偏序的拓扑分类，建立隐私数据多视图聚类方案，针对不同类别的隐私数据给出对应的保护策略。

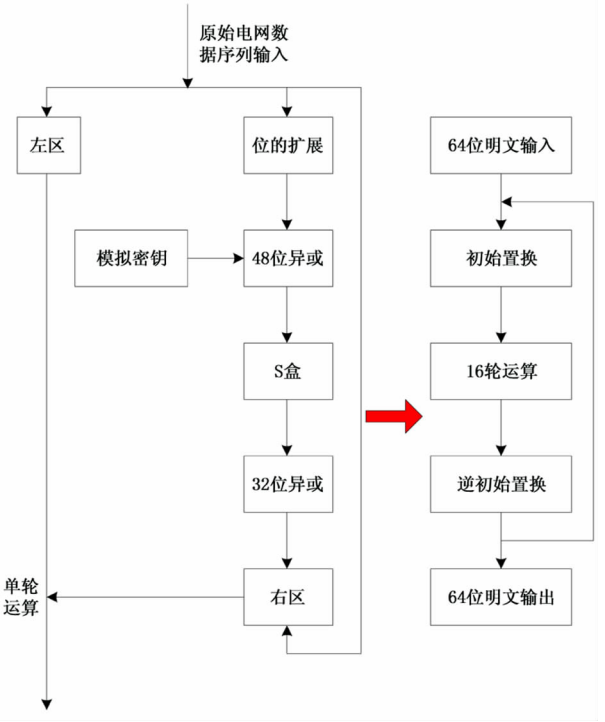


图 1 预处理初始序列过程

从电力网络数据中筛选出所有隐私数据，定义一个隐私数据集，在求出隐私数据集的极小隐私集后，推算出任意一个首隐私极元数据在极小隐私集内的相对隐私秩[8]，如下式：

$$|e>=\sum_{e'\in D}^{D}|\mathrm{sign}(e-e')| \tag{1}$$

其中：

$$e-e'=\sum_{i=1}^{n}(s_i-s_i') \tag{2}$$

式中，e 表示首隐私极元数据，$|e>$ 表示相对隐私秩，D 表示隐私数据集，e' 表示更新后的隐私数据，sign 表示符号函数，n 表示隐私数据中包含的属性数量，i 表示属性，s_i，s_i' 表示属性的隐私度。

假设隐私数据集中的极小隐私集处于非空状态，对于任意一个首隐私极元数据来说，隐私线序集的队尾节点指向该首隐私极元数据。已知层数和相对隐私秩的情况下，不断更新极小隐私集，如式(3)所示。

$$E'=E-\{e\} \tag{3}$$

式中，E 表示初始极小隐私集，E' 表示更新后的极小隐私集。

按照上述操作不断进行迭代计算，即可输出一组隐私线序，其包含隐私数据记录指针、偏序隐私

层号以及相对隐私秩,基于这一输出结果可以完成隐私偏序的拓扑分类,并描述每个类别数据的个性化隐私保护需求。为了将这一分析结果有效应用到后续数据安全与隐私保护过程中,将该分类结果看作一个视图,并从原始数据、隐私度等多个视角入手,实现个性化隐私多视图聚类,得到图 2 所示的聚类结果。

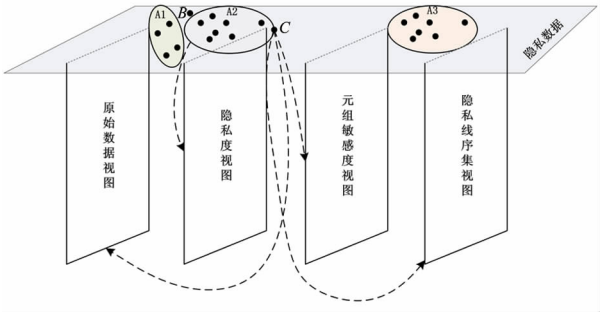


图 2　隐私数据多视图聚类示意图

如图 2 所示,A1、A2、A3 三个聚类簇代表的是多个视图共同作用下产生的聚类结果。而点 B 和点 C 是两个典型的聚类点,前者受到多视图聚类环境的影响,不属于聚类簇,而聚类是由多视图组成的,描述了其与不同视图之间的联系[9],最终归入聚类簇 A2。通过上述处理完成电力网络数据的有效聚类,根据每个聚类中数据的敏感程度,可以给出个性化隐私保护方案。

