典型密码结构的不可能差分区分器研究*

刘 健[1],毕鑫杰[2],李艳俊[1,2],金 达[1]

(1.中国电子科技集团公司第十五研究所 信息产业信息安全测评中心,北京 100083;
2.北京电子科技学院 密码科学与技术系,北京 100070)

摘 要:20世纪40年代Shannon提出了对称密码设计的两个重要原则"混淆"和"扩散",之后密码学者们基于这两个原则构造了Feistel、SP、广义Feistel、MISTY等主要整体结构,目前这些结构被广泛运用于各种标准密码算法和新型认证加密算法。对这几种主要密码算法的整体结构进行了介绍和研究,并基于具体结构的特点,系统地对广义Feistel结构中TYPE-I、TYPE-II、TYPE-III型结构构建了不可能差分区分器,对区分器轮数下界进行了推导和证明,为网络安全领域分组密码、序列密码、认证加密、Hash函数等对称密码的设计和分析提供了参考。

关键词:分组密码;整体结构;不可能差分区分器

中图分类号:TP309.7 **文献标识码**:A **DOI**:10.20044/j.csdg.2097-1788.2022.03.007

引用格式:刘健,毕鑫杰,李艳俊,等.典型密码结构的不可能差分区分器研究[J].网络安全与数据治理,2022,41(3):40-47.

Research on impossible differential distinguisher for typical cryptographic structures

Liu Jian[1], Bi Xinjie[2], Li Yanjun[1,2], Jin Da[1]

(1.Information Industry Information Security Evaluation Center,
The 15th Research Institute of China Electronic Technology Group Corporation, Beijing 100083, China;
2.Department of Cryptography and Technology, Beijing Electronic Science and Technology Institute, Beijing 100070, China)

Abstract: In the 1940s, two important principles for symmetric cryptography design were proposed by Shannon, "confusion" and "diffusion", then based on which Feistel, SP, generalized Feistel, MISTY and other major overall structures were constructed. At present, these structures are widely used in various standard cryptographic algorithms and new authentication encryption algorithms. In this paper, the overall structures of these major cryptographic algorithms are introduced and researched. Based on the characteristics of TYPE-I, TYPE-II and TYPE-III of general Feistel structures, the corresponding impossible differential distinguishers are systematically constructed, and the lower bounds of the number of distinguisher rounds are deduced and proved. Our results are benefit for symmetric cryptographic structures design and analysis such as block ciphers, sequence ciphers, authenticated encryption, and Hash functions.

Key words: block ciphers; the overall structure; impossible differential distinguisher

0 引言

1949年Shannon发表了经典论文"Communication Theory of Secrecy System"[1],该文从抵抗攻击的角度出发,提出了加密算法的"混淆"和"扩散"准则。混淆和扩散成功地实现分组密码明文、密钥和密文之间呈现多种伪随机性质,因而成为现代分组密码设计的重要原则之一。进一步,Shannon还在文章中介绍了代替(Substitution)-置换(Permutation)网络(简称SPN),其主要是基于代替S盒和P置换两种最基本组件的密码运算,又叫做混合变换(mixing transformations)。不同的混合变换组合成了不同的整体结构,以实现"混淆"和"扩散"的目标。目前分组密码中比较主流的整体结构有Feistel结构、SP结构、广义Feistel结构、MISTY结构等。

*基金项目:数学工程与先进计算国家重点实验室与河南省网络密码技术重点实验室联合开放课题(LNCT2020-A09)

随着分组密码设计与分析的发展，一方面算法结构方面的研究越来越细化，比如 Feistel-SP 组合结构、ARX 结构、基于逻辑单元设计的整体结构等[2-4]；同时，以往主要用于分组密码的整体结构越来越广泛地应用于网络空间安全领域的数据快速加密认证体制中，如序列密码设计、Hash 函数设计以及认证加密算法设计等，最具代表性的是 2018 年 NIST 发起的轻量级认证算法征集活动，第一轮候选算法广泛采用了这些整体结构。另一方面对结构的安全性分析和证明也有了丰富的成果[5-9]。与差分分析、线性分析相比，不可能差分区分器基于截断差分构建，对于差分性能较好的算法攻击效果更好，如对 CLEFIA 的攻击可以达到 13 轮[10]，对 Camellia 的攻击最长可以达到 14 轮[11]；然而，密码学者们更多地关注具体密码算法的不可能差分安全性，对于一般的结构安全性分析证明较少，以至于新的密码算法设计会出现结构方面的安全隐患，比如 2019 年全国密码设计竞赛中候选算法 TASS1[12]，基于广义 Feistel 结构设计，并且采用了随机密钥池保证安全性，但是由于未对整体结构进行评估，导致了存在全轮不可能差分区分器[13]。因此，随着信息安全技术及其应用的快速发展，不管是现在还是将来，密码结构安全始终是密码算法安全的首要保障。

本文对 Feistel 结构、SP 结构、广义 Feistel 结构、MISTY 结构四种主要整体结构进行了介绍和研究，重点对广义 Feistel 结构的 TYPE-I 型、TYPE-II 型和 TYPE-III 型进行了详细分析，基于这些结构的特点构建了不可能差分区分器，进一步给出了详细证明过程。本文研究希望能够为网络空间安全领域分组密码、序列密码、Hash 函数、认证加密等对称密码结构的设计与分析提供参考。

