

MDS 矩阵构造方法

李鹏飞^{1,2}, 李永强¹

(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, 北京 100049)

摘要: 针对 MDS 矩阵的设计策略做了综述。阐述了 MDS 矩阵构造中的关键问题, 并对当前典型和常见 MDS 矩阵的构造方法从原理、实现机制等方面进行了分析和讨论。另外, 调研了最近几年关于轻量级 MDS 矩阵的研究成果。

关键词: 分组密码; 最优扩散层; 分支数; MDS 矩阵; 线性变换

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2016.00063

Construction of MDS matrices

LI Peng-fei^{1,2}, LI Yong-qiang¹

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

Abstract: A survey for MDS matrices design strategy was made. Design strategies and the key issues during the design were elaborated, and many aspects such as principle and implementation mechanisms of some typical and common construction of MDS matrices were analyzed and discussed. In addition, the research results on lightweight MDS matrices in recent years were investigated.

Key words: block cipher, optimal diffusion layer, branch number, MDS matrix, linear transformation

1 引言

随着信息技术的快速发展, 互联网已经融入人们生活的方方面面, 然而, 人们在享受互联网带来便利的同时, 信息安全问题也越来越突出。现代密码学作为信息安全的核心和关键技术, 在保护数据安全和用户隐私上发挥着巨大的作用。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, 受到广泛关注且成为密码学研究的热点课题。分组密码在对大批量数据加密的应用中扮演着举足轻重的作用, 它们以硬件、软件等不同的实现方式广泛应用在个人通信、电子支付、数据库加密等诸多领域。早在 1949 年,

香农 (Shannon) 在他的《保密系统的通信理论》中就提到密码系统设计的 2 种基本方法: 混淆和扩散^[1], 这是现今密码算法设计和分析的基础。现在广泛使用的分组密码算法通常采用迭代型结构, 迭代型是指所有轮 (除第一轮和最后一轮外) 均采用相同轮变换。迭代型分组密码设计中最重要 2 个基本部件是混淆层 (confusion layer) 和扩散层 (diffusion layer)。混淆层通常使用非线性的几个并置 S 盒来构造, 扩散层由线性的变换函数构成。扩散层作为迭代型分组密码的一个很重要的部件, 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。性能良好的扩散层可以有效地抵抗一些著名的密

收稿日期: 2016-04-27; 修回日期: 2016-05-30。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, No.61303255)

Foundation Item: The National Natural Science Foundation of China (No.61379142, No.61303255)

码攻击,如差分密码分析^[2]和线性密码分析^[3]。扩散层的安全性能主要由 Daemen 提出来的分支数^[4]概念来衡量,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。在实际设计中,最受瞩目是那些分支数达到最大时的扩散层,简称最优扩散层,所对应的矩阵称为 MDS (maximum distance separable) 矩阵。MDS 矩阵首次被使用在分组密码 SHARK^[5]的设计中,随后,越来越多的分组密码算法将 MDS 矩阵用于扩散层的设计中,如 Rijndael^[4]、Twofish^[6,7]、Square^[8]、Anubis^[9]、Khazad^[10]、FOX^[11]、CLEFIA^[12]、LED^[13]等。流密码算法也使用 MDS 矩阵作为扩散层,如 MUGI^[14]。另外,散列函数,如 Maelstrom^[15]、Grøstl^[16]、Whirlpool^[17]和 PHOTON 轻量级散列函数族^[18]等都将 MDS 矩阵作为扩散层使用。

本文针对 MDS 矩阵的设计策略做了综述。归纳总结了常见的构造 MDS 矩阵的方法,分别为利用线性码构造 MDS 矩阵;采用随机检测矩阵的方法来构造 MDS 矩阵,通过检测特殊矩阵来构造 MDS 矩阵,如循环矩阵、Hadamard 矩阵、对合矩阵和正交矩阵等,以节省软硬件实现开销;利用一些数学上具有特殊性质的矩阵,如 Cauchy 矩阵、Vandermonde 矩阵构造 MDS 矩阵;基于简单的移位和异或构造高效的 MDS 矩阵;基于线性反馈移位寄存器 (LFSR, linear feedback shift register) 构造硬件实现友好的迭代型最优扩散层。本文阐述了这些 MDS 矩阵构造方法中的关键问题,并对当前典型的构造方法从原理、实现机制等方面进行了分析和讨论,另外,随着物联网技术的快速发展,设计和构造轻量级的 MDS 矩阵受到了越来越多研究人员的关注,本文也对近几年轻量级 MDS 矩阵的研究成果进行了调研。

2 基本概念

2.1 分支数

定义 1 对于输入向量 $X = (x_1, x_2, \dots, x_n) \in (\mathbb{F}_2^m)^n$, X 的束权值^[4]定义为 X 中非零分量的个数,如下

$$w_b(X) = |\{x_i, x_i \neq 0, 1 \leq i \leq n\}|$$

在迭代型密码结构中,将输入差分或者输出掩码非零的 S 盒称为活跃 S 盒。一般情况下,如果混淆层是由 n 个 $m \times m$ 的 S 盒并置而成,则扩散层一般设计成 $(\mathbb{F}_2^m)^n \rightarrow (\mathbb{F}_2^m)^n$ 的一个置换,其中 $(\mathbb{F}_2^m)^n = \mathbb{F}_2^m \times \mathbb{F}_2^m \times \dots \times \mathbb{F}_2^m$, 如图 1 所示。

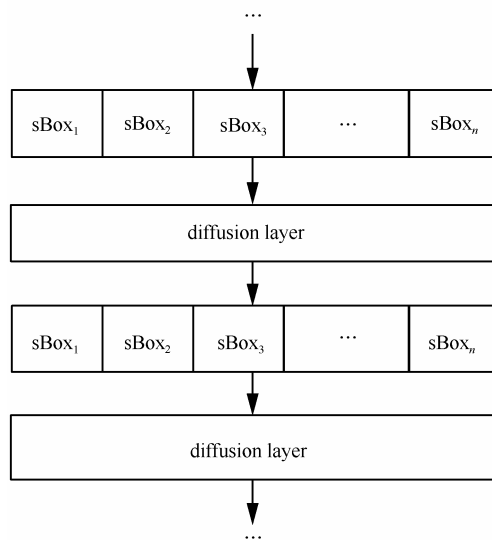


图 1 混淆层和扩散层结构

分支数又分为差分分支数和线性分支数,具体定义如下。

定义 2 扩散层 θ 的差分分支数定义为^[4]

$$B_d(\theta) = \min_{a, b \neq a} \{w_b(a \oplus b) + w_b(\theta(a) \oplus \theta(b))\} \quad (1)$$

