文章编号：2095-2163(2024)03-0111-05 中图分类号：TP309.7 文献标志码：A

基于分组改进密钥扩展算法的医院信息系统实现

沈吉芳
（北海市妇幼保健院 医疗信息科，广西 北海 536000）

摘 要：当前，医院信息系统加密大多使用传统高级加密标准算法（AES 算法），存在安全稳定性差、计算工作量大、敏感数据无法得到有效管理等问题，亟需改进。本文基于分组改进密钥扩展算法对传统 AES 算法进行改进，通过最佳仿射变换和乘法逆运算，提高 S 盒的抗攻击性，并通过算法平行化，提高数据的加解密效率。实验分析表明，基于分组改进密钥扩展算法能够使医院信息加密系统加密的运行效率得到改善，运行效率得到提升，安全性能增加。

关键词：分组改进；密钥扩展算法；医院信息系统；加密

Implementation and research of hospital information system encryption based on packet improved key extension algorithm

SHEN Jifang
（Information Department of Beihai Maternal and Child Health Hospital, Beihai 536000, Guangxi, China）

Abstract: Currently, most hospital information system encryption uses traditional advanced encryption standard algorithms (AES algorithms), which urgently need improvement due to their poor security stability, large computational workload, and inability to effectively manage sensitive data. This article improves the traditional AES algorithm based on the group improvement key extension algorithm. By using the best affine transformation and multiplication inverse operation, the attack resistance of the S - box is improved, and the efficiency of data encryption and decryption is improved through algorithm parallelization. Experimental analysis shows that improving the key extension algorithm based on grouping can improve the calculated efficiency of hospital information encryption systems, enhance operational efficiency, and enhance security performance.

Key words: group improvement; key extension algorithm; hospital information system; encryption

0 引 言

随着医院医疗水平的提高，医疗数据得到大幅增长，原有的医疗数据存储方式已无法满足实际需要，既增加了医院运营成本，又降低了工作效率。云数据库技术的应用，使医院信息数据的存储和传输需求得到一定程度的解决，不仅能够使医院信息拥有较大的存储空间，而且能够降低医院的运营成本[1]。但是云数据库技术在给医院信息系统建设带来便捷的同时，也存在着信息数据被攻击的危险。因此，需要对医院信息系统进行加解密，确保医院信息能够得到更好的存储和传输[2]。

针对数据加密问题，相关工程技术人员对加密方法不断展开研究，先后提出 DES 算法、3DES 算法、AES 算法等[3]。文献[4]将 AES 和 DES 混合，设计了加密方案，通过 Hadoop 平台得到实现。文献[5]将 AES 算法应用于混沌系统，进一步降低运算量，提升了密钥所占的空间。文献[6]面向云存储的系统，应用 AES 算法实现自动加密系统，还集成了密文检索新兴功能。文献[7]基于 M-AES 和 P-RSA 的优点形成改进后的 AES-RSA 混合加密算法，数据更难破解，安全性也得以大幅度提升。文献[8]将 AES 和 SHA-52 算法进行融合，应用于防窃听信息安全系统。文献[9]将 AES 和 QR 二维码进行整合应用于快递加密系统，防止冒领，减少用户财产损失。本文在 AES 算法的基础上，根据医院信息系统的安全和运行效率的实际需求，建立基于分组改进密钥扩展算法，通过最佳仿射变换和乘法逆运算，提高 S 盒的抗攻击性，并通过算法平行化提高数据的加解密效率，再利用实验对基于分组改进密钥扩展算法的安全性和运行效率进行验证。

1 AES 加密算法

AES 是美国国家标准与技术研究院发布的一种

作者简介：沈吉芳（1986-），女，学士，工程师，主要研究方向：计算机科学与技术。Email：dpmsoe@163.com

收稿日期：2023-03-20

对称加密算法。作为 DES 加密算法的替代方案,在安全性和加解密运行效率方面有了显著提升,并已广泛应用到诸多领域中。AES 加密算法是以分组迭代为基础的加密算法,能有效地抵抗现有的攻击方法[10]。研究中以 AES-128 为例说明其加解密的过程如图 1 所示。

