文章编号:1000-2367(2020)05-0016-06 DOI:10.16366/j.cnki.1000-2367.2020.05.003

MISTY 结构的不可能差分和零相关线性

刘畅,沈璇,何俊

(国防科技大学 信息通信学院,武汉 430010)

摘 要:不可能差分分析和零相关线性分析是目前分组密码安全性分析方法中常用的两种分析方法.针对分组密码设计中常用的一种结构——MISTY 结构,研究了 MISTY 结构的不可能差分和零相关线性.首先,给出了 MISTY 结构的对偶结构,然后从密码结构的角度出发,从理论上证明了 MISTY 结构的结构不可能差分和结构零相关线性最长轮数均为 4 轮.最后,当考虑 MISTY 结构中轮函数的具体细节时,给出了 MISTY 结构存在 5/6 轮不可能差分和零相关线性的充分条件.所得结果不仅对设计具有 MISTY 结构的分组密码具有一定的指导意义,同时对分析该类密码的安全性提供了具体的研究方法.

关键词:MISTY 结构;不可能差分;零相关线性

中图分类号:TN918.1 **文献标志码**:A

差分分析和线性分析是目前针对分组密码安全性分析最重要的两种分析方法.基于这两种分析方法,密码学者提出了多种延伸的分析方法,包括截断差分分析、多重差分分析、不可能差分分析以及多维线性分析、多重线性分析、零相关线性分析等等.不可能差分和零相关线性是其中比较重要的两类分析方法.

不可能差分分析是由 KNUDSER[1]和 BIHAM 等人[2]独立提出的.该分析方法主要针对基于字节设计的分组密码,它对包括国际密码标准 AES,Camellia,ARIA,MISTY 等在内的算法取得了很好的攻击效果[3-5].不可能差分分析的主要思想是利用概率为零的差分来筛除错误密钥,进而得到正确密钥.不可能差分分析分为两步:一是构造尽可能长的不可能差分,二是利用构造的不可能差分进行密钥恢复攻击.其中第一步构造不可能差分是该分析方法的关键所在.

零相关线性分析是一种特殊的线性分析方法,该方法是文献[6]提出的.与不可能差分分析类似,它主要利用相关性为零的线性特征构造区分器,并且利用该零相关线性恢复密钥.在零相关线性分析中,零相关线性的构造同样是该分析方法的核心.

目前,构造不可能差分和零相关线性的主要自动化搜索方法有如下四类方法:U 方法、UID 方法、线性化方法、基于混合整线性规划(MILP)方法.这些方法均是基于计算机搜索得到,无法从理论上说明区分器是否到达最优,同时也无法准确给出区分器最长轮数的上界.为了从理论上刻画这些问题,文献[7]在 CRYPTO 2015 上给出了密码结构的概念,并基于此证明了:对于 SPN 结构和 Feistel-SP 结构而言,它们的不可能差分与对偶结构的零相关线性等价.该结果在密码结构层面上,将不可能差分和零相关线性统一起来了.后来,文献[8]在 EUROCRYPT 2016 上进一步给出了 SPN 和 Feistel-SP 结构的不可能差分上界.与此同时,考虑到不可能差分和零相关线性在密码结构层面的等价性,该结果同样可以推广到结构零相关线性上来.

MISTY 结构是 MATSUI 设计的一种分组密码结构[9],在标准密码算法 MISTY1 的设计中利用该结构进行了组件设计.针对 MISTY1 算法的安全性分析结果较多,如差分分析、线性分析、高阶差分等等[10-12].但是针对 MISTY 结构的研究不多,文献[13]指出针对 MISTY 结构,当轮函数为 SPN 型时,它的活跃 S 盒数

收稿日期:2019-06-14;**修回日期**:2020-05-25.

基金项目:国家自然科学基金(61702537)

作者简介:沈璇(1990—),男,湖北荆门人,国防科技大学讲师,博士,研究方向为网络安全、密码学,E-mail:shenxuan_08@163.com.

