

基于密码结构的扩散层构造

李鹏飞^{1,2}

(1. 中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093;
2. 中国科学院大学网络空间安全学院, 北京 100049)

摘要: 以分组密码扩散层为研究对象, 根据轻量级分组密码的特点, 基于2种密码结构构造轻量级扩散层, 分别是基于Feistel结构构造面向软件实现的扩散层和基于LFSR构造面向硬件实现的扩散层。利用三轮Feistel结构, 轮函数采用基于循环移位和异或的线性变换, 构造出作用在8个4 bit和8 bit S盒上分支数为7的轻量级对合扩散层。基于LFSR构造出作用在4个4 bit和8 bit S盒上的次最优扩散层和作用在8个4 bit和8 bit S盒上分支数为7的扩散层。另外, 利用LFSR构造出了6、7、8维MDBL矩阵以及16、18、32维分支数分别为7、7、12的大维数二进制矩阵。研究结果在分组密码的设计方面具有较高的应用价值。

关键词: 分组密码; 扩散层; Feistel结构; 反馈移位寄存器; MDBL矩阵

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00170

Construction of diffusion layers based on cipher structures

LI Peng-fei^{1,2}

(1. The State Key Lab of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China;
2. School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Taken diffusion layers of block cipher algorithms as the research object, lightweight diffusion layers were constructed by two cipher structures based on the characteristics of diffusion layers of lightweight block cipher algorithms, which were the construction of software-oriented diffusion layers based on Feistel structure and the construction of hardware-oriented diffusion layers based on LFSR. Lightweight involution diffusion layers with branch numbers 7 over eight 4-bit and 8-bit S-boxes were constructed by 3-round Feistel structure and the round functions adopt linear transformations with rotation and XORs. Some suboptimal diffusion layers over four 4 bit and 8 bit S-boxes and diffusion layers with branch numbers 7 over eight 4 bit and 8 bit S boxes based on LFSR were constructed. In addition, 6, 7, 8 dimension MDBL matrices and many 16, 18, 32 dimension binary matrices with big dimension and branch numbers 7, 7, 12 based on LFSR were constructed. The experimental results have high practical significance in realm of the design of block cipher algorithms.

Key words: block cipher, diffusion layer, Feistel structure, linear feedback shift register, MDBL matrix

1 引言

随着物联网 (IoT, Internet of things) 技术的快速发展, 射频识别 (RFID, radio frequency

identification) 标签、无线传感器网络 (WSN, wireless sensor network)、个人数字助理 (PDA, personal digital assistant) 终端等微型嵌入式设备越来越发达, 它们广泛应用于人们生活的方方面面

收稿日期: 2017-04-07; 修回日期: 2017-05-20。通信作者: 李鹏飞, lipengfei@iie.ac.cn

基金项目: 国家自然科学基金资助项目 (No.61379142)

Foundation Item: The National Natural Science Foundation of China (No.61379142)

面,将任何物品与互联网连接起来,实现物与物、物与人、物与网络的信息交互,达到万物的智能化识别、定位、跟踪、监控和管理。然而,由于这些微型嵌入式设备只有有限的计算能力、通信能力、存储空间和能量来源,消耗更多软硬件资源、运行速度较差的传统密码算法(如 DES^[1]、AES^[2]、SM4^[3]等)已很难适用,给安全带来了极大的挑战,为了保障用户的数据和隐私安全,轻量级密码学应运而生,轻量级是相对于普通密码提供的安全保护级别和实现所需资源而言的,旨在安全性、面积功耗、时延速度等多个方面实现较好的折中。近几年,随着物联网的安全问题逐渐成为重要的研究课题,研究者相继提出了许多轻量级密码算法,包括轻量级分组密码、Hash 函数、认证加密算法(如 HIGHT^[4]、PRESENT^[5]、CLEFIA^[6]、LED^[7]、LBlock^[8]、PRINCE^[9]、SIMON 和 SPECK^[10]、Zorro^[11]、SIMECK^[12]、PHOTON^[13]、PRIMATES^[14])等,这些算法的典型特点是:在严格规定的硬件资源条件下,能够达到一定的安全级别。

分组密码因其加解密速度快,便于软硬件实现和易于标准化等特点,成为轻量级密码学研究的重点,受到了学者的广泛关注。扩散层作为分组密码的一个重要部件,它的设计不但影响分组密码算法的安全性,而且影响分组密码在软硬件中的实现效率。一方面,扩散层为分组密码提供主要的扩散性,在抵抗差分分析和线性分析中扮演着重要的角色;另一方面,实现相同的安全性指标时,精心选择的扩散层可以显著提升分组密码算法在软硬件中的实现效率。目前,扩散层不仅是分组密码算法的必备部件,也在其他对称密码体制(如 Hash 函数、认证加密算法)中有广泛应用。扩散层的安全性能主要由文献[2]中提出的分支数的概念衡量,它是度量连续两轮差分 and 线性特征中活跃 S 盒数目下界的一个重要指标,利用它可以有效地计算差分特征概率和线性逼近概率的上界,估计密码算法的安全性。扩散层的分支数越小,分组密码越容易遭受差分分析、线性分析以及一些未知分析方法的攻击;反之,分支数越大,扩散层的扩散效果越好、安全性越好,因此,分组密码设计者面临的一大挑战是如何设

计分支数大、软硬件实现代价低的扩散层,特别是在资源极端受限的物联网环境下。近几年,分组密码设计与改进的重点以及有所创新的地方主要集中在扩散层,有很多研究成果。

MDS (maximum distance separable) 矩阵可以保证分支数达到最大,扩散性能达到最优,从而可以最大限度地保证密码算法在差分 and 线性分析下的安全性。许多密码算法都将 MDS 矩阵作为扩散层使用,分组密码如 SHARK^[15]、Rijndael^[2]、Twofish^[16,17]、Square^[18]、Anubis^[19]、Khazad^[20]、FOX^[21]、CLEFIA、LED 等,流密码如 MUGI^[22],Hash 函数如 Maelstrom^[23],Grøstl^[24],WHIRLPOOL^[25]和 PHOTON 轻量级 Hash 函数族^[13]等。尽管这么多算法的扩散层都采用 MDS 矩阵,但不可否认,MDS 矩阵在提供最优扩散性的同时,也使算法的效率有所降低,它们通常需要较长的执行时间,消耗更多的软硬件资源,例如,硬件实现 AES 所需的最少电路门数为 2 400 等效门数^[26](GE, gate equivalents),其中仅列混淆部分就需要 263 GE。关于 MDS 矩阵的研究也有很多^[27-39],这些 MDS 矩阵主要面向硬件实现,所需的异或个数极少,但没有过多地考虑软件实现效率。

分组密码算法设计中还经常采用 MDBL (maximum distance binary linear) 矩阵作为扩散层使用,如 ARIA^[40]、Camellia^[41]、E2^[42]、MIBS^[43]、Midori^[44]、FIDES^[45]、Minalpher^[46]等密码算法中的扩散层都是使用 MDBL 矩阵,MDBL 矩阵是二进制矩阵中具有最大分支数的矩阵^[47],它们相对于 MDS 矩阵而言具有较高的软硬件实现效率,实现过程只需要异或操作,大大降低了软硬件资源消耗。表 1 给出了一些采用 MDBL 矩阵作为扩散层使用的密码算法。

相对于 MDS 矩阵,关于 MDBL 矩阵的研究比较少^[48,49],Kang 等^[50]证明了可逆 8×8 二进制矩阵的分支数小于等于 5,即具有分支数 5 的 8×8 二进制矩阵是最优的。Kwon 等^[40]证明了可逆 16×16 二进制矩阵的最大分支数为 8,同时构造了许多分支数为 8 的 16×16 对合二进制矩阵,并且使用一些数学方法找到了矩阵乘积的形式,使二进制矩阵在 8 bit 和 32 bit 处理器上软件的实现