由于线性变换 $\lambda(a) \oplus \lambda(b) = \lambda(a \oplus b)$, 上式可转化为

$$B_d(\theta) = \min_{a' \neq 0} \{w_b(a') + w_b(\lambda(a'))\} \quad (2)$$

类似于差分分支数,可以给出扩散层线性分支数的定义。

定义 3 扩散层 θ 的线性分支数定义为^[4]

$$B_l(\theta, \alpha) = \min_{\alpha, \beta, Cor(\alpha^T x, \beta^T \theta(x)) \neq 0} \{w_b(\alpha) + w_b(\beta)\} \quad (3)$$

如果 θ 是一个由 λ 表示的线性变换,则存在一个矩阵 M , 使 $\lambda(x) = Mx$, 所以,扩散层可表示成 $\mathbb{F}_2$ 上的 $mn \times mn$ 矩阵或 $\mathbb{F}_2^m$ 上的 $n \times n$ 分块矩阵,那么式(2)、式(3)可以简化为

$$B_d(\theta) = \min_{\alpha \neq 0} \{w_b(\alpha) + w_b(M\alpha)\} \quad (4)$$

$$B_i(\theta) = \min_{\alpha \neq 0} \{w_b(\alpha) + w_b(M^T \alpha)\} \quad (5)$$

其中, M^T 为矩阵 M 的转置。

差分(线性)分支数即连续两轮的差分(线性)特征中活跃 S 盒的最小数目, 设计者可以根据差分(线性)分支数的大小给出理论上最大差分特征概率(最佳线性逼近偏差)的界, 由此可以分析密码算法抵抗差分和线性分析的能力。关于分支数有如下性质^[19]。

1) 扩散层矩阵 M 的线性分支数等于转置矩阵 M^T 的差分分支数。

2) 扩散层的分支数等于其逆变换的分支数。

3) 扩散层差分分支数达到最大, 当且仅当其线性分支数也达到最大。

定义 4 分支数达到最大的扩散层称为最优扩散层, 所对应的矩阵称为 MDS 矩阵。

2.2 线性码

线性码理论对于研究扩散层的分支数很重要, 本节结合文献[4,5], 给出线性码的一些重要性质和定理。

定义 5 域 $GF(2^p)$ 上的线性码 $C=[n,k,d]$ 是指向量空间 $GF(2^p)^n$ 上任意 2 个不同向量之间汉明距离至少为 d 的一个 k 维子空间, 空间的元素称为一个码字。线性码 C 的最小汉明距离 d 等于线性码 C 中非零码字的最小汉明重量。

定义 6 一个线性码 $C=[n,k,d]$ 的生成矩阵 G 大小为 $k \times n$, 生成矩阵 G 的行构成线性码 C 的一个基。因为向量空间中可以有多个不同的基, 所以一个线性码会有多个不同的生成矩阵, 但是这些生成矩阵之间可以通过初等行变换相互转换, 生成矩阵的梯形形式可以唯一地表示为 $G_e=[I_{k \times k} A_{k \times (n-k)}]$, 称该形式为标准形式, 其中, I 是 k 阶单位矩阵。

定义 7 一个线性码 $C=[n,k,d]$ 的校验矩阵 H 是一个 $(n-k) \times n$ 大小的矩阵, 该矩阵可以用来检验某个码字是否是线性码 C 的码字, 具体来说, 向量 X 是线性码 C 的码字当且仅当 $HX^T = 0$ 。

由定义 7 可知, 若假设线性码 C 的生成矩阵为 G , 校验矩阵为 H , 则有 $GX^T = 0$, 而且, 如果 $G=[I C_1]$ 是码 C 的生成矩阵, 则 $H=[-C_1^T I]$ 是码 C 的校验矩阵。

定义 8 将与线性码 C 中所有向量都正交的

向量集合称为 C 的对偶码 $C^\perp$, 具体定义为

$$C^\perp = \{x | xy^T = 0, \forall y \in C\} \quad (6)$$

由此可以看出, 线性码 C 的校验矩阵就是 $C^\perp$ 的生成矩阵。

下面介绍几个重要定理。

定理 1 设 C 是一个 $[n,k,d]$ 线性码, H 是它的校验矩阵, 如果 H 的任意 $d-1$ 列线性无关, 且存在 d 列线性相关, 则线性码 C 的最小汉明距离等于 d 。

定理 2 (Singleton 界) 对于线性码 $C=[n,k,d]$, 必然有 $d \leq n-k+1$ 。

定理 3 设 C 是一个 $[n,k,d]$ 线性码, 当 $d=n-k+1$ 时, 称线性码 C 为最大距离可分 MDS 码, 它是构造 MDS 矩阵的重要工具。

定理 4 (MDS 码的判定定理) 设线性码 $C=[n,k,d]$ 的生成矩阵为 $G=[I_{k \times k} A_{k \times (n-k)}]$ 的标准形式, 若 C 是 MDS 码, 当且仅当矩阵 A 的所有子方阵都是非奇异的。

定理 5 (MDS 矩阵的判定定理) 设矩阵 M 是与扩散层 θ 对应的 n 阶矩阵, 则 M 为 MDS 矩阵(即 $B_d(\theta)=n+1$)的充要条件是 M 的任意 k 阶子式都不为零 ($1 \leq k \leq n$)。

定理 6 (MDS 矩阵的判定定理) 设矩阵 M 是与扩散层 θ 对应的 n 阶矩阵, 则 M 为 MDS 矩阵(即 $B_d(\theta)=n+1$)的充要条件是 M 的任意 k 阶子方阵均满秩 ($1 \leq k \leq n$)。

2.3 构造 MDS 的相关矩阵

定义 9^[20] 具有以下形式的 n 阶方阵 A 称为循环矩阵。

$$A = \begin{bmatrix} a_1 & a_2 & \cdots & a_n \\ a_n & a_1 & \cdots & a_{n-1} \\ \vdots & \vdots & \cdots & \vdots \\ a_2 & a_3 & \cdots & a_1 \end{bmatrix}_{n \times n} \quad (7)$$

显然, 矩阵 A 的每一行向量的每一个元素由前一行向量各元素依次循环右移一个位置得到, 循环矩阵 A 可简记为 $A = \text{circ}(a_1, a_2, \dots, a_n)$ 。

定义 10^[21] 一个 n 阶方阵 A 称为对合矩阵当且仅当该矩阵满足 $A^2 = I$, 即 $A = A^{-1}$, 其中, I 表示 n 阶单位阵。

定义 11^[21] 一个 n 阶方阵 A 称为正交矩阵当且仅当该矩阵满足 $AA^T = I$, 其中, I 表示 n 阶

单位阵, A^T 表示矩阵 A 的转置矩阵。

定义 12^[9] 一个 $2^n \times 2^n$ 矩阵 H 称为 Hadamard 矩阵, 则它具有如下形式。

$$H = \begin{bmatrix} U & V \\ V & U \end{bmatrix} \quad (8)$$

其中, U, V 是 2 个 $2^{n-1} \times 2^{n-1}$ 大小的 Hadamard 矩阵。例如, 一个 4×4 大小的 Hadamard 矩阵可表示为

$$\text{Had}(a, b, c, d) = \begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$$

