软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(11):3544−3553 [doi: 10.13328/j.cnki.jos.005296]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

SIMON 不可能差分及零相关路径自动化搜索算法*

张仕伟[1,2], 陈少真[1,2]

[1](解放军信息工程大学,河南 郑州 450001)

[2](数学工程与先进计算国家重点实验室(解放军信息工程大学),河南 郑州 450001)

通讯作者: 张仕伟, E-mail: yunwumountain@163.com

摘 要: 对于分组密码,不可能差分和零相关线性分析都是很重要的分析手段.通过研究非线性组件与(AND)的性质,首先得到用于刻画 SIMON 轮函数差分及线性传播特性的约束式,再基于布尔可满足约束问题(SAT),提出一种普适性不可能差分和零相关路径自动化搜索算法,并利用该算法搜索得到 SIMON 更多的不可能差分及零相关路径.除用于自动化搜索外,该算法还可判断特定的差分对(掩码对)是否能构成一条有效不可能差分和零相关路径.此外,基于该算法,从抵抗不可能差分攻击的角度出发,给出 SIMON 轮函数设计中循环移位常数的选取依据.

关键词: 分组密码;不可能差分分析;零相关线性分析;自动搜索算法;SIMON

中图法分类号: TP309

中文引用格式: 张仕伟,陈少真.SIMON 不可能差分及零相关路径自动化搜索算法.软件学报,2018,29(11):3544−3553. http://www.jos.org.cn/1000-9825/5296.htm

英文引用格式: Zhang SW, Chen SZ. Automatic search algorithm for impossible differential trials and zero-correlation linear trials in SIMON. Ruan Jian Xue Bao/Journal of Software, 2018,29(11):3544−3553 (in Chinese). http://www.jos.org.cn/1000-9825/5296.htm

Automatic Search Algorithm for Impossible Differential Trials and Zero-Correlation Linear Trials in SIMON

ZHANG Shi-Wei[1,2], CHEN Shao-Zhen[1,2]

[1](PLA Information Engineering University, Zhengzhou 450001, China)

[2](State Key Laboratory of Mathematical Engineering and Advanced Computing (PLA Information Engineering University), Zhengzhou 450001, China)

Abstract: Impossible differential cryptanalysis and zero-correlation linear cryptanalysis are two of the most useful cryptanalysis methods in the field of symmetric ciphers. Taking the non-linear components into consideration, this article proposes a method for searching the impossible differentials and zero-correlation linear approximations of SIMON based on a technique of SAT. In applications, the proposed method is used to find more impossible differentials and zero-correlation linear approximations for 11-round SIMON. Furthermore, this tool can be used to prove whether there are impossible differentials (zero-correlation linear approximations) in certain rounds of SIMON, particularly for certain subset of input and output patterns of differences (masks). Utilizing this tool, the security of SIMON as well as the choice of its parameter set when resisting the impossible differential cryptanalysis are also explored.

Key words: block cipher; impossible differential cryptanalysis; zero-correlation linear cryptanalysis; automatic search algorithm; SIMON

---

* 基金项目: 数学工程与先进计算国家重点实验室开放基金(2018A03); 国家密码发展基金(MMJJ20180203); 信息保障技术重点实验室开放基金(KJ-17-002)

Foundation item: State Key Laboratory of Mathematical Engineering and Advanced Computation Open Fund (2018A03); National Cipher Development Fund (MMJJ20180203); Key Laboratory of Information Assurance Technology Open Fund (KJ-17-002)

收稿时间: 2017-01-11; 修改时间: 2017-02-28; 采用时间: 2017-04-17; jos 在线出版时间: 2018-04-16

CNKI 网络优先出版: 2018-04-16 10:59:47, http://kns.cnki.net/kcms/detail/11.2560.TP.20180416.1059.005.html

物联网通过在物品上嵌入电子标签、条形码等标识,从而可达到对物品进行跟踪、监控等智能化管理的目的.但随着物联网的高速发展,人们对信息数据的安全性需求也越来越多.从典型的物联网硬件平台(如 RFID 芯片、无线传感器)来看,直接采用现在广泛应用的分组密码(AES、SHA 等),并不能完全适应其计算资源受限的硬件环境.因此,越来越多的密码学家开始设计能适应这种环境中的分组密码,并提出了许多轻量级分组密码算法,如 PRESENT[1]、PRINCE[2]、KATANTAN[3]、PRIDE[4]等.轻量级分组密码算法的分组和密钥长度一般较短,非线性组件规模较小,但迭代次数较高,从而便于软硬件的快速实现.