1.3　设计基于混合加密的数据保护算法

无论是处理哪一种敏感程度的数据,都需要通过加密处理和解密处理,实现数据安全与隐私保护。本研究以提升数据隐私保护的实时性为目标,结合椭圆曲线密码学(ECC)算法和高级加密标准(AES)算法,设计基于混合加密的数据保护算法。利用 AES 加密算法将原始明文数据转换为密文数据,并利用 ECC 加密算法进一步管理随机密钥[10],提升数据保护的安全性。依托于混合加密算法进行电力网络数据保护,需要经历数据加解密、会话密钥加解密和数字签名三个环节。

首先,运用 AES 加密算法处理原始数据,生成式(4)所示的随机加密序列。

$$0 \leqslant x_j \leqslant 2^6 E' \left(1 \leqslant j \leqslant \frac{\lambda^2}{6}\right)^4 \tag{4}$$

式中,x 表示随机加密序列,j 表示阶数,λ 表示密钥矩阵中包含的元素数量。

并定义子密钥矩阵如式(5)所示。

$$\boldsymbol{\eta} = \begin{bmatrix} \boldsymbol{x}_1 & \cdots & \boldsymbol{x}_{\frac{\lambda}{2}} \\ \vdots & & \vdots \\ \boldsymbol{x}_{1+(\frac{\lambda}{2}-1)\times\frac{\lambda}{2}} & \cdots & \boldsymbol{x}_{\frac{\lambda^2}{6}} \end{bmatrix} \tag{5}$$

式中,$\boldsymbol{\eta}$ 表示子密钥矩阵。

汇总所有子密钥矩阵,仅展开进一步运算,即可生成混合密钥矩阵。同样地,混合密钥矩阵主要由四个子矩阵组成,只要确定任意一块的子密钥矩阵,就可以推算出其他子矩阵,具体计算过程如下式:

$$\begin{cases} \boldsymbol{\theta}_{12} = \boldsymbol{\eta}(\boldsymbol{R} + \boldsymbol{\theta}_{22}) \times 2M \times 2^6 \\ \boldsymbol{\theta}_{11} = -\boldsymbol{\theta}_{22} \times \boldsymbol{\eta} \times M \times 2^6 \\ \boldsymbol{\theta}_{21} = \boldsymbol{\eta}(\boldsymbol{R} + \boldsymbol{\theta}_{11}) \times \dfrac{1}{2} M \times 2^6 \end{cases} \tag{6}$$

式中,$\boldsymbol{\theta}_{11}$、$\boldsymbol{\theta}_{12}$、$\boldsymbol{\theta}_{21}$、$\boldsymbol{\theta}_{22}$ 表示四个子密钥矩阵,$\boldsymbol{R}$ 表示单位矩阵,M 表示求余函数。

通过 AES 加密算法的运算,得到电力网络数据密文和会话密钥。将其传递给接收者后,结合 ECC 私钥可以解密 AES 会话密钥,从而解密出原始数据。

在对 AES 会话密钥进行加解密处理时,接收端必须画出一条适当的椭圆曲线,将其和随机选定的私有密钥同步传给发送者。发送方在结合一个随机整数后,结合 ECC 算法可以计算出如下两个点:

$$\begin{cases} H_1 = \boldsymbol{\theta}_{12}\boldsymbol{\theta}_{21}\sigma + rK \\ H_2 = \boldsymbol{\theta}_{11} rG \end{cases} \tag{7}$$