定义 13^[22,23] 给定 $x_0, x_1, \dots, x_{n-1}, y_0, y_1, \dots, y_{n-1}$, 令 $a_{ij} = \frac{1}{x_i + y_j} (0 \leq i, j \leq n-1)$, 且 $x_i + y_j \neq 0$, 则将 n 阶方阵 $A = (a_{ij})$, $0 \leq i, j \leq n-1$ 称为柯西 (Cauchy) 矩阵, 其行列式为

$$\det(A) = \frac{\prod_{0 \leq i, j \leq n-1} (x_j - x_i)(y_j - y_i)}{\prod_{0 \leq i, j \leq n-1} (x_i + y_j)} \quad (9)$$

定义 14^[23,24] 给定 $a_0, a_1, \dots, a_{n-1}$, 则满足以下形式的 n 阶方阵 A 称为范德蒙 (Vandermonde) 矩阵。

$$A = \text{van}(a_0, a_1, \dots, a_{n-1}) = \begin{bmatrix} 1 & a_0 & a_0^2 & a_0^3 & \cdots & a_0^{n-1} \\ 1 & a_1 & a_1^2 & a_1^3 & \cdots & a_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_j & a_j^2 & a_j^3 & \cdots & a_j^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & a_{n-1}^3 & \cdots & a_{n-1}^{n-1} \end{bmatrix} \quad (10)$$

其行列式为

$$\det(A) = \prod_{0 \leq j < i \leq n-1} (a_j - a_i) \quad (11)$$

3 利用线性码构造 MDS 矩阵

一直以来, MDS 码是构造密码算法最优扩散层的主要工具, 通过 MDS 码构造的扩散层分支数达到最大, 具有良好的扩散能力, 能够更好地抵抗差分分析、线性分析和其他未知的密码分析。许多分组密码算法如 AES、Khazad、SHARK、Square 等扩散层中所使用的 MDS 矩阵就是从

MDS 码中提取出来的。Reed-Solomon 码^[23,25]是一种 MDS 码, 它的最小汉明距离达到了最大, 可以用来构造 MDS 矩阵。另外, BCH 码^[23,26]、Goppa 码^[27]这 2 种线性码的最小距离都是可以设计的, 通过控制这 2 种线性码的最小汉明距离, 使其达到最大值, 即可从它们的生成矩阵提取 MDS 矩阵。另外, 文献[28]提出通过 Gabidulin 码来构造 MDS 码的新方法。

3.1 分支数与线性码的关系

根据线性码的一些重要性质和定理, 可利用 $\text{GF}(2^n)$ 上的线性码来进一步分析扩散层的分支数, 以得到线性码和扩散层分支数间的关系, 以下定义参考文献[29]。

定义 15 令扩散层 θ 为一个从 $\text{GF}(2^n)^n$ 到 $\text{GF}(2^n)^n$ 的线性变换, 则扩散层 θ 的相关线性码 C_θ 是由向量 $(x, \theta(x))^T$ 产生的码字组成, 共有 2^n 个码字且每个码字长度为 $2n$ 。

进一步, 如果 θ 被定义为 $\theta(x) = Ax$, 则向量 $(x, \theta(x))^T$ 可以写成 $(x, Ax)^T$ 的形式, 那么 C_θ 即为一个 $[2n, n, d]$ 的线性码, 它是 $(x, Ax)^T$ 所有向量的组合, 其中, x 为所有可能的输入。

由此, 将线性码和扩散层联系起来, 结合差分分支数的定义 2, 可以进一步得到扩散层差分分支数与线性码的关系。

定理 7 扩散层 θ 的差分分支数等于它的相关线性码中 2 个不同码字之间的最小汉明距离。这是因为, 根据扩散层 θ 的差分分支数定义 2 有

$$\begin{aligned} B_d(\theta) &= \min_{a' \neq 0} \{w_b(a') + w_b(\theta(a'))\} \\ &= \min_{x \neq 0} \{w_b(x) + w_b(\theta(x))\} \\ &= \min_{x \neq 0} \{w_b(x, \theta(x))\} \end{aligned}$$

并且 θ 的相关码 C_θ 由向量 $(x, \theta(x))^T$ 给出的码字组成, C_θ 的最小汉明距离为 $d_{\min} = w_b(x, \theta(x))$, 因此, 扩散层 θ 的差分分支数等于 θ 的相关线性码中 2 个不同码字之间的最小汉明距离。

得到了扩散层和线性码之间的关系, 即可利用线性码来构造 MDS 矩阵。

3.2 构造 MDS 矩阵的方法

对于扩散层 $P: (\mathbb{F}_2^n)^m \rightarrow (\mathbb{F}_2^n)^m$, 显然有分支数 $B \leq m+1$, 利用线性码的知识, 可以构造分支数达到最佳的扩散层 P 。

定理 8^[5] 令 C 是有限域 $\text{GF}(2^n)$ 上的一个 $[2m, m, m+1]$ 线性码, $G = [I_{m \times m} B_{m \times m}]$ 是 C 的生成矩阵的梯次形, 则 C 定义了如下置换。

$$\theta: \text{GF}(2^n)^m \rightarrow \text{GF}(2^n)^m: x \mapsto y = Bx \quad (12)$$

且 θ 的分支数为 $m+1$ 。

根据定理 8, 只需构造出 $[2m, m, m+1]$ 线性码 C , 则矩阵 $B_{m \times m}$ 便为 MDS 矩阵, 将其应用于扩散层中将得到最大的分支数。矩阵 $B_{m \times m}$ 是基于有限域 $\text{GF}(2^n)$ 的, 其中, n 通常为混淆层中 S 盒的比特数。由于已知的 MDS 码较少, 所以, 这种构造 MDS 矩阵的方法受到很大局限性, 另外, 这类扩散层中有限域上的乘法操作使软硬件实现效率很低, 为了提高实现效率, 减少软硬件实现开销, 希望 MDS 矩阵中有限域上不同元素的个数尽量少, 同时元素“1”的个数尽可能多^[30]。

4 利用随机检测矩阵来构造 MDS 矩阵

为了节省软硬件实现的系统资源, 减少开销, 提高密码算法运行速度, 通常根据定理 5 和定理 6 通过检测特殊矩阵来构造 MDS 矩阵, 如循环矩阵、Hadamard 矩阵、对合矩阵和正交矩阵等。循环矩阵和 Hadamard 矩阵可使矩阵中不同元素的数量极其少, 对合矩阵可使密码算法加解密一致, 节省解密的开销, 正交矩阵同样可以使用几乎相同的电路实现加解密操作。