表 1 一些采用 MDBL 矩阵作为扩散层的密码算法

密码算法	矩阵维数	扩散层作用在 $\mathbb{F}_2^m$ 上	对合性	分支数	汉明重量
ARIA	16	$\mathbb{F}_2^8$	是	8	112
Camellia	8	$\mathbb{F}_2^8$	否	5	44
E2	8	$\mathbb{F}_2^8$	否	5	44
MIBS	8	$\mathbb{F}_2^4$	否	5	44
Midori	4	$\mathbb{F}_2^4$ 或 $\mathbb{F}_2^8$	是	4	12
FIDES	4	$\mathbb{F}_2^5$ 或 $\mathbb{F}_2^6$	是	4	12
Minalpher	4	$\mathbb{F}_2^4$	是	4	12

效率大大提高。

Kanda 等^[51]通过搜索所有候选矩阵找到 10 080 个具有分支数 5 的 8×8 二进制矩阵, 这些矩阵的汉明重量均为 44, 其中, 4 个列(行)向量的汉明重量为 6, 另外 4 个列(行)向量的汉明重量为 5, 这些结果对 E2 和 Camellia 算法扩散层的设计具有一定的指导意义。

文献[52]提出了一种统一化的方法构造所有具有最大分支数 5 的 8×8 二进制矩阵, 并且总结了它们的特征, 发现这些矩阵的汉明重量集中在 33~44。文献[53,54]采用组合小矩阵的方式构造大维数的二进制矩阵 (16×16 或 32×32 矩阵)。文献[55]基于 4×4 的 Hadamard 矩阵和循环矩阵构造带有一个固定点并且分支数为 7 的 16×16 二进制矩阵。

关于 MDBL 矩阵的研究, 研究者很少提及二进制矩阵的软硬件实现, Dehnavi 等^[56]提出一种特殊类型(按位异或)的线性变换, 这些线性变换可以表示成具有最大分支数的二进制矩阵的形式, 可以有效地在软硬件上实现。

Feistel 和线性反馈移位寄存器(LFSR, linear feedback shift register)是 2 种重要的密码结构。Feistel 结构不仅广泛应用于对称密码算法(如 DES、LBlock、SIMON 和 SIMECK)中, 而且也被用来构造密码算法的关键部件——S 盒和扩散层, 如 CRYPTON 算法^[57]、ZUC^[58]、CS-Cipher^[59]均采用三轮 Feistel 结构构造 S 盒, MISTY^[60]算法也使用三轮 Feistel 结构构造它的非线性部分 FI, 文献[61]对三轮 Feistel 结构构造的 S 盒做了进一步研究, 文献[62]使用三轮 Feistel 结构和 MISTY

结构构造轻量级 S 盒。同时, 文献[63]研究了利用 Feistel 结构构造最优二进制矩阵, 其轮函数采用比特置换。

对称密码中的流密码广泛应用于信息加密、分布式计算、码分多址(CDMA, code division multiple access)系统等领域。流密码技术的核心是构造性能优良的密钥流, 线性反馈移位寄存器是一种基本的密钥流生成器, 由于采用逻辑运算, 具有原理简单、计算速度快、便于硬件实现等优点, 成为构造密钥流生成器的重要部件之一^[64]。正是由于 LFSR 的诸多优点, 有学者将 LFSR 应用于分组密码扩散层的构造上, 文献[7,16,29,30]设计的迭代型扩散层中就用到了 LFSR。

本文结合 Feistel 和 LFSR 这 2 种密码结构的优势, 将其用来构造分组密码的扩散层, 首先研究了基于 Feistel 结构构造轻量级扩散层, 轮函数采用基于循环移位和异或的线性变换, 利用三轮 Feistel 结构构造出了作用在 8 个 4 bit 和 8 bit S 盒上的分支数为 7 的轻量级对合扩散层; 接着研究了基于 LFSR 构造轻量级扩散层, 使用 LFSR 构造出了作用在 n 个 m 比特 S 盒上($n=4, 8; m=4, 8$)的轻量级扩散层和 6、7、8 维 MDBL 矩阵以及分支数分别为 7、7、12 的 16、18、32 维二进制矩阵。

2 预备知识

本节给出分支数的定义和 Feistel 结构以及 LFSR 的基础知识。

2.1 分支数

定义 1 假设 $\theta: (\mathbb{F}_2^m)^n \rightarrow (\mathbb{F}_2^m)^n, X \rightarrow \theta(x) = Ax^T$ 为如下形式的线性变换(扩散层)。

$$\theta(\mathbf{x}) = \mathbf{Ax}^T = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}$$

其中, $\mathbf{x} = (x_1, x_2, \dots, x_n)^T$, $x_i \in \mathbb{F}_2^m$, $i = 1, \dots, n$ 。一般情况下, n 是 S 盒的个数, m 是 S 盒的比特长度。扩散层 θ 的系数矩阵为 $\mathbf{A} = (a_{ij})_{n \times n}$, $a_{ij} \in \mathbb{F}_2^{\tilde{m}}$, $1 \leq i, j \leq n$, 若 $\tilde{m} > 1$ 时, 有 $\tilde{m} = m$ 。矩阵 $\mathbf{A}$ 的分支数定义为^[53]

$$\beta(\mathbf{A}) = \min \{ wt(\mathbf{x}) + wt(\mathbf{Ax}^T) \mid \mathbf{x} \in (\mathbb{F}_2^m)^n, \mathbf{x} \neq \mathbf{0} \} \quad (1)$$

也称为扩散层 θ 的分支数, 其中 $wt(\mathbf{x})$ 表示 $\mathbf{x}$ 中非零分量的个数。

由定义 1 可知, 扩散层的分支数 $\beta \leq n+1$ 。

定义 2 将分支数达到最大 $(n+1)$ 时的扩散层称为最优扩散层, 对应的矩阵 $\mathbf{A} = (a_{ij})_{n \times n}$ 称为 MDS 矩阵, 其中, $a_{ij} \in \mathbb{F}_2^{\tilde{m}}$, $1 \leq i, j \leq n$, $\tilde{m} > 1$ 。

定义 3 将分支数达到次最大 n 时的扩散层称为次最优扩散层, 对应的矩阵 $\mathbf{A} = (a_{ij})_{n \times n}$ 称为次 MDS 矩阵, 其中, $a_{ij} \in \mathbb{F}_2^{\tilde{m}}$, $1 \leq i, j \leq n$, $\tilde{m} > 1$ 。

定义 4 若矩阵 $\mathbf{A} = (a_{ij})_{n \times n}$ 分支数达到最大, 则称矩阵 $\mathbf{A}$ 为 MDBL 矩阵, 其中, $a_{ij} \in \mathbb{F}_2$, $1 \leq i, j \leq n$ 。

2.2 Feistel 结构

Feistel 结构^[65]广泛应用于对称密码算法中, 许多分组密码算法都采用 Feistel 结构, 其中最著名的是由 IBM 公司在 20 世纪 70 年代设计的 DES 算法。图 1 给出了 Feistel 密码结构的加解密过程。加密算法的输入是长度为 $2w$ bit 的明文分组和用户密钥 K , 明文分组被分为等长 (w bit) 的两部分: LE_0 和 RE_0 , 这两部分数据经过 n 轮迭代后组合成密文分组, 第 i 轮迭代的输入 LE_{i-1} 和 RE_{i-1} 来自于上一轮迭代的输出, 第 i 轮迭代的轮密钥 K_i 是由用户密钥 K 推导出来的, 一般地, K_i 不同于 K , 并且 K_i 之间也互不相同。

Feistel 密码结构代替操作作用在数据的左半部分, 整个结构通过将轮函数 F 作用于数据的右半部分后, 与左半部分数据进行异或完成。Feistel 结构每轮迭代都有相同的轮变换, 但每轮的轮密钥 K_i 不同, 也就是说, 轮函数 F 是 w bit