SIMON[5]算法是 2013 年由 NSA 提出的一簇轻量级分组密码算法,自提出以来,就受到密码分析者的广泛关注.Abed 等人[6]利用低重量的差分路径对 SIMON 进行了差分攻击.接着,Alkhzaimi 等人[7]利用差分分析对 SIMON 的安全性进行了估计.此外,Alizadeh 等人在文献[8]中对 SIMON 进行了线性攻击,并得到关于 SIMON 更好的线性分析结果.Abed 等人[6,9,10]将攻击轮数拓展到 SIMON 整个轮数的一半.Biryukov 等人在文献[11]中利用分支边界算法对 SIMON 和 SPECK 差分路径进行搜索.2015 年,Yu 等人[12]利用零相关线性分析的方法对缩减轮数的 SIMON 进行了攻击.在 2015 美密会,Kölbl 等人[13]详尽分析了 SIMON 轮函数的性质,并利用 SAT/SMT 求解器给出了自动化搜索 SIMON 差分和线性路径的算法.

不可能差分分析[14]最早由 Biham 等人提出,与差分分析寻找一条概率最大的差分路径不同,不可能差分的分析目的在于寻找一条概率为零的差分路径来排除错误的候选密钥,从而恢复正确密钥,目前被广泛地应用到了各种结构的分组密码攻击中,在 AES[15],MISTY1[16]等密码上有非常好的攻击效果.零相关线性分析方法[17]由 Bogdanov 等人于 2012 年提出,零相关线性分析的第 1 步是构造密码算法的零相关线性逼近关系,我们通常让线性掩码在非零偏差下从两头向中间传播,并在中间相遇,若任何一个位置产生矛盾,则找到一条零相关线性逼近.构造完密码算法的零相关线性逼近关系后,接下来就可以对密钥进行恢复.

除中间相错技术外,目前还存在几种自动化搜索不可能差分路径的算法,如μ-method[18],UID-method[19],MILP[20]等.然而它们均未能充分考虑非线性组件与的性质,所以不能精确给出每一轮的差分传播特征.

布尔可满足性问题(SAT)是当今计算机科学研究的核心问题,很多不容易处理的问题都可以通过某些途径转换成 SAT 问题,从而进行求解.本文提出了一种基于 SAT 的普适性的 SIMON 不可能差分和零相关路径自动化搜索算法.利用该算法,我们共搜索到 32 条 11 轮不可能差分和零相关路径.该算法除用于自动化搜索不可能差分(零相关)路径外,还可以在短时间内判断任意一对输入输出差分(掩码)是否构成一条不可能差分(零相关)路径.此外,SIMON 设计者并未给出其轮函数中循环移位常数(a,b,c)的选取依据,我们尝试从抵抗不可能差分攻击的角度,对该常数的选取进行分析.

本文第 1 节给出 SIMON 算法介绍.第 2 节给出 SIMON 不可能差分路径搜索算法.第 3 节给出 SIMON 零相关路径搜索算法.第 4 节给出不可能差分路径搜索算法的其他应用.第 5 节总结全文.

1 SIMON 算法介绍

1.1 概念与性质

我们用F_2代表二元有限域;F_2^n代表F_2上的n维向量;对于$a\in F_2^n$,用$wt(a)$代表a的汉明重量;用$\oplus$表示F_2^n中的异或运算;用$\odot$表示F_2^n中的与运算;用$\vee$表示F_2^n中的或运算;设$x\in F_2^n$,用$\bar{x}$代表其非运算;用S^i代表$F_2^n\to F_2^n$中的左循环移位运算.

SIMON 的轮函数表示如下:

$$f_{a,b,c}(x)=S^a(x)\odot S^b(x)\oplus Sc^a(x),$$

其中,循环移位常数(a,b,c)为(8,1,2).

为研究轮函数f的线性传播性质,我们首先给出如下概念.

定义 1. 对于n元布尔函数$f:F_2^n\to F_2^n$,其输入掩码α和输出掩码β对应的 Walsh 谱为

$$\hat{f}(\alpha,\beta)=\sum_x \mu(\langle\beta,f\rangle+\langle\alpha,x\rangle).$$

为方便书写,我们定义$\mu(x)=(-1)^x$.

定义 2. 对于 n 元布尔函数 $f:F_2^n \to F_2^n$,其输入掩码和输出掩码分别为α,β,则 f 对应的平方线性系数为

$$C^2(\alpha \to \beta)=\left(\frac{\hat{f}(\alpha,\beta)}{2^n}\right)^2.$$

定义 3. 给定输入输出差分α,β,则α通过 f 输出β的概率为

$$\Pr(\alpha \to \beta)=\frac{|\{x \mid f(x)\oplus f(x\oplus\alpha)=\beta\}|}{2^n}.$$

最后,我们用 $Dom(f)$表示 f 的定义域,用 $Img(f)$代表其值域.