1 Feistel 结构

20 世纪 60 年代 Horst Feistel 设计出基于 SP 结构的 LUCIFER 体制，在该体制中没有给出具体 S 盒，而且加解密不同，需要消耗更多的硬件电路。后来 Horst Feistel 由“流水线”工作模式想到每次只加密一半的明文数据，进而设计了加解密相似的结构，并以 Feistel 命名。1967 年公开发表的几篇技术报告为 Feistel 密码结构的安全性研究奠定了基础。加解密相似是 Feistel 型密码的一个实现优点，但其每轮只对一部分数据进行处理，需要两轮甚至多轮才能改变输入的每一个比特。基于 Feistel 结构的代表算法有数据加密标准 DES、日本分组密码标准 Camellia 等。

1.1 Feistel 结构描述

定义 1 Feistel 结构是一种典型的迭代结构，它能够实现扩散与混乱，构成安全强度高的密码算法。假设圈函数为 Q_K，输入为 X_0, X_1，一轮加密可以表示为：

$$Q_K:(X_0,X_1)\rightarrow(Y_0,Y_1) \tag{1}$$

$$Y_0=X_1,\ Y_1=X_0\oplus F(K,X_1) \tag{2}$$

Feistel 结构如图 1 所示。函数 F 不一定可逆，可由一些非线性组件和线性组件构成，起到扩散和混淆的效果。

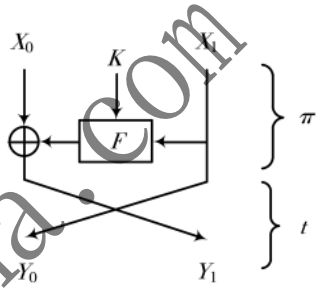

图 1 Feistel 结构

圈变换 Q_K 可以被分解为 $t\circ\pi$，这里 π 由 $\pi(X_0,X_1)=(X_0\oplus F_K(X_1),X_1)$ 定义。容易验证 π 是恒等变换，即 π 是它自身的逆，也称为对合函数；t 是交换函数，也是对合的。容易得到圈函数 Q_K 逆 $Q_K^{-1}=\pi\circ t$。

将 Feistel 结构迭代 r 轮，当最后一轮去掉交换时解密过程与加密过程一样，这是因为 $E_K=\pi_r\circ t\cdots\circ\pi_2\circ t\circ\pi_1$，$E_K^{-1}=\pi_1\circ t\cdots\circ\pi_{r-1}\circ t\circ\pi_r$。所以解密时只需将密文作为输入，轮子密钥的次序与加密过程相反。

1.2 不可能差分区分器

性质 1 假设函数 F 为随机置换，则 Feistel 结构存在 5 轮不可能差分区分器[14]。

如图 2 所示，对于一个 5 轮 Feistel 结构，假设 α 为非零差分，那么当输入差分为 $(0,\alpha)$ 时，输出差分为 $(0,\alpha)$ 的概率为 0。证明过程主要利用了 F 为置换的特点，详细过程见文献[14]。

2 SP 结构

根据混淆-扩散原则，SP 结构设计得非常清晰，由 S 盒层和 P 扩散层组合生成。S 盒层一般被称为混淆层，主要起混淆作用；P 置换一般组成扩

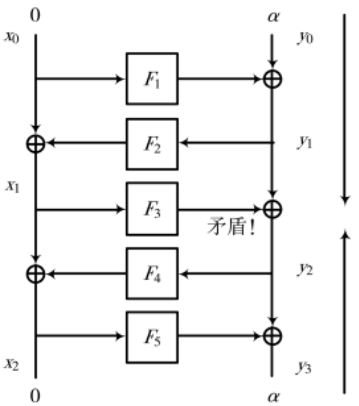

图 2 Feistel 的 5 轮不可能差分区分器

散层,主要起扩散作用。在明确 S 盒和 P 置换的某些密码指标后,设计者能估计 SP 结构密码抵抗差分分析和线性分析的能力。SP 结构与 Feistel 结构相比,可以得到更快速的扩散,但是 SP 密码的加/解密通常不相似,若要相似需采用逆等函数作为组件。SP 结构代表算法有国际加密标准 AES、韩国标准 ARIA、2019 竞选胜出算法 uBlock[15]等。

2.1 SP 结构描述

定义 2 假设 SP 结构每轮的圈函数包含三层变换:先是将 mn 比特明文数据分为 n 个子块,每块含 m 比特,即 S 层为 n 个 S 盒并置;然后置换层 P 为线性变换。S 盒是 m 比特随机置换:$X\mapsto Y:F_2^m\to F_2^m$,设 S 盒输入为 $X_i\oplus K_i$,输出为 Y_i;P 是线性变换:$Y\mapsto Z:F_{2^m}^n\to F_{2^m}^n$;最后输出的 Z_i 与轮密钥 K_i 运算:$Z_i\oplus K_i$,$1\leqslant i\leqslant n$。圈函数用公式描述为:

$$Q_K:(X_1,X_2,\cdots,X_n)\to(Z_1,Z_2,\cdots,Z_n) \tag{3}$$

S 盒层变换:$Y_i=S(X_i\oplus K_i)$,$1\leqslant i\leqslant n$;P 层变换:$[Z_1,Z_2,\cdots,Z_n]^{\mathrm{T}}=P[Y_1,Y_2,\cdots,Y_n]^{\mathrm{T}}$。