长的右半分组数据以及 y bit 长的轮密钥函数, 第 i 轮轮函数的输出为 w bit 长的值 $F(RE_{i-1}, K_i)$ 。轮函数操作后, $F(RE_{i-1}, K_i)$ 与左半部分数据异或得到第 $i+1$ 轮右半部分数据 RE_i , 第 $i+1$ 轮的左半部分数据 LE_i 是第 i 轮的右半部分数据。在最后一轮迭代之后有一个交换, 用以抵消在最后一轮迭代中的左右部分数据的交换。

Feistel 密码结构的解密过程本质上和加密过程一致, 其规则如下: 将密文作为算法的输入, 但逆序使用轮密钥 K_i , 也就是说, 第一轮使用 K_n , 第二轮使用 K_{n-1} , 直到最后一轮使用 K_1 。基于以上特点, Feistel 结构只需实现一个算法便可以完成加密和解密操作, 大大简化了硬件实现的电路和软件实现的代码量。

2.3 LFSR

反馈移位寄存器由两部分组成: 移位寄存器和反馈函数, 移位寄存器是一个比特序列, 它的长度用比特表示, 若移位寄存器的长度为 n bit, 则称为 n 级移位寄存器。图 2 给出了二元域 $GF(2)$ 上的 n 级反馈移位寄存器, 其中, n 个寄存器从右至左依次称为第 1, 2, $\dots$, n 级。 $f(x_1, x_2, \dots, x_n)$ 为反馈函数, 它是 n 个变量的布尔函数 $GF(2^n) \rightarrow GF(2)$ 。 n 级反馈移位寄存器的工作原理是: 当一个时钟脉冲到来时, 第 i 级寄存器的内容传送给第 $i-1$ 级寄存器 ($i = 2, 3, \dots, n$), 第 1 级寄存器的内容为反馈移位寄存器的输出。反馈函数 $f(x_1, x_2, \dots, x_n)$ 的值传送给第 n 级寄存器, 可以看出, 第 n 级寄存器的值是根据其他寄存器的值计算得到的。反馈移位寄存器的输出序列 (称为反馈移位寄存器序列) 为 $k_0, k_1, k_2, \dots, k_n, \dots$ 。

定义 5 如果一个 n 级反馈移位寄存器的反馈函数是线性函数

$$f(x_1, x_2, \dots, x_n) = c_0 x_1 + c_1 x_2 + \dots + c_{n-2} x_{n-1} + c_{n-1} x_n \quad (c_i \in \mathbb{F}_2, 0 \leq i \leq n-1)$$

则称该反馈移位寄存器为线性反馈移位寄存器, 输出序列称为线性反馈移位寄存器序列, 记为 LFSR 序列。LFSR 只有一种运算: 异或运算, 系数 $c_0, c_1, \dots, c_{n-1}$ 不全为 0, 若 $c_0 \neq 0$, 则称 LFSR 为非退化的, 若 $c_0 = 0$, 则称为退化的 LFSR。图 3 给出了 n 级 LFSR 的结构图。

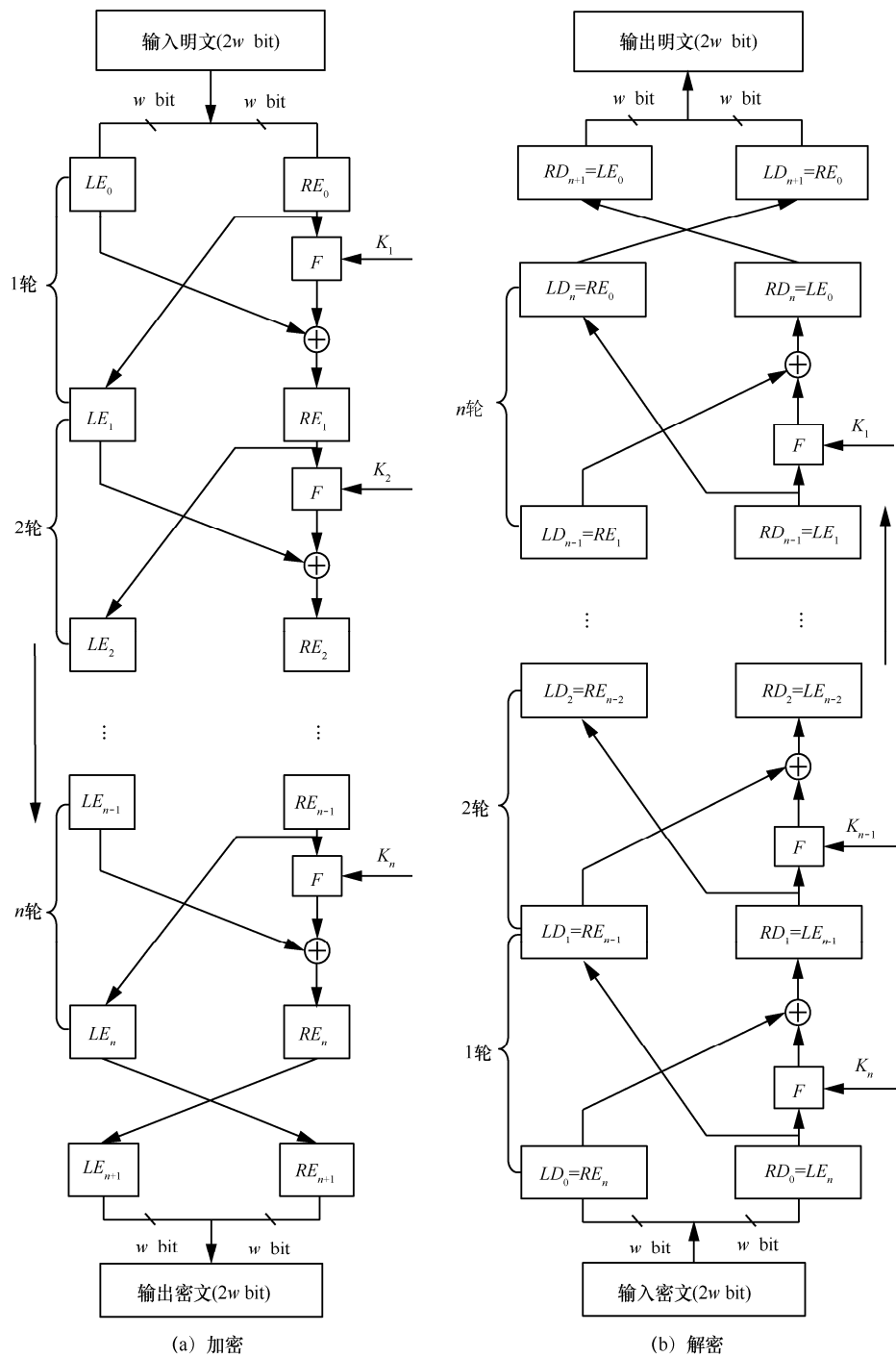


图 1 Feistel 密码结构加解密过程

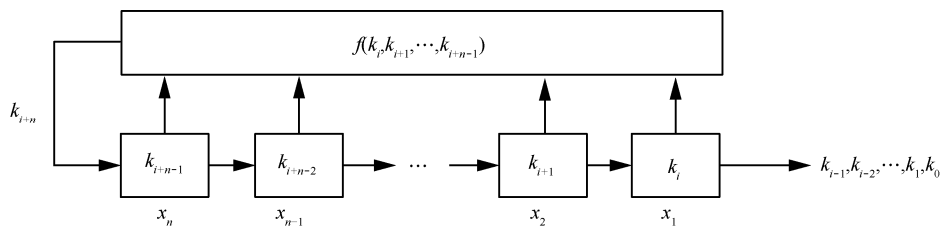


图 2 反馈移位寄存器基本结构

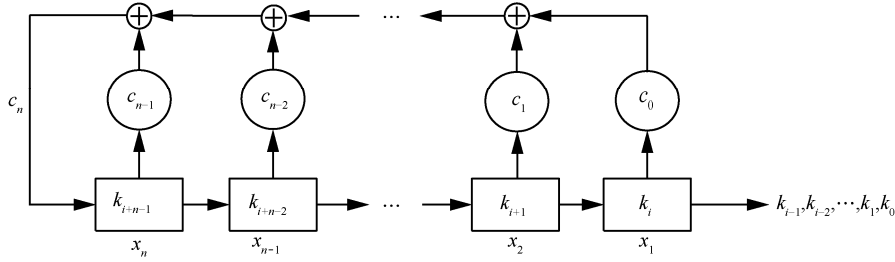


图3 n级LFSR结构

n 级 LFSR 可以由它的状态转移矩阵唯一表示, n 级 LFSR 矩阵可以由状态转移矩阵的 n 次方计算得到, n 级 LFSR 的状态转移矩阵 S_i^n 如下。