公式中,H_1、H_2 表示椭圆曲线上的两个点,σ 表示已知点,r 表示随机整数,K 表示公开密钥,G 表示椭圆上的基点。

将式(7)所示的计算结果发送给接收方,实现会话密钥加密处理。而在接收方得到这一密文信息后,需要进行反推计算,得到:

$$\begin{aligned} H_1 - kH_2 &= \sigma + rK - k(rG) = \\ &\sigma + rK - r(kG) = G \end{aligned} \tag{8}$$

式中,k 为私钥。椭圆曲线的基点由式(8)计算,以此为基础可以实现电力网络数据密文的解码,得到解密后的明文数据。

在混合加密算法的数字签名阶段,使用安全 Hash 函数获取原始数据对应的散列函数,再结合基于椭圆曲线产生的参数、随机选择整数、一个大素数,完成数字签名。针对该签名进行验证时,具体计算式为:

$$\alpha = g(\omega) \tag{9}$$

$$\begin{cases} u = \tau^{-1}\alpha M\beta \\ \upsilon = \tau^{-1}\gamma M\beta \\ (o', y') = u\sigma + \upsilon Q \\ l' = o' M\beta \end{cases} \tag{10}$$

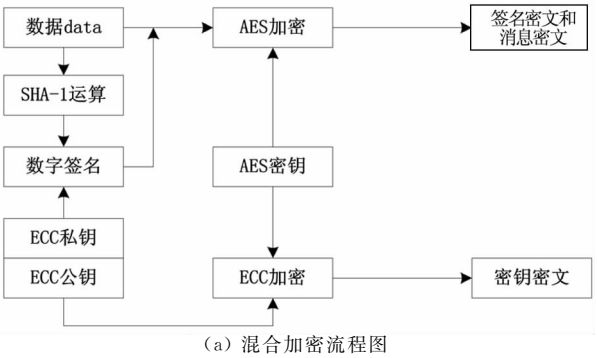
式中,ω 表示消息,g 表示安全散列函数,α 表示数字签名所需的安全 Hash 函数,(l,τ) 表示消息的签名,(β,Q) 表示公钥,β 表示一个满足安全要求的素数,Q 表示随机数与椭圆上基点的乘积,(o', y') 表示验证得到的椭圆上坐标,u、υ 表示验

证参数，l' 表示验证后得到的签名。

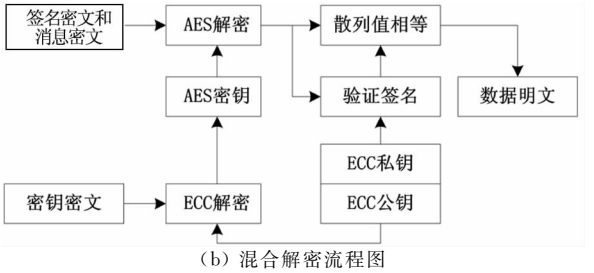
按照上述计算方式，得出验证后的签名，当其与显示的签名保持一致时，代表当前签名有效，用户可以根据自身需求访问电力网络数据，反之则代表签名无效，无权访问电网隐私数据。

1.4 实现电网数据安全与隐私保护

依托于基于混合加密的数据保护算法，实现电网数据安全与隐私保护，其主要操作步骤就是数据的加密和解密处理。其中，混合算法的数据加密流程如图 3(a)所示，在 AES 加密算法的作用下，得到数据密文和消息密文。再通过安全散列函数获取原始电力网络数据的散列值，与 ECC 私钥相结合得出数字签名，对 AES 会话密钥进行进一步处理，生成密钥密文。



(a) 混合加密流程图



(b) 混合解密流程图

图 3 混合加解密流程图

另外，用户发送电力网络数据访问请求后，会先接收到签名密文、消息密文和密钥密文。通过自身拥有的 ECC 私钥完成密钥解密，再进行签名验证，分析用户自身的安全性，符合要求的用户可以解密得到数据明文，如图 3(b)所示。

将上述加解密处理流程结合起来，即可实现电力网络数据安全与隐私保护。

2 实验分析

2.1 实验准备

为了验证基于混合加密的电力网络数据安全与隐私保护算法的应用效果，以某存在多个信任域的电力网络为实验对象，获取实验数据。本次实验的电力网络通信拓扑结构如图 4 所示。

