E-Commerce Letters 电子商务评论, 2024, 13(4), 526-534
Published Online November 2024 in Hans. https://www.hanspub.org/journal/ecl
https://doi.org/10.12677/ecl.2024.1341180

Hans汉斯

基于AES算法的电商财务数据加密方法

宗烜逸[1]，周　宇[1]，陈晓勇[1,2*]

[1]南通大学信息科学技术学院，江苏　南通
[2]南通大学杏林学院信息学部，江苏　启东

收稿日期：2024年7月2日；录用日期：2024年10月10日；发布日期：2024年10月17日

摘　要

当前电商财务数据加密测算多为单元独立加密的形式计算，目标加密效率较低，导致最终加密速率降低，为此提出对基于AES算法的电商财务数据加密方法的设计与分析。结合当前的测定需求，先进行财务数据加密密钥扩展，展开轮密钥加密处理，结合AES算法，提升目标加密的实际效率，构建AES测算电商财务数据多轮加密模型，采用输出密文及动态解密的方式完成数据加密处理。测试结果表明：对比于传统新型真随机数财务数据加密方法、传统加权傅里叶变换数学模型财务数据加密方法，此次所设计的AES测算电商财务数据加密方法最终得出的加密速率相对较高，这说明通过AES算法的辅助与支持，设计的加密方式更为具体、加密覆盖范围扩展，加密速度与效率大幅度提升。

关键词

AES算法，电商财务，财务数据，数据加密，加密方法，财务信息

Electronic Business Financial Data Encryption Method Based on AES Algorithm

Xuanyi Zong[1], Yu Zhou[1], Xiaoyong Chen[1,2*]

[1]School of Information Science and Technology, Nantong University, Nantong Jiangsu
[2]Department of Information Science, Nantong University Xinglin College, Qidong Jiangsu

Received: Jul. 2nd, 2024; accepted: Oct. 10th, 2024; published: Oct. 17th, 2024

Abstract

At present, the calculation of e-commerce financial data encryption is mostly calculated in the form of unit independent encryption, and the target encryption efficiency is low, resulting in the reduction of the final encryption rate. Therefore, this paper proposes the design and analysis of e-commerce

*通讯作者。

文章引用: 宗烜逸, 周宇, 陈晓勇. 基于 AES 算法的电商财务数据加密方法[J]. 电子商务评论, 2024, 13(4): 526-534.
DOI: 10.12677/ecl.2024.1341180

financial data encryption method based on AES algorithm. Combined with the current measurement requirements, the financial data encryption key expansion is carried out first, the round key processing is carried out, and the actual efficiency of target encryption is improved by combining the AES algorithm, and the AES multi-round encryption model is constructed to measure the financial data of e-commerce, and the data encryption is completed by the output ciphertext and dynamic decryption. The test results show that: Compared with the traditional new true random number financial data encryption method and the traditional weighted Fourier transform mathematical model financial data encryption method, the designed AES calculation of e-commerce financial data encryption method finally obtained a relatively high encryption rate, which indicates that with the assistance and support of AES algorithm, the designed encryption method is more specific and the encryption coverage is expanded. The encryption speed and efficiency have been greatly improved.

Keywords

AES Algorithm, E-Commerce Finance, Financial Data, Data Encryption, Encryption Methods, Financial Information

