

自动化搜索 ARX 分组密码不可能差分与零相关线性闭包

韩亚^{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, 北京 100049)

摘要: 首先, 构造了 ARX 分组密码差分特征及线性掩码的传播方程; 然后, 利用 SAT 求解器求解传播方程并且判定该传播系统是否为有效传播; 最后, 遍历差分特征及线性掩码自动化搜索不可能差分及零相关线性闭包。利用该算法搜索 TEA、XTEA 和 SIMON 的不可能差分与零相关线性闭包, 并得到 TEA、XTEA 及 SIMON 族分组密码的最优不可能差分与零相关线性闭包。此外, 利用差分以及线性分布表, 该算法能有效搜索基于 S 盒分组密码的不可能差分及零相关线性闭包。

关键词: 不可能差分; 零相关线性; ARX 结构; SAT 求解器

中图分类号: TP309

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00175

Automatic method for searching impossible differentials and zero-correlation linear hulls of ARX block ciphers

HAN Ya^{1,2}

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

Abstract: Firstly, the differences and linear masks propagation equations of ARX ciphers were established. Secondly, the propagation equations were solved by SAT solver and judged valid or not. Finally, differences and linear masks were traversed to search impossible differentials and zero-correlation linear hulls automatically. The proposed algorithm was applied to TEA, XTEA and SIMON family block ciphers. The optimal impossible differentials and zero-correlation linear hulls for TEA, XTEA and SIMON family block ciphers were proposed. Moreover, with DDT and LAT, the algorithm can also be applied to search the impossible differentials and zero-correlation linear hulls of S-box based block ciphers.

Key words: impossible differential, zero-correlation linear hull, ARX structure, SAT solver

1 引言

不可能差分分析^[1]由 Knudsen 提出用于分析 DEAL 分组密码, 随后 Biham 等^[2]利用该方法分

析 Skipjack^[2]和 IDEA^[3]。针对 AES^[4,5]、CLEFIA^[6]和 LBlock^[7]等分组密码, 不可能差分分析已经成为一种行之有效的攻击方法。不可能差分分析利用差分传播概率为零的区分器(不可能差分)筛

收稿日期: 2017-05-10; 修回日期: 2017-06-15。通信作者: 韩亚, hanya@iie.ac.cn

基金项目: 国家自然科学基金资助项目(No.61379142); 国家重点基础研究发展计划(“973”计划)基金资助项目(No.2013CB834203)

Foundation Items: The National Natural Science Foundation of China (No. 61379142), The National Basic Research Program of China (973 Program)(No. 2013CB834203)

除错误轮密钥，并通过穷举候选密钥恢复正确密钥。零相关线性分析方法由 Bogdanov 等^[8]第一次提出用于分析分组密码算法。现在，零相关线性分析已经成功应用到 CLEFIA^[9]、LBlock^[10,11]和 SIMECK^[12]等分组密码中。与不可能差分分析类似，零相关线性分析利用线性传播掩码为零的区分器（零相关线性闭包）筛除错误轮密钥，结合穷举恢复正确密钥。不可能差分分析与零相关线性分析区分器的长度直接决定其攻击轮长度。因此，如何有效地搜索更长更多的不可能差分及零相关线性闭包至关重要。

早期密码研究者利用中间相错法（miss-in-the-middle）搜索不可能差分及零相关线性闭包。2003 年，Kim 等^[13]提出了一种自动化搜索不可能差分的方法—— μ 方法，该方法只适用于搜索具有双射轮函数的分组密码算法。2009 年，Luo 等^[14]通过改进 μ 方法提出一种搜索不可能差分方法——UID 方法。UID 方法提出了更一般化的不可能差分判定条件。2012 年，Wu 等^[15]提出了更一般化的自动化搜索不可能差分方法——WW 方法。WW 方法通过构建 r 轮差分路径传播方程，并通过全部求解线性方程以及部分求解非线性方程判定不可能差分，最后通过穷举输入输出差分自动化搜索分组密码 r 轮不可能差分。由于 μ 方法、UID 方法以及 WW 方法不能够有效地刻画差分经过“&”运算以及模加运算的传播方程，因此，这 3 种方法都不适用于搜索 ARX 结构分组密码的不可能差分。