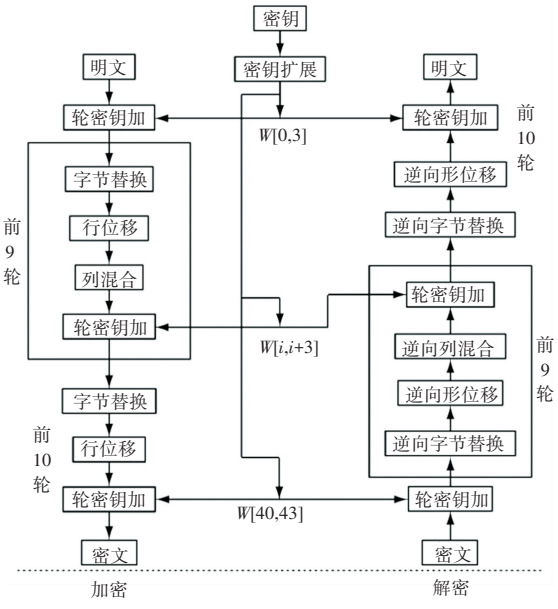


图 1 AES-128 加解密过程图

Fig. 1 AES-128 encryption and decryption process diagram

AES-128 加密流程共有 4 个步骤:轮密钥加、字节替换、行位移和列混合变换;AES-128 解密过程共有 4 个步骤:轮密钥加以及逆向的字节替换、行位移和列混合变换[11]。

1.1 轮密钥加

将输入矩阵和密钥矩阵进行异或运算,数据加密。以 AES-128 算法为例,该过程需要 1 个初始轮,9 个 4 种操作的重复轮,1 个 3 种操作的最终轮,合计 11 轮,最终得到密文。

1.2 字节替换/逆向字节替换

字节替换是指将字节通过 S 盒映射到状态矩阵上,使数据的混淆性得到提高。字节替换的具体步骤:将字节的高四位替换为新字节的行,将字节的低四位替换为新字节的列,得到字节替换后的状态矩阵,其过程是非线性的[12]。逆向字节替换是字节替换的反向过程,是对状态矩阵进行映射,得到原来的字节数据。

1.3 行位移/逆向行位移

行位移的目的是提高数据加密算法的扩散性,根据密钥的长度将状态矩阵每一行的字节向左进行一定位移量的循环移动。对于 128 位密钥,状态矩阵的第 1 至 3 行分别向左位移 1 至 3 位。逆向行位移是行位移的反向过程。

1.4 列混合变换/逆向列混合变换

列混合变换的过程是用多项式乘以状态矩阵各列,可以用式(1)表示:

$$C(x) = \{03\}\ x^3 + \{01\}\ x^2 + \{01\}x + \{02\} \quad (1)$$

对式(1)进行模 $x^4 + 1$ 运算,得到式(2):

$$b'x = c(x)b(x) \bmod (x^4 + 1) \quad (2)$$

列混合变换后,状态矩阵中各字节都和该字节所在的列中其它的字节有关,提高了字节间的混淆性,其实质是矩阵乘法。逆向列混合变换是列混合变换的反向操作。

1.5 密钥扩展

在 AES-128 算法中,根据密钥加解密的要求,共有 11 个初始密钥需要进行扩展,用矩阵形式表示,矩阵中每一列都有 4 个字节,用 $\boldsymbol{w}[i]$ 表示矩阵,其中 i 取值 0,1,2,3,根据状态矩阵的规模,经 AES-128 算法后,得到 44 列密钥[13]。密钥扩展过程用式(3)表示:

$$\begin{cases} \boldsymbol{w}[j] = \boldsymbol{w}[j-4] \oplus \boldsymbol{w}[j-4], & j \text{ 不能被 4 整除} \\ \boldsymbol{w}[j] = g(\boldsymbol{w}[j-4] \oplus \boldsymbol{w}[j-4]), & j \text{ 能被 4 整除} \end{cases} \quad (3)$$