1. 引言

电子商务的发展，知识财务数据保护成为平台管控不可或缺的一环。一般情况下，财务数据中包含了用户交易记录、资金流转信息等重要内容，一旦泄露或被篡改，不仅会对用户造成巨大损失，也会严重影响电商平台的声誉和运营。为避免上述情况的发生，当前多采用财务数据加密的形式进行处理。参考文献[1]提出的传统新型真随机数财务数据加密方法利用真随机数生成器产生与财务数据长度相同的密钥，确保密钥的随机性和不可预测性。随后，通过一对一的顺序相加或异或操作，将真随机数字节与财务数据结合，实现加密；文献[2]提出的传统加权傅里叶变换数学模型财务数据加密方法则是结合傅里叶变换将财务数据从时域转换至频域，使数据的频率成分得以凸显。在频域内，利用加权系数对数据的不同频率成分进行加权处理，实现数据的加密。这一类的数据加密形式虽然可以实现预期的加密目标，但是由于环境的变化以及数据的不断增加，再加上外部环境与特定因素的影响，导致最终得出的加密结果难以达到预期的标准。为此提出对基于 AES 算法的电商财务数据加密方法的设计与实践应用分析。AES (Advanced Encryption Standard)算法，采用对称密钥体制，加密和解密过程使用相同的密钥，这种设计使得 AES 算法在加密速度和密钥管理上都具备优势[3]。同时，AES 算法的分组密码设计，通过多轮迭代和混淆操作，一定程度上也确保了数据的安全性。在电商财务数据的加密过程中，AES 算法的应用可以确保数据的机密性和完整性[4]。通过对财务数据进行 AES 加密，将敏感信息转化为无法直接解读的密文，更好地防止数据在传输和存储过程中被窃取或泄露[5]。即使攻击者获取了密文，也难以通过暴力破解等方式恢复出原始数据，形成更强的安全机制，进一步提升系统的安全性，以期为电商行业提供更为安全、可靠的数据保护方案。

2. 设计电商财务数据 AES 测算加密方法

2.1. 财务数据加密秘钥扩展

密钥扩展过程需要从原始密钥中生成的轮密钥，增加实际加密的复杂性与随机性，提升整体的加密

高层级。结合 AES 算法支持 128 位、192 位和 256 位三种密钥的长度，根据电商财务数据的日常加密需求，选择合适的密钥长度，一般基础的财务数据选择 128 位的秘钥长度即可[6]。将用户提供的原始密钥将作为密钥扩展的输入引导目标，使用初始密钥和一个固定的进行加密处理，此时将预设的密文导入加密的结构之中，形成独立的加密程序，至此生成第一个轮密钥。具体的执行结构如图 1 说明。

图 1 主要是对第一轮密钥的加密处理。此时，按照上述设计的加密处理结构，为增加此时的加密等级，需要将第一个轮密钥和初始密钥融合，并使用 Rcon 数组对当前融合的秘钥进行转换[7]。具体如图 2 说明。

图 2 主要是对 Rcon 数组加密秘钥转换处理。根据转换后的财务数据加密秘钥，形成新一轮的融合性加密秘钥。此时需要计算出当前的扩展加密强度[8]。见公式(1)：