图 3 所示为 SP 结构示意图。

SP 结构中,由于最后一轮的线性变换没有加强密码性能,同时为了减小加解密变换的差异,因此在设计迭代结构时通常将最后一轮的线性变换省略掉。这种 SP 结构既可以用来构建分组密码算法的整体结构,例如 AES、uBlock;也可以作为 Feistel 整体结构中圈函数的部件,例如SM4、CLEFIA、Camellia 等算法。

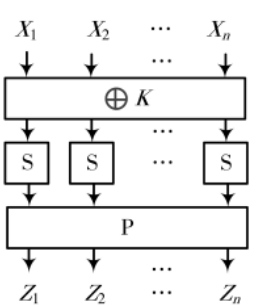

图 3 SP 结构

2.2 不可能差分区分器

性质 2 对于 SP 结构密码算法,若 S 盒为随机置换,那么无论 P 取哪一种线性变换,必存在 2 轮不可能差分区分器[16]。

性质 3 若扩散层 P 对应系数矩阵中的元素含 0,则基于字节(半字节)设计的 SP 结构存在 3 轮不可能差分区分器[16]。

采用二元域上矩阵作为扩散层 P,则矩阵中必有零元素出现。根据这个性质容易推出 3 轮不可能差分区分器,如图 4 所示。

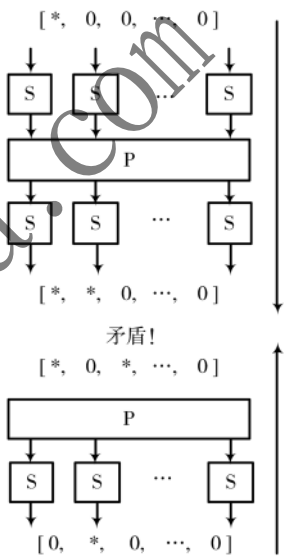

图 4 SP 结构 3 轮不可能差分路径

在实际使用的分组密码算法中,扩散层 P 通常由多级扩散构成,结合 S 盒差分分布表,通常存在更多轮数的区分器,如 AES、ARIA、uBlock 都存在 4 轮不可能差分区分器[16]。

3 广义 Feistel 结构

广义 Feistel 结构(Generalized Feistel Structure, GFS)[17]是 Feistel 结构的推广,特点是对分组再进行小分块处理,使同时处理的分块长度较小。目前出现的主要有 TYPE-I、TYPE-II、TYPE-III 三种结构。2010 年 FSE 会议上 Suzaki 等人基于图论的知识对 TYPE-II 型进行了改进,减小了全扩散的轮数[18]。

3.1 广义 Feistel 结构描述

基于 TYPE-I 结构设计的分组密码有 CAST[19]、SMS4 等;基于 TYPE-II 结构设计的分组密码有 CLEFIA 等;基于 TYPE-III 结构设计的分组密码有 MARS[20]、

轻量级 LEA[21]等；基于改进 TYPE-II 结构设计的分组密码有轻量级 LBlock、TWINE[22]等。下面对 TYPE-I、TYPE-II 和 TYPE-III 型结构依次进行介绍和不可能差分区分器证明。

定义 3 假设输入一组明文分成 n 个子块，即 $X_0, X_1, \cdots, X_{n-1}$，定义一个函数 F_K(不要求可逆)，则圈函数可以表示成：

$$Q_K:(X_0, X_1, \cdots, X_{n-1}) \rightarrow (Y_0, Y_1, \cdots, Y_{n-1}) \tag{4}$$

$$Y_0 = F_K(X_0) \oplus X_1, Y_1 = X_2, \cdots, Y_{n-1} = X_0 \tag{5}$$

由这种方式获得的函数被称为 TYPE-I 型结构，其结构如图 5 所示。

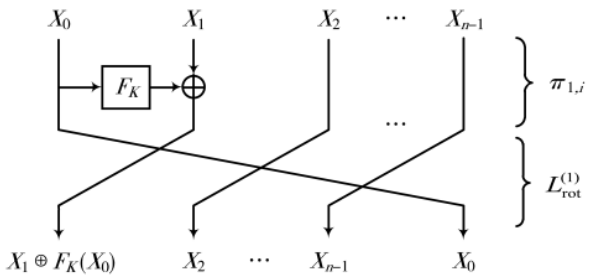

图 5 TYPE-I 型结构

图 5 中 TYPE-I 型结构可以被分解为 $L_{\text{rot}}^{(1)} \circ \pi_{1,i}$，这里 $\pi_{1,i}$ 由 $\pi_{1,i}(X_0, X_1, \cdots, X_{n-1}) = (X_0, X_1 \oplus F_K(X_0), X_2, \cdots, X_{n-1})$ 定义。容易验证 $\pi_{1,i} \circ \pi_{1,i}$ 是恒等变换，即 $\pi_{1,i}$ 是对合函数。现在可以看出圈函数 Q_K 是一个可逆排列，并且它的逆 $Q_K^{-1} = \pi_{1,i} \circ R_{\text{rot}}^{(1)}$。