1.2 SIMON算法

SIMON 类算法是典型的 Feistel 结构,其轮函数 $f(x)$采用按位与运算、循环移位运算和异或运算,其分组规模为 $2n(n=16,24,32,48,64)$,密钥规模为 mn,根据不同的主密钥规模 m,取 2,3 或 4,称为 SIMON $2n/mn$.SIMON 类算法结构如图 1 所示.

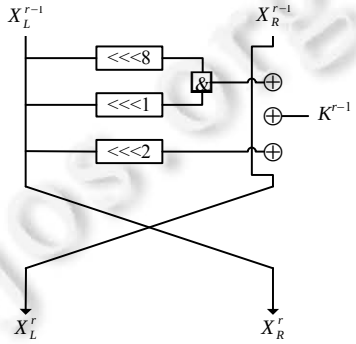

Fig.1 r-Round structure of SIMON

图 1 SIMON 第 r 轮结构

2 SIMON 不可能差分路径搜索

针对不同的密码算法,存在几种搜索不可能差分路径的方法,包括μ-method,UID-method 等.但这些算法也存在一些缺点和不足,由于没充分考虑非线性组件的性质,往往不能准确描述密码算法的差分传播性质.

本节,我们提出一种基于 SAT 的 SIMON 不可能差分路径自动搜索算法.利用该算法,可快速给出 SIMON 的 32 条 11 轮不可能差分路径.第 2.1 节介绍 SIMON 轮函数的差分传播性质;第 2.2 节给出基于 SAT 的 SIMON 不可能差分路径搜索方法;第 2.3 节给出 SIMON 的 32 条 11 轮不可能差分路径,并用中间相错方法对其进行验证.

2.1 SIMON轮函数的差分传播性质

在 2015 年的美密会,Kölbl 等人深入研究了 SIMON 中的 AND 组件,给出了准确的轮函数差分传播特性.

定理 1[13]. 给定输入输出差分α,β,则α通过函数 $f(x)=x\odot S^a(x)$输出为β的概率 $p_{\alpha,\beta}$为

$$p_{\alpha,\beta}=\begin{cases}2-n-d, & \text{if } \beta\oplus\alpha\odot S^8(\alpha)\in Img(L_\alpha)\\ 0, & \text{else}\end{cases},$$

其中,$d=dimker(L_\alpha)$,$L_\alpha(x)=x\odot S^a(\alpha)\oplus\alpha\odot S^a(x)$.

定理 2[13]. 令 $\mathrm{var}\,ibits=S^1(\alpha)\vee\alpha, doublebits=\alpha\odot\overline{S^1(\alpha)}\odot S^2(\alpha)$,则

$$P(\alpha\to\beta)=\begin{cases}2^{-n+1}, & \text{if } \alpha=1 \text{ and } wt(\beta)\equiv 0 \bmod 2\\ 2^{-wt(\mathrm{var}ibits\oplus doublebits)}, & \text{if } \alpha\neq 1 \text{ and } \beta\odot\overline{\mathrm{var}\,ibits}=0 \text{ and } (\beta\oplus S^1(\beta))\odot doublebits=0.\\ 0, & \text{else}\end{cases}$$

2.2 不可能差分路径搜索算法

为了得到一条有效的差分路径,根据第 2.1 节中的定理,我们构造出α和β需满足的如下约束式:

$$\left.\begin{array}{l}\text{if } \alpha!=1\\ \quad varibits=S^{8}(\alpha)\vee S^{1}(\alpha)\\ \quad doublebits=S^{1}(\alpha)\odot\overline{S^{8}(\alpha)}\wedge S^{15}(\alpha)\\ \quad \beta\odot varibits=0\\ \quad (\beta\oplus S^{7}(\beta))\odot doublebits=0\\ \text{else}\\ \quad wt(\beta)\equiv 0 \bmod 2\end{array}\right\}\tag{1}$$

再根据 SIMON 的算法结构,利用约束式(1)写出 n 轮差分的传播约束式;接着,对特定集合下的每一对差分,利用 SAT 求解器,对其 n 轮差分传递的有效性进行验证.该算法如算法 1 所示.

算法 1. SIMON 不可能差分路径搜索.

```
//SIMON 的分组长度为 n
//将所有刻画 SIMON 轮函数差分传播特性的约束式写入 model.cvc
Write all the constraints into model.cvc
//检测是否有一对输入输出差分特征构成一条不可能差分路径
for the given input difference Δx_i∈Δ do
    for the given output difference Δy_i∈Γ do
        Modify constraints on the fixed input
        and output differences of model.cvc
        m=dispose(model.cvc)
        if m==Invalid then
            //输出不可能差分路径
            print input and output difference
        else then
            print nothing
    end
end
```

算法 1 为遍历算法,其复杂度与输入输出差分对的选取集合有关.对于分组长度为 32 的密码算法,遍历起来不现实,我们通常选取特定集合来遍历.其中的 dispose 函数,将所列的约束式转化为合取范式(CNF),再将 CNF 送入特定的 SAT 求解器,验证其可否满足.目前存在多种 SAT 求解器,本文采用的是 CryptoMiniSat4.对于不同求解器,其求解效率也存在差异.