4.1 循环矩阵

由循环矩阵的定义 9 可知, 循环矩阵的元素基本相同, 只用实现一行, 然后通过不断更新输入向量, 便可以得到全部的输出向量, 另外, 与一般的随机矩阵相比, 循环矩阵所对应的扩散层达到最优的概率更大^[8]。采用循环矩阵作为扩散层的密码算法很多, 典型的是 AES 算法中列混淆部分所使用的 MDS 矩阵 $M = \text{circ}(02, 03, 01, 01)$, 另外, 还有基于分组密码的 Hash 函数 Whirlpool 扩散层中使用的 MDS 矩阵 $M = \text{circ}(01, 01, 04, 01, 08, 05, 02, 09)$, 它们均作用在有限域 $\text{GF}(2^8)$ 上。实际中, 还可以根据下面 2 个定理构造循环 MDS 矩阵。

定理 9^[31] 设 c_0, c_1, c_2, c_3 为 $\text{GF}(2^8)$ 上可逆多项式 $c(x) = c_3x^3 + c_2x^2 + c_1x + c_0$ 的系数, $c(x)$ 对应的线性变换 $\theta(x) = Dx$, 其中, D 为 4 阶循环矩阵 $D = \text{circ}(c_3, c_0, c_1, c_2)$, 如果 c_0, c_1, c_2, c_3 满足以下条件。

- 1) $c_0 = c_1$, 且 c_0, c_2, c_3 互不相等且不为零。
- 2) c_0, c_2, c_3 任意 2 个数的乘积不等于第 3 个数的平方, 即 $c_0^2 \neq c_2c_3$, $c_2^2 \neq c_0c_3$ 且 $c_3^2 \neq c_0c_2$ 。

- 3) c_0, c_2, c_3 分别与 $(c_0 \oplus c_2)^2, (c_0 \oplus c_3)^2$ 相乘, 其结果两两不等。

则循环矩阵 D 为 MDS 矩阵, 即线性变换 $\theta(x)$ 分支数达到最大 5。

定理 10^[32] 设 $c(x) = c_0x^3 + c_1x^2 + c_2x + c_3$ 是 $\frac{F_2[x]}{x^4+1}$ 上的一个可逆多项式, 设其逆多项式为

$d(x) = d_0x^3 + d_1x^2 + d_2x + d_3$, $c(x)$ 对应的线性变换为 $\theta(x) = Dx$, 其中, D 为 4 阶循环矩阵, $D = \text{circ}(c_3, c_0, c_1, c_2)$, 如果 $c_i, d_i (0 \leq i \leq 3)$ 满足如下条件。

- 1) $c_i \neq 0, d_i \neq 0 (0 \leq i \leq 3)$ 。
- 2) $c_0 = c_1, c_3 = c_2 + 1$ 。
- 3) $c_0 \neq c_2$ 且 $c_0 \neq c_2 + 1$ 。
- 4) $(c_0)^2 \neq c_2(c_2 + 1)$ 。

则 4 阶循环矩阵 D 为 MDS 矩阵, 线性变换 $\theta(x)$ 分支数达到最大 5。

4.2 Hadamard 矩阵

由 Hadamard 矩阵的定义 12 可知, 与循环矩阵类似, Hadamard 矩阵的每一行均是第一行的置换, 因此节省了软硬件实现开销, 采用 Hadamard 矩阵的典型算法是 CLEFIA、Anubis 和 Khazad。轻量级分组密码算法 CLEFIA 中所使用的 2 个 Hadamard MDS 矩阵为 $H = \text{Had}(01, 02, 04, 06)$ 和 $H = \text{Had}(01, 08, 02, 0a)$, 它们均作用在有限域 $\text{GF}(2^8)$ 上。Anubis 算法中使用的 MDS 矩阵和 CLEFIA 算法中的第一个矩阵相同。Khazad 算法中所使用的 MDS 矩阵为 $H = \text{Had}(01, 03, 04, 05, 06, 08, 0b, 07)$, 它也是作用在有限域 $\text{GF}(2^8)$ 上。关于 Hadamard 矩阵, 有如下性质和定理^[33, 34]。

性质 1 有限域 $\text{GF}(2^n)$ 上的 Hadamard 矩阵是对称矩阵。

性质 2 有限域 $\text{GF}(2^n)$ 上 Hadamard 矩阵的差分分支数等于它的线性分支数。

性质 3 有限域 $\text{GF}(2^n)$ 上的 Hadamard 型 MDS 矩阵的逆矩阵仍是 Hadamard 型 MDS 矩阵。

定理 11 有限域 $\text{GF}(2^n)$ 上的 Hadamard 矩阵 $\text{Had}(a_0, a_1, \dots, a_{2^n-1})$ 是 MDS 矩阵的必要条件:

$a_0, a_1, \dots, a_{2^m-1}$ 两两不同且不为 0。

定理 12 有限域 $\text{GF}(2^n)$ 上的 2^m 阶 Hadamard 矩阵 $\text{Had}(a_0, a_1, \dots, a_{2^m-1})$ 可逆且 $\prod_{i=0}^{2^m-1} a_i \neq 0$, 则该矩阵的 $2^m - 1$ 阶子方阵均是非退化的。

定理 13 有限域 $\text{GF}(2^n)$ 上的 4 阶 Hadamard 矩阵 $\text{Had}(a_0, a_1, a_2, a_3)$ 是 MDS 矩阵的充要条件:

$$\prod_{i=0}^3 a_i \neq 0, \quad \bigoplus_{i=0}^3 a_i \neq 0 \text{ 且 } a_i a_{j \oplus k} \neq a_{i \oplus k} a_j, i \neq j, k = \{1, 2, 3\}.$$

定理 14 有限域 $\text{GF}(2^n)$ 上的 2^m 阶 Hadamard 矩阵 $\text{Had}(a_0, a_1, \dots, a_{2^m-1})$ 是对合 MDS 矩阵的必要

条件: 矩阵元素互不相同, $\prod_{i=0}^{2^m-1} a_i \neq 0$ 且 $\bigoplus_{i=0}^{2^m-1} a_i = 1$ 。

4.3 对合矩阵和正交矩阵

对合矩阵的优点在于可以使用相同的电路实现加解密操作, 节省了密码算法加解密的实现开销, 典型的是 Anubis 和 Khazad 算法扩散层中使用的对合 MDS 矩阵。正交矩阵的优点是通过实现矩阵的转置来得到逆变换, 可以使用几乎相同的电路实现加解密操作, 所以, 正交矩阵同对合矩阵一样, 简化了逆矩阵的实现, 使解密实现效率更高。