$$K = \theta^2 - \rho \times \frac{QZ}{W} \tag{1}$$

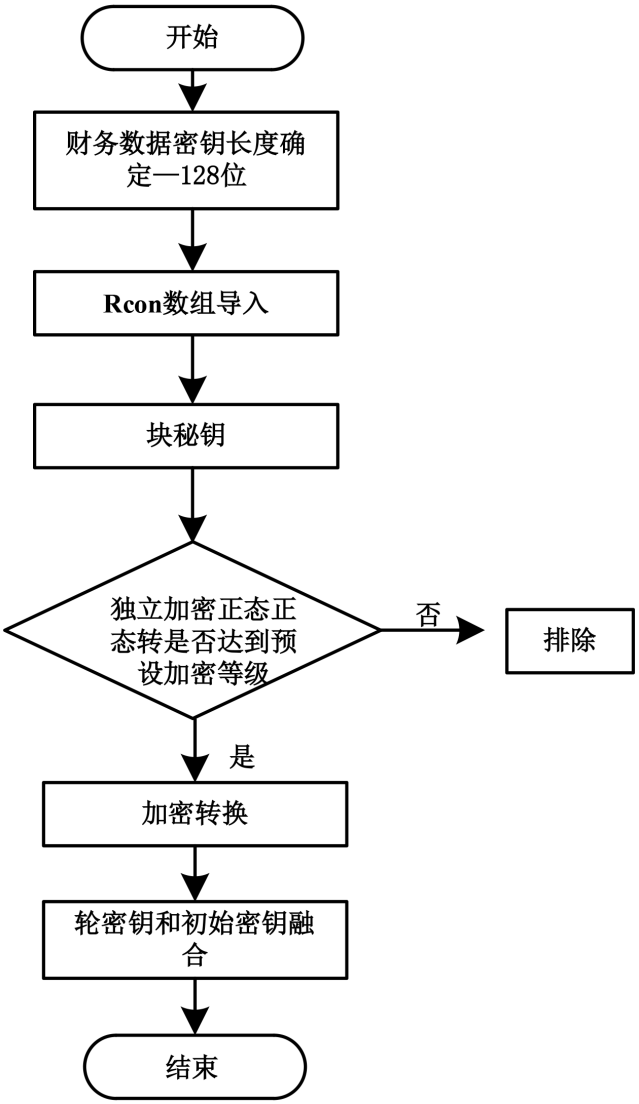
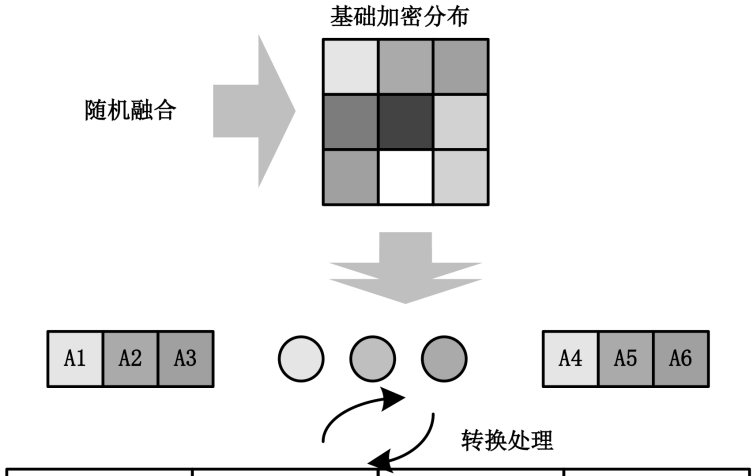


Figure 1. First round key encryption processing diagram
图 1. 第一轮密钥加密处理图示



U（加密特征）	1	2	3
RCON1	010000	020000	030000
U（加密特征）	4	5	6
RCON2	200000	400000	60000

Figure 2. Rcon array encryption key conversion icon
图 2. Rcon 数组加密秘钥转换图示

式(1)中：K 代表扩展加密强度，θ 代表加密覆盖区域，ρ 代表加密处理频次，Q 代表秘钥空间大小，Z 代表秘钥长度，W 代表加密保护范围。在完成当前加密扩展之后，分析此时的加密强度是否符合后期加密处理的需求，为后续的执行和电商财务数据的处理奠定基础条件[9]。需要注意的是，当前所设定的加密扩展秘钥并不是固定的，可以结合实际的需求做出定期的调整，增加密钥的灵活度与稳定性。但是在加密的过程中，必须保持加密的 Rcon 数组转换，进一步确保加密的稳定与可控。

2.2. 轮密钥加密处理

初始轮密钥加密的目的是将原始的财务数据(明文)与初始轮密钥多阶结合，进一步完善当前的加密环境。将原始的财务数据分为多个 128 位(即 16 字节)的分组[10]。需要注意的是，如果数据的总长度不是 16 字节的倍数，要先进行填充(Padding)至最近的 16 字节倍数，同时对加密的状态进行移位处理，可以先对状态矩阵的行进行循环左移，按位异操作，对于每一个数据分组，测定计算出加密的位异差，见公式(2)：