$$S_i^n = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & \cdots & 0 & \beta_{n-1} \\ 1 & 0 & 0 & 0 & 0 & \cdots & 0 & \beta_{n-2} \\ 0 & 1 & 0 & 0 & 0 & \cdots & 0 & \beta_{n-3} \\ 0 & 0 & 1 & 0 & 0 & \cdots & 0 & \beta_{n-4} \\ 0 & 0 & 0 & 1 & 0 & \cdots & 0 & \beta_{n-5} \\ 0 & 0 & 0 & 0 & 1 & \cdots & 0 & \beta_{n-6} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \cdots & 1 & \beta_0 \end{pmatrix}$$

其中, $\beta_{n-1}\beta_{n-2}\beta_{n-3}\beta_{n-4}\beta_{n-5}\beta_{n-6}\cdots\beta_0$ 为 i 的二进制表示, 即 $(i)_2 = \beta_{n-1}\beta_{n-2}\beta_{n-3}\beta_{n-4}\beta_{n-5}\beta_{n-6}\cdots\beta_0$ 。

例如, 当 $n=8, i=150$ 时, 状态转移矩阵 S_{150}^8 为

$$S_{150}^8 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

其中, S_{150}^8 的最后一列: 10010110 为 150 的二进制表示。计算 S_{150}^8 的 8 次方 $(S_{150}^8)^8 = M_{150}^8$, 得到 8 维 LFSR 矩阵 M_{150}^8 。

$$M_{150}^8 = \begin{pmatrix} 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 \end{pmatrix}$$

3 基于 Feistel 结构构造扩散层

本节使用三轮 Feistel 结构构造分组密码的扩散层, 并且主要集中在对合扩散层的构造上。假设 $X = (X_L, X_R) \in (\mathbb{F}_2^m)^{2n}$, $X_L, X_R \in (\mathbb{F}_2^m)^n$, $Y = (Y_L, Y_R) \in (\mathbb{F}_2^m)^{2n}$, 其中 $Y_L, Y_R \in (\mathbb{F}_2^m)^n$ (m 是 S 盒的比特长度, n 是 S 盒的个数), 基于 Feistel 结构的扩散层如图 4 所示, 这类扩散层可以由矩阵表示为

$$M = \begin{pmatrix} 0 & I \\ I & 0 \end{pmatrix} \begin{pmatrix} P_r & I \\ I & 0 \end{pmatrix} \cdots \begin{pmatrix} P_1 & I \\ I & 0 \end{pmatrix}$$

其中, 每一个分块矩阵 $P_i (1 \leq i \leq r)$ 为 $\mathbb{F}_2^m$ 上的大小为 $n \times n$ 的矩阵, I 为 $n \times n$ 大小的单位矩阵。为简化起见, 用 $[P_1, P_2, \dots, P_r]$ 表示矩阵 M , 那么根据第 2.2 节对 Feistel 结构的介绍, 可知矩阵 M 的逆矩阵为 $M^{-1} = [P_r, P_{r-1}, \dots, P_1]$ 。

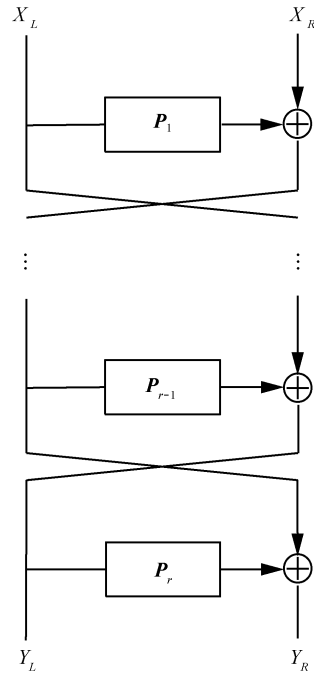


图4 r轮Feistel结构构造的扩散层

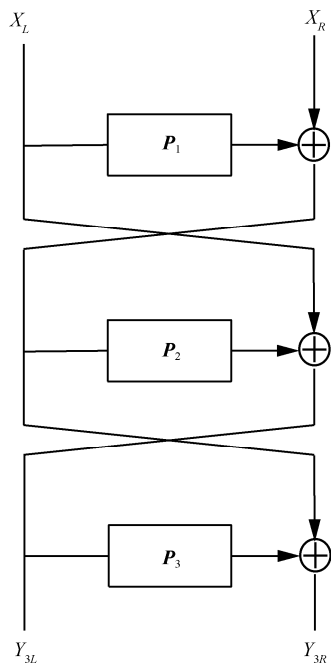


图5 三轮 Feistel 结构构造的扩散层

基于 Feistel 结构构造轻量级扩散层的特点如下。一方面, 基于 Feistel 结构构造的扩散层逆变换和其本身具有相同的结构, 只需简单地按顺序反向使用轮函数即可实现逆变换。这种结构使扩散层和它的逆变换拥有相同的异或数, 特别地, 对合的扩散层可以使用相同的代码和电路实现加密和解密, 大大节省了软硬件资源, 当轮函数是对称的时候, 矩阵 M 为对合矩阵, 如 $[P_1, P_2, P_1]$ 和 $[P_1, P_2, P_2, P_1]$ 。另一方面, Feistel 结构简单, 它实际上是利用小矩阵构造大矩阵, 如果采用简单的轮函数, 将会构造出十分容易实现的扩散层。为了构造出既安全又高效的扩散层, 限定采用三轮 Feistel 结构, 并且只搜索对合扩散层。图 5 给出了三轮 Feistel 结构构造的扩散层, 矩阵 $M = [P_1, P_2, P_3]$, 逆矩阵为 $M^{-1} = [P_3, P_2, P_1]$, 对合扩散层要求轮函数 P_1 和 P_3 相同。下面给出作用在 $(\mathbb{F}_2^m)^{2n}$ 上的基于三轮 Feistel 结构构造的轻量级对合扩散层。

本节研究使用循环移位和异或线性变换作为三轮 Feistel 的轮函数构造轻量级对合扩散层。基于 $(\mathbb{F}_2^m)^n$ 上的循环移位和异或运算的线性变换 $l(x): (\mathbb{F}_2^m)^n \rightarrow (\mathbb{F}_2^m)^n$, 构造作用在 $(\mathbb{F}_2^m)^{2n}$ 上的扩散层 $L(X): (\mathbb{F}_2^m)^{2n} \rightarrow (\mathbb{F}_2^m)^{2n}$, 即轮变换 P_i ($i=1, 2, 3$) 为基于循环移位和异或运算的线性变换:

$$P_i(x) = \bigoplus_{j=1}^k (x \lll b_j), \text{ 共含有 } k \text{ 项, 并且 } 0 \leq b_j \leq$$

$mn-1$, $x \in (\mathbb{F}_2^m)^n$ 。为了节省软硬件实现开销, 利用 3 项及以下的基于循环移位和异或运算的线性变换构造分组密码的扩散层, 即 $1 \leq k \leq 3$, 并且只考虑对合扩散层。由于实际密码算法中 8 个 4 bit 和 8 bit 的 S 盒比较常见, 所以这里令 $n=4$; $m=4, 8$ 。对合扩散层矩阵为 $M = [P_1, P_2, P_3]$, $P_3 = P_1$ 。为简便起见, 令轮变换为

$$P_i(x) = \bigoplus_{j \in S_i} (x \lll j), i=1, 2, 0 \leq j \leq mn-1, x \in (\mathbb{F}_2^m)^n。$$