利用特殊矩阵来构造 MDS 矩阵的研究成果很多, 文献[22]利用 MDS 码来构造对合 MDS 矩阵, Sajadieh 等[24]提出一种基于有限域 $\text{GF}(2^q)$ 构造对合 Hadamard MDS 矩阵的方法。文献[35]提出了一种构造拥有低汉明重量的对合 MDS 矩阵。早在 2009 年, Nakahara 等[36]就证明 4 阶循环 MDS 矩阵不可能是对合的。ISPEC 2014 上, Gupta 等[21]又证明了基于有限域的 $n \times n$ 循环对合 MDS 矩阵是不存在的, 同时也证明了基于有限域的 $2^d \times 2^d$ 的循环正交 MDS 矩阵也是不存在的。文献[37]从数学角度通过分解循环矩阵, 构造出一种新型的循环 MDS 矩阵。

FSE 2015 上, Sim 等[38]通过证明一些有关循环矩阵、Hadamard 矩阵、Cauchy 矩阵和 Hadamard-Cauchy 矩阵的等价类, 提出一个新的算法来搜索具有更少异或数的轻量级对合 MDS 矩阵, 该算法减少了搜索空间, 使 MDS 矩阵的搜索变得更容易, 并且找到了更大维数的 MDS 矩阵。FSE 2016 上, Liu 等[39]通过分析循环矩阵

的一些新的等价类性质, 缩小了搜索空间, 得到了一系列的循环 MDS 矩阵, 另外, 他们提出一种新型的具有类似于循环矩阵性质且具有潜在自逆性的 cyclic 矩阵, 构造出对合 left-circulant MDS 矩阵。FSE 2016 上, Li 等[40]直接基于向量空间 $\mathbb{F}_2^m$ 构造 MDS 矩阵, 采用非交换元素首次构造了作用在 4 bit 和 8 bit S 盒上的 4 阶和 5 阶轻量级循环对合 MDS 矩阵 (这一类型的基于有限域的矩阵之前在文献[21,36]中被证明是不存在的), 并且构造了一系列循环非对合 MDS 矩阵, 循环正交 MDS 矩阵, Hadamard 对合 MDS 矩阵和 Hadamard 非对合 MDS 矩阵, 这些轻量级 MDS 矩阵硬件实现所需的异或数均极少。

由于循环矩阵、Hadamard 矩阵、对合矩阵和正交矩阵等特殊矩阵相对于普通矩阵具有更低的软硬件实现代价, 所以受到研究人员的青睐, 一般来说, 利用随机检测矩阵来构造 MDS 矩阵, 可以找到足够轻量的 MDS 矩阵, 但由于需要搜索的空间非常大, 需要搜索所有可能的置换, 所以一般从理论上分析它们的一些等价类特征和自身所具有的一些性质, 以此来缩小搜索空间, 但当矩阵的维数较大时, 直接进行穷举搜索也显得不太现实, 此时, 一般在具有特定结构的矩阵中搜索 MDS 矩阵, 这样的好处是搜索的空间比较小, 可以得到这种特定结构中最轻量的 MDS 矩阵, 但可能会漏失一些更加轻量的其他 MDS 矩阵。

5 利用数学方法构造 MDS 矩阵

Cauchy 矩阵和 Vandermonde 矩阵由于具有数学上的特性, 通常被用来构造大阶 MDS 矩阵。

5.1 利用 Cauchy 矩阵构造 MDS 矩阵

根据 Cauchy 矩阵的定义 13, 结合式(9)可知, 如果对于任意的 i, j 均满足 x_i 各不相同, y_i 各不相同, 且 $x_i + y_j \neq 0$, 那么该类型矩阵的任意子方阵均非奇异, 由定理 5 可知, 可以很容易地通过 Cauchy 矩阵来构造 MDS 矩阵。有不少学者利用 Cauchy 矩阵来构造 MDS 矩阵, 文献[34]证明了 Cauchy-Hadamard 型 MDS 矩阵等效于对合 Cauchy-Hadamard 型 MDS 矩阵, 并且给出了由 Cauchy-Hadamard 型 MDS 矩阵构造对合 Cauchy-Hadamard 型 MDS 矩阵的方法。文献[41]证明了有限域上 Cauchy 矩阵的个数, 也证明了

Cauchy 矩阵一定不是循环移位矩阵。文献[42]提出一种紧凑型的 Cauchy 矩阵 (CCM, compact cauchy matrices), 它们拥有最少的不同元素数目, 更加利于软硬件实现, 他们还证明所有的紧凑型 Cauchy 矩阵可以转化为对合紧凑型 Cauchy 矩阵。文献[43]对 Cauchy 矩阵和 MDS 矩阵分别从 Hadamard 矩阵和循环移位矩阵以相结合的方式构造最优扩散层的方法进行了研究。文献[22]利用 Cauchy 矩阵的性质构造了新型的对合 MDS 矩阵。文献[35]提出一种基于 Cauchy 矩阵构造有效 MDS 矩阵的一般方法。

5.2 利用 Vandermonde 矩阵构造 MDS 矩阵

根据 Vandermonde 矩阵的定义 14, 结合式(11)可知, 当 $a_0, a_1, \dots, a_{n-1}$ 互不相同且不为 0 时, 该类型矩阵的任意子式非零, 由定理 5 可知, 可以使用 Vandermonde 矩阵来构造 MDS 矩阵。

文献[44]介绍了 2 个利用 Vandermonde 矩阵构造 MDS 矩阵的方法。文献[24]提出一种使用 Vandermonde 矩阵构造任意阶对合 MDS 矩阵的方法。文献[35]基于 Vandermonde 和 Cauchy 矩阵构造了对合 Hadamard MDS 矩阵。

采用随机检测特殊矩阵来构造 MDS 矩阵的方法通常只适用于矩阵维数较小时, 当需要构造更大维数的 MDS 矩阵时, 这种方法不适用, 此时, 可以利用数学上具有某些特性的矩阵来构造 MDS 矩阵, Cauchy 矩阵和 Vandermonde 矩阵因其独特的结构可用来构造任意阶的 MDS 矩阵。但由于这类 MDS 矩阵中元素汉明重量通常较大, 实现过程需要消耗很大的软硬件资源, 因此, 在密码算法设计中不常用。

6 利用移位和异或构造 MDS 矩阵

基于简单移位和异或构造的扩散层由于具有软硬件实现效率高, 能够增强密码算法抵抗时间、能量等密码分析能力的特点, 已被很多对称密码算法所使用, 比如, 我国无线局域网产品中使用的密码算法 SM4^[45]、3GPP LTE 国际加密标准 ZUC 算法^[46]、HIGHT^[47]、SHA-256^[48]、MD6^[49]等, 其中, SM4 和 ZUC 中所使用的就是这种类型的最优扩散层, 其分支数达到了最大。SM4 中的扩散层为 $((\mathbb{F}_2^8)^4 \rightarrow (\mathbb{F}_2^8)^4)$, $L(X) = X \oplus (X \lll 2) \oplus (X \lll 10) \oplus (X \lll 18) \oplus (X \lll 24)$, ZUC 中使用了 2 个最优扩散层, 其中一个和 SM4 中的相同,