$$L=\upsilon\left(1+\phi\right)^{2}-\sum_{n=1}\upsilon n+f \tag{2}$$

式(2)中：L 代表加密位异差，υ 代表左移长度，ϕ 代表自相关函数，n 代表加密字节倍数，f 代表行异次数。结合当前测定，根据电商财务数据加密位异差的变化，将两个等长的轮密钥和数据分组每一位进行异运算，实现对轮密钥加基础处理。接下来，设定当前轮秘钥的加密序列，并按照加密的顺序进行排列分布，基于当前加密序列的分布情况，结合电商财务数据的具体类型，以多个字符序列进行编码，并计算出齐次分布加密特征值，见公式(3)：

$$m\left(c\right)=j+\frac{s\left(t\right)+g\left(e\right)}{s} \tag{3}$$

式(3)中：$m(c)$代表齐次分布加密特征值，j代表序列波动幅值，$s(t)$和$g(e)$分别代表密钥协议和特征协议，s代表加密标识位。根据当前测定，通过齐次分布加密特征值的来增加秘钥的加密层级，同时调整加密序列的处理结构，由于轮密钥的复杂性和随机性，还需要设计者对主密钥进行标定，更好地保证了数据的安全性。

2.3. 构建 AES 测算电商财务数据多轮加密模型

结合 AES 算法，针对电商财务数据的处理，进行多轮加密建模。基于上述设定的加密程序，当前针对电商财务平台的运行状态，根据预设的加密需求，进行基础安全性分析。一般情况下，AES 的轮数(Rounds)决定了加密的强度和安全性。轮数越多，加密的安全性越高，但加密速度会相应降低。反之，轮数越少，加密的安全性越低，但加密速度会相应增加。将上述设定的块加密数据包传输到预设的位置之上，基于加密序列排列分布，进行基础加密模型结构的设计，见图 3 说明：

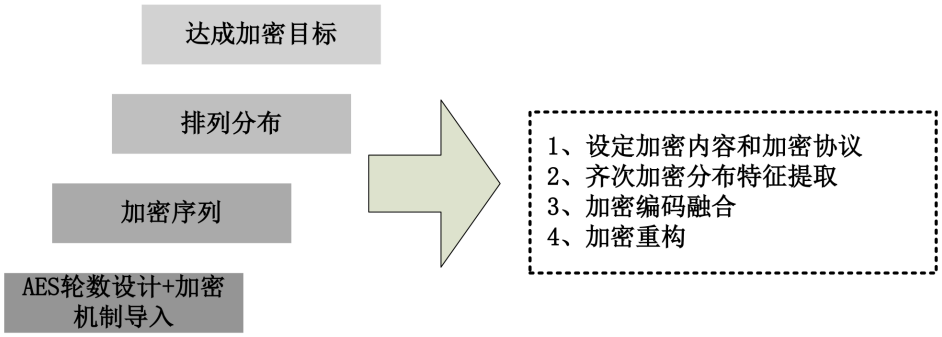


Figure 3. AES calculates the structure of multi-round encryption model of e-commerce financial data
图 3. AES 测算电商财务数据多轮加密模型结构图示

图 3 主要是对 AES 测算电商财务数据多轮加密模型结构的设计与实践验证。随后，需要在模型中，根据加密的内容设定加密和解密协议。结合齐次分布加密特征进行编码融合，进行加密重构，见公式(4)：

$$R(u)=\iota^{d}+\psi_{o}+\lambda \tag{4}$$

式(4)中：$R(u)$代表加密重构，ι^{d}代表加密维数，ψ_{o}代表随机线性加密差，λ代表边界系数。根据当前测定，通过加密重构，进一步调整初始的加密协议，进而展开加密序列的重组处理，结合 AES 测算，构建数据加密模型的表达式，见公式(5)：

$$C=E(K,P) \tag{5}$$

式 5 中：C代表加密模型的输出密文，E代表加密目标，K代表设定密钥，P代表明文。结合模型输出的加密结果，进行对比验证及实践分析。通过参数调整和算法优化，完善模型的综合应用能力，为电商财务数据提供有力的保护。