ARX 结构分组密码轮函数由模加运算（addition）、循环移位运算（rotation）和异或运算（XOR）组成。Lipmaa 等^[16]给出对数时间算法计算差分特征值经过模加运算的差分传播概率，并给出差分传播以概率 1 经过模加运算的传播条件。Wallén^[17]给出线性掩码经过模加运算的相关系数计算方程，并给出线性掩码以概率 1 经过模加运算的传播条件。结合 Lipmaa 和 Wallén 提出的计算方程，通过构造 ARX 分组密码差分，线性传播方程，利用求解器的方法实现自动化搜索 ARX 结构分组密码的不可能差分和零相关线性闭包。

本文利用 SAT/SMT 求解器，通过构建差分

及线性掩码传播方程，自动化搜索 ARX 结构分组密码的不可能差分及零相关线性闭包。结果如表 1 所示。

表 1 最优不可能差分及零相关线性闭包轮数

分组密码	最优不可能差分	最优零相关线性闭包
TEA	15	15
XTEA	15	15
SIMON32	11	11
SIMON48	12	12
SIMON64	13	13
SIMON96	16	16
SIMON128	19	19

2 差分、线性掩码部件传播模型

ARX 结构分组密码轮函数包括模加运算、循环移位运算、异或运算和分支操作。差分及线性掩码经过各部件的传播可以通过方程的形式表示。

2.1 模加运算

定义 1 $x, y, z \in F_2^n, z = (x + y) \bmod 2^n$ ，其中， α, β, γ 分别表示 x, y, z 的差分特征，当满足 $eq(\alpha \ll 1, \beta \ll 1, \gamma \ll 1) \wedge (\alpha \oplus \beta \oplus \gamma \ll 1) = 0$

时，差分特征 α, β 经过模加运算传播到 γ 的传播概率为

$$P_r(\alpha, \beta \mapsto \gamma) = 2^{-wt(-eq(\alpha, \beta, \gamma) \wedge \text{mask}(n-1))} \quad (2)$$

否则

$$P_r(\alpha, \beta \mapsto \gamma) = 0 \quad (3)$$

其中

$$eq(x, y, z) = (-x \oplus y) \wedge (-x \oplus z) \quad (4)$$

$wt(x)$ 表示 x 的汉明重量， $\text{mask}(n)$ 表示 n bit 掩码。

定义 2 $x, y, z \in F_2^n, z = (x + y) \bmod 2^n$ ，其中 μ, v, ω 分别表示 x, y, z 的线性掩码，则线性相关系数为

$$C(\mu, v, \omega) = 1_{\{\mu \oplus \omega \ll z\}} 1_{\{v \oplus \omega \ll z\}} (-1)^{(\mu \oplus \omega)(v \oplus \omega)} 2^{-wt(z)} \quad (5)$$

其中， 1_{G_f} 是 $G_f := \{(x, f(x)) \mid x \in F_2^n\}$ 的指示函数。

$$z := M_n^T(\mu \oplus v \oplus \omega) \quad (6)$$

$$M_n(x) = (x_{n-2} \oplus \cdots \oplus x_0, \cdots, x_1 \oplus x_0, 0) \quad (7)$$

2.2 循环移位运算

定义 3 $x, y \in F_2^n, r \in N, y = x \lll r$, 其中, α, β 分别表示 x, y 的差分特征, 则差分传播概率为

$$P_r(\alpha \mapsto \beta) = \begin{cases} 1, & \beta = \alpha \lll r \\ 0, & \text{其他} \end{cases} \quad (8)$$

定义 4 $x, y \in F_2^n, r \in N, y = x \lll r$, 其中, μ, v 分别表示 x, y 的线性掩码, 则线性相关系数为

$$C(\mu, v) = \begin{cases} 1, & v = \mu \lll r \\ 0, & \text{其他} \end{cases} \quad (9)$$

2.3 异或运算

定义 5 $x, y, z \in F_2^n, z = x \oplus y$, 其中, α, β, γ 分别表示 x, y, z 的差分特征, 则差分传播概率为

$$P_r(\alpha, \beta \mapsto \gamma) = \begin{cases} 1, & \gamma = \alpha \oplus \beta \\ 0, & \text{其他} \end{cases} \quad (10)$$