2.3 11轮SIMON的不可能差分路径

目前,关于 SIMON 的 3 条 11 轮不可能差分路径由 Wang 等人[21]利用中间相错技术给出,本文利用基于 SAT 的自动化搜索算法给出了 32 条 11 轮不可能差分路径,接着又用中间相错技术对其进行了验证.

2.3.1 32 条 11 轮不可能差分路径

SIMON 的分组长度是 32,遍历所有可能的差分对复杂度太高,所以我们只考虑输入、输出差分重量均为 1 的情况.利用该算法,我们在短时间内给出 32 条 SIMON 的 11 轮不可能差分路径,结果见表 1,其中,$v_i(0\leqslant i\leqslant 7)$代表只有第 i bit 为 1.而 0 则代表一个字节中所有 bit 均为 0.

搜索在一台 Intel Core i7-6700 笔记本上进行,时间为 29s.

Table 1 Impossible differential trails of SIMON

表 1 SIMON 不可能差分路径

SIMON不可能差分路径		
$(0,0,0,v_0)\to(0,v_7,0,0)$	$(0,0,0,v_0)\to(v_1,0,0,0)$	$(0,0,0,v_1)\to(v_2,0,0,0)$
$(0,0,0,v_1)\to(v_0,0,0,0)$	$(0,0,0,v_2)\to(v_3,0,0,0)$	$(0,0,0,v_2)\to(v_1,0,0,0)$
$(0,0,0,v_3)\to(v_2,0,0,0)$	$(0,0,0,v_3)\to(v_4,0,0,0)$	$(0,0,0,v_4)\to(v_3,0,0,0)$
$(0,0,0,v_4)\to(v_5,0,0,0)$	$(0,0,0,v_5)\to(v_4,0,0,0)$	$(0,0,0,v_5)\to(v_6,0,0,0)$
$(0,0,0,v_6)\to(v_5,0,0,0)$	$(0,0,0,v_6)\to(v_7,0,0,0)$	$(0,0,0,v_7)\to(0,v_0,0,0)$
$(0,0,0,v_7)\to(v_6,0,0,0)$	$(0,0,v_0,0)\to(0,v_1,0,0)$	$(0,0,v_0,0)\to(v_7,0,0,0)$
$(0,0,v_1,0)\to(0,v_0,0,0)$	$(0,0,v_1,0)\to(0,v_2,0,0)$	$(0,0,v_2,0)\to(0,v_1,0,0)$
$(0,0,v_2,0)\to(0,v_3,0,0)$	$(0,0,v_3,0)\to(0,v_2,0,0)$	$(0,0,v_3,0)\to(0,v_4,0,0)$
$(0,0,v_4,0)\to(0,v_3,0,0)$	$(0,0,v_4,0)\to(0,v_5,0,0)$	$(0,0,v_5,0)\to(0,v_4,0,0)$
$(0,0,v_5,0)\to(0,v_6,0,0)$	$(0,0,v_6,0)\to(0,v_5,0,0)$	$(0,0,v_6,0)\to(0,v_7,0,0)$
$(0,0,v_7,0)\to(0,v_6,0,0)$	$(0,0,v_7,0)\to(v_0,0,0,0)$	–

2.3.2 32 条不可能差分路径验证

中间相错技术的基本原理是:加密方向 $\Delta X \xrightarrow{E_1} \Delta M$ 寻找到一条概率为 1 的差分路径;接着,在解密方向 $\Delta Y \xrightarrow{D_1} \Delta N$ 也寻找到一条概率为 1 的差分路径.寻找到一条概率为 1 的差分路径,但$\Delta M\neq\Delta N$,构成矛盾,从而形成不可能差分.如图 2 所示.

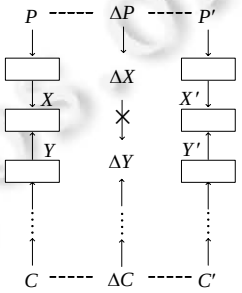

Fig.2 Schematic diagram of miss-in-the-middle

图 2 中间相错示意图

我们利用中间相错技术,对 32 轮不可能差分结果进行了验证,例如$(0,0,0,v_7)\to(v_6,0,0,0)$这条路径,验证结果在表 2 中给出,表 2 中的问号,即代表我们无法确定该比特位是 1 还是 0.