其中,j 表示密钥矩阵每一列的列数;根据字节替换、行位移和轮密钥加等加密环节的不同,$g(\cdot)$ 分别表示各加密环节函数。

2 基于分组改进密钥扩展 AES 算法

2.1 S 盒构造改进

S 盒主要工作于轮密钥加、密钥扩展阶段,增强系统加密抵抗攻击的能力,可以用多项式形式表示,即从输入 $GF(2^n)$ 变化为 $GF(2^m)$,对此可表示为:

$$F(x) = (f_1(x), f_2(x), \cdots, f_m(x)) \quad (4)$$

传统 AES 算法在加解密的过程中,S 盒的迭代周期较短,减弱了代数性质,最终使 AES 算法的抵抗攻击的性能降低[14]。

本文以 AES-128 算法为例,以传统 S 盒的构造原理为基础,对 S 盒的构造进行改进。使用仿射变换、乘法逆运算等方式,提高迭代周期和代数性质,从而使 AES 算法能够更好地抵抗外部攻击。

S 盒构造改进的具体过程见如下:

(1)对具有较好代数性的多项式进行提取,即提取分析有限域 $GF(2^8)$ 中存在的多项式进行乘法逆运算,在保持仿射变换不变前提下,使用乘法逆运算形成 30 个 S 盒;

(2)建立仿射变换对,使变换对能够符合多项式的要求,同时参考雪崩准则,并以仿射和迭代周期为依据,从所有的仿射变换对中找出一组最优仿射变换对,用(u,v)表示,确保多项式$x^8+x^4+x^3+x+1$不发生变化;对变换后的S盒和原S盒的代数指标进行对比,分析改进后的S盒抵抗攻击能力是否得到提升;

(3)在前述步骤得到相关数据的基础上,首先进行一次仿射变换,再进行乘法逆运算,接着进行仿射变换,使得到的 S 盒能更好地抵抗攻击。

2.2　基于分组改进密钥扩展算法

传统 AES 算法是基于分组密钥的加密算法,应用于诸多需要对数据进行加密的场合,但是其分组密钥是通过对初始密钥扩展而形成的。在密钥扩展后,各分组的密钥相互之间存在关联性,对于加密算法的性能带来一定的影响。一是传统 AES 算法的初始密钥有可能会被攻破,对于数据的安全性能造成损害;二是在信息数据存储和传输的过程中发生的错误,将导致数据解密错误,制约着加解密的准确性[15]。为了使数据加解密更加安全和准确,需要消除各列密钥之间的关联,本文使用平方剩余算法,进行密钥扩展,从而提高了密钥的扩展性能。

基于分组改进密钥扩展算法的实现过程具体如下:

(1)使用平方剩余算法生成随机序列 ,使用加密算法得到的素数用u、v分别表示,用式(5)表示平方剩余集合[16]:

$$Q_R=\{a\mid \exists x\in Z,x^2\equiv a \bmod n\} \tag{5}$$

其中,Z表示整数集合。

由式(5)可以得到随机数值,数值是将n取模后再进行平方的剩余数。

设定$s_i\in Q_R$,由式(6)可以得到一随机序列:

$$s_i\equiv s_{i-1}^2 \bmod n \tag{6}$$

(2)对数据进行加密。在对分组进行加密时,按照字节长度大小不同,分别对明文和密钥流进行加密。设密钥流序列分别为$K_1,K_2,\cdots,K_t$,用式(7)分别表示明文的分组M和密文的分组C:

$$\begin{cases}M=(m_1,m_2,\cdots,m_t)\\C=(c_1,c_2,\cdots,c_t)\end{cases} \tag{7}$$

用其中一个分组(M_i,C_i)举例说明,其中M_i表示加密前的明文,C_i表示加密后的密文,其加密过程可以用式(8)表示:

$$C_i=E(M_i,K_i) \tag{8}$$

其中,$E(\cdot)$表示的是改进后的S盒的加密全过程。

用此方法形成的密钥相互之间没有关联性,即使数据被攻击,加密的密钥序列也不能被破解,数据更加安全。

(3)对数据进行解密。对数据进行解密的过程是对数据进行加密的逆向过程,将数据加密过程中的代码$C[i]\leftarrow E(M[i],K[i])$,用$M[i]\leftarrow E^{-1}(C[i],K[i])$进行替换,实现对数据的解密。其中,$E^{-1}(\cdot)$表示的是改进后的$S$盒的解密全过程。

2.3　算法并行化分组改进

医院信息系统中的数据大小不一,有些数据的长度在万字节以上,有些数据的长度不足百字节。运用 AES 算法进行加解密时,数据的不同长度对其影响极大,长度过大会使医院信息系统的响应时间变慢,影响着人机交互体验。