通信作者:刘畅,E-mail:412562709@qq.com.

目上界与 Feistel 结构一致，并且进一步约定轮函数中置换层为二元矩阵时，证明了该结构存在 6 轮积分区分器以及存在 5/6/7 轮不可能差分的条件.

1　密码结构及其不可能差分上界

不可能差分的构造在很长时间内均与密码算法中的非线性组件 S 盒无关，即替换 S 盒后该不可能差分仍然成立.为了刻画与非线性组件无关的分析方法，文献[7]首次提出了如下密码结构的概念：

令 $E:F_2^k\to F_2^k$ 是一个分组密码算法，其中非线性组件是双射的 S 盒.

(1)结构 ε^E 表示一族分组密码算法，在该分组密码算法族中，除了非线性组件 S 盒外其他组件均相同，并且 S 盒取遍所有可能的双射变换.

(2)令 $\alpha,\beta\in F_2^k$.如果任意 $E'\in\varepsilon^E$，$\alpha\to\beta$ 是 E' 的一条不可能差分，那么 $\alpha\to\beta$ 称为 ε^E 结构的一条结构不可能差分.

从上述定义知，如果 $\alpha\to\beta$ 是 ε^E 的一条结构不可能差分，则 $\alpha\to\beta$ 一定是算法 E 的一条算法不可能差分.因此，结构不可能差分长度一定不超过算法不可能差分长度.在文献[7]中作者证明了结构的不可能差分和其对偶结构的零相关线性是等价的.故考虑密码结构时，结构不可能差分和结构零相关线性二者只需要考虑其中一种即可.本文主要研究结构不可能差分，结构零相关线性的结果以推论形式给出.

密码结构的定义刻画了不可能差分与非线性组件无关的特点，因此结构不可能差分只与分组密码中的线性变换有关.在 EUROCRYPT 2016 上，SUN 等人[8]给出了 SPN 结构不可能差分的上界，即当 $m\le 2^{n-2}-2$ 时(m 为线性变换矩阵的规模，n 为 S 盒的规模)，其结构不可能差分的上界为 $\gamma(P)+\gamma(P^{-1})$，这里 $\gamma(P)$ 表示线性变换矩阵 P 的本原指数.

此外，针对通用的分组密码结构而言，成磊[14]研究了 Tpye-I 型的广义 Feistel 结构的结构不可能差分和结构零相关线性.特别地，他证明了 Feistel 结构的结构不可能差分恰好为 5 轮.

2　MISTY 结构的结构不可能差分和零相关线性上界

本节首先给出 MISTY 结构的描述，然后给出其对偶结构 MISTY* 结构，最后证明了 MISTY 结构的结构不可能差分和零相关线性上界均为 4 轮.

MISTY 结构是由 MATSUI 设计的一种分组密码结构[9]，其一轮加密流程如图 1 所示，对应的表达式为：

$$\begin{cases}y_0=x_1,\\ y_1=x_1\oplus F(x_0,k),\end{cases}$$

这里 (x_0,x_1) 表示一轮输入；(y_0,y_1) 表示一轮输出；F 表示轮函数，由于解密的需要，轮函数 F 需为可逆函数；k 表示轮密钥.由于考虑密码结构的不可能差分和零相关线性时，轮密钥 k 不影响其差分传播和线性传播，故不影响这两种区分器的构造.

当 MISTY 结构的轮函数仅视为双射函数时，参照 SUN 等人[7]在 CRYPTO 2015 上的方法，定义 MISTY 结构的对偶结构为 MISTY* 结构，如图 2 所示.