Table 2 Result of miss-in-the-middle

表 2 中间相错结果

不可能差分路径验证	
ΔL_0(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	ΔR_0(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0)
ΔL_1(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0)	ΔR_1(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
ΔL_2(?,0,0,0,0,0,1,?,0,0,0,0,0,0,0,0)	ΔR_2(0,0,0,0,0,0,0,0,1,0,0,0,0,0,0,0)
ΔL_3(0,0,0,0,1,?,?,0,?,0,0,0,0,0,?,?)	ΔR_3(?,0,0,0,0,0,1,?,0,0,0,0,0,0,0,0)
ΔL_4(?,0,1,?,?,?,?,?,0,0,0,0,?,?,?,0)	ΔR_4(0,0,0,0,1,?,?,0,?,0,0,0,0,0,?,?)
ΔL_5(1,?,?,?,?,?,?,0,?,0,?,?,?,?,?,?)	ΔR_5(?,0,1,?,?,?,?,?,0,0,0,0,?,?,?,0)
ΔL_6(?,?,?,?,?,?,?,?,?,?,?,?,?,?,?,?)	ΔR_6(1,?,?,?,?,?,?,0,?,0,?,?,?,?,?,?)
ΔL_6(?,0,0,0,0,?,?,?,0,?,0,1,?,?,?,?)	ΔR_6(0,?,0,?,?,?,?,?,?,1,?,?,?,?,?,?)
ΔL_7(0,?,0,0,0,0,0,?,?,0,0,0,0,1,?,?)	ΔR_7(?,0,0,0,0,?,?,?,0,?,0,1,?,?,?,?)
ΔL_8(?,0,0,0,0,0,0,0,0,?,0,0,0,0,0,1)	ΔR_8(0,?,0,0,0,0,0,?,?,0,0,0,0,1,?,?)
ΔL_9(0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	ΔR_9(?,0,0,0,0,0,0,0,0,?,0,0,0,0,0,1)
ΔL_{10}(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	ΔR_{10}(0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)
ΔL_{11}(0,1,0,0,0,0,0,0,0,0,0,0,0,0,0,0)	ΔR_{11}(0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0)

从表 2 中可以看到,差分$(\Delta L_0,\Delta R_0)$(即$(0,0,0,v_7)$)向下传递 6 轮与差分$(\Delta L_{11},\Delta R_{11})$(即$(v_6,0,0,0)$)向上传递 5 轮以后,在$(\Delta L_6,\Delta R_6)$相遇.观察差分前后传递得到的$\Delta R_6$ 值,(1,?,?,?,?,?,?,0,?,0,?,?,?,?,?,?)与(0,?,0,?,?,?,?,?,?,1,?,?,?,?,?,?)在最高比特位构成矛盾.

3 SIMON 零相关路径搜索

目前,关于 SIMON 的 11 轮零相关路径由 Wang 等人[21]给出.本节提出一种基于 SAT 的 SIMON 零相关路径自动搜索算法,利用该算法,可以快速地给出 SIMON 的 32 条 11 轮不可能差分路径.第 3.1 节介绍 SIMON 轮函数的线性传播性质;第 3.2 节给出基于 SAT 的 SIMON 零相关路径搜索方法;第 3.3 节给出 SIMON 条 11 轮零相关路径.

3.1 SIMON轮函数的线性传播性质

与(AND)运算对 SIMON 线性掩码的传递有着重要影响,Kölbl 等人[13]对非线性组件与进行了深入的研究,并给出了一些能够精确描述 SIMON 轮函数线性传播性质的表达式.

定理 3[13]. SIMON 算法中, $u \xrightarrow{f} v$ 的平方线性相关系数 $C(u\to v)$为

$$C(u\to v)=\begin{cases}2^{-n+2}, & \text{if } v=1 \text{ and } u\in U_{1/v}\\ 2^{-\theta(v)}, & \text{if } v\neq 1 \text{ and } u\in U_{1/v}\\ 0, & \text{else}\end{cases}.$$

3.2 零相关分路径搜索算法

本节中,首先构造描述 SIMON 轮函数线性传播性质的约束式,然后,利用约束式构造一个用于自动搜索 SIMON 零相关路径的算法.