定义 6 $x, y, z \in F_2^n, z = x \oplus y$, 其中, μ, v, ω 分别表示 x, y, z 的线性掩码, 则线性相关系数为

$$C(\mu, v, \omega) = \begin{cases} 1, & \mu = v = \omega \\ 0, & \text{其他} \end{cases} \quad (11)$$

2.4 分支运算

定义 7 $x, y, z \in F_2^n, x = y = z$, 其中, α, β, γ 分别表示 x, y, z 的差分特征, 则差分传播概率为

$$P_r(\alpha, \beta \mapsto \gamma) = \begin{cases} 1, & \alpha = \beta = \gamma \\ 0, & \text{其他} \end{cases} \quad (12)$$

定义 8 $x, y, z \in F_2^n, z = x \oplus y$, 其中, μ, v, ω 分别表示 x, y, z 的线性掩码, 则线性相关系数为

$$C(\mu, v, \omega) = \begin{cases} 1, & \omega = \mu \oplus v \\ 0, & \text{其他} \end{cases} \quad (13)$$

2.5 类 SIMON 轮函数

定义 9^[18] $F(x) = ((x \lll a) \wedge (x \lll b)) \oplus (x \lll c)$, $\gcd(n, a-b)=1$, 其中, n 为偶数, a, b, c 为循环移位常数, 且 $a > b$ 。令 α, β 分别为 $F(x)$ 的输入输出差分特征, 令

$$vaibits = (\alpha \lll a) \vee (\alpha \lll b) \quad (14)$$

$$doublebits = (\alpha \lll b) \wedge \overline{\alpha \lll a} \wedge (\alpha \lll (2a-b)) \quad (15)$$

$$\gamma = \beta \oplus (\alpha \lll c) \quad (16)$$

则差分传播概率为

$$P_r(\alpha \mapsto \beta) = \begin{cases} 2^{-n+1}, & \alpha = 2^n - 1, wt(\gamma) \equiv 0 \pmod{2} \\ 2^{-wt(vaibits \oplus doublebits)}, & \alpha \neq 2^n - 1, \gamma \wedge \overline{vaibits} = 0, \\ & (\gamma \oplus (\gamma \lll (a-b))) \wedge doublebits = 0 \\ 0, & \text{其他} \end{cases} \quad (17)$$

定义 10^[18] $f(x) = ((x \lll a) \wedge (x \lll b))$, $\gcd(n, a-b)=1$, 其中, n 为偶数, a, b, c 为循环移位常数, 且 $a > b$ 。令 α, β 分别为 $F(x)$ 的输入输出线性掩码, 令

$$U_\beta = \{x \mid \beta(x \lll (a-b)) \oplus ((\beta x) \ggg (a-b)) = 0\} \quad (18)$$

$$d = \dim U_\beta \quad (19)$$

则线性平方相关系数为

$$C^2(\alpha, \beta) = \begin{cases} 2^{-n+2}, & \beta = 2^n - 1, \alpha \in U_\beta^\perp \\ 2^{-n+d}, & \alpha \neq 2^n - 1, \alpha \in U_\beta^\perp \\ 0, & \text{其他} \end{cases} \quad (20)$$

可知, 线性平方相关系数 $C^2(\alpha, \beta) \neq 0$, 当且仅当满足条件

$$((S^{-a}(\beta) \mid S^{-b}(\beta)) \oplus \alpha) \wedge \alpha = 0 \quad (21)$$