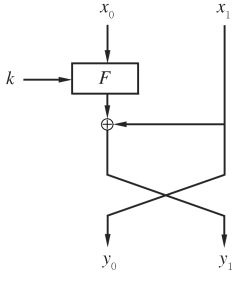

图1　MISTY结构一轮加密流程

Fig.1　One round encryption process of MISTY structure

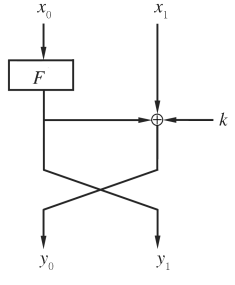

图2　MISTY*结构一轮加密流程

Fig.2　One round encryption process of MISTY* structure

进一步，图 3 给出了 MISTY 结构的一轮差分传播和 MISTY* 结构的一轮线性传播.从图 3 中，能够看出 MISTY 结构的一轮差分传播和 MISTY* 结构的一轮线性传播是等价的.

在本文中,令 $\Delta F(a)$ 表示输入差分为 a,经过轮函数 F 后,所有可能的输出差分值集合.同理 $\Delta F^r(a)$ 表示输入差分 a 经过连续 r 个轮函数 F 后,所有可能的输出差分值集合.显然,当函数 F 为双射,输入差分 a 非零时,$\Delta F^r(a)$ 中的元素均非零.

若 MISTY 结构的输入差分为 $(a,0)$,这里 a 为非零差分,则其加密方向差分传播规律如表 1 所示.

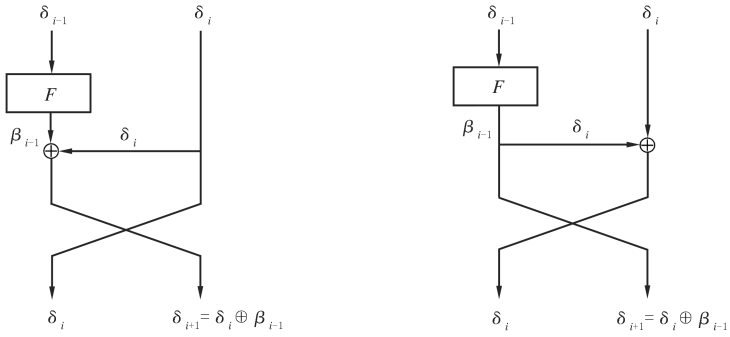

图3 MISTY结构的一轮差分传播(左边)和MISTY*结构一轮线性传播(右边)

Fig.3 One round differential propagation of MISTY structure(left) and one round linear propagation of MISTY* structure(right)

表 1 加密方向的差分传播

Tab.1 Differential propagation in the encryption direction

轮数	差分传播	约束条件	轮数	差分传播	约束条件
0	$(a,0)$		3	$(u_0,u_0\oplus u_1)$	$u_1\in\Delta F^2(a)$
1	$(0,u_0)$	$u_0\in\Delta F(a)$	4	$(u_0\oplus u_1,u_0\oplus u_1\oplus u_2)$	$u_2\in\Delta F^2(a)$
2	(u_0,u_0)				

若 MISTY 结构的输出差分为 (b,b),这里 b 是非零差分,则其解密方向差分传播如表 2 所示.

表 2 解密方向的差分传播

Tab.2 Differential propagation in the decryption direction

轮数	差分传播	约束条件	轮数	差分传播	约束条件	轮数	差分传播	约束条件
0	(b,b)		1	$(0.b)$		2	$(v,0)$	$v\in\Delta F^{-1}(b)$

当 MISTY 结构的轮函数仅为双射函数时,有如下定理成立.

定理 1 MISTY 结构的结构不可能差分上界为 4 轮.

证明 根据密码结构的定义可得,当 r 轮任意非零差分均为可能的差分时,则 $s\geq r$ 轮的任意非零差分也都是可能的差分.为证明 MISTY 结构的结构不可能差分上界为 4 轮,先证明对于 5 轮 MISTY 结构,任意非零的差分均是可能的差分.如图 4 所示,若 5 轮 MISTY 结构的任意非零输入差分为 (a_0,a_1),任意非零输出差分为 (b_0,b_1),则需证明 $(a_0,a_1)\nrightarrow(b_0,b_1)$ 是可能的差分.证明过程如下.