传统的 AES 算法为串行计算结构,只有在完成一组加解密操作以后,才能进行下一分组的加解密操作,在数据明文的长度不大时,该算法可以得到很好的应用。但是当数据明文的长度过大时,需采用将明文长度拆分处理的方式,却随即降低了加解密的运行效率[17]。本文对 AES 算法的串行计算结构进行改进,使其成为并行计算结构,从而在操作时可以同时对多个分组进行加解密操作,提升信息数据加解密的计算效率。

以 AES-128 加密算法为例,对明文数据进行 4 线程的并行化处理,分组改进结构如图 2 所示。

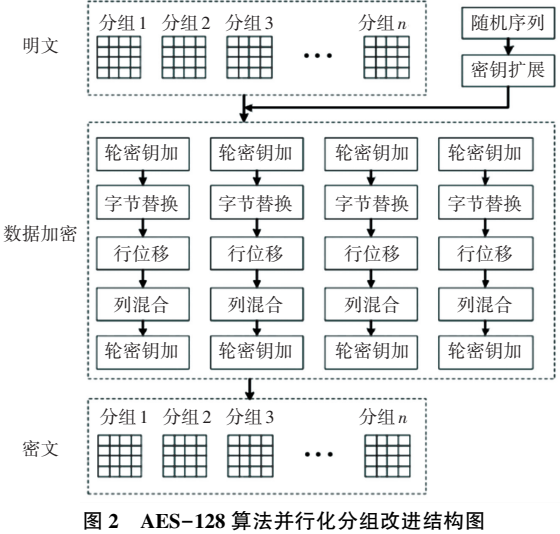


图 2　AES-128 算法并行化分组改进结构图

Fig. 2　AES-128 algorithm parallelization grouping improvement structure diagram

对于字节较长的明文数据,采用改进后的并行化分组进行数据加解密操作,算法的计算效率得到了明显提升。

3 基于分组改进密钥扩展算法的有效性分析

将基于分组改进密钥扩展算法的对医院信息系统加解密性能与传统 AES 算法进行对比,从而对本文所提出的基于分组改进密钥扩展算法的有效性进行验证。

3.1 2 种算法的扩展性比较

采用对 128 字符串进行加密操作方式,对传统 AES 算法和基于分组改进密钥扩展算法的扩展性进行测试。在密钥不变化的情况下,记录明文数据在加密操作后每变化 1 比特,密文数据变化多少比特,来对 2 种算法的扩展性进行评价。共进行 10 次扩展性实验,实验得到的密文数据变化比特数统计如图 3 所示。

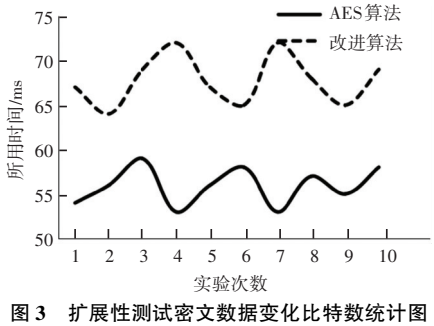


图 3 扩展性测试密文数据变化比特数统计图

Fig. 3 Scalability test ciphertext data change bit count statistical chart

实验得到密文比特数的变化范围,采用传统 AES 算法为 55(±7),而采用基于分组改进密钥扩展算法为 68(±4),可见基于分组改进密钥扩展算法的扩展性得到改进。

3.2 2 种算法的混淆性比较

采用对 128 字符串进行加密操作方式,对传统 AES 算法和基于分组改进密钥扩展算法的混淆性进行测试。在明文字符保持不变的基础上,通过观察在加密操作以后,密钥每变化 1 比特,密文数据变化多少比特,来对 2 种算法的混淆性进行评价。共进行 10 次混淆性实验,实验得到的密文数据变化比特数统计如图 4 所示。

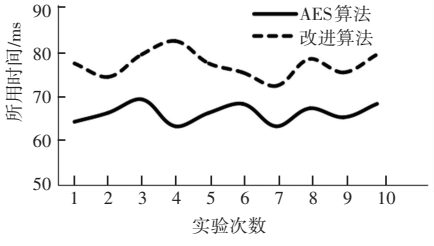


图 4 混淆性测试密文数据变化比特数统计图

Fig. 4 Confusion test ciphertext data change bit count statistical chart

实验得到密文比特数的变化范围,采用传统 AES 算法为 65(±4),而采用基于分组改进密钥扩展算法为 77(±7),可见基于分组改进密钥扩展算法的加密混淆性得到改进,能够更好地抵抗攻击。

