文章编号：1004-4353(2015)03-0244-05

AES 改进算法在 CCMP 协议中的应用

李京， 李永珍*
（延边大学工学院 计算机科学与技术学科 网络与信息安全研究室，吉林 延吉 133002）

摘要：AES 针对 IEEE 802.11i 中 CCMP 所采用的高级加密标准 AES 算法的实现较为复杂且对硬件要求较高的情况，对 AES 算法进行了优化改进. 首先对列变换进行了优化，并基于系数的正交化统一了算法加解密过程的运算；然后对轮变换过程进行了简化，并将优化后的列变换系数应用于其中进一步简化了轮变换过程. 将本文的改进算法与原 AES 算法和 S-AES 算法进行对比表明，本文算法在不降低算法本身安全性的前提下，减小了其实现代价，提高了算法的效率.

关键词：无线网络协议；高级加密标准；CCMP 协议；轮变换；AES 改进算法
中图分类号：TP393.1 **文献标识码**：A

Improvement of the AES encryption algorithm and its application in CCMP protocol

LI Jing， LI Yongzhen*
(*Network and Information Security Lab.*, *Dept. of Computer Science & Technology*, *College of Engineering*, *Yanbian University*, *Yanji* 133002, *China*)

Abstract: In view of the Advanced Encryption Standard (AES) algorithm is hard to realize in the CCMP of IEEE 802.11i because of its higher hardware requirements, based on this problem author optimize and improve the algorithm. Firstly, optimize the column transformation and unify the computation process of encryption and decryption base on the orthogonal of coefficient. Then to simplify the wheel transformation process, and apply optimized coefficient of column transformation in it to simplifying the process of wheel transformation. Finally, this paper algorithm compare with AES and S-AES shows that this algorithm reduce the cost of algorithm without reduce security, improved the efficiency of the algorithm.

Key words: IEEE 802.11i; AES; CCMP protocol; wheel transformation; improved AES algorithm

随着无线局域网络的飞速发展，如何更加安全而又高效地使用无线网络越来越受到人们的关注[1]. 无线局域网的信息安全通常包括数据的认证性、完整性、机密性以及可用性. 2004 年，局域网标准委员会发布了新一代的 IEEE 802.11i 无线网络标准，其定义了基于高级加密标准(Advanced Encryption Standard，AES)的全新加密协议 CCMP(Counter Mode/CBC-MAC Protocol，CCMP). CCMP 协议的 CTR/CBC-MAC 模式可以为 WLAN 提供更好的加密、认证、完整性和抗重放攻击的能力，但因协议采用的是 AES 算法，使得数据的运算变得较为复杂，并且加密解密的过程不同，对硬件的要求也较高[2]. 针对这种情况，本文优化了 AES 加密过程的轮变换，统一并简化了加解密过程，提高了算法的实现效率.

收稿日期：2015-07-13

* **通信作者**：李永珍(1971—)，男，博士，副教授，研究方向为网络安全、无线网络协议.

1　CCMP 协议和 AES 标准

1.1　AES 标准

CCMP 协议完全废除了 WEP，采用新型加密标准 AES 作为加密算法来保障信息的安全传输. AES 标准在密码学中又称为 Rijndael 密码算法[3]，AES 密码是一种迭代分组密码，其明文分组长度为 128 位，即 16 字节，密钥长度可为 16、24 或 32 字节(128、192 或 256 位)[4]. 加密过程首先需要确定加密的轮数(N_r)，然后对每一组明文分别进行 N_r 轮变换(10、12 或 14 轮)，秘钥长度越长则所需轮数越多. 每一轮变换由字节替换(BytesSub)、行移位(ShiftRow)、列混合(MixColumn)和加轮密钥(AddRoundKey)4 个步骤组成.

1.2　CCMP 协议

CCMP 协议由 CTR mode 以及 CBC-MAC mode 两个算法组合而成. 先由 AES 算法在计数器模式下加密成数据块，然后对数据块进行计算生成消息认证码以达到数据的加密认证功能[5]. CCMP 协议的具体实现过程如图 1 所示.