如图 4 所示,首先将 5 轮差分传播分为正向传播 2 轮,逆向传播 1 轮,中间匹配 2 轮共 3 部分,然后证明对于给定的非零输入差分 (a_0,a_1) 经过正向加密 2 轮与非零输出差分 (b_0,b_1) 经过反向解密 1 轮能够匹配成功,即可得证.

先分析输入差分正向传播 2 轮的情况:不妨设 (a_0,a_1) 经过两轮传播后的差分为 (α_0,α_1),则根据传播规律得:

$$\begin{cases}\alpha_0\in a_1\oplus\Delta F(a_0),\\ \alpha_1\in a_1\oplus\Delta F(a_0)\oplus\Delta F(a_1).\end{cases}$$

然后对输入差分 (a_0,a_1) 分 3 种情况讨论,并给出相应 (α_0,α_1) 的取值范围,注意轮函数 F 是双射函数.

(1)当 $a_0=0,a_1\neq 0$ 时,则 $\alpha_0=a_1,\alpha_1\in a_1\oplus\Delta F(a_1)$.因此,$\alpha_0=a_1\neq 0,\alpha_1\neq a_1$.

(2)当 $a_0\neq 0,a_1=0$ 时,则 $\alpha_0\in\Delta F(a_0),\alpha_1\in\Delta F(a_0)$.因此,$\alpha_0\neq 0,\alpha_1\neq 0$.

(3)当 $a_0\neq 0,a_1\neq 0$ 时,则 $\alpha_0\in a_1\oplus\Delta F(a_0),\alpha_1\in a_1\oplus\Delta F(a_0)\oplus\Delta F(a_1)$.因此,$\alpha_0\neq a_1,\alpha_1\in F_2^t$,这里假设 MISTY 结构的分组长度为 $2t$ bit,每一支的分组长度为 t bit.

综上所述,(α_0,α_1) 的取值范围为:

$$\begin{cases}\alpha_0 \neq a_1 \neq 0, \alpha_1 \neq a_1, a_0 = 0, a_1 \neq 0;\\ \alpha_0 \neq 0, \alpha_1 \neq 0, a_0 \neq 0, a_1 = 0;\\ \alpha_0 \neq a_1, \alpha_1 \in F_2^t, a_0 \neq 0, a_1 \neq 0.\end{cases}$$

再分析输出差分逆向传播 1 轮的情况:不妨设(b_0,b_1)经过 1 轮逆向传播后的差分为(β_0,β_1),则根据传播规律得:

$$\begin{cases}\beta_0 = b_1,\\ \beta_1 \in \Delta F^{-1}(b_0 \oplus b_1).\end{cases}$$

下面对输出差分(b_0,b_1)分两种情况讨论,并给出相应(β_0,β_1)的取值范围.

(1)当 $b_0 = b_1 \neq 0$ 时,则 $\beta_0 = b_1 \neq 0, \beta_1 = 0$.因此,$\beta_0 \neq \beta_1$.

(2)当 $b_0 \neq b_1$ 时,则 $\beta_0 = b_1$, $\beta_1 \neq 0$.

综上所述,(β_0,β_1)的取值范围为:

$$\begin{cases}\beta_0 = b_1 \neq 0, \beta_1 = 0, b_0 = b_1 \neq 0;\\ \beta_0 = b_1, \beta_1 \neq 0, b_0 \neq b_1.\end{cases}$$

最后分析中间 2 轮匹配的情况:若输入差分为(α_0,α_1),输出差分为(β_0,β_1),则当它们满足如下条件:

$$\begin{cases}\alpha_0 \neq 0;\\ \alpha_1 \neq 0;\\ \beta_1 \neq \alpha_1;\\ \beta_0 \neq \beta_1.\end{cases}$$

此时,下式成立,

$$\begin{cases}\beta_1 \in \alpha_1 \oplus \Delta F(\alpha_0);\\ \beta_0 \in \beta_1 \oplus \Delta F(\alpha_1).\end{cases}$$

结合(α_0,α_1)和(β_0,β_1)的取值范围知,存在满足上述条件的(α_0,α_1)和(β_0,β_1).即中间 2 轮能够匹配成功.