TYPE-I 型结构迭代 r 轮后，加密变换 $E_K = \pi_{1,r} \circ L_{\text{rot}}^{(1)} \circ \cdots \circ \pi_{1,2} \circ L_{\text{rot}}^{(1)} \circ \pi_{1,1}$，解密变换 $E_K^{-1} = \pi_{1,1} \circ R_{\text{rot}}^{(1)} \circ \cdots \circ \pi_{1,r-1} \circ R_{\text{rot}}^{(1)} \circ \pi_{1,r}$，不仅要变换轮密钥顺序，还需改变循环移位的方向。

定义 4 假设输入一组明文分成 n 个子块，即 $X_0, X_1, \cdots, X_{n-1}$，定义一个函数 F_K(一般情况下是双射)，则 TYPE-II 圈函数可以表示成：

$$Q_K:(X_0, X_1, \cdots, X_{n-1}) \rightarrow (Y_0, Y_1, \cdots, Y_{n-1}) \tag{6}$$

$$Y_0 = F_{K0}(X_0) \oplus X_1, Y_1 = X_2, \cdots, Y_{n-2} = F_{Kt}(X_{n-2}) \oplus X_{n-1}, Y_{n-1} = X_0 \tag{7}$$

其中 $t = \dfrac{n-1}{2} - 1$，称由这种方式获得的函数为 TYPE-II 型结构，其结构图如图 6 所示。

图 6 中 TYPE-II 型结构可以被分解为 $L_{\text{rot}}^{(1)} \circ \pi_{2,i}$，这里 $\pi_{2,i}$ 由 $\pi_{2,i}(X_0, X_1, \cdots, X_{n-1}) = (X_0, F_{K0}(X_0) \oplus X_1, X_2, \cdots, F_{Kt}(X_{n-2}) \oplus X_{n-1})$ 定义。容易验证 $\pi_{2,i} \circ \pi_{2,i}$ 是

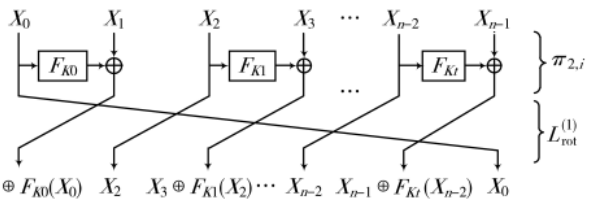

图 6 TYPE-II 型结构

恒等变换，即 $\pi_{2,i}$ 是对合函数。可以看出圈函数 Q_K 是一个可逆变换，并且它的逆 $Q_K^{-1} = \pi_{2,i} \circ R_{\text{rot}}^{(1)}$。

TYPE-II 型结构迭代 r 轮后，加密变换 $E_K = \pi_{2,r} \circ L_{\text{rot}}^{(1)} \circ \cdots \circ \pi_{2,2} \circ L_{\text{rot}}^{(1)} \circ \pi_{2,1}$，解密变换 $E_K^{-1} = \pi_{2,1} \circ R_{\text{rot}}^{(1)} \circ \cdots \circ \pi_{2,r-1} \circ R_{\text{rot}}^{(1)} \circ \pi_{2,r}$，不仅要变换轮密钥顺序，还需改变循环移位的方向。

定义 5 假设输入一组明文分成 n 个子块，即 $X_0, X_1, \cdots, X_{n-1}$，定义一个函数 F_K(一般情况下是双射)，则圈函数可以表示成：

$$Q_K:(X_0, X_1, \cdots, X_{n-1}) \rightarrow (Y_0, Y_1, \cdots, Y_{n-1}) \tag{8}$$

$$Y_0 = X_1 \oplus F_{K0}(X_0), Y_1 = X_2 \oplus F_{K1}(X_1), \cdots, Y_{n-2} = X_{n-1} \oplus F_{Kt}(X_{n-2}), Y_{n-1} = X_0 \tag{9}$$

其中 $t = n-2$，称由这种方式获得的函数为 TYPE-III 结构。

基于 TYPE-III 设计的分组密码相对较少，MARS 和 LEA 算法基于这种结构设计。

图 7 轮变换可以被分解为 $L_{\text{rot}}^{(1)} \circ \pi_{3,i}$，这里 $\pi_{3,i}$ 由 $\pi_{3,i}(X_0, X_1, \cdots, X_{n-1}) = (X_0, X_1 \oplus F_{K0}(X_0), X_2 \oplus F_{K1}(X_1), \cdots, X_{n-1} \oplus F_{Kt}(X_{n-2}))$ 定义。容易验证 $\pi_{3,i} \circ \pi_{3,i}$ 不再是恒等变换。圈函数 Q_K 是一个可逆变换，并且它的逆 $Q_K^{-1} = \pi_{3,i}^{-1} \circ R_{\text{rot}}^{(1)}$。