另外一个 $L(X) = X \oplus (X \lll 8) \oplus (X \lll 14) \oplus (X \lll 22) \oplus (X \lll 30)$ 。

近几年, 有一些利用移位和异或构造 MDS 矩阵的研究, 文献[50]研究了基于循环移位和异或构造的扩散层分支数达到最优时需要满足的一些必要条件, 文献[51]研究了 SM4 型的扩散层, 指出在一定的等价意义下, 这样的最优扩散层仅有 2 个, 文献[52]研究了基于循环移位和异或运算设计的对合线性变换, 给出了这类线性变换的计数公式, 指出它们的分支数上界为 4。

7 利用 LFSR 构造迭代型最优扩散层

近几年, 随着物联网 (IoT, Internet of things) 技术的发展, 射频识别 (RFID, radio frequency identification) 标签、无线传感器网络 (WSN, wireless sensor network)、个人数字助理终端 (PDA, personal digital assistant) 等微型嵌入式设备越来越发达, 由于这些微型嵌入式计算设备在面积、通信能力、电源能量、计算速度和存储空间等方面严峻的资源限制, 要保护数据安全和用户隐私就必须设计更加轻量的密码算法, 于是, 设计更加轻量、安全的部件, 特别是扩散层成为研究焦点。

为了满足资源受限设备加解密的需求, 节省软硬件实现开销, 除了上述利用随机检测矩阵和基于移位和异或构造轻量级 MDS 矩阵外, PHOTON 轻量级 Hash 函数族的设计者们^[18]还提出一种新的最优扩散层设计策略——迭代型扩散层设计。这种设计方式借用流密码算法中的 LFSR 的设计思想, 如图 2 所示, 每次只更新一个元素, 其余元素则通过移位得到。

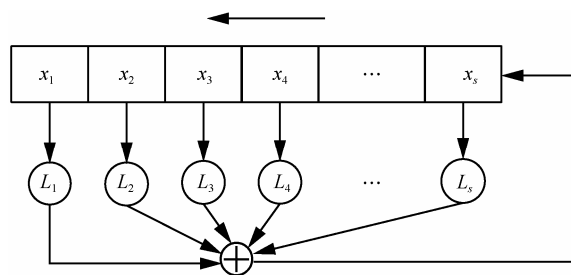


图2 PHOTON 中最优扩散层设计方式

图 2 中每个 L_i 选自有限域 $\text{GF}(2^n)$, 迭代 s 步后的最终状态作为扩散层的输出。假设 A 是 LFSR 的状态转移矩阵, 则这种方式构造的扩散层矩阵是 $\text{GF}(2^n)$ 上的 $n \times n$ 矩阵 A^s 。此外, 轻量级分组

密码算法 LED 和认证加密算法 PRIMATES^[53]的最优扩散层也采用这种方式设计。

状态转移矩阵 (也称为相伴矩阵) A 的具体形式如下。

$$A = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ L_1 & L_2 & L_3 & \cdots & L_s \end{bmatrix} \quad (13)$$

状态转移矩阵 A 的 s 次方之后得到的矩阵 $M = A^s$ 为 MDS 矩阵, 一般只提取矩阵 A 的最后一行来描述 LFSR 的选取, 即 $A_{lfsr}^{(s)} = [L_1, L_2, \dots, L_s]$ 。例如, LED 算法和 PRIMATE 算法中所使用的 MDS 矩阵分别如下。它们分别作用在有限域 $GF(2^4)$ 和有限域 $GF(2^5)$ 上。

$$\begin{aligned} (A)^4 &= \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 4 & 1 & 2 & 2 \end{bmatrix} \\ &= \begin{bmatrix} 4 & 1 & 2 & 2 \\ 8 & 6 & 5 & 6 \\ 11 & 14 & 10 & 9 \\ 2 & 2 & 15 & 11 \end{bmatrix} \\ &= M \\ (A)^5 &= \begin{bmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 18 & 2 & 2 & 18 \end{bmatrix} \\ &= \begin{bmatrix} 1 & 18 & 2 & 2 & 18 \\ 18 & 8 & 19 & 3 & 11 \\ 11 & 5 & 30 & 5 & 20 \\ 20 & 1 & 8 & 19 & 15 \\ 15 & 1 & 31 & 22 & 6 \end{bmatrix} \\ &= M \end{aligned}$$

迭代型扩散层的设计在得到 MDS 矩阵的同时, 也具有很高的硬件实现效率, 只需实现 LFSR 且能在不需要增加额外逻辑控制电路的情形下重用已有的存储, 因此, 十分适合硬件实现, 但是, 软件需要使用类似于 AES 中的查表过程实现该

扩散层, 矩阵需要用表来存储, 消耗一定的存储空间, 另外, 这种设计方式在节省硬件实现面积的同时, 增加了时钟周期, 具有一定的延迟, 因此, 它不适合在延迟性要求比较高的场景下使用。

受到 PHOTON 扩散层的启发, 越来越多的学者把关注点放在了迭代型扩散层的设计上, 涌现出了一大批研究成果。FSE 2012 上, Sajadieh 等^[54]对该设计方式进行了扩展, 并给出了一系列最优扩散层。他们将图 2 中线性变换 L_i ($1 \leq i \leq s$) 的选取从有限域 $GF(2^n)$ 扩展到了向量空间 $\mathbb{F}_2^n$ 上, 得到的 MDS 矩阵 A^s 可以表示成 $\mathbb{F}_2$ 上的 $sn \times sn$ 矩阵或者 $GF(2^n)$ 上的 $s \times s$ 分块矩阵。由于有限域 $GF(2^n)$ 上的乘法运算是向量空间 $\mathbb{F}_2^n$ 上的特殊线性变换, 因此, Sajadieh 等的工作扩展了扩散层的选择空间, 这使设计者可能构造出硬件实现代价更低的扩散层。

SAC 2012 上, Wu 等^[55]在 Sajadieh 等基础上, 通过改变线性变换的选择范围, 得到了一系列最优分支数为 5~9 的轻量级扩散层。Augot 等^[56]摆脱以上方法中复杂的符号计算, 构造出了阶数更大的迭代型 MDS 矩阵。另外, 迭代型的 MDS 矩阵构造还与码理论有关。Berger^[57]利用 Gabidulin 码构造了迭代型 MDS 矩阵。FSE 2014 上, Augot 等^[26]直接采用 BCH 码来构造迭代型 MDS 矩阵。