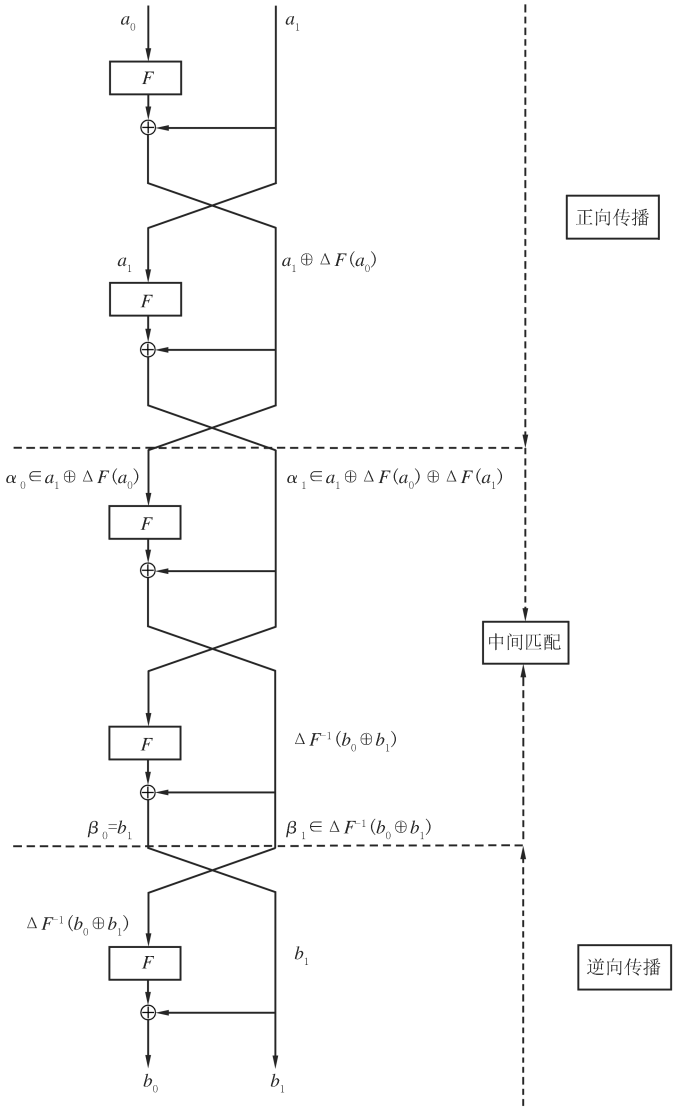

图4　5轮MISTY结构的差分匹配

Fig.4　Differential match of 5-round MISTY structure

综上所述,5 轮 MISTY 结构的任意非零输入差分和输出差分均是可能的差分.这意味着 MISTY 结构的结构不可能差分最多为 4 轮.注意到,在表 1 中,输入差分 $(a,0)$ 经过 4 轮传播后为$(u_0 \oplus u_1, u_0 \oplus u_1 \oplus u_2)$,若 4 轮输出差分为$(b,b)$,则有 $0 = u_2 \in \Delta F^2(a)$.因为轮函数 F 为双射函数,所以 $a = 0$,这与假设 $a \neq 0$ 矛盾.因此,$(a,0) \to (b,b)$ 是 MISTY 结构的一条 4 轮结构不可能差分.所以,MISTY 结构的结构不可能差分最长为 4 轮,定理得证.

MISTY 结构的结构零相关线性等价于 MISTY* 结构的结构不可能差分,按照上述定理的证明方法,同理可证明 MISTY* 结构的结构不可能差分最长也为 4 轮,故有如下推论成立.

推论　MISTY 结构的结构零相关线性最长为 4 轮.

因此,从密码结构层面上看,MISTY 结构的结构不可能差分和结构零相关线性最长均为 4 轮.