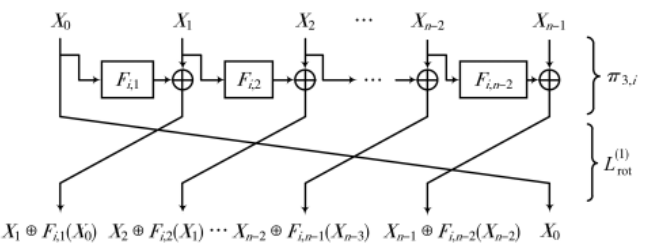

图 7 TYPE-III 型结构

TYPE-III 型结构迭代 r 轮后，加密变换 $E_K = \pi_{3,r} \circ L_{\text{rot}}^{(1)} \circ \cdots \circ \pi_{3,2} \circ L_{\text{rot}}^{(1)} \circ \pi_{3,1}$，解密变换 $E_K^{-1} = \pi_{3,1}^{-1} \circ R_{\text{rot}}^{(1)} \circ \cdots \circ \pi_{3,r-1}^{-1} \circ R_{\text{rot}}^{(1)} \circ \pi_{3,r}^{-1}$，不仅要变换轮密钥顺序，还

需改变循环移位的方向。

3.2 不可能差分区分器

性质4 设函数F是随机置换,则n轮全扩散的TYPE-I型分组密码必有n^2+n-1轮不可能差分区分器。

证明:TYPE-I型分组密码扩散较慢,所以以表的形式给出各轮输入差分模式。如表1所示,对于n分块的TYPE-I型结构输入差分为$[0,0,0,\cdots,0,0,a]$,经过n轮加密之后为$[\Delta_F(a),0,0,\cdots,0,0,a]$,$\Delta_F(a)$为非零值;再经过$n-1$轮,即在第$2n-1$轮输入处差分为$[\Delta_F^n(a)\oplus a,\Delta_F(a),\Delta_F^2(a),\cdots,\Delta_F^{n-3}(a),\Delta_F^{n-2}(a),\Delta_F^{n-1}(a)]$,因为$\Delta_F^n(a)\oplus a=?$,差分值不确定,而$\Delta_F^i(a)$为非零,所以记作$[?,*,*,\cdots,*]$;在加密方向继续推导,在第$2n+1$轮输出处差分模式为$[?,*,*,\cdots,\Delta_F^n(a)\oplus a,?]$。其中"*"表示非零子块。

如表2所示,假设若干轮加密后输出差分模式为$[a,0,0,\cdots,0,0,0]$,解密方向经过1轮输出$[0,a,0,\cdots,0,0,0]$,容易推导出n^2-n-2轮后输出为$[?,?,?,\cdots,?,a,?]$,共解密n^2-n-2轮。与加密方向第$2n+1$轮输出处差分模式$[?,*,*,\cdots,\Delta_F^n(a)\oplus a,?]$发生矛盾,所以共有$n^2-n-2+2n+1=n^2+n-1$轮不可能差分区分器,如图8所示。

例如,当分块为3时,容易推导不可能差分区分器轮数为8;当分块为4时,如MARS-256算法,容易验证其区分器轮数大于15。

性质5 设函数F是随机置换,则n轮全扩散的TYPE-II型分组密码必有$2n+1$轮不可能差分区分器。

表2 TYPE-I型结构解密方向差分模式

轮数	X_0	X_1	X_2	…	X_{n-3}	X_{n-2}	X_{n-1}
0	a	0	0	…	0	0	0
1	0	a	0	…	0	0	0
…	…	…	…	…	…	…	…
$n-1$	0	0	0	…	0	0	a
n	a	*	0	…	0	0	0
$n+1$	0	a	*	…	0	0	0
…	…	…	…	…	…	…	…
$2n-3$	0	0	0	…	a	*	0
$2n-2$	0	0	0	…	0	a	*
$2n-1$	*	*	0	…	0	0	a
$2n$	a	?	*	…	0	0	0
…	…	…	…	…	…	…	…
n^2-2n	a	?	?	…	?	*	0
n^2-2n+1	0	a	?	…	?	?	*
n^2-2n+2	*	*	a	…	?	?	?
…	…	…	…	…	…	…	…
n^2-n-2	?	?	?	…	?	a	?

证明:n轮全扩散的TYPE-II型结构分块为n,下面从加密方向和解密方向进行推导。

在加密方向,假设n个子块$X_0,X_1,\cdots,X_{n-1}$的输入差分模式为$[0,0,\cdots,0,a]$,即X_{n-1}处差分非零,其余子块差分全为0,经过n轮变换之后输出差分模式为$[*,*,\cdots,*,a]$。

在解密方向,假设第$2n+1$轮输出的n个子块$[X_0,X_1,\cdots,X_{n-1}]$差分模式为$[0,0,\cdots,a,0]$,即X_{n-2}处差分非零,其余子块差分全为0,经过n轮解密