2.4. 输出密文及动态解密完成数据加密处理

当电商财务数据经过多轮 AES 加密处理后，模型最终会生成一个密文。这个密文是原始财务数据经过复杂的加密算法变换后得到的，其内容与原始数据完全不同，具有高度的随机性和复杂性。输出密文后，通过信道将其安全地存储或传输。由于密文已经经过了加密处理，因此即使被截获，攻击者也无法直接读取其中的内容。基于此，为进一步完善加密的程序，完成传输之后，进行动态解密处理。利用 AES 加密逆过程，将密文还原为原始数据。通常情况下，解密的流程与加密的流程相反，在每一轮解密中，

都会使用对应的轮密钥进行异或运算等操作，逐步还原出原始数据。但是这部分值得注意的是，在完成解密处理之后，如果发生错误密钥错误、数据损坏等，需要展开错误处理。此时结合加密过程中的处理条件和数据，计算出错误加密次数限值，见公式(6)：

$$N=\frac{\vartheta}{Y} \tag{6}$$

式(6)中：N 代表错误解密次数限值，ϑ 代表解密财务数据，Y 代表初错误解密数据，将计算得出的错误解密次数限值设定为加密核验的限制标准，在超出该错误解密的上限之后，需要导入密文进行加密处理，按照上述设计的加密流程重新加密处理，进一步确保电商数据加密处理的实际效果，增加财务数据的安全性和完整性。

3. 方法测试

结合 AES 算法，对电商财务数据加密方法的实际应用效果进行分析与验证研究，考虑到最终测试结果的真实性与可靠性，采用对比的形式展开分析，以 G 企业的电商财务平台作为测试的目标对象。参考文献设定传统新型真随机数财务数据加密方法、传统加权傅里叶变换数学模型财务数据加密方法以及此次所设计的 AES 测算电商财务数据加密方法。采集汇总平台中所应用的数据以及信息，分类存储之后，以待后续使用。接下来，在 AES 算法的辅助下，进行测试环境的设定与搭建。

3.1. 测试准备

在复杂的背景下，搭建 AES 算法的电商财务数据加密方法的测试环境，并稳定实际的测试程序。首先，将数据加密平台与 G 企业电商财务平台进行搭接，设定数据信息的共享传输程序，分 6 个周期进行数据的获取，此时数据的大小为 45 Gbit，非隐私财务数据大小为 30 Gbit，隐私财务数据大小为 15 Gbit。在实际的传输过程中，需要对隐私数据和非隐私数据进行同时加密，并对非隐私数据进行双重加密处理。当前，在复杂的背景下，根据财务数据的应用类型，将采集的数据进行分类处理，见图 4 所示：

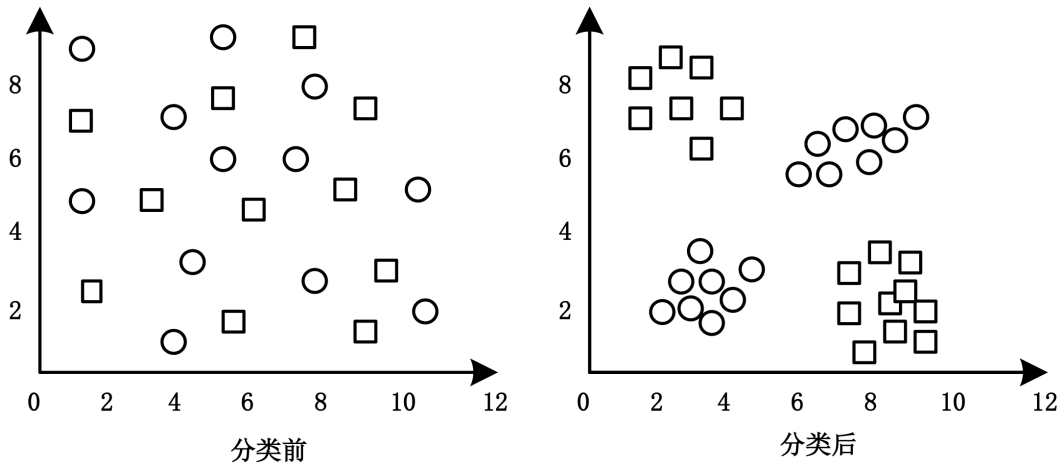


Figure 4. G diagram of classification and processing of enterprise financial data
图 4. G 企业财务数据分类处理图示