3 MISTY 结构的 5/6 轮不可能差分和零相关线性

上节从密码结构层面给出了 MISTY 结构的结构不可能差分和零相关线性上界,本节将利用轮函数 F 更多的信息,结合方程求解的方法,给出 MISTY 结构存在 5 轮和 6 轮不可能差分以及零相关线性的充分条件.

根据定理 1 知,若想构造 MISTY 结构更长的不可能差分,不能仅仅将轮函数 F 视为双射函数,必须要利用轮函数 F 更多的信息.下面给出如下命题:

命题 1 对于 MISTY 结构,若输入差分为$(a,0)$,输出差分为(b,b)时,这里 a,b 均为非零差分,则

(1)当 $b\in\Delta F^2(a)$时,$(a,0)\to(b,b)$是 MISTY 结构的一条 5 轮算法不可能差分;

(2)当 $b\notin\Delta F^3(a)$时,$(a,0)\to(b,b)$是 MISTY 结构的一条 6 轮算法不可能差分.

证明 在表 1 中,当输入差分$(a,0)$正向传播 3 轮后,差分变为$(u_0,u_0\oplus u_1)$;正向传播 4 轮后,差分变为$(u_0\oplus u_1,u_0\oplus u_1\oplus u_2)$;输出差分$(b,b)$逆向传播 2 轮后,差分变为$(v,0)$.

若$(a,0)\to(b,b)$是 5 轮可能的差分,则中间差分能够匹配成功,即下述差分方程组有解:

$$\begin{cases}u_0=v,\\ u_0\oplus u_1=0.\end{cases}$$

根据上述方程组知 $u_0=v$.因为 $u_0\in\Delta F(a)$,$v\in\Delta F^{-1}(b)$,所以 $v\in\Delta F^{-1}(b)\cap\Delta F(a)$.若 $b\notin\Delta F^2(a)$,则 $\Delta F^{-1}(b)\cap\Delta F(a)=\varnothing$.此时不存在某个元素 $v\in\Delta F^{-1}(b)\cap\Delta F(a)$,故$(a,0)\to(b,b)$是 MISTY 结构的一条 5 轮算法不可能差分.

同理,若$(a,0)\to(b,b)$是 6 轮可能的差分,则中间差分能够匹配成功,即下述差分方程组有解:

$$\begin{cases}u_0\oplus u_1=v,\\ u_0\oplus u_1\oplus u_2=0.\end{cases}$$

根据上述方程组有 $u_2=v$.因为 $u_2\in\Delta F^2(a)$,$v\in\Delta F^{-1}(b)$,所以 $v\in\Delta F^{-1}(b)\cap\Delta F^2(a)$.

若 $b\notin\Delta F^3(a)$,则 $\Delta F^{-1}(b)\cap\Delta F^2(a)=\varnothing$.此时不存在某个元素 $v\in\Delta F^{-1}(b)\cap\Delta F^2(a)$,故$(a,0)\to(b,b)$是 MISTY 结构的一条 6 轮算法不可能差分.综上所述,命题成立.

利用上述证明方法,同样可以证明如下命题成立.

命题 2 对于 MISTY 结构,若输入掩码为$(0,a)$,输出掩码为(b,b)时,这里 a,b 均为非零掩码,则

(1)当 $b\notin\Delta F^2(a)$时,$(0,a)\to(b,b)$是 MISTY 结构的一条 5 轮算法零相关线性;

(2)当 $b\notin\Delta F^3(a)$时,$(0,a)\to(b,b)$是 MISTY 结构的一条 6 轮算法零相关线性.

注意在命题 2 中,$\Delta F^r(a)$表示输入掩码 a 经过连续 r 个轮函数 F 后,所有可能的输出掩码值集合.

4 结 论

本文从密码结构和算法两个层面研究了 MISTY 结构的不可能差分和零相关线性.从密码结构的层面看,本文从理论上证明了 MISTY 结构的结构不可能差分和零相关线性最长轮数均为 4 轮.从算法层面看,即考虑 MISTY 结构轮函数的具体细节,本文给出了 MISTY 结构存在 5 轮和 6 轮不可能差分和零相关线性的充分条件.本文的研究结果对设计和分析采用 MISTY 结构的算法具有十分重要的指导意义,同时对分析其他分组结构模型的安全性具有一定的借鉴意义.