表1 TYPE-I型结构加密方向差分模式

轮数	X_0	X_1	X_2	…	X_{n-3}	X_{n-2}	X_{n-1}
0	0	0	0	…	0	0	a
1	0	0	0	…	0	a	0
…	…	…	…	…	…	…	…
$n-1$	a	0	0	…	0	0	0
n	$\Delta_F(a)$	0	0	…	0	0	a
$n+1$	$\Delta_F^2(a)$	0	0	…	0	a	$\Delta_F(a)$
…	…	…	…	…	…	…	…
$2n-4$	$\Delta_F^{n-3}(a)$	0	0	…	$\Delta_F^{n-6}(a)$	$\Delta_F^{n-5}(a)$	$\Delta_F^{n-4}(a)$
$2n-3$	$\Delta_F^{n-2}(a)$	0	a	…	$\Delta_F^{n-5}(a)$	$\Delta_F^{n-4}(a)$	$\Delta_F^{n-3}(a)$
$2n-2$	$\Delta_F^{n-1}(a)$	a	$\Delta_F(a)$	…	$\Delta_F^{n-4}(a)$	$\Delta_F^{n-3}(a)$	$\Delta_F^{n-2}(a)$
$2n-1$	$\Delta_F^n(a)\oplus a$	$\Delta_F(a)$	$\Delta_F^2(a)$	…	$\Delta_F^{n-3}(a)$	$\Delta_F^{n-2}(a)$	$\Delta_F^{n-1}(a)$
$2n$	?	*	*	…	*	*	$\Delta_F^n(a)\oplus a$
$2n+1$	?	*	*	…	*	$\Delta_F^n(a)\oplus a$	?

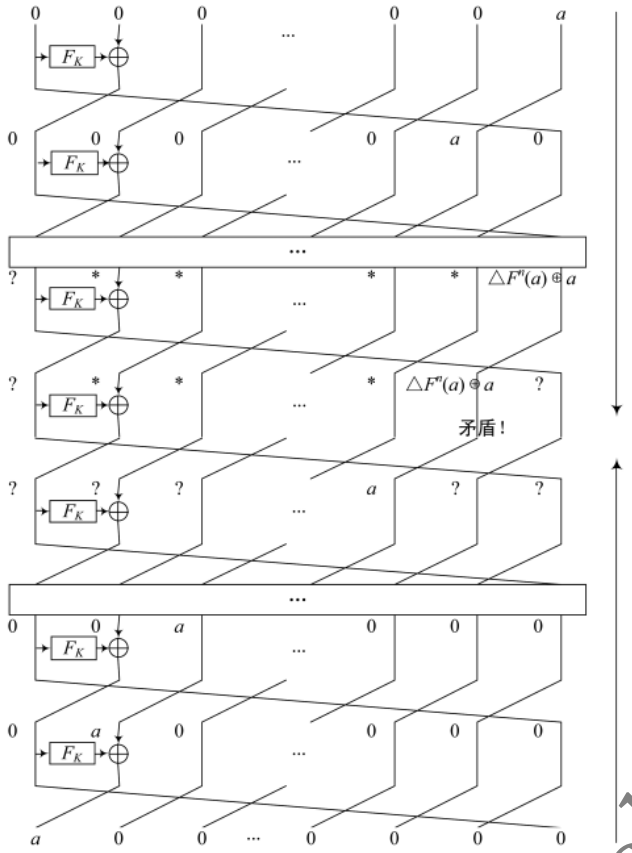

图 8 TYPE-I 型不可能差分区分器

变换之后得到第 $n+1$ 轮输出差分模式为[*,*,…,a,*]。

由于第 $n+1$ 轮输入 X_{n-2} 的差分非 0，F_k 是置换，因此此处出现矛盾，即不可能出现 $F_k(X_{n-2})\oplus a=a$。图 9 为 $2n+1$ 轮不可能差分区分器。

性质 6 设函数 F_i 是由密钥控制的随机置换，则 n 个子块的 TYPE-III 型分组密码必有 $n+2$ 轮不可能差分区分器。

证明：如图 10 所示，假设输入差分模式为[0,0,…,0,a]，经过 2 轮加密变换为[0,0,…,a,$\Delta_{F_n}(a)$,0]，由于 $\Delta_{F_n}(a)$为非零，可以记为“*”，n 轮加密之后第 $n+1$ 轮输入为[?,?,…,?,*,a]；假设第 $n+2$ 轮输出为[0,…,0,a,0,0]，解密 1 轮并经过循环移块之后得到[*,0,…,0,0,a]，由于 F_n 为随机置换，因此非零差分“*”输入，输出差分必定非零，即 $F_n(*)\oplus a\neq a$，此处矛盾。