图 4 主要是对 G 企业财务数据的分类处理，接下来，将划分好的数据进行存储，并转换为格式一致、数量一致的数据包，基于此，还需要在信道上设定加密保护机制，扩大实际的加密范围。随后，根据加密的需求，设定辅助测试指标与参数，见表 1 所示：

Table 1. Financial data auxiliary test index and parameter setting table
表 1. 财务数据辅助测试指标与参数设定表

财务数据辅助测试指标	参数标准值
加密标识位	6
嵌入维数	11.58
逆变加密差	1.3~1.5
最优阈值	5.2
自相关函数	20.57
权重	11.57

表 1 主要是对财务数据辅助测试指标与参数的设定。在此基础之上，对当前企业的财务管理平台运行进行稳定性调整，主频为 3.55 GHz，内存为 2.5 GB，带宽/延时此时设定为 1 .2 GB/s，120 ms。至此实现对测试环境的设定及搭建，接下来，结合 AES 算法，对电商财务数据加密方法测定与实践对比。

3.2. 测试过程与结果分析

在上述搭建的测试环境之中，结合 AES 算法，对电商财务数据加密方法的实践分析。当前将分类处理之后的数据进行组合加密，根据以上设计的加密方法，此次针对隐私数据和非隐私数据，采用组合的方式进行加密处理。在程序中导入密文，转换实时的加密形式，分三个阶段进行加密处理，分别设置加密的公钥与私钥，在此基础之上，需要针对隐私数据进行二次深度加密，此时计算出加密数据的 Lyapunov 指数，见公式(7)：

$$D_q = \left(1-\beta^2 \times \frac{\wp}{va}\right) + v\chi \tag{7}$$

式(7)中：D_q 代表数据加密 Lyapunov 指数，β 代表加密均值，$\wp$ 代表数据总量，v 代表加密关联系数，a 代表加密临界值，χ 代表定向加密分布区域。结合当前计算得出的数据加密 Lyapunov 指数，对采集的数据进行区域分布处理，并依据 Lyapunov 指数的变化趋势展开局域加密处理，见图 5 所示：

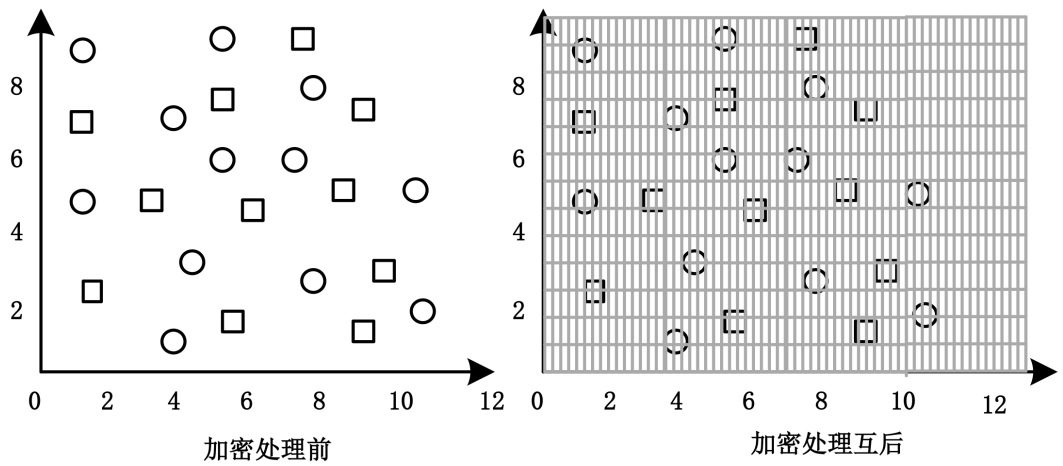


Figure 5. Financial data area encryption processing diagram
图 5. 财务数据区域加密处理图示

图 5 主要是对财务数据区域加密处理，结合 Lyapunov 指数转换此时的加密特征，利用 AES 算法，

将此时加密的数据转换为块加密的形式，结合加密数据量大小固定统一。完成数据加密之后，利用预设的信道将数据包传输到指定的位置，按照预设的程序进行阶级处理之后，计算出最终的加密速率，见公式(8)：