1) $(\mathbb{F}_2^4)^8$ 上构造对合扩散层

当 $n=4, m=4$ 时, 穷搜了 3 项及以下循环移位和异或运算的线性变换作为轮函数的三轮 Feistel 的所有可逆扩散层, 没有找到 MDS 矩阵, 得到最好的作用在 $(\mathbb{F}_2^4)^8$ 上的对合扩散层分支数为 7, 共找到 1 248 个这样的对合扩散层, 并且每一个轮函数均为 3 项 ($k=3$)。表 2 给出了部分分支数为 7 的对合扩散层 $L(X)$ 的例子。

表2 $(\mathbb{F}_2^4)^8$ 上构造分支数为 7 的对合扩散层 $L(X)$

S_1	S_2
{0, 4, 9}	{0, 3, 7}
{0, 4, 9}	{0, 10, 15}
{1, 5, 9}	{0, 7, 11}
{1, 5, 9}	{1, 2, 14}
{2, 6, 13}	{1, 8, 11}
{2, 6, 13}	{2, 9, 15}
{5, 9, 13}	{0, 1, 4}
{5, 9, 13}	{0, 2, 14}
{6, 10, 14}	{0, 1, 5}
{6, 10, 14}	{0, 3, 7}

2) $(\mathbb{F}_2^8)^8$ 上构造对合扩散层

当 $n=4, m=8$ 时, 搜索了部分三轮 Feistel 结构构造的可逆扩散层, 并且轮函数采用 3 项及以下的循环移位和异或运算的线性变换, 没有找到 MDS 矩阵, 找到部分作用在 $(\mathbb{F}_2^8)^8$ 上的分支数为 7 的对合扩散层, 表 3 给出了部分分支数为 7 的对合扩散层 $L(X)$ 的例子。

表 3 $(\mathbb{F}_2^8)^8$ 上构造分支数为 7 的对合扩散层 $L(X)$

S_1	S_2
{6, 14, 22}	{6, 14, 23}
{6, 14, 22}	{6, 14, 25}
{6, 14, 22}	{6, 14, 27}
{6, 14, 23}	{8, 13, 28}
{6, 14, 23}	{8, 13, 30}
{6, 21, 29}	{6, 13, 29}
{6, 21, 29}	{6, 13, 31}
{6, 21, 29}	{6, 14, 17}
{6, 22, 30}	{6, 14, 15}
{6, 22, 30}	{23, 24, 31}
{6, 22, 30}	{23, 25, 31}

4 基于 LFSR 构造扩散层

本节采用 n 级 LFSR 构造作用在 $(\mathbb{F}_2^m)^{\tilde{n}}$ 上的扩散层和作用在 $(\mathbb{F}_2^m)^n$ 上的 $n \times n$ 的二进制矩阵。搜索性能良好的由 LFSR 构造的扩散层，方法是穷举 n 级 LFSR 的状态转移矩阵 S_i^n 最后一列的值 i ($0 \leq i \leq 2^n - 1$)，再求出状态转移矩阵 S_i^n 的 n 次方，得到 LFSR 矩阵 M_i^n ，然后将矩阵 M_i^n 作用在 $(\mathbb{F}_2^m)^{\tilde{n}}$ 上计算分支数（这里 $m\tilde{n} = n$ ），或者将 LFSR 矩阵 M_i^n 作用在 $(\mathbb{F}_2^m)^n$ 上计算 $n \times n$ 的二进制矩阵的分支数。

4.1 利用 LFSR 构造作用在 $(\mathbb{F}_2^m)^{\tilde{n}}$ 上的扩散层

本节研究利用 n 维 LFSR 构造作用在 $(\mathbb{F}_2^m)^{\tilde{n}}$ 上的扩散层，其中 m 是 S 盒的比特长度， $\tilde{n}$ 是 S 盒的个数， $m\tilde{n} = n$ 。通过穷举搜索 n 维 LFSR 状态转移矩阵 S_i^n 的最后一列的值 i ($0 \leq i \leq 2^n - 1$)，求出状态转移矩阵 S_i^n 的 n 次方，得到 n 维 LFSR 矩阵 $M_i^n = (S_i^n)^n$ ，并且只关注 n 维可逆 LFSR 矩阵，将 M_i^n 作为 $(\mathbb{F}_2^m)^{\tilde{n}}$ 上的扩散层，计算它的分支数，寻找性能良好的 LFSR 矩阵。

4.1.1 $(\mathbb{F}_2^4)^4$ 上构造扩散层

当 $\tilde{n} = 4, m = 4, n = 16$ 时，穷搜了所有的 65 535 ($2^{16} - 1$) 个 16 维 LFSR 矩阵，并且只关注其中的可逆矩阵，将其作为 $(\mathbb{F}_2^4)^4$ 上的扩散层，计算分支数，得到最好的分支数是 4，也就是说，

使用 16 维 LFSR 可以构造出作用在 $(\mathbb{F}_2^4)^4$ 上的次最优扩散层，不能构造出 MDS 矩阵，共有 12 543 个次最优扩散层。表 4 列出了部分利用 16 维 LFSR 构造出的作用在 $(\mathbb{F}_2^4)^4$ 上的次最优扩散层。

表 4 利用 LFSR 构造出 $(\mathbb{F}_2^4)^4$ 上的次最优扩散层

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
16	32966, 32970, 32978, 32990, 32994, 33003, 33011, 33032, 33033
16	33037, 33039, 33040, 33041, 33042, 33046, 33047, 33051, 33052
16	33061, 33072, 33073, 33075, 33079, 33080, 33082, 33093, 33097
16	33098, 33106, 33114, 33131, 33139, 33145, 33161, 33165, 33167

4.1.2 $(\mathbb{F}_2^8)^4$ 上构造扩散层

当 $\tilde{n} = 4, m = 8, n = 32$ 时，穷搜了所有的 4 294 967 295 ($2^{32} - 1$) 个 32 维 LFSR 矩阵，并且只关注其中的可逆矩阵，将其作为 $(\mathbb{F}_2^8)^4$ 上的扩散层，计算分支数，得到最好的分支数也是 4，也就是说使用 32 维 LFSR 可以构造出作用在 $(\mathbb{F}_2^8)^4$ 上的次最优扩散层，也不能构造出 MDS 矩阵，共有 263 368 个次最优扩散层。表 5 给出了部分利用 32 维 LFSR 构造出的作用在 $(\mathbb{F}_2^8)^4$ 上的次最优扩散层。

表 5 利用 LFSR 构造出 $(\mathbb{F}_2^8)^4$ 上的次最优扩散层

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
32	2147520533, 2147520538, 2147520547, 2147520551, 2147520562
32	2147520565, 2147520571, 2147520574, 2147520578, 2147520587
32	2147520590, 2147520593, 2147520598, 2147520599, 2147520619
32	2147520630, 2147520631, 2147520634, 2147520642, 2147520650

4.1.3 $(\mathbb{F}_2^4)^8$ 上构造扩散层

当 $\tilde{n} = 8, m = 4, n = 32$ 时，搜索了部分 32 维可逆 LFSR 矩阵，将其作为 $(\mathbb{F}_2^4)^8$ 上的扩散层，计算分支数，得到最好的分支数是 7，也没有构造出 MDS 矩阵，表 6 给出了一些利用 32 维 LFSR 构造出的作用在 $(\mathbb{F}_2^4)^8$ 上分支数为 7 的扩散层，表中的 i 表示 32 维 LFSR 状态转移矩阵 S_i^{32} 的最后一列值。