由第 3.1 节可知,若 $u\to v$ 有效当且仅当 $u\in U_{1/v}$.为得到一条有效的线性路径,我们构造如下的约束式:

$$\left.\begin{array}{l}
u=u\oplus S^{-c}(v)\\
((S^{-a}(v)\mid S^{-b}(v))\oplus u)\odot u!=0\\
\text{if }(f,v==(2^n-1))\\
\quad t,l=u,0\\
\quad \text{while } t!=0\\
\qquad l=l\oplus(t\odot 3)\\
\qquad t=(t\gg 2)\\
\quad l=0\\
\text{else}\\
\quad tmp=v\\
\quad abits=v\\
\quad \text{while } tmp!=0\\
\qquad tmp=v\odot S^{-(a-b)}(tmp)\\
\qquad abits=abits\oplus tmp\\
\quad sbits=S^{-(a-b)}(v)\odot(-v)\odot(-S^{-(a-b)}(abits))\\
\quad sbits=S^{-b}(sbits)\\
\quad pbits=0\\
\quad \text{while } sbits!=0\\
\qquad pbits\wedge=sbits\odot u\\
\qquad sbits=S^{a-b}(sbits)\odot S^{-b}(v)\\
\qquad sbits=S^{a-b}(sbits)\\
\qquad pbits=S^{2*(a-b)}(pbits)\\
\quad pbits=0
\end{array}\right\}\tag{2}$$

结合约束式(2),我们构造了一种用于搜索 SIMON 零相关路径的算法.该算法是一种遍历算法,通过穷举特

定的输入输出掩码集合(Δ,Γ),判断每一对输入输出掩码是否构成一条有效线性路径:若否,则输出一条零相关路径.考虑到 SIMON 的分组长度.我们无法遍历所有可能的输入输出掩码,(Δ,Γ)只是掩码全集中的一个子集,该算法如算法 2 所示.

算法 2. SIMON 零相关路径搜索.

```
//SIMON 的分组长度为 n
//将所有刻画 SIMON 轮函数线性传播特性的约束式写入 model.cvc
Write all the constraints into model.cvc
//检测是否有一对输入输出线性掩码构成一条零相关路径
for the given input mask Δx_i∈Δ do
    for the given output mask Δy_i∈Γ do
        Modify constraints on the fixed input
        and output masks of model.cvc
        m=dispose(model.cvc)
        if m==Invalid then
            //输出零相关路径
            print input and output mask
        else then
            print nothing
    end
end
```

3.3 11轮SIMON零相关路径

类似于搜索不可能差分,我们只考虑输入输出掩码重量均为 1 的情况.利用第 3.2 节中的算法,我们共找到 32 条零相关路径,见表 3.

Table 3 Zero-Correlation linear trails of SIMON

表 3 SIMON 零相关路径

SIMON零相关路径		
$(0,v_0,0,0)\to(0,0,0,v_7)$	$(0,v_0,0,0)\to(0,0,v_1,0)$	$(0,v_1,0,0)\to(0,0,v_0,0)$
$(0,v_1,0,0)\to(0,0,v_2,0)$	$(0,v_2,0,0)\to(0,0,v_1,0)$	$(0,v_2,0,0)\to(0,0,v_3,0)$
$(0,v_3,0,0)\to(0,0,v_2,0)$	$(0,v_3,0,0)\to(0,0,v_4,0)$	$(0,v_4,0,0)\to(0,0,v_3,0)$
$(0,v_4,0,0)\to(0,0,v_5,0)$	$(0,v_5,0,0)\to(0,0,v_4,0)$	$(0,v_5,0,0)\to(0,0,v_6,0)$
$(0,v_6,0,0)\to(0,0,v_5,0)$	$(0,v_6,0,0)\to(0,0,v_7,0)$	$(0,v_7,0,0)\to(0,0,0,v_0)$
$(0,v_7,0,0)\to(0,0,v_6,0)$	$(v_0,0,0,0)\to(0,0,0,v_1)$	$(v_0,0,0,0)\to(0,0,v_7,0)$
$(v_1,0,0,0)\to(0,0,0,v_0)$	$(v_1,0,0,0)\to(0,0,0,v_2)$	$(v_2,0,0,0)\to(0,0,0,v_1)$
$(v_2,0,0,0)\to(0,0,0,v_3)$	$(v_3,0,0,0)\to(0,0,0,v_2)$	$(v_3,0,0,0)\to(0,0,0,v_4)$
$(v_4,0,0,0)\to(0,0,0,v_3)$	$(v_4,0,0,0)\to(0,0,0,v_5)$	$(v_5,0,0,0)\to(0,0,0,v_4)$
$(v_5,0,0,0)\to(0,0,0,v_6)$	$(v_6,0,0,0)\to(0,0,0,v_5)$	$(v_6,0,0,0)\to(0,0,0,v_7)$
$(v_7,0,0,0)\to(0,0,0,v_6)$	$(v_7,0,0,0)\to(0,0,v_0,0)$	–

由于线性传播特性刻画复杂,上述结果的搜索时间约为 17min.

4 不可能差分路径搜索算法的其他应用

4.1 SIMON不可能差分存在性证明

本文提出的算法除用于自动化搜索不可能差分外,还可以快速判断给定的输入输出差分是否能构成一条有效路径.我们将输入差分分成左右两部分(左右各为 16bit),并将左半部分设为 0x0000,右半部分从 0x0000 遍历到 0xFFFF,接着设定输出差分重量为 1.通过遍历上述集合中所有可能的输入输出差分,我们确定在该集合下

SIMON 最长不可能差分的轮数确为 11 轮.上述结果的搜索时间为 21h,如果计算能力允许,还可给出比现有结果更强的结论.