由于迭代型 MDS 矩阵具有高延迟的缺点, LFSR 需要进行好多拍才能得到输出向量, 于是, 研究如何构造非迭代型的轻量级 MDS 矩阵成为接下来的研究重点。一些学者重新基于有限域来构造轻量级 MDS 矩阵, 经过精心选择有限域上元素, 可以使软硬件实现代价降低。最近, CHES 2014 上, Khoo 等^[58]指出不可约多项式的选取对有限域上元素乘法实现有很大影响, 这意味着可以选择有效的不可约多项式来构造 MDS 矩阵, 节省软硬件实现开销。文献[38]对该性质进行了进一步的研究。

8 MDS 矩阵的实现方法

在实际应用中, 密码算法需要在不同软硬件平台上高效实现, 而扩散层作为密码算法一个很重要的部分, 它的实现性能直接影响整个密码算法的高效性能。一般来说, 实现 MDS 矩阵的常用方法有基于 `xtime()` 乘法^[4]、基于字的乘法、查

小表、查大表,后2种是通过预置乘法表的方法,利用空间换取时间来提高运行速度。为了节省软硬件资源,提高密码算法运行速度,需要根据不同的应用场景,选用不同的实现方式,在资源空间受限的情况下,适宜采用基于字的乘法实现方式;在资源空间充足的情况下,宜采用查大表的方法实现MDS矩阵^[36,59]。

9 结束语

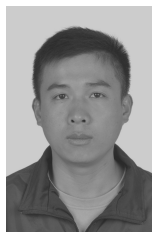
MDS矩阵广泛应用于分组密码算法、Hash函数、认证加密算法,使用MDS矩阵作为扩散层,可以保证分支数达到最大,从而可以最大限度地保证密码算法在差分和线性分析下的安全性。本文比较系统地阐述了常见的构造MDS矩阵的方法:从线性码中提取MDS矩阵;采用随机检测矩阵构造特殊MDS矩阵,如循环MDS矩阵、Hadamard MDS矩阵、对合MDS矩阵和正交MDS矩阵;使用数学上具有特殊性质的矩阵,如Cauchy矩阵和Vandermonde矩阵构造MDS矩阵。本文基于移位和异或构造高效的MDS矩阵和利用LFSR构造硬件实现友好的迭代型最优扩散层,介绍了构造MDS矩阵的原理,并详细给出了各种方法的研究现状以及其中的优缺点,最后,给出了MDS矩阵的实现方法,设计者可以根据应用场景的不同选用不同的实现方式以提高算法运行速度,节省软硬件资源。

参考文献:

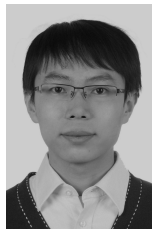
- [1] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 2015, 28(4):656-715.
- [2] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.
- [3] MATSUI M. Linear cryptanalysis method for DES cipher[M]// Advances in Cryptology — EUROCRYPT. Berlin Heidelberg: Springer, 1993:386-397.
- [4] DAEMEN J, RIJMEN V. The design of rijndael, AES—the advanced encryption standard[M]. Berlin Heidelberg: Springer, 2002.
- [5] RIJMEN V, DAEMEN J. The cipher SHARK[C]//Fast Software Encryption. c1996:99-112.
- [6] 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. c1998.
- [7] SCHNEIER B, KELSEY J, WHITING D, et al. The twofish encryption algorithm[M].1999.
- [8] DAEMEN J, KNUDSEN L R, RIJMEN V. The block cipher square[C]//The 4th fast software encryption workshop. c1997: 149-165.
- [9] BARRETO P, RIJMEN V. The anubis block cipher[EB/OL]. <http://www.larc.usp.br/~pbarreto/AnubisPage.html>.
- [10] BARRETO P, RIJMEN V. The khazad legacy-level block cipher[J]. Primitive Submitted to NESSIE, 2000.
- [11] JUNOD P, VAUDENAY S. FOX: a new family of block ciphers[C]//Selected Areas in Cryptography. c2004:114-119.
- [12] SHIRAI T, SHIBUTANI K, AKISHITA T, et al. The 128 bit block cipher CLEFIA[C]//International Workshop on Fast Software Encryption. c2007: 181-195.
- [13] GUO J, PEYRIN T, POSCHMANN A, et al. The LED block cipher[C]//International Workshop on Cryptographic Hardware and Embedded Systems. c2011: 326-341.
- [14] WATANABE D, FURUYA S, YOSHIDA H, et al. A new key-stream generator MUGI[C]//FSE 2002. c2002:179-194.
- [15] FILHO G D, BARRETO P, RIJMEN V. The maelstrom-0 Hash function[C]//The 6th Brazilian Symposium on Information and Computer Systems Security. c2006.
- [16] GAURAVARAM P, KNUDSEN L R, MATUSIEWICZ K, et al. Groestl a SHA-3 candidate[EB/OL]. <http://www.groestl.info>.
- [17] BARRETO P S L M, RIJMEN V. Encyclopedia of cryptography and security[C]//2nd Edn. c2011:1384-1385.
- [18] GUO J, PEYRIN T, POSCHMANN A. The PHOTON family of lightweight hash functions[C]// Rogaway-CRYPTO 2011. c2011: 222-239.
- [19] DAMGÅRD I B. A design principle for hash functions[C]// Advances in Cryptology-CRYPTO'89. c1990: 416-427.
- [20] RAO A R, BHIMASANKARAM P. Linear algebra[M]. Hindustan Book Agency.
- [21] KISHAN C G, INDRANIL G R. On constructions of circulant MDS matrices for lightweight cryptography[C]// ISPEC. c2014: 564-576.
- [22] YOUSSEF A M, MISTER S, TAVARES S E. On the design of linear transformations for substitution permutation encryption networks[C]//Workshop On Selected Areas in Cryptography(SAC). c1997:40-48.
- [23] WILLIAMS F J M, SLOANE N J A. The theory of error correcting codes[M]. Elsevier, 1977.
- [24] SAJADIEH M, DAKHILALIAN M, MAL H, et al. On construction of involutory MDS matrices from vandermonde matrices in [C]// Design, Codes Cryptography. c2012:1-22.
- [25] LINT J H V. Algebraic geometric codes[M]//Coding theory and design theory. New York :Springer, 1990: 137-162.
- [26] AUGOT D, FINIASZ M. Direct construction of recursive MDS diffusion layers using shortened BCH codes[C]//International Workshop on Fast Software Encryption. c2014: 3-17.
- [27] GOPPA V D. A new class of linear correcting codes[J]. Problemy Peredachi Informatsii, 1970, 6(3): 24-30.
- [28] BERGER T P, OURIVSKI A. Construction of new MDS codes from gabidulin codes[C]// ACCT. c2009: 40-47.
- [29] 杨谱. 分组迭代密码函数的扩散层分析及应用[D]. 西安: 西安电子科技大学, 2013.
YANG P. Cryptanalysis and applications for diffusion layer of iterated block function[D]. Xi'an: Xidian University, 2013.
- [30] JUNOD P, VAUDENAY S. Perfect diffusion primitives for block ciphers[C]//International Workshop on Selected Areas in Cryptography. c2004: 84-99.
- [31] 何凌云. 分组密码扩散层的改进研究[D]. 杭州: 杭州电子科技大学, 2011.
HE L Y. Research on the improvement of block cipher diffusion layer[D]. Hangzhou: Hangzhou Dianzi University, 2011.
- [32] 郭艳珍, 韩文报, 赵龙, 等. AES 列混合变换[J]. 解放军理工大学学报(自然科学版), 2009 (3): 232-236.
GUO Y Z, HAN W B, ZHAO L, et al. AES mixColumns transfor-