表 6 利用 LFSR 构造出 $(\mathbb{F}_2^4)^8$ 上分支数为 7 的扩散层

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
32	2148618279、2149459469、2149669179、2149717069、 2150038164
32	2150165475、2150195621、2150962835、2151045265、 2151128281
32	2151446953、2151536558、2151650836、2151803149、 2151849147
32	2151871370、2151936204、2152034193、2152036577、 2152054356

4.1.4 $(\mathbb{F}_2^8)^8$ 上构造扩散层

当 $\tilde{n}=8, m=8, n=64$ 时, 搜索了部分 64 维可逆 LFSR 矩阵, 将其作为 $(\mathbb{F}_2^8)^8$ 上的扩散层, 计算分支数, 得到最好的分支数是 7, 也没有构造出 MDS 矩阵, 表 7 给出了一些利用 64 维 LFSR 构造出的作用在 $(\mathbb{F}_2^8)^8$ 上分支数为 7 的扩散层。

表 7 利用 LFSR 构造出 $(\mathbb{F}_2^8)^8$ 上分支数为 7 的扩散层

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
64	9296019069125191687、9300522668752562183、 9300523218508376071
64	9300523218508376199、9300523218508376215、 9300523218508376727
64	9300523218541931159、9300525417565186711、 9300525417565187735
64	9300525417565253271、9300525692443160215、 9309532891697901207
64	9311784691511586455、9311925428999941783、 9311960613372030615
64	9311960613908901527、9311961713420529303、 9311966111467040407

4.2 构造二进制矩阵

二进制矩阵因为具有结构简单、实现过程只需要异或操作等优点, 被广泛应用于分组密码算法中, MDBL 矩阵是二进制矩阵中具有最大分支数的矩阵, 很多密码算法, 如 ARIA、Camellia、E2、MIBS、Midori、FIDES、Minalpher 等的扩散层都使用 MDBL 矩阵。本节讨论了基于 n 维 LFSR 构造作用在 $(\mathbb{F}_2^m)^n$ 上 $n \times n$ 大小的二进制矩阵 M_n , 这里 m 是 S 盒的比特长度, n 是 S 盒的个数。

通过对 $n(n=4, 5, 6, 7, 8, 9, 10, 12, 14, 16, 18, 32)$ 维 LFSR 矩阵分支数进行计算, 并且只关注其中的 n 维可逆 LFSR 矩阵, 统计出了利用 n 维 LFSR 构造扩散层的最大分支数 $\beta_{\max}^{\text{lfsr}}$ 的实验结果, 如表 8 所示, 其中 β^{mdbl} 表示 MDBL 矩阵的

分支数^[47,63,66], 即 n 维二进制矩阵中能达到最好的分支数。32 维 LFSR 只搜索了部分结果。从表 8 中可以看出, 当 $n=6, 7, 8$ 时, 利用 LFSR 可以构造出 MDBL 矩阵, MDBL 矩阵具有最大分支数, 在降低软硬件消耗的同时, 提供了较好的扩散性。表 8 中 12* 表示 32×32 大小的二进制矩阵, 12 是目前已知的最大分支数。

表 8 n 维 LFSR 矩阵最大分支数 $\beta_{\max}^{\text{lfsr}}$ 和MDBL 矩阵的分支数 β^{mdbl}

n	$\beta_{\max}^{\text{lfsr}}$	β^{mdbl}	n	$\beta_{\max}^{\text{lfsr}}$	β^{mdbl}
4	3	4	5	3	4
6	4	4	7	4	4
8	5	5	9	5	6
10	5	6	12	7	8
14	6	8	16	7	8
18	7	8	32	12	12*

表 9 统计了当矩阵维数为 6, 7, 8 时, 利用 n 维 LFSR 构造出的 MDBL 矩阵。表 9 中的 S_i^n 为 n 维 LFSR 的状态转移矩阵, S_i^n 的 n 次方表示对应的 MDBL 矩阵 M_n , 即 $M_n = (S_i^n)^n$ 。

表 9 当 $n=6, 7, 8$ 时, 利用 LFSR 构造出的 MDBL 矩阵

矩阵维数 n	状态转移矩阵 S_i^n
6	S_{46}^6 、 S_{53}^6 、 S_{55}^6 、 S_{61}^6
7	S_{69}^7 、 S_{70}^7 、 S_{77}^7 、 S_{83}^7 、 S_{88}^7 、 S_{91}^7 、 S_{94}^7 、 S_{101}^7 、 S_{103}^7 、 S_{104}^7 、 S_{105}^7 、 S_{108}^7 、 S_{111}^7 、 S_{114}^7 、 S_{118}^7 、 S_{121}^7 、 S_{125}^7
8	S_{156}^8 、 S_{235}^8

对常用的 $n(n=4, 16, 18, 32)$ 维矩阵的实验结果也做了统计。4 维 LFSR: $S_9^4, S_{11}^4, S_{12}^4, S_{14}^4$ 可以使所得到的 4 维 LFSR 矩阵分支数达到 3, 32 维 LFSR: $S_{2224121979}^{32}, S_{2280084668}^{32}, S_{2317426409}^{32}, S_{2324550308}^{32}, S_{2650444827}^{32}, S_{2660594672}^{32}, S_{3172389411}^{32}, S_{3924269910}^{32}$ 可使对应的 32 维 LFSR 矩阵分支数达到 12。表 10 列出了部分利用 16 维 LFSR 构造出的分支数为 7 的二进制矩阵, i 表示 16 维 LFSR 状态转移矩阵 S_i^{16} 的最后一列值。

表 10 利用 16 维 LFSR 构造出的分支数为 7 的二进制矩阵

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
16	33622、34296、35685、36613、36617、36816、36827、37517
16	38310、38313、39183、39897、40157、40522、40745、41951
16	42078、43324、45780、45937、46067、46432、46975、47081
16	47095、47305、47711、48402、50281、50575、51046、51320

表 11 给出了部分利用 18 维 LFSR 构造出的分支数为 7 的二进制矩阵,表中 i 表示 18 维 LFSR 状态转移矩阵 S_i^{18} 的最后一列值。

表 11 利用 18 维 LFSR 构造出的分支数为 7 的二进制矩阵

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
18	131557、131646、131675、131708、131740、131769、131804
18	131805、131822、131877、131899、131934、131961、132007
18	132023、132075、132150、132198、132214、132217、132222
18	132283、132306、132315、132316、132317、132331、132402

表 12 给出了部分利用 32 维 LFSR 构造出的分支数为 11 的二进制矩阵,表中 i 表示 32 维 LFSR 状态转移矩阵 S_i^{32} 的最后一列值。

表 12 利用 32 维 LFSR 构造出的分支数为 11 的二进制矩阵

LFSR 维数	LFSR 状态转移矩阵的最后一列值 i
32	2150821773、2151069970、2152304252、2152391529、2153175026
32	2154711100、2154846137、2155309285、2155490387、2155573406
32	2156275643、2157025527、2157934661、2158434609、2158704433
32	2159191160、2159834530、2161810985、2164872486、2166188686

5 结束语

扩散层作为分组密码的一个重要部件,在密码算法中扮演着重要角色,近几年,很多研究者都将目光转移到该问题上,产生了一系列的研究成果^[27~56]。然而,目前的结果主要是面向硬件实现的,很少针对软件实现设计扩散层。本文首先介绍扩散层的研究现状,接着基于两大密码结构构造扩散层,分别是基于 Feistel 结构构造面向软件实现的扩散层和基于 LFSR 构造面向硬件实现的扩散层。