4.2 SIMON循环移位常数选取分析

SIMON 设计者从未给出图 1 中循环移位常数(8,1,2)的选取思路.我们尝试从抵抗不可能差分的角度,来分析循环移位常数对 SIMON 安全性的影响,希望能起到一些抛砖引玉的作用.

Kölbl 等人[13]主要从抵抗差分攻击的角度对循环移位常数的选取进行了分析.通过研究 SIMON 循环移位常数对其扩散性的影响,文献[13]从所有可能的移位常数(a,b,c)中选出一个集合Δ,由Δ中元素构成的 SIMON32, SIMON48,SIMON64 算法,均有类似于标准算法的 10 轮差分概率,具有较好的扩散性和抵抗差分攻击能力.Δ见表 4.

Table 4 Cyclic shift constant set of SIMON

表 4 SIMON 循环移位常数选取集合

循环移位常数(a,b,c)选取集合			
(1,0,2)	(1,0,3)	(2,1,3)	(4,3,5)
(5,0,10)	(5,0,15)	(5,4,3)	(7,0,14)
(7,6,5)	(8,1,3)	(8,3,14)	(8,7,5)
(10,5,15)	(11,6,1)	(12,1,7)	(12,5,3)
(12,7,1)	(13,0,10)	(13,0,7)	(13,8,2)

分别对Δ中元素构成的 SIMON 算法进行不可能差分路径搜索,以测试其抵抗不可能差分攻击的能力.利用自动搜索算法,设定输入输出重量均为 1,分别对Δ中元素构成的 SIMON 算法进行 11 轮不可能差分路径搜索,结果见表 5;利用自动搜索算法,设定输入输出重量均为 1,分别对Δ中元素构成的 SIMON 算法进行 12 轮不可能差分路径搜索,结果见表 6.

Table 5 Impossible differential trails of 11-round SIMON with different parameters

表 5 SIMON 不同参数 11 轮不可能差分路径

SIMON 不同参数 11 轮不可能差分路径搜索结果			
(1,0,2)	(1,0,3)	(2,1,3)	(4,3,5)
1008 条	464 条	464 条	96 条
(5,0,10)	(5,0,15)	(5,4,3)	(7,0,14)
1008 条	464 条	96 条	1008 条
(7,6,5)	(8,1,3)	(8,3,14)	(8,7,5)
464 条	464 条	1008 条	464 条
(10,5,15)	(11,6,1)	(12,1,7)	(12,5,3)
464 条	464 条	96 条	96 条
(12,7,1)	(13,0,10)	(13,0,7)	(13,8,2)
96 条	1008 条	464 条	1008 条

Table 6 Impossible differential trails of 12-round SIMON with different parameters

表 6 SIMON 不同参数 12 轮不可能差分路径

SIMON 不同参数 12 轮不可能差分路径搜索结果			
(1,0,2)	(1,0,3)	(2,1,3)	(4,3,5)
944 条	176 条	176 条	0 条
(5,0,10)	(5,0,15)	(5,4,3)	(7,0,14)
944 条	176 条	0 条	944 条
(7,6,5)	(8,1,3)	(8,3,14)	(8,7,5)
176 条	176 条	944 条	176 条
(10,5,15)	(11,6,1)	(12,1,7)	(12,5,3)
176 条	176 条	0 条	0 条
(12,7,1)	(13,0,10)	(13,0,7)	(13,8,2)
0 条	944 条	176 条	944 条

由第 2.3 节可知,用原始移位参数(8,1,2)搜索 SIMON 的 11 轮不可能差分路径条数为 32 条,搜索到 12 轮不

可能差分路径条数为 0 条,结果均小于或等于Δ中元素搜索到的条数.可见,SIMON 原始参数更能抵抗不可能差分攻击.

5 总 结

本文提出了一种SIMON不可能差分及零相关路径自动化搜索算法.利用该算法,我们能够快速地搜索到更多条数的 11 轮 SIMON 不可能差分及零相关路径.该算法还可以准确地判断任意差分对(掩码对)能否构成一条不可能差分(零相关路径).此外,我们还给出了特定输入输出差分集合下,SIMON 算法不存在 12 轮不可能差分路径的结论.最后,我们从抵抗不可能差分攻击的角度,对 SIMON 循环移位参数的安全性进行估计,并验证了相对于其他参数,SIMON 原始参数具有更强的抵抗不可能差分攻击能力.在后续工作中,我们拟对该算法做出进一步的优化,并将其推广到其他结构的分组密码上.