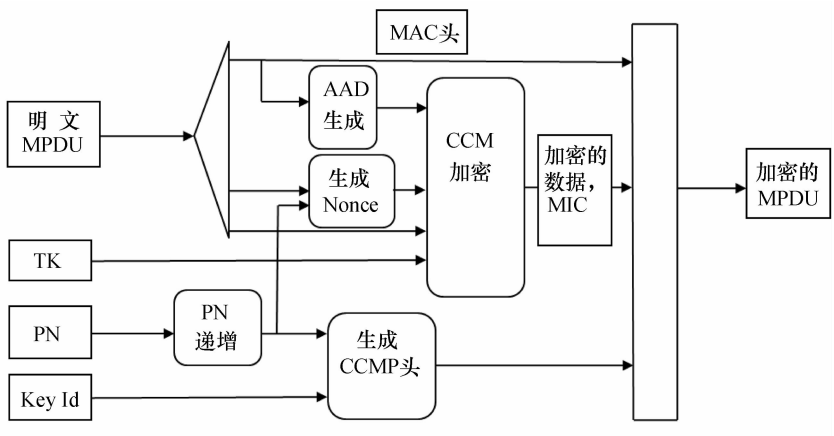

图 1　CCMP 的封装过程

2　基于 AES 轮变换对变换矩阵的改进

AES 算法主要由 4 个变换组合成整个轮变换函数：字节代替变换(BS)、行移位变换(SR)、列混淆变换(MC)、轮密钥加变换(AK)[6]. 为了改进 AES 算法，文献[7]的作者使用一个变换矩阵将行移位变换和列混淆变换合并成一个行列变换，从而提高了算法的运行速度. 但由于作者在合成变换矩阵时所用的列混淆及其逆变换在加解密时所用的算法完全不同，使得算法在加解密过程中不能充分利用资源，导致算法需要不同的软硬件来实现加密或解密. 基于这种情况，本文在文献[7]的基础上优化了变换矩阵，使算法加解密拥有相同的复杂性，进而提高了算法的效率.

2.1　列混淆变换系数矩阵的优化

列混淆变换的正向列混淆变换是对矩阵每列独立地进行操作，每列中的各个字节被相应地映射为一个新值，此值由该列中的 4 个字节通过列混淆函数变换得到. 该变换用矩阵乘法表示为

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} s_{00} & s_{01} & s_{02} & s_{03} \\ s_{10} & s_{11} & s_{12} & s_{13} \\ s_{20} & s_{21} & s_{22} & s_{23} \\ s_{30} & s_{31} & s_{32} & s_{33} \end{pmatrix} = \begin{pmatrix} s'_{00} & s'_{01} & s'_{02} & s'_{03} \\ s'_{10} & s'_{11} & s'_{12} & s'_{13} \\ s'_{20} & s'_{21} & s'_{22} & s'_{23} \\ s'_{30} & s'_{31} & s'_{32} & s'_{33} \end{pmatrix}.$$

乘积矩阵中的每个元素均是行列对应元素的乘积之和,这里的乘法和加法都是定义在有限域 GF(2^8)上的,而列混淆变换的系数的选择是基于算法实现的角度去考虑的,即{01}、{02}、{03},因为这些系数的乘法涉及至多一次移位和一次异或.但由于算法逆向列混淆变换的变换系数跟正向的不一致,从而使得列混淆变换在加解密时需用到不同的软件或固件模块.基于这种情况,本文根据文献[8]中的方法对系数矩阵做了正交化处理使得其逆矩阵等于本身.有限域 GF(2^8)上的正交矩阵有如下性质:

1) 其行向量模为 1,两两正交;列向量模也为 1,且两两正交.

2) 有 $\boldsymbol{A}\boldsymbol{A}^{\mathrm{T}}=\boldsymbol{I}$, $\boldsymbol{A}^{\mathrm{T}}\boldsymbol{A}=\boldsymbol{I}$, $\boldsymbol{I}$ 是单位矩阵(所以对于正交矩阵来说矩阵的转置就是该矩阵的逆).

3) 正交矩阵如有特征值,其特征值只能为 1.

根据以上性质,可得到具有相同系数矩阵的正 / 逆向列混淆的系数矩阵,由此使得在加解密过程中可具有同样的运算量.正交化后的系数矩阵为

$$\boldsymbol{A}=\begin{pmatrix}02 & 01 & 03 & 01\\ 01 & 02 & 01 & 03\\ 03 & 01 & 02 & 01\\ 01 & 03 & 01 & 02\end{pmatrix}=\begin{pmatrix}02 & 01 & 03 & 01\\ 01 & 02 & 01 & 03\\ 03 & 01 & 02 & 01\\ 01 & 03 & 01 & 02\end{pmatrix}^{-1}=\boldsymbol{A}^{-1}.$$

2.2 加密过程的优化

优化以 AES-128 进行 10 轮的轮变换为例,除最后一轮没有进行 MC 外,其余 9 轮都进行了完整的 4 个变换,并且轮变换的顺序依次为 BS、SR、MC、AK.本文对前 9 轮的 SR、MC 变换进行了改进.