Feistel 结构因其软硬件实现效率高,加解密一致,加解密速度快等优点受到广大研究者的青睐,Feistel 结构不仅广泛应用于分组密码算法的整体设计中,而且也用来构造分组密码的主要部件 S 盒和扩散层。本文基于三轮 Feistel 结构构造轻量级扩散层,轮函数采用基于循环移位和异或的线性变换,构造出了一系列作用在 $(\mathbb{F}_2^4)^8$ 和 $(\mathbb{F}_2^8)^8$ 上分支数为 7 的对合扩散层,一方面,对合性质使扩散层的加密和解密操作在硬件上可以使用相同的电路,在软件上可以使用相同的代码,并且轮函数采用基于循环移位和异或运算的线性变换,在支持循环移位指令的处理器中,循环移位运算通常可以通过一条指令实现,而在不支持循环移位的处理器中,通常只需要将该指令分解成 3 条指令:逻辑左移 1 次、逻辑右移 1 次、两者异或^[67]。不管是移位运算还是循环移位运算,软件实现所需的 CPU 周期数均很低,大大提高了软件实现效率;另一方面,对于作用在 8 个 4 bit 或 8 bit S 盒上的扩散层,分支数为 7 的扩散层已经可以提供较好的扩散效果,并且分支数为 7 的扩散层是安全性和效率方面的权衡。

LFSR 因其具有原理简单、计算速度快、便于硬件实现等优点,通常被用来构造密钥流生成器,而且也被用来构造分组密码的扩散层^[7,13,14,29,30],基于 LFSR 构造的扩散层具有很高的硬件实现效率,扩散层只需实现 LFSR 且能在不需要额外逻辑控制电路的情形下重用已有的存储,大大降低了硬件消耗。本文基于 LFSR 构造出作用在 $(\mathbb{F}_2^4)^4$ 和 $(\mathbb{F}_2^8)^4$ 上的次最优扩散层,这些次最优扩散层应用于软硬件要求极其苛刻的环境下,可以使密码算法软硬件消耗极度降低。利用 LFSR 也构造出了作用在 $(\mathbb{F}_2^4)^8$ 和 $(\mathbb{F}_2^8)^8$ 上分支数为 7 的扩散层。另外,二进制矩阵相对于 MDS 矩阵(实现过程需要异或、查表和 xtime 操作^[68])而言,实现过程只需要异或操作,具有较高的软硬件实现效率,非常适合轻量级密码的设计,本文利用 n 维 LFSR 构造了作用在 $(\mathbb{F}_2^m)^n$ 上 $n \times n$ 大小的二进制矩阵,列出了 n ($n=4,5,6,7,8,9,10,12,14,16,18,32$) 维二进制矩阵的分支数,并给出了采用 LFSR 构造的 6、7、8 维 MDBL 矩阵的具体构造,以及分支数分别为 7、7、12 的 16、18、32 维二进制矩阵的具体构造。本文构造的扩散层在轻量

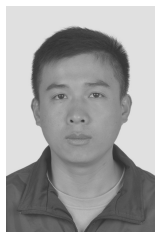
级密码的设计方面具有较高的应用价值。

参考文献:

- [1] SCHNEIER B, SCHNEIER B. Data encryption standard (DES)[C]// *Advances in Cryptology — EUROCRYPT' 85*. 1985:3-5.
- [2] DAEMEN J, RIJMEN V. The design of Rijndael: AES, the advanced encryption standard[M]. Berlin: Springer, 2002.
- [3] 无线局域网产品中使用的 SMS4 算法[EB/OL]. <http://www.oscca.gov.cn/UpFile/200621016423197990.pdf>. SMS4 algorithm used in wireless LAN products[EB/OL]. <http://www.oscca.gov.cn/UpFile/200621016423197990.pdf>.
- [4] HONG D, SUNG J, HONG S, et al. HIGHT: a new block cipher suitable for low-resource device[C]// *Cryptographic Hardware and Embedded Systems*. 2006: 46-59.
- [5] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[C]// *Cryptographic Hardware and Embedded Systems*. 2007:450-466.
- [6] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128 bit blockcipher CLEFIA[C]// *The 14th International Conference on Fast Software Encryption*. 2007:181-195.
- [7] GUO J, PEYRIN T, POSCHMANN A, et al. The LED block cipher[C]// *Cryptographic Hardware and Embedded Systems*. 2011: 326-341.
- [8] WU W, ZHANG L. LBlock: a lightweight block cipher[C]// *Applied Cryptography and Network Security*. 2011: 327-344.
- [9] BORGHOFF J, CANTEAUT A, GÜNEYSU T, et al. PRINCE—a low-latency block cipher for pervasive computing applications[C]// *The International Conference on the Theory and Application of Cryptology and Information Security*. 2012: 208-225.
- [10] RAY B, DOUGLAS S, JASON S. The simon and speck families of lightweight block ciphers[R]. 2013.
- [11] GÉRARD B, GROSSO V, NAYA-PLASENCIA M, et al. Block ciphers that are easier to mask: How far can we go?[C]// *International Workshop on Cryptographic Hardware and Embedded Systems*. 2013: 383-399.
- [12] YANG G, ZHU B, SUDER V, et al. The simeck family of lightweight block ciphers[C]// *The International Workshop on Cryptographic Hardware and Embedded Systems*. 2015: 307-329.
- [13] GUO J, PEYRIN T, POSCHMANN A. The photon family of lightweight Hash functions[C]// *Advances in Cryptology Conference*. 2011:222-239.
- [14] ANDREEVA E, BILGIN B, BOGDANOV A, et al. Submission to the CAESAR competition[EB/OL]. <http://competitions.cr.yp.to/round1/primatesv1.pdf>.
- [15] RIJMEN V, DAEMEN J. The cipher shark[C]// *Fast Software Encryption*. 1996:99-112.
- [16] SCHNEIER B, KELSEY J, WHITING D, et al. Twofish: a 128 bit block cipher[C]// *The 1st AES Candidate Conference on National Institute for Standards and Technology*. 1998.
- [17] SCHNEIER B, KELSEY J, WHITING D, et al. The twofish encryption algorithm[M]. New York: John Wiley & Sons. 1999.
- [18] DAEMEN J, KNUDSEN L R, RIJMEN V. The block cipher square[C]// *The 4th Fast Software Encryption Workshop*. 1997: 149-165.
- [19] BARRETO P, RIJMEN V. The anubis block cipher[EB/OL]. <http://www.larc.usp.br/~pbarreto/AnubisPage.html>.
- [20] BARRETO P, RIJMEN V. The khazad legacy-level block cipher[C]// *Primitive Submitted to NESSIE*. 2000.
- [21] JUNOD P, VAUDENAY S. FOX: a new family of block ciphers[C]// *Selected Areas in Cryptography*. 2004:114-119.
- [22] DAI W, FURUYA S, YOSHIDA H, et al. A new keystream generator MUGI[M]// *Fast Software Encryption*. Berlin: Springer, 2002:37-45.
- [23] FILHO G D, BARRETO P, RIJMEN V. The maelstrom-0 Hash function[C]// *The 6th Brazilian Symposium on Information and Computer Systems Security*. 2006.
- [24] GAURAVARAM P, KNUDSEN L R, MATUSIEWICZ K, et al. Grøstl a SHA-3 candidate[EB/OL]. <http://www.groestl.info>.
- [25] BARRETO P S L M, RIJMEN V. The Whirlpool hashing function[EB/OL]. <http://read.pudn.com/downloads67/sourcecode/disk/240939/Whirlpool.pdf>.
- [26] MORADI A, POSCHMANN A, LING S, et al. Pushing the limits: a very compact and a threshold implementation of AES[C]// *Advances in Cryptology – EUROCRYPT*. 2011.
- [27] 崔霆, 金晨辉. 对合 Cauchy-Hadamard 型 MDS 矩阵的构造[J]. *电子与信息学报*, 2010, 32(2):500-503.
- [28] CUI T, JIN C H. Construction of involution cauchy-hadamard type MDS matrices[J]. *Journal of Electronics & Information Technology*, 2010, 32(2): 500-503.
- [29] SAJADIEH M, DAKHILALIAN M, MALA H, et al. On construction of involutory MDS matrices from Vandermonde Matrices in GF [J]. *Designs, Codes and Cryptography*, 2012, 64(3):287-308.
- [30] SAJADIEH M, DAKHILALIAN M, MALA H, et al. Recursive diffusion layers for block ciphers and Hash functions[C]// *The International Conference on Fast Software Encryption*. 2012:385-401.
- [31] WU S, WANG M, WU W. Recursive diffusion layers for (lightweight) block ciphers and Hash functions[C]// *Selected Areas in Cryptography*. 2012:355-371.
- [32] AUGOT D, FINIASZ M. Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and Hash functions[C]// *IEEE International Symposium on Information Theory Proceedings*. 2013:1551-1555.
- [33] BERGER T P. Construction of recursive MDS diffusion layers from Gabidulin codes[C]// *INDOCRYPT*. 2013:274-285.
- [34] AUGOT D, FINIASZ M. Direct construction of recursive MDS diffusion layers using shortened BCH codes[C]// *Fast Software Encryption*. 2014:3-17.
- [35] KHOO K, PEYRIN T, POSCHMANN A Y, et al. FOAM: searching for hardware-optimal SPN structures and components with a fair comparison[C]// *Cryptographic Hardware and Embedded System*. 2014:433-450.
- [36] SIM S M, KHOO K, OGGIER F, et al. Lightweight MDS involution matrices[C]// *Fast Software Encryption*. 2015:471-493.
- [37] NAKAHARA J, ABRAHO L. A new involutory MDS matrix for the AES[J]. *International Journal of Network Security*, 2009, 9(2): 109-116.
- [38] GUPTA K C, RAY I G. On constructions of circulant MDS matrices for lightweight cryptography[C]// *Information Security Practice and Experience*. 2014:564-576.
- [39] LIU M, SIM S M. Lightweight MDS generalized circulant matrices