References:

[1] Bogdanov A, Knudsen LR, Leander G, Paar C, Poschmann A, Robshaw MJB, Seurin Y, Vikkelsoe C. PRESENT: An ultra-lightweight block cipher. In: Proc. of the CHES 2007. LNCS 4727, Berlin: Springer-Verlag, 2007. 350−466.

[2] Borghoff J, Canteaut A, Gneysu T, Lender G, *et al*. PRINCE—A low-latency block cipher for pervasive computing applications: Extended abstract. In: Proc. of the ASIACRYPT 2012. LNCS 7658, Berlin: Springer-Verlag, 2012. 208−225.

[3] De Canniére C, Dunkelman O, Knezevic M. KATAN and KTANTAN: A family of small and efficient hardware-oriented block ciphers. In: Proc. of the CHES 2009. LNCS 5747, Berlin: Springer-Verlag, 2009. 272−288.

[4] Albrecht MR, Driessen B, Kavun EB, Leander G, Paar C, Yalcn T, *et al*. Block ciphers-focus on the linear layer (feat. PRIDE). In: Proc. of the CRYPTO 2014. LNCS 8616, Berlin: Springer-Verlag, 2014. 57−76.

[5] Beaulieu R, Shors D, Smith J, Clark ST, Weeks B, Wingers L. The SIMON and SPECK families of lightweight block ciphers. Technical Report, 2013/404, 2013.

[6] Abed F, List E, Lucks S, Wenzel J. Differential and linear cryptanalysis of reduced-round SIMON. Technical Report, 526, 2013.

[7] Alkhzaimi H, Lauridsen M. Cryptanalysis of the SIMON family of block ciphers. Technical Report, 543, 2013.

[8] Alizadeh J, Bagheri N, Gauravaram P, Kumar A, Sanadhya SK. Linear cryptanalysis of round reduced SIMON. Technical Report, 663, 2013.

[9] Abed F, List E, Lucks S, Wenzel J. Cryptanalysis of the SPECK family of block ciphers. Technical Report, 568, 2013.

[10] Abed F, List E, Lucks S, Wenzel J. Differential cryptanalysis of round-reduced SIMON and SPECK. In: Proc. of the FSE 2014. LNCS 8540, Berlin: Springer-Verlag, 2014. 525−545.

[11] Biryukov A, Roy A, Velichkov V. Differential analysis of block ciphers SIMON and SPECK. In: Proc. of the FSE 2014. LNCS 8540, Berlin: Springer-Verlag, 2014. 546−570.

[12] Yu XL, Wu WL, Shi ZQ, Member S, Shi ZQ, Zhang J, Zhang L, Wang YF. Zero-Correlation linear cryptanalysis of reduced- round SIMON. Journal of Computer Science and Technology, 2015,30(6):1358−1369.

[13] Köbl S, Leander G, Tiessen T. Observations on the SIMON block cipher family. In: Proc. of the CRYPTO 2015. LNCS 9215, Berlin: Springer-Verlag, 2015. 161−185.

[14] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials. In: Proc. of the EUROCRYPT'99. Berlin, Heidelberg: Springer-Verlag, 1999. 12−23.

[15] FIPS PUB 197. Announcing the Advanced Encryption Standard (AES). Washington: National Institute of Standards and Technology, 2001.

[16] Matsui M. New block encryption algorithm MISTY. In: Proc. of the FSE'97. LNCS 1267, Berlin: Springer-Verlag, 1997. 64−67.

[17] Bogdanov A, Rijmen V. Linear hulls with correlation zero and linear cryptanalysis of block ciphers. Designs, Codes and Cryptography, 2014,70(3):369−383.

[18] Kim J, Hong S, Lim J. Impossible differential cryptanalysis using matrix method. Discrete Mathematics, 2010,310(5):988−1002.

[19] Luo YY, Lai XJ, Wu ZM, Gong G. A unified method for finding impossible differentials of block cipher structures. Information Sciences, 2014,263(1):211−220.

[20] Cui TT, Jia KT, Fu K, Chen SY, Wang MQ. New automatic search tool for impossible differentials and zero-correlation linear approximations. IACR Cryptology ePrint Archive, 2016. https://eprint.iacr.org/2016/689.pdf

[21] Wang QJ, Liu ZQ, Varici K, Sasaki Y, Rijmen V, Yosuke T. Cryptanalysis of reduced-round SIMON32 and SIMON48. In: Proc. of the INDOCRYPT 2014. LNCS 8885, Berlin: Springer-Verlag, 2014. 143−160.

张仕伟(1988－),男,河北迁安人,硕士生,主要研究领域为密码学,信息安全.

陈少真(1967－),女,博士,教授,博士生导师,主要研究领域为密码学,信息安全.