假设经过 BS 变换后的状态为

$$\boldsymbol{s}=\begin{pmatrix}s_{00} & s_{01} & s_{02} & s_{03}\\ s_{10} & s_{11} & s_{12} & s_{13}\\ s_{20} & s_{21} & s_{22} & s_{23}\\ s_{30} & s_{31} & s_{32} & s_{33}\end{pmatrix},$$

经过 SR、MC 变换后,矩阵的状态为

$$\boldsymbol{s}'=\begin{pmatrix}s'_{00} & s'_{01} & s'_{02} & s'_{03}\\ s'_{10} & s'_{11} & s'_{12} & s'_{13}\\ s'_{20} & s'_{21} & s'_{22} & s'_{23}\\ s'_{30} & s'_{31} & s'_{32} & s'_{33}\end{pmatrix}.$$

对矩阵进行展开:

$$\boldsymbol{s}'=\begin{pmatrix}s'_{00} & s'_{01} & s'_{02} & s'_{03}\\ s'_{10} & s'_{11} & s'_{12} & s'_{13}\\ s'_{20} & s'_{21} & s'_{22} & s'_{23}\\ s'_{30} & s'_{31} & s'_{32} & s'_{33}\end{pmatrix}=\begin{pmatrix}02 & 01 & 03 & 01\\ 01 & 02 & 01 & 03\\ 03 & 01 & 02 & 01\\ 01 & 03 & 01 & 02\end{pmatrix}\begin{pmatrix}s_{00} & s_{01} & s_{02} & s_{03}\\ s_{11} & s_{12} & s_{13} & s_{10}\\ s_{22} & s_{23} & s_{20} & s_{21}\\ s_{33} & s_{30} & s_{31} & s_{32}\end{pmatrix}.$$

矩阵中的每个元素计算如下:

$$s'_{00}=2s_{00}+1s_{11}+3s_{22}+1s_{33},\quad s'_{01}=2s_{01}+1s_{12}+3s_{23}+1s_{30},$$
$$s'_{02}=2s_{02}+1s_{13}+3s_{20}+1s_{31},\quad s'_{03}=2s_{03}+1s_{10}+3s_{21}+1s_{32},$$
$$s'_{10}=1s_{00}+2s_{11}+1s_{22}+3s_{33},\quad s'_{11}=1s_{01}+2s_{12}+1s_{23}+3s_{30},$$
$$s'_{12}=1s_{00}+2s_{13}+1s_{20}+3s_{31},\quad s'_{13}=1s_{03}+2s_{10}+1s_{21}+3s_{32},$$
$$s'_{20}=3s_{00}+1s_{11}+2s_{22}+1s_{33},\quad s'_{21}=3s_{01}+1s_{12}+2s_{23}+1s_{30},$$
$$s'_{22}=3s_{02}+1s_{13}+2s_{20}+1s_{31},\quad s'_{23}=3s_{03}+1s_{10}+2s_{21}+1s_{32},$$

$s'_{30}=1s_{00}+3s_{11}+1s_{22}+2s_{33}$，　$s'_{31}=1s_{01}+3s_{12}+1s_{23}+2s_{30}$，

$s'_{32}=1s_{02}+3s_{13}+1s_{20}+2s_{31}$，　$s'_{33}=1s_{03}+3s_{10}+1s_{21}+2s_{32}$.

将其写成一个向量变换的形式为

$$\begin{pmatrix} s'_{00} \\ s'_{01} \\ s'_{02} \\ s'_{03} \\ s'_{10} \\ s'_{11} \\ s'_{12} \\ s'_{13} \\ s'_{20} \\ s'_{21} \\ s'_{22} \\ s'_{23} \\ s'_{30} \\ s'_{31} \\ s'_{32} \\ s'_{33} \end{pmatrix} = \begin{pmatrix} 2&0&0&0&0&1&0&0&0&0&3&0&0&0&0&1 \\ 0&2&0&0&0&0&1&0&0&0&0&3&1&0&0&0 \\ 0&0&2&0&0&0&0&1&3&0&0&0&0&1&0&0 \\ 0&0&0&2&1&0&0&0&0&3&0&0&0&0&1&0 \\ 1&0&0&0&0&2&0&0&0&0&1&0&0&0&0&3 \\ 0&1&0&0&0&0&2&0&0&0&0&1&3&0&0&0 \\ 0&0&1&0&0&0&0&2&1&0&0&0&0&3&0&0 \\ 0&0&0&1&2&0&0&0&0&1&0&0&0&0&3&0 \\ 3&0&0&0&0&1&0&0&0&0&2&0&0&0&0&1 \\ 0&3&0&0&0&0&1&0&0&0&0&2&1&0&0&0 \\ 0&0&3&0&0&0&0&1&2&0&0&0&0&1&0&0 \\ 0&0&0&3&1&0&0&0&0&2&0&0&0&0&1&0 \\ 1&0&0&0&0&3&0&0&0&0&1&0&0&0&0&2 \\ 0&1&0&0&0&0&3&0&0&0&0&1&2&0&0&0 \\ 0&0&1&0&0&0&0&3&1&0&0&0&0&2&0&0 \\ 0&0&0&1&3&0&0&0&0&1&0&0&0&0&2&0 \end{pmatrix} \begin{pmatrix} s_{00} \\ s_{01} \\ s_{02} \\ s_{03} \\ s_{10} \\ s_{11} \\ s_{12} \\ s_{13} \\ s_{20} \\ s_{21} \\ s_{22} \\ s_{23} \\ s_{30} \\ s_{31} \\ s_{32} \\ s_{33} \end{pmatrix}.$$