3.3 2 种算法的运行效率比较

对传统 AES 算法与基于分组改进密钥扩展算法的运行效率比较时,需要对短数据(如医嘱信息)和长数据(如电子病历)分别进行加密和解密实验,对 2 种算法所用时间进行统计[18]。加密所用时间是对明文数据进行加密后存入数据库过程所用时间;解密所用时间是将数据从数据库提取出来转化为明文过程所用时间。共进行 10 次实验,实验得到的所用时间统计如图 5 所示。

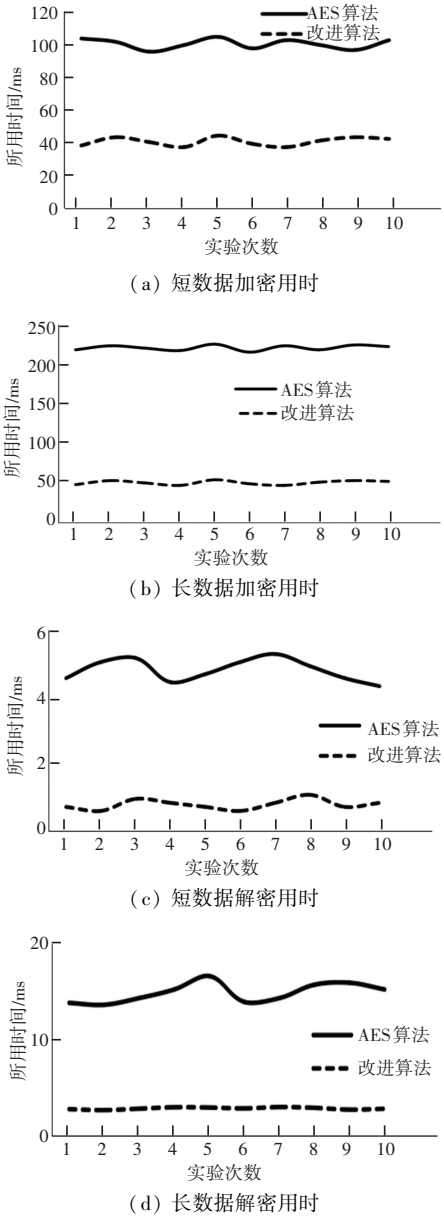


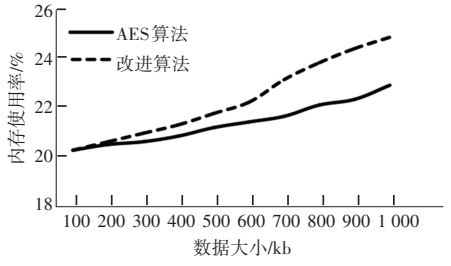
图 5 2 种算法运行时间比较

Fig. 5 Comparison of the operational time of two algorithms

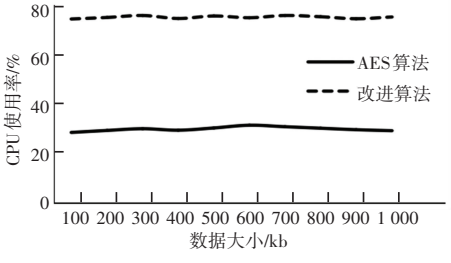
实验表明：基于分组改进密钥扩展算法在短数据和长数据的加解密过程中所用时间均小于传统 AES 算法，尤其是长数据的加解密过程的运行效率有显著提升，证明并行处理结构算法的加解密运行效率优于串行处理结构。

3.4　2 种算法的内存和 CPU 使用率比较

基于分组改进密钥扩展算法将传统 AES 的串行运算结构改进为多组并行运算结构，减少了加解密时间。从原理上来说，加解密时间减少会增加内存和 CPU 使用率[19]。通过实验对传统 AES 算法和基于分组改进密钥扩展算法的内存和 CPU 使用率进行比较，明文数据最初为 100 kb，将明文数据的长度逐渐增加，每次增加 100 kb，直至1 000 kb，共进行 10 次加解密实验，2 种算法内存与 CPU 使用率实验统计如图 6 所示。