因此，n 个子块的 TYPE-III 型分组密码必有 $n+2$ 轮不可能差分区分器。

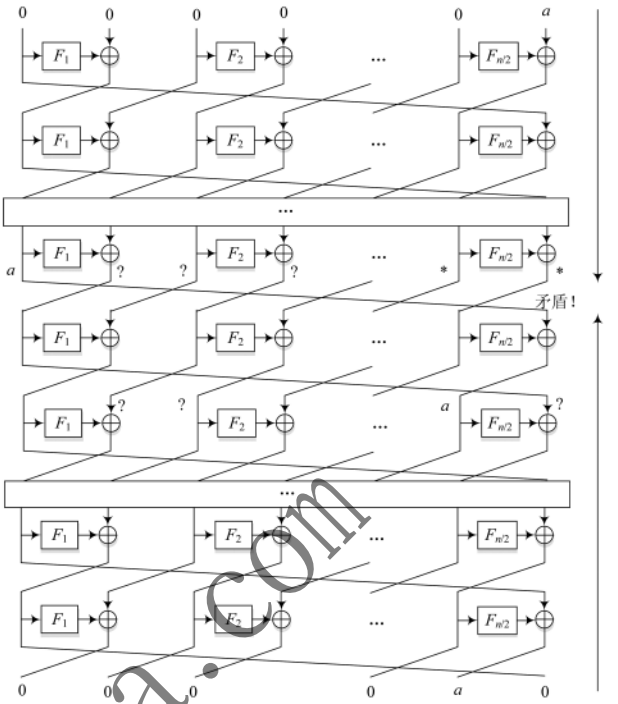

图 9 TYPE-II 型不可能差分区分器

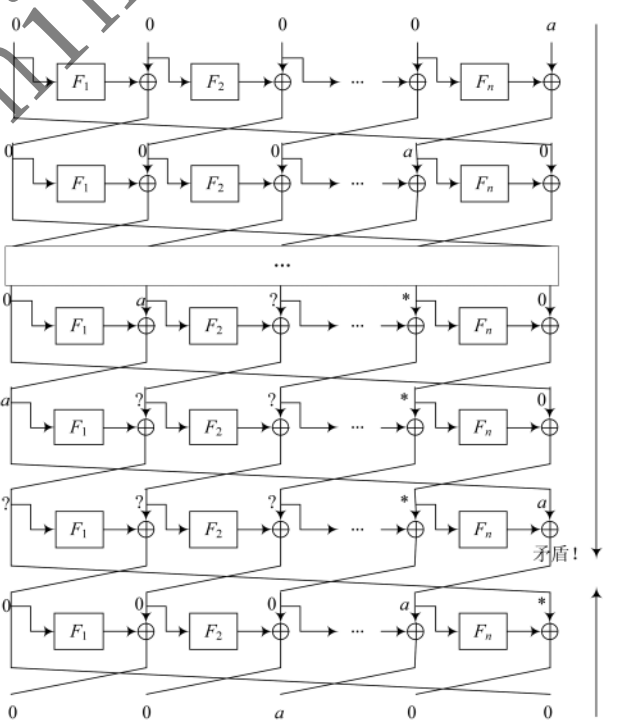

图 10 TYPE-III 型不可能差分区分器

4 MISTY 结构

MISTY 结构[23]由日本著名密码学家 Mitsuru Matsui 等人于 1995 年提出，基于此结构系列算法被设计出，包含 MISTY1、MISTY2 和 KASUMI，其中 KASUMI

算法是基于 MISTY1 算法的改进版本,是第三代移动通信技术中的一种核心加密算法。

4.1 MISTY 结构描述

定义 6 假设输入明文 P 为 X_0, X_1,密钥为 K,输入函数为 F,则 MISTY 圈函数可以表示为:

$$Q_K:(X_0, X_1)\rightarrow(Y_0, Y_1) \tag{10}$$

$$Y_0=X_1, Y_1=X_1\oplus F(K, X_0) \tag{11}$$

如图 11 所示,MISTY 结构类似于 Feistel,函数 F 只对输入的一半数据加密。

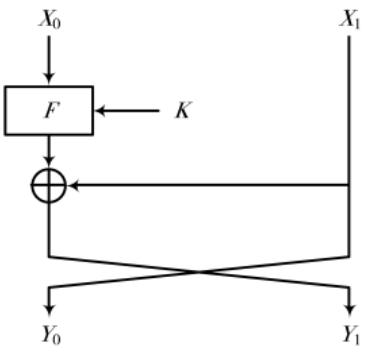

图 11 MISTY 结构

4.2 不可能差分区分器

性质 7 当 F_i 函数$(1\leqslant i\leqslant 4)$为随机置换时,MISTY 至少存在 4 轮不可能差分区分器[23]。

如图 12 所示,假设输入差分$[x_0, y_0]=[\alpha, 0]$,经过两轮变换之后在 y_1 处必为非零;再假设4 轮加密之后输出差分为$[x_2, y_2]=[\beta, \beta]$,经过两轮解密之后在 y_1 处必为零。由此构成矛盾,所以$[\alpha, 0]\rightarrow[\beta, \beta]$为 4 轮不可能差分区分器。

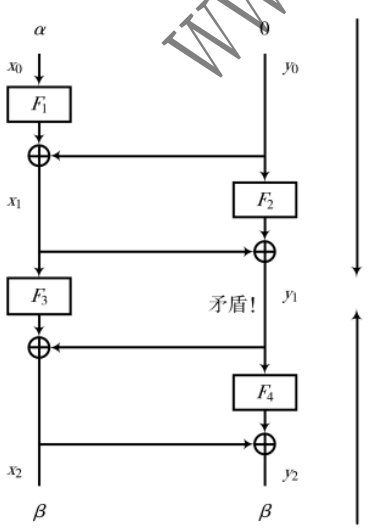

图 12 MISTY 的 4 轮不可能差分区分器

5 结论

本文对四种主要密码整体结构进行了不可能差分区分器介绍和研究,重点给出了 TYPE-I、TYPE-II 和 TYPE-III 型结构的不可能差分区分器证明过程。虽然这些密码整体结构有一定长度的区分器,但是当设计具体密码算法时,由于无法使圈变换中 F 函数完全随机,因此基于这类结构设计的对称密码算法往往有更长的不可能差分区分器,如基于 SP 结构设计的 AES、ARIA 都存在 4 轮不可能差分区分器,基于 TYPE-II 设计的 CLEFIA 存在 9 轮不可能差分区分器。因此关于对称密码整体结构在不同计算模型下的细化研究和分析是本文下一步的研究重点。

参考文献

[1] SHANNON C E. Communication theory of secrecy systems[J]. Bell System Technical Journal, 1949, 28(4): 656-715.