再将行移位变换和列混淆变换合并为行列变换，此操作过程为 $\boldsymbol{S}'=\boldsymbol{R}\otimes\boldsymbol{S}$（$\boldsymbol{R}$ 是该变换中的 16×16 的变换矩阵），整个加密过程的简化如图 2 所示.

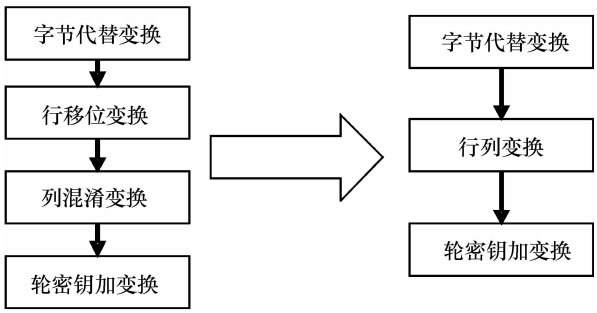

图 2　优化前后轮变换比照

3　算法优化结果分析

3.1　算法实现代价分析

CCMP 协议作为 IEEE802.11i 提出的一种新的加密机制，无法在原有设备的基础上通过直接升级来实现（需要更换硬件设备），而它又是 IEEE802.11i 机制中必须实现的安全机制. 本文改进后的算法其行列变换的正向运算与逆向运算是一致的，因此可以将行列变换和逆行列变换集成在同样的硬件上，较原算法和 S-AES 算法相比减少了算法的实现代价.

3.2　算法实现效率与安全性分析

本文提出的改进型 AES 算法合并了轮变换中的行移位变换和列混淆变换，用函数的复合方式可把

一轮加密过程简单地表示为 AK→BS→SM(行列变换)→AK. 以 128 位的本文算法为例,其每轮行列变换在有限域 GF(2^8)上要进行 2 次的乘法操作,在完整进行 10 轮变换后,正/逆行列变换的运算量为 40 次乘法,单以行列变换的加解密运算量来说,较原 AES 算法 140 次乘法的计算量有了大幅降低;与 S-AES 算法(采用 AK→MC→SR→NS(半字节代替变换)→AK 的模式)相比,本文的改进型 AES 算法减少了一个运算过程,而且没有改变原来的安全性(S-AES 算法的安全性有所降低).

4 结论

本文在分析 CCMP 协议中 AES 算法的基础上,提出了改进型 AES 算法:1)对算法的正向列混淆和逆向列混淆的变换系数进行了同一化处理,避免了算法的加解密不同;2)对算法的轮变换过程进行了简化,并将改进后的列混淆变换系数应用于其中,减少了算法的轮变换步骤. 与原 AES 算法和 S-AES 算法进行对比表明,本文算法在不降低算法本身安全性的前提下,减小了其实现代价,提高了算法的效率. 由于本文只优化了算法的行移位和列混淆函数,未对字节替换函数改进,今后将对此做进一步研究.

参考文献:

[1] 朱敏. 无线局域网安全协议 IEEE 802.11i 的分析与研究[D]. 苏州:苏州大学,2005:1-4.
[2] IEEE 802.11 Working Group. IEEE Standard for Information Technology-Telecommunications and Information Exchange between Systems-Local and Metropolitan Area Networks-Specific Requirements-Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments[S]. IEEE Std, 2010: Part 11.
[3] 刘景美. 现代密码算法分析与研究[D]. 西安:西安电子科技大学,2006:15-27.
[4] 任伟. 无线网络安全[M]. 北京:电子工业出版社,2011:11-30.
[5] 邓达. 无线局域网安全性问题研究与改进[D]. 成都:电子科技大学,2007:50-56.
[6] William S. 密码编码学与网络安全[M]. 王张宜,杨敏,杜瑞颖译. 5 版. 北京:电子工业出版社,2012:104-117.
[7] 贾旭. AES 算法的安全性分析及其优化改进[D]. 长春:吉林大学,2010:30-39.
[8] 周李京. 基于有限域上正交矩阵构造最佳扩散层[D]. 西安:西安电子科技大学,2012:19-27.
[9] Mohammad A Musaa, Edward F Schaefer. A simplified AES algorithm and its linear and differential cryptanalyses [J]. Taylor & Francis, 2010,27(2):148-177.