3 算法实现

分组密码 $B_{(n,r)} : c = E_k^r(p)$, 其中, n 表示分组密码的分组长度, r 表示分组密码轮数, k 表示分组密码密钥, p 和 c 分别表示分组密码明文和密文。定义 x_{i-1}, x_i 分别表示分组密码 $B_{(n,r)}$ 的第 i 轮输入输出差分 (线性掩码), 其中 x_0, x_r 分别表示明文和密文差分 (线性掩码)。根据差分、线性掩码经过部件的传播模型, 得到第 i 轮差分 (线性掩码) 传播方程 $x_i = F(x_{i-1})$ 满足差分传播概率 $P(x_{i-1} \rightarrow x_i) = 1$ (线性掩码相关系数 $C(x_{i-1}, x_i) = 1$)。根据第 i 轮差分 (线性掩码) 传播方程, 可以建立分组密码 $B_{(n,r)}$ 的 r 轮差分 (线性掩码) 传播方程 $S_B(x_0, x_r)$ 满足差分传播概率 $P(x_0 \rightarrow x_r) = 1$ (线性掩码相关系数 $C(x_0, x_r) = 1$)。利用 SAT/SMT 求解器求解传播方程 $S_B(x_0, x_r)$, 如果求解器能够返回一组或多组解, 则表明该传播方程 $S_B(x_0, x_r)$ 满足 $P(x_0 \rightarrow x_r) \neq 0$ (线性掩码相关系数 $C(x_0, x_r) \neq 0$)。反之, 则表明 (x_0, x_r) 是分组密码 $B_{(n,r)}$ 的一组不可能差分 (零相关线性闭包)。通过遍历 x_0 和 x_r 的所

有可能,可以自动化地搜索分组 $B_{(n,r)}$ 的所有 r 轮不可能差分(零相关线性闭包)。下面是基于 SAT/SMT 求解器的自动化搜索算法的具体描述。

1) 初始化参数。给定分组密码 $B_{(n,r)}$ 、 x_0 、 x_r 。
 2) 构建解析传播方程。根据分组密码 $B_{(n,r)}$, 构建 r 轮差分(线性掩码)传播方程 $S_B(x_0, x_r)$ 满足差分传播概率 $P(x_0 \rightarrow x_r) \neq 0$ (线性掩码相关系数 $C(x_0, x_r) \neq 0$) ; 解析 $S_B(x_0, x_r)$ 方程组为 SAT/SMT 求解器能够识别的模式。

3) 求解。利用 SAT/SMT 求解器求解并返回结果。

4) 搜索分组密码 $B_{(n,r)}$ 所有可能的不可能差分(零相关线性闭包)。

```

for 遍历  $x_0$  do
  for 遍历  $x_r$  do
    step 1;
    step 2;
    step 3;
    if  $S_B(x_0, x_r)$  存在解空间 then
      break;
    else
      记录  $(x_0, x_r)$  为一组不可能差分(零相关线性闭包);
      总条数加 1;
    end if
  end for
end for
  
```

其中,称 step1、step2、step3 为一个会话,遍历 x_0 与 x_r 的时间复杂度为 2^{2n} 个会话。当 n 取值较大时,计算机很难实现整个搜索过程。因此,在遍历 x_0 与 x_r 时,限制其汉明重量使 $wt(x_0)=1, wt(x_r)=1$ 。因此该算法的时间复杂度约为 $O(n^2)$, 数据复杂度为 $O(n^2)$, 空间复杂度为 $O(1)$ 。当 n 取值为 128 时,所需时间复杂度约为 $O(2^{14})$, 数据复杂度为 $O(2^{14})$, 空间复杂度为 $O(1)$ 。

4 应用

4.1 TEA 和 XTEA

TEA 是由 Wheeler 等^[19]提出的一种轻量级分组密码算法。TEA 的分组长度为 64 bit, 密钥长度为 128 bit。TEA 分组密码轮函数包括模加运算、循环移位和异或运算, 轮函数表示为

$$\begin{cases} X_{out} = Y_{in} \\ Y_{out} = X_{in} + ((Y_{in} \ll 4 + K_0) \oplus (Y_{in} + \delta) \oplus (Y_{in} \gg 5 + K_1)) \end{cases} \quad (22)$$

XTEA 是 Needham 等^[19]对 TEA 的一种改进方案,保持了 TEA 的分组长度和密钥长度,改进了轮函数结构, 轮函数表示为

$$\begin{cases} X_{out} = Y_{in} \\ Y_{out} = X_{in} + (((Y_{in} \ll 4 \oplus Y_{in} \gg 5) + Y_{in}) \oplus K) \end{cases} \quad (23)$$