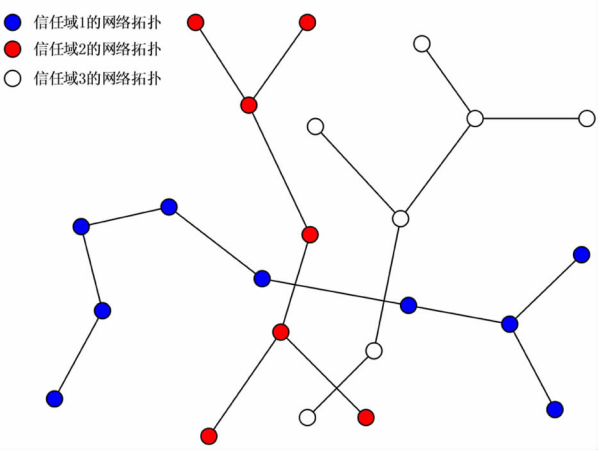


图 4 电力网络通信拓扑结构

从图 4 可以看出，在这个电力网络中，有 3 个信任域的信息采集网络，每个节点只能与同一信任域中的节点进行通信。针对该电力网络进行数据采集，得到一个可用于后续数据安全与隐私保护算法测试的模拟数据集，该数据集的部分数据如图 5 所示。

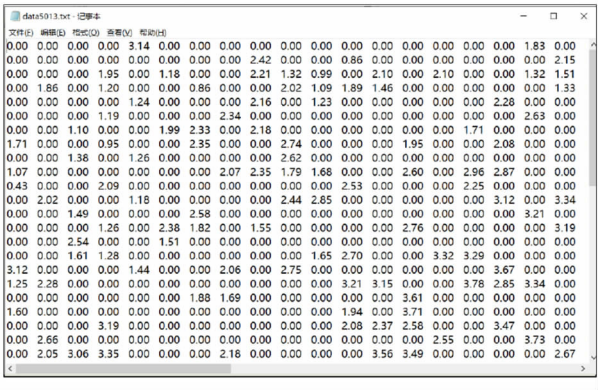


图 5 模拟数据集部分数据示意图

考虑到模拟数据集中的数据可能存在噪声数据、丢失数据等情况，影响最终的隐私保护效果。为此，相对模拟数据集分析其数据分布规律，以此来实现丢失数据的补充和噪声数据的去除，再将处理后的电力网络数据应用到后续隐私保护过程中。

2.2 隐私保护结果

按照所提算法对上述采集的电力网络模拟数据集进行隐私保护处理时，若客户端符合电力网络数据安全访问要求，即可得到电力网络数据明文信息。当客户端解密过程中出现验证错误时，会出现无权访问界面，如图 6 所示。

图 6　无权访问界面

无权访问界面的出现,代表当前客户端不满足电力网络数据安全要求。通过这一测试结果,可以证明所提算法是可行的,可以起到良好的数据保护效果。

2.3　算法性能分析

在进一步验证所提算法应用性能时,本次实验从数据加密时间、解密时间两个方面进行分析。在电力网络数据包数量为 50 MB 的情况下,采用所提算法、基于 RSA 加密的保护算法(文献[3]算法)、基于 ECC 加密的保护算法(文献[4]算法)进行电力网络数据安全与隐私保护,记录不同算法的加密时间,如图 7 所示。

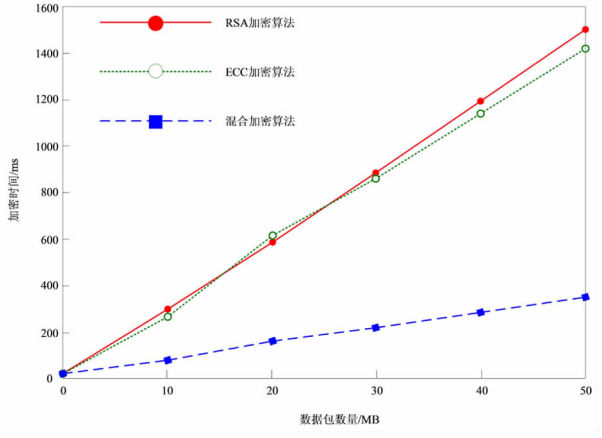


图 7　不同算法的加密时间对比

由图 7 可知,随着数据包数量的增加,三种算法的加密时间随之增加。当数据包数量为50 MB 时,RSA 加密算法和 ECC 加密算法的加密时间分别为 1486 ms 和 1409 ms,而混合加密算法的加密时间仅为 430 ms。