参 考 文 献

[1] KNUDSEN L.DEAL-a 128-bit block cipher[J].complexity,1998,258(2):216.

[2] BIHAM E,BIRYUKOV A,SHAMIR A.Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[J].Journal of Cryptology,2005,18(4):291-311.

[3] LUO Y,LAI X,WU Z.A unified method for finding impossible differentials of block cipher structures[J].Information Sciences,2014,263(1):211-220.

[4] WU S,WANG M.Automatic search of truncated impossible differentials for word-oriented block ciphers[C]//International Conference on

Cryptology in India. Berlin: Springer, 2012: 283-302.
[5] CUI T, JIA K, FU K. New automatic search tool for impossible differentials and zero-correlation linear approximations[EB/OL]. [2019-06-10]. https://eprint.iacr.org/2016/689.pdf.
[6] BOGDANOV A, WANG M. Zero correlation linear cryptanalysis with reduced data complexity[C]//International Workshop on Fast Software Encryption. Berlin: Springer, 2012: 29-48.
[7] SUN B, LIU Z, RIJMEN V. Links among impossible differential, integral and zero correlation linear cryptanalysis[C]//Gennaro R, Robshaw M. In Advances in Cryptology-CRYPTO 2015. Berlin: Springer, 2015: 95-115.
[8] SUN B, LIU M, GUO J. Provable security evaluation of structures against impossible differential and zero correlation linear cryptanalysis [C]//Advances in Cryptology-EUROCRYPT 2016. Berlin: Springer, 2016: 196-213.
[9] MATSUI M. New structure of block ciphers with provable security against differential and linear cryptanalysis[C]//Fast Software Encryption-FSE 1996. Berlin: Springer, 1996: 205-218.
[10] KUHN U. Cryptanalysis of reduced-round MISTY[C]//International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer, 2001: 325-339.
[11] TANAKA H, HISAMATSU K, KANEKO T. Strength of ISTY1 without FL function for higher order differential attack[C]//International Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes. Berlin: Springer, 1999: 221-230.
[12] TANAKA H, HISAMATSU K, Kaneko T. Higher order differential attack of MISTY1 without FL functions[J]. ISEC, 1998(466): 9-15.
[13] LI R, LI C, SU J, et al. Security evaluation of MISTY structure with SPN round function[J]. Computers & Mathematics with Applications, 2013, 65(9): 1264-1279.
[14] 成磊. 分组密码结构的安全性分析[D]. 长沙：国防科技大学, 2017.
CHENG L. Cryptanalysis on Block Cyphers Structures[D]. Changsha: Graduate School of National University of Defense Technology, 2017.

Impossible differentials and zero correlation linear hulls of MISTY structure

Liu Chang, Shen Xuan, He Jun

(College of Information and Communication, National University of Defense Technology, Wuhan 430010, China)

Abstract: Impossible differential cryptanalysis and zero correlation linear cryptanalysis are two popular methods in the security analysis of block cipher. For MISTY structure which is often used to design block ciphers, this research mainly studies the impossible differentials and zero correlation linear hulls of MISTY structure. Firstly, the dual structure of MISTY structure is provided. Then, from the perspective of structure, we theoretically prove that the maximum rounds of impossible differentials and zero correlation linear hulls in MISTY structure are both 4 rounds. Finally, when considering the details of the round function in MISTY structure, we present that the sufficient conditions for the existence of 5/6-round of impossible differentials and zero correlation linear hulls in MISTY structure. The results in this paper not only give guidance for designing block ciphers with MISTY structure, but also provide specific methods for analyzing the security of them.

Keywords: MISTY structure; impossible differentials; zero correlation linear hulls

[责任编校　陈留院　赵晓华]