[2] 张文涛,卿斯汉,吴文玲.嵌套 Feistel 结构的 SP 型分组密码的可证明安全性[J].计算机研究与发展, 2004, 41(8): 1389-1397.

[3] CHEN S Y, FAN Y H, SUN L, et al. SAND: an AND-RX Feistel lightweight block cipher supporting S-box-based security evaluations[J]. Designs, Codes and Cryptography, 2022, 90(1): 155-198.

[4] PATIL J, BANSOD G, KANT K S. Dot: a new ultra-lightweight SP network encryption design for resource-constrained environment[C]//Proceedings of the 2nd International Conference on Data Engineering and Communication Technology. Springer, Singapore, 2019: 249-257.

[5] SONG H, FINK G A, JESCHKE S. Security and privacy in cyber-physical systems: foundations, principles, and applications[M]. IEEE Press, 2017.

[6] HONG S, LEE S, LIM J, et al. Provable security against differential and linear cryptanalysis for the SPN structure[C]//International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2000: 273-283.

[7] GUO C, WANG L. Revisiting key-alternating Feistel ciphers for shorter keys and multi-user security[C]// International Conference on the Theory and Application of Cryptology and Information Security. Springer, Cham, 2018: 213-243.

[8] LIU J, SUN B, LI C. New approach towards general-

izing Feistel networks and its provable security[J]. Security and Communication Networks, 2021, 2021: 2751797: 1-2751797: 26.

[9] KANEKO Y, SANO F, SAKURAI K. On provable security against differential and linear cryptanalysis in generalized Feistel ciphers with multiple random functions[C]// Proceedings of SAC, 1997, 97: 185-199.

[10] TSUNOO Y, TSUJIHARA E, SHIGERI M, et al. Impossible differential cryptanalysis of CLEFIA[C]//International WorksHop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2008: 398-411.

[11] JIA K, WANG N. Impossible differential cryptanalysis of 14-round camellia-192[C]//Australasian Conference on Information Security and Privacy. Springer, Cham, 2016: 363-378.

[12] 中国密码学会. 2019 年全国密码算法设计竞赛参赛算法[EB/OL]. [2022-05-05]. https://sfjs.cacrnet.org.cn/site/term/list_73_1.html.

[13] 李艳俊, 林昊, 梁萌, 等. TASS1 算法的不可能差分区分器搜索[J]. 密码学报, 2020, 7(6): 875-885.

[14] KNUDSEN L R. DEAL-a 128-bit block cipher[R]. AES Proposal, Technical Report 151, Department of Informatics, University of Bergen, 1998.

[15] 吴文玲, 张蕾, 郑雅菲, 等. 分组密码 uBlock[J]. 密码学报, 2019, 6(6): 690-703.

[16] 李艳俊, 许星霖. 一类 SP 结构的不可能差分区分器证明[J]. 计算机应用研究, 2021, 38(5): 1-6.

[17] ZHENG Y, MATSUMOTO T, IMAI H. On the construction of block ciphers provably secure and not relying on any unproved hypotheses[C]//Conference on the Theory and Application of Cryptology. Springer, New York, 1989: 461-480.

[18] SUZAKI T, MINEMATSU K. Improving the generalized Feistel[C]//International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 2010: 19-39.

[19] ADAMS C, GILCHRIST J. The CAST-256 encryption algorithm[R]. 1999.

[20] BURWICK C, COPPERSMITH D, D'AVIGNON E, et al. MARS-a candidate cipher for AES[C]//Proceeding of 1st Advanced Encryption Standard Candidate Conference, Venture, California, 1998.

[21] HONG D, LEE J K, KIM D C, et al. LEA: a 128-bit block cipher for fast encryption on common processors[C]//International workshop on information security applications. Springer, Cham, 2013: 3-27.

[22] SUZAKI T, MINEMATSU K, MORIOKA S, et al. Twine: a lightweight, versatile block cipher[C]//ECRYPT Workshop on Lightweight Cryptography, 2011.

[23] MATSUI M. New structure of block ciphers with provable security against differential and linear cryptanalysis[C]//International Workshop on Fast Software Encryption. Springer, Berlin, Heidelberg, 1996: 205-218.

(收稿日期: 2022-06-15)

作者简介:

刘健(1983-), 男, 硕士, 高级工程师, 主要研究方向: 信息管理系统、网络空间安全。

毕鑫杰(1998-), 男, 硕士研究生, 主要研究方向: 分组密码设计和分析。

李艳俊(1979-), 通信作者, 女, 博士, 副教授, 主要研究方向: 密码算法设计与分析、密码协议应用。E-mail: liyjwuyh@163.com。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部