在此基础上,记录不同算法的解密时间,如图 8 所示。

由图 8 可知,当数据包数量为 50 MB 时,RSA 加密算法和 ECC 加密算法的解密时间分别为 1473 ms 和 1284 ms,而混合加密算法的解密时间仅为 430 ms。综合上述分析可知,所提算法能够有效提高数据安全与隐私保护的实时性。

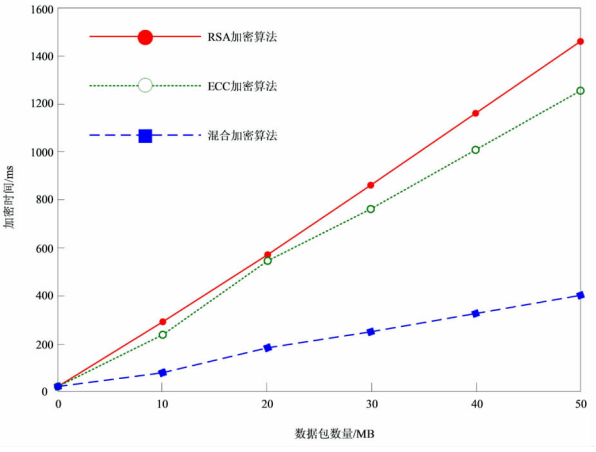


图 8　不同算法的解密时间对比

3　结　论

在智能电网不断发展的环境下,其内部通信数据量不断增长,数据泄露问题频发,电力网络数据安全与隐私保护算法的研究备受重视。为此,提出了基于混合加密的电力网络数据安全与隐私保护算法,可以在保证电网数据安全的情况下满足数据保护实时性要求。

参考文献

[1]　叶帅,蒋文保,祁亚楠. 基于 SM9 多密钥中心的用户身份隐私保护模型[J]. 计算机工程与设计,2023,44(7):1985－1992.

[2]　张玉立,张麦玲. 私有区块链下个人信息隐私保护算法仿真[J]. 计算机仿真,2023,40(4):397－401.

[3]　王晶宇,马兆丰,徐单恒,等. 支持国密算法的区块链交易数据隐私保护方案[J]. 信息网络安全,2023,23(3):84－95.

[4]　翟冉,陈学斌,张国鹏,等. 基于不同敏感度的改进 *K*-匿名隐私保护算法[J]. 计算机应用,2023,43(5):1497－1503.

[5]　何建江,陈玉玲. 基于 DLIN 加密的可监管联盟链隐私保护方案[J]. 计算机工程,2023,49(6):170－179.

[6]　郝玉蓉,朴春慧,颜嘉麒,等. 一种面向 LDP 的政府民意数据隐私保护方法[J]. 计算机仿真,2023,40(3):377－384.

[7]　杨挺,李大帅,蔡绍堂,等. 面向用户隐私保护的用电数据压缩加密方法[J]. 中国电机工程学报,2022,42(S1):58－69.

[8]　李帅,常锦才,李吕牧之,等. 基于差分隐私保护的 Stacking 集成聚类算法研究[J]. 计算机工程与科学,2022,44(8):1402－1408.

[9]　王军,徐彦惠,李莉. 基于分片的轻量级数据融合隐私保护算法[J]. 计算机工程与设计,2022,43(5):1207－1213.

[10] 周治平,钱新宇. 一种面向深度神经网络的差分隐私保护算法[J]. 电子与信息学报,2022,44(5):1773－1781.