$$H=\frac{\pi_1^2+(1-\Im)}{\gamma}\times o\pi_2 \tag{8}$$

式(8)中：H 代表财务数据加密速率，π_1 和 π_2 分别代表基础加密收敛速度和实际的加密收敛速度，代表重复加密数据，γ 代表加密分配特征量，o 代表自适应函数。结合当前测定，完成对测试结果的验证，见表 2 说明：

Table 2. Results table of AES measure financial data encryption test
表 2. AES 测算财务数据加密测试结果表

数据采集测试周期	传统新型真随机数财务数据加密方法加密速率/kbps	传统加权傅里叶变换数学模型财务数据加密方法加密速率/kbps	AES 测算电商财务数据加密方法加密速率/kbps
周期 1	1050	860	1650
周期 2	850	950	1500
周期 3	895	1150	1500
周期 4	970	1050	1850
周期 5	950	760	1650
周期 6	820	800	1550

结果表 2，实现对测试结果的分析：对比于传统新型真随机数财务数据加密方法、传统加权傅里叶变换数学模型财务数据加密方法，此次所设计的 AES 测算电商财务数据加密方法最终得出的加密速率相对较高，这说明通过 AES 算法的辅助与支持，设计的加密方式更为具体、加密覆盖范围扩展，加密速度与效率大幅度提升。

4. 结束语

总之，以上便是对基于 AES 算法的电商财务数据加密方法的设计与实践分析。在 AES 算法的辅助与支持下，此次所设计的财务数据加密形式更加灵活、多变，自身的优势逐渐凸显出来。针对于电商所形成的财务数据保护效果得到了进一步的提升，在确保数据安全的同时，提高数据处理效率，共同推动电商财务数据加密技术的创新与发展。

参考文献

[1] 朱金坛. 一种基于新型真随机数发生器的大数据加密方法[J]. 微型电脑应用, 2024, 40(2): 184-187.

[2] 李婧彬, 郑真真. 基于加权傅里叶变换数学模型的通信数据加密传输方法[J]. 长江信息通信, 2024, 37(2): 99-101.

[3] 曲美红, 赵铭涛. 基于数据加密技术的计算机软件安全防护技术[J]. 长江信息通信, 2024, 37(2): 47-49.

[4] 李叶飞, 马昊燕, 荆树君, 等. 基于数据聚类的共享电源无线网络通信数据加密系统[J]. 电子设计工程, 2024, 32(1): 19-23.

[5] 袁炳夏, 王震. 基于四维超混沌系统的光通信数据加密研究[J]. 激光杂志, 2023, 44(11): 126-130.

[6] 晏银芳, 田维维. 基于随机森林的财务报表隐私数据自动加密方法研究[J]. 兰州文理学院学报(自然科学版), 2023, 37(4): 46-51.

[7] 安世俊. 基于国密算法的财务数据加密存储方法[J]. 信息记录材料, 2023, 24(4): 198-200.

[8] 李青, 王洋. 财务机器人绩效预算数据传输威胁抑制方法设计[J]. 自动化与仪器仪表, 2023(2): 231-236, 241.
[9] 张梅. 数据加密技术在计算机网络信息安全中的应用[J]. 佳木斯职业学院学报, 2022, 38(12): 152-154.
[10] 邓一新. 基于全同态加密算法的医院财务数据安全存储系统[J]. 自动化技术与应用, 2022, 41(7): 44-47.