- mation[J]. Journal of PLA University of Science and Technology (Natural Science Edition), 2009(3): 232-236.
- [33] 刘丽辉, 徐林杰, 张祖平, 等. 有限域上 Hadamard 型 MDS 矩阵研究[J]. 舰船电子工程, 2014(5):41-45.
- LIU L H, XU L J, ZHANG Z P, et al. Investigate for MDS matrix of hadamard type on finite fields[J]. Ship Electronic Engineering, 2014(5):41-45.
- [34] 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.
- CUI T, JIN C H. Construction of involution cauchy-hadamard type MDS matrices[J]. Journal of Electronics & Information Technology, 2010, 32(2): 500-503.
- [35] GUPTA K C, RAY I G. On constructions of involutory MDS matrices[C]//International Conference on Cryptology in Africa. c2013: 43-60.
- [36] NAKAHARA J R, Élcio A. A new involutory mds matrix for the AES[J]. Network Security, 2009,9(2):109-116.
- [37] DEHNAVI S M, SHAMSABAD M R M, RISHAKANI A M, et al. Efficient MDS diffusion layers through decomposition of matrices[M]// IACR Cryptology. ePrint Archive, 2015.
- [38] SIM S M, KHOO K, OGGIER F, et al. Lightweight MDS Involution Matrices[C]//FSE 2015. c2015.
- [39] LIU M, SIM S M. Lightweight MDS generalized circulant matrices[C]//Fast Software Encryption. c2016.
- [40] LI Y, WANG M. On the construction of lightweight circulant involutory MDS matrices[C]//Fast Software Encryption. c2016.
- [41] 崔霆, 金晨辉. 分组密码 Cauchy 型 MDS 扩散结构的几点笔记[J]. 电子学报, 2011, 39(7): 1603-1607.
- CUI T, JIN C H. Several remarks of Cauchy type MDS diffusion layer for block cipher[J]. Acta Electronica Sinica, 2011, 39(7): 1603-1607.
- [42] CUI T, JIN C, KONG Z. On compact cauchy matrices for substitution-permutation networks[J]. IEEE Transactions on Computers, 2015, 64(7): 2098-2102.
- [43] 马庆禄, 魏悦川, 潘晓中. 基于 Cauchy 矩阵的线性变换的研究[J]. 计算机应用研究, 2015, 32(7): 2144-2146.
- MA Q L, WEI Y C, PAN X Z. Research on linear transformations based on Cauchy matrix[J]. Application Research of Computers, 2015, 32(7), 2144-2146.
- [44] LACAN J, FIMES J. Systematic MDS erasure codes based on vandermonde matrices[J]. IEEE Communications Letters, 2004, 8(9): 570-572.
- [45] 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>.
- [46] ETSI/SAGE TS 35.222-2011, specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3; document 2: ZUC Specification[S].
- [47] HONG D, SUNG J, HONG S, et al. HIGHT: a new block cipher suitable for low-resource device[M]//Cryptographic Hardware and Embedded Systems-CHES 2006. Berlin Heidelberg: Springer, 2006: 46-59.
- [48] National institute of standards and technology[S]. The Secure Hash Standard, 2002.
- [49] RIVEST R L, AGRE B, BAILEY D V, et al. The MD6 hash function[J]. Invited Talk at CRYPTO, 2008.
- [50] ZHANG W, WU W, FENG D, et al. Some new observations on the SMS4 block cipher in the Chinese WAPI standard[M]//Information Security Practice and Experience. Berlin Heidelberg: Springer, 2009: 324-335.
- [51] 王金波. 基于循环移位构造最优线性变换[C]. 中国密码学会 2007 年会, 成都. c2007:306-307.
- WANG J B. The optimal permutation in cryptography based on cyclic-shift linear transform[C]//China Crypt'2007, Chengdu. c2007: 306-307.
- [52] 李瑞林, 熊海, 李超. 基于循环移位和异或运算的对合线性变换研究[J]. 国防科技大学学报, 2012, 34(2): 46-50.
- LI R, XIONG H, LI C. Research on involutorial linear transformations based on rotation and XOR[J]. Journal of National University of Defense Technology, 2012, 34(2): 46-50.
- [53] ANDREEVA E, BILGIN B, BOGDANOV A, et al. PRIMATES v1.02 submission to the CAESAR competition[EB/OL]. <http://competitions.cr.yt.to/round2/primatesv102.pdf>.
- [54] SAJADIEH M, DAKHILALIAN M, MALA H, et al. Recursive diffusion layers for block ciphers and Hash functions[C]// FSE 2012. c2012:385-401.
- [55] WU S, WANG M, WU W. Recursive diffusion layers for (lightweight) block ciphers and Hash functions[C]//SAC 2012. c2012: 355-371.
- [56] AUGOT D, FINIASZ M. Exhaustive search for small dimension recursive MDS diffusion layers for block ciphers and hash functions[C]// 2013 IEEE International Symposium on Information Theory (ISIT). c2013:1551-1555.
- [57] BERGER T P. Construction of recursive MDS diffusion layers from gabidulin codes[C]//Indocrypt. c2013:274-285.
- [58] KHOO K, PEYRIN T, POSCHMANN A, et al. FOAM: searching for hardware optimal spn structures and components with a fair comparison[C]//Cryptographic Hardware and Embedded Systems (CHES). c2014: 433-450.
- [59] 刘鸿博, 金晓刚, 段俊红. 分组密码中 MDS 矩阵的实现方法效能分析[J]. 信息安全与通信保密, 2013(10):77-78.
- LIU H B, JIN X G, DUAN J H. Efficiency analysis of MDS matrix applied in block cipher[J]. Information Security and Communications Privacy, 2013(10):77-78.

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。



李永强 (1982-), 男, 吉林集安人, 博士, 中国科学院信息工程研究所副研究员, 主要研究方向为对称密码算法关键部件的构造、对称密码算法分析。