TEA 和 XTEA 分组密码轮函数如图 1 所示。

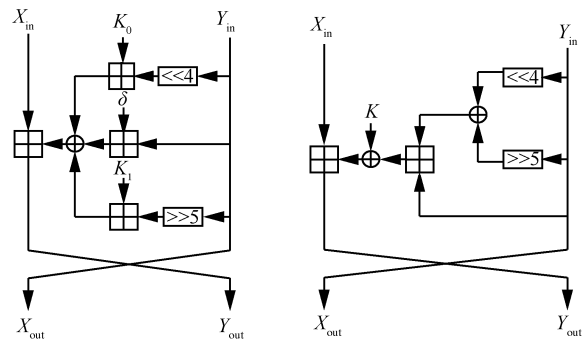


图 1 TEA 和 XTEA 轮函数

遍历所有输入输出汉明重量为 1 的差分、线性特征值,利用差分以及线性经过分组密码部件传播模型并结合 TEA 和 XTEA 轮函数结构,构建 r 轮差分(线性掩码)传播方程 $S_B(x_0, x_r)$ 满足差分传播概率 $P(x_0 \rightarrow x_r) \neq 0$ (线性掩码相关系数 $C(x_0, x_r) \neq 0$)。解析 r 轮差分(线性掩码)传播方程 $S_B(x_0, x_r)$ 为 SAT 求解器识别模型,并判断该条路径是否为不可能差分(零相关线性掩码)。该搜索算法对 TEA 和 XTEA 分组密码的搜索结果如表 2 所示。

表 2

TEA 和 XTEA 分组密码搜索结果

分组密码	不可能差分				零相关线性闭包			
	轮数	搜索空间	条数	耗时/min	轮数	搜索空间	条数	耗时/min
TEA	15	2^{12}	2	7.45	15	2^{12}	2	3.39
XTEA	15	2^{12}	2	5.91	15	2^{12}	2	0.96

4.2 SIMON

SIMON^[20]是 NSA 提出的轻量级分组密码算法。SIMON 是类 Feistel 结构分组密码, 其分组长度为 $2n$, 表示为 SIMON $2n$, 字长度 $n \in \{16, 24, 32, 48, 64\}$ 。SIMON 分组密码轮函数表示为

$$\begin{cases} Y_{\text{out}} = X_{\text{in}} \\ X_{\text{out}} = ((X_{\text{in}} \ll \alpha) \wedge (X_{\text{in}} \ll \beta)) \oplus \\ (X_{\text{in}} \ll \gamma) \oplus Y_{\text{in}} \oplus K_i \end{cases} \quad (24)$$

循环移位常数 $\alpha = 8$, $\beta = 1$, $\gamma = 2$ 。SIMON 分组密码轮函数如图 2 所示。

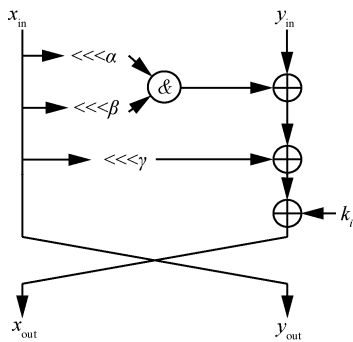


图2 SIMON 轮函数

利用该搜索算法, 针对不同版本的 SIMON 分组密码搜索结果如表 3 所示。

5 结束语

本文利用 SAT/SMT 求解器, 提出一种全新的自动化搜索分组密码不可能差分 and 零相关线性闭包的方法。该方法针对分组长度大于 64 bit 的 ARX 结构分组密码算法仍然有效。本文应用该方法搜索 TEA、XTEA 及 SIMON 分组密码的不可能差分及零相关线性闭包。针对 TEA 和 XTEA, 最优不可能差分及零相关线性闭包长度分别为 15 轮、15 轮。本文提出的 SIMON32/48/64/96/128

的最优不可能差分及零相关线性闭包长度分别为 11 轮、12 轮、13 轮、16 轮和 19 轮。

参考文献:

- [1] KNUDSEN L R. Deal - a 128 bit block cipher[J]. Complexity, 1998.
- [2] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]//Advances in Cryptology — EUROCRYPT '99. 1999:12-23.
- [3] BIHAM E, BIRYUKOV A, SHAMIR A. Miss in the middle attacks on IDEA and Khufu[C]//The International Workshop on FAST Software Encryption. 1999:124-138.
- [4] PHAN C W. Impossible differential cryptanalysis of 7-round advanced encryption standard(AES)[J]. Information Processing Letters, 2004, 91(1):33-38.
- [5] LU J, DUNKELMAN O, KELLER N, et al. New impossible differential attacks on AES[C]// Progress in Cryptology-INDOCRYPT. 2008:279-293.
- [6] BOURA C, NAYA-PLASENCIA M, SUDER V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, camellia, lblock and simon[C]//The International Conference on the Theory and Application of Cryptology and Information Security. 2014:179-199.
- [7] CHEN J, FUTA Y, MIYAJI A, et al. Improving impossible differential cryptanalysis with concrete investigation of key scheduling algorithm and its application to lblock[C]//The 8th International Conference on Network and System Security. 2014:184-197.
- [8] BOGDANOV A, RIJMEN V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers[J]. Designs Codes & Cryptography, 2014, 70(3):369-383.
- [9] YI W T, CHEN S Z. Improved integral and zero-correlation linear cryptanalysis of reduced-round CLEFIA block cipher[J]. IACR Cryptology ePrint Archive, 2016:149.
- [10] SOLEIMANY H, NYBERG K. Zero-correlation linear cryptanalysis of reduced-round LBlock[J]. Designs Codes & Cryptography, 2014, 73(2):683-698.
- [11] XU H, JIA P, HUANG G, et al. Multidimensional zero-correlation

表 3

SIMON 分组密码搜索结果

分组密码	不可能差分				零相关线性闭包			
	轮数	搜索空间	条数	耗时/min	轮数	搜索空间	条数	耗时/min
SIMON32	11	2^{10}	32	0.72	11	2^{10}	32	0.45
SIMON48	12	$2^{11.2}$	48	2.23	12	$2^{11.2}$	48	1.27
SIMON64	13	2^{12}	192	5.41	13	2^{12}	192	2.62
SIMON96	16	$2^{13.2}$	192	15.72	16	$2^{13.2}$	192	8.72
SIMON128	19	2^{14}	256	42.16	19	2^{14}	256	23.36

- linear cryptanalysis on 23-round LBlock-s[M]//Information and Communications Security. Berlin: Springer, 2015.
- [12] ZHANG K, GUAN J, HU B, et al. Security evaluation on simeck against zero correlation linear cryptanalysis[J]. IACR Cryptology ePrint Archive, 2015.
- [13] KIM J, HONG S, SUNG J, et al. Impossible differential cryptanalysis for block cipher structures[C]//The 4th International Conference on Cryptology. 2003:82-96.
- [14] LUO Y, LAI X, WU Z, et al. A unified method for finding impossible differentials of block cipher structures[J]. Information Sciences, 2014, 263(1):211-220.
- [15] WU S, WANG M. Automatic search of truncated impossible differentials for word-oriented block ciphers[C]//The International Conference on Cryptology. 2012:283-302.
- [16] LIPMAA H, MORIAI S. Efficient algorithms for computing differential properties of addition[C]//The 8th International Workshop on Fast Software Encryption. 2001:336-350.
- [17] WALLÉN J. Linear approximations of addition modulo 2^n [C]//The 10th International Workshop on Fast Software Encryption (2003). 2003:261-273.
- [18] KÖLBL S, LEANDER G, TIESSEN T. Observations on the SIMON block cipher family[C]// Advances in Cryptology - CRYPTO 2015:161-185.
- [19] WHEELER D J, NEEDHAM R M. Tea, a tiny encryption algorithm[M]//Fast Software Encryption. Berlin : Springer, 1994:363-366.
- [20] BEAULIEU R, SHORS D, SMITH J, et al. The simon and speck families of lightweight block ciphers[J]. IACR Cryptology ePrint Archive, 2013(6): 404.

作者简介:



韩亚（1989-），男，河南商丘人，中国科学院信息工程研究所博士生，主要研究方向为密码学。