（a）2 种算法内存使用率



（b）2 种算法 CPU 使用率

图 6　2 种算法内存与 CPU 使用率实验统计

Fig. 6　Experimental statistics on memory and CPU usage of two algorithms

实验结果表明，传统 AES 算法和基于分组改进密钥扩展算法在内存使用率方面，差别不是很明显，随着数据长度的增加，基于分组改进密钥扩展算法在内存使用率上高出传统 AES 算法约 3%。在 CPU 使用率方面，基于分组改进密钥扩展算法远远高于传统 AES 算法，有效运用计算资源，减少加解密所用时间[20]。

4　结束语

本文在AES加密算法的基础上，采用仿射变换、乘法逆运算、算法平行化等方法，得到基于分组改进密钥扩展算法，提高医院信息系统加密的安全性、时间效率，计算资源得到良好运用。实验结果表明，基于分组改进密钥扩展算法可以成为医院信息系统加密的新方法。

参考文献

[1] 宁淼. 浅谈网络环境下医院计算机信息系统管理的加强[J]. 信息与电脑(理论版)，2015(22)：7-8.
[2] 马连志. 关于对医院网络安全现状及防范策略的分析[J]. 电子技术与软件工程，2015(20)：225.
[3] 刘晖，彭智勇. 数据库安全[M]. 武汉：武汉大学出版社，2007.
[4] 战非，赵侃，曹国振，等. 面向云计算的混合同态加密算法研究[J]. 电子设计工程，2018，26(2)：6-9，13.
[5] 温贺平，陈俞强. 面向大数据的超混沌和 AES 混合加密方法研究[J]. 计算机应用与软件，2018，35(5)：318-322.
[6] 韩培义，刘川意，王佳慧，等. 面向云存储的数据加密系统与技术研究[J]. 通讯学报，2020，41(8)：55-65.
[7] 刘博文. AES-RSA 混合加密算法的研究及其在军队后勤管理系统中的应用[D]. 杭州：浙江大学，2022.
[8] 陈浩东. 基于 AES 算法和 SHA-512 设计数据加密系统[J]. 网络安全技术与应用，2023(6)：26-29.
[9] 辜双佳. 基于改进 AES 算法和 QR 码的快递信息加密研究及应用[D]. 重庆：重庆理工大学，2022.
[10] 祝婕，夏芳，孙琪. 浅议我国医院信息化的现状和发展趋势[J]. 电子技术与软件工程，2017(9)：215-215.
[11] 余启航，李斌勇，杨雄凯，等. DES 加密算法的过程分析研究[J]. 网络安全技术与应用，2018(2)：43-44.
[12] BABITHA M P，BABU K P R. Secure cloud storage using AES encryption[C]// 2016 International Conference on Automatic Control and Dynamic Optimization Techniques (ICACDOT). Pune，India：IEEE，2017：859-864.
[13] 温贺平，陈俞强. 面向大数据的超混沌和 AES 混合加密方法研究[J]. 计算机应用与软件，2018，35(5)：318-322.
[14] WANG Xijin，FAN Linxiu. The application research of MD5 encryption algorithm in DCT digital watermarking[J]. Physics Procedia，2012，25：1264-1269.
[15] 杨新国. 基于 AES 的加密技术研究及应用[D]. 长春：长春理工大学，2010.
[16] 杨晓东，王毅. AES 密钥扩展新方法[J]. 微电子学与计算机，2012，29(1)：102-104.
[17] BONEH D，FRANKLIN M. Efficient generation of shared RSA keys(Extended abstract)[J]. Journal of the ACM，2001，48(4)：702-722.
[18] 闫乐乐，李辉. 基于复合混沌序列的动态密钥 AES 加密算法[J]. 计算机科学，2017，44(6)：133-138，160.
[19] 李贵勇，何斌，方磊. 基于差异阈值循环分组的密钥生成方案[J/OL]. 计算机应用：1-8[2024-03-08]. http://kns.cnki.net/kcms/detail/51.1307.TP.20230927.1826.022.html.
[20] 陈怡，包珍珍，申焱天，等. 用于大状态分组密码的深度学习辅助密钥恢复框架[J]. 中国科学：信息科学，2023，53(7)：1348-1367.