- es[C]// Fast Software Encryption. 2016.
- [39] LI Y, WANG M. On the construction of lightweight circulant involutory MDS matrices[C]// Fast Software Encryption. 2016.
- [40] KWON D, KIM J, PARK S, et al. New block cipher: ARIA[C]// ICISC. 2003:432-445.
- [41] AOKI K, ICHIKAWA T, KANDA M, et al. Camellia: a 128 bit block cipher suitable for multiple platforms design and analysis[C]//Selected Areas in Cryptography. 2000:39-56.
- [42] KANDA M, MORIAI S, AOKI K, et al. E2—a new 128 bit block cipher[J]. *Ice Transactions on Fundamentals of Electronics Communications & Computer Sciences*, 2000, 83(1):48-59.
- [43] IZADI M, SADEGHIYAN B, SADEGHIAN S S, et al. MIBS: a new lightweight block cipher[C]//The International Conference on Cryptology and Network Security. 2009:334-348.
- [44] BANIK S, BOGDANOV A, ISOBE T, et al. Midori: a block cipher for low energy[C]//The International Conference on the Theory and Application of Cryptology and Information Security. 2014: 411-436.
- [45] BILGIN B, BOGDANOV A, KNEŽEVIĆ M, et al. Fides: lightweight authenticated cipher with side-channel resistance for constrained hardware[C]//The International Workshop on Cryptographic Hardware and Embedded Systems. 2013: 142-158.
- [46] SASAKI Y, TODO Y, AOKI K, et al. Minalpher v1[C]//Submission to the CAESAR Competition. 2014.
- [47] KWON D, SUNG S H, SONG J H, et al. Design of block ciphers and coding theory[J]. *Trends in Mathematics*, 2005, 8(1): 13-20.
- [48] KOO B W, JANG H S, SONG J H. Constructing and cryptanalysis of a 16×16 binary matrix as a diffusion layer[C]//The International Workshop on Information Security Applications. 2003:489-503.
- [49] KOO B W, JANG H S, SONG J H. On constructing of a 32×32 binary matrix as a diffusion layer for a 256-bit block cipher[C]// Information Security and Cryptology (ICISC). 2006:51-64.
- [50] KANG J S, HONG S, LEE S, et al. Practical and provable security against differential and linear cryptanalysis for substitution permutation networks[J]. *ETRI Journal*, 2001, 23(4): 158-167.
- [51] KANDA M, TAKASHIMA Y, MATSUMOTO T, et al. A strategy for constructing fast round functions with practical security against differential and linear cryptanalysis[C]//Selected Areas in Cryptography. 1998: 264-279.
- [52] GAO Y, GUO G. Unified approach to construct 8×8 binary matrices with branch number 5[C]// The 1st Asia International Symposium on Cryptography, and Network Security, Data Mining and Knowledge Discovery, E-Commerce and ITS Applications, and Embedded Systems. 2010:413-416.
- [53] ASLAN B, SAKALLI M. Algebraic construction of cryptographically good binary linear transformations[J]. *Security and Communication Networks*, 2014, 7(1):53-63.
- [54] SAKALLI M T, ASLAN B. On the algebraic construction of cryptographically good 32×32 binary linear transformations[J]. *Journal of Computational & Applied Mathematics*, 2014, 259: 485-494.
- [55] SAKALLI S M T, ASLAN B. Algebraic construction of 16×16 binary matrices of branch number 7 with one fixed point[EB/OL]. http://www.singacom.uva.es/~edgar/cactc2012/trabajos/CACT2012_Sakalli.pdf.
- [56] DEHNAVI S M, RISHAKANI A M, SHAMSABAD M R M. Bitwise linear mappings with good cryptographic properties and efficient implementation[J]. *Antiquity*, 2015, 75.
- [57] LIM C H. CRYPTON: a new 128-bit block cipher[J]. *Nist Aes Proposal*, 1998.
- [58] ETSI/SAGE TS 35.222-2011, Specification of the 3GPP Confidentiality and Integrity Algorithms 128-EEA3 & 128-EIA3; Document 2: ZUC Specification[S].
- [59] STERN J, VAUDENAY S. CS-Cipher[J]. *Lecture Notes in Computer Science*, 1998, 1372:189-205.
- [60] MATSUI M. New block encryption algorithm MISTY[C]//The International Workshop on Fast Software Encryption. 1997:54-68.
- [61] LI Y, WANG M. Constructing s-boxes for lightweight cryptography with feistel structure[C]//Cryptographic Hardware and Embedded Systems. 2014:127-146.
- [62] CANTEAUT A, DUVAL S, LEURENT G. Construction of lightweight s-boxes using feistel and misty structures[C]//The International Conference on Selected Areas in Cryptography. 2015: 373-393.
- [63] GUO Z, WU W, GAO S. Constructing lightweight optimal diffusion primitives with feistel structure[C]//The International Conference on Selected Areas in Cryptography. 2015: 352-372.
- [64] 张雪锋, 范九伦. 基于线性反馈移位寄存器和混沌系统的伪随机序列生成方法[J]. *物理学报*, 2010, 59(4):2289-2297.
- ZHANG X F, FAN J L. Pseudo-random sequence generating method based on LFSR and chaotic system[J]. *Acta Physica Sinica*, 2010, 59(4):2289-2297.
- [65] STALLINGS W. Cryptography and network security: principles and practice, fifth edition[M]. Pearson Education, 2011.
- [66] TODO Y, AOKI K. Wide trail design strategy for binary mixcolumns[M]. *Applied Cryptography and Network Security*. 2016.
- [67] 公丽丽. 分组密码的软件实现评估方法研究及 RECTANGLE 在 X86 平台的软件实现测评[D]. 北京: 中国科学院大学, 2015.
- GONG L L. A study of software implementation of block cipher and software implementation of RECTANGLE on X86 platforms[D]. Beijing: The University of Chinese Academy of Sciences, 2015.
- [68] NAKAHARA J, ABRAHÃO E. A new involutory MDS matrix for the AES[J]. *International Journal of Network Security*, 2009, 9(2): 109-116.

作者简介:



李鹏飞 (1991-), 男, 陕西渭南人, 中国科学院信息工程研究所硕士生, 主要研究方向为密码学。