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		
$(0,0,0,v_0)\rightarrow(0,v_7,0,0)$	$(0,0,0,v_0)\rightarrow(v_1,0,0,0)$	$(0,0,0,v_1)\rightarrow(v_2,0,0,0)$
$(0,0,0,v_1)\rightarrow(v_0,0,0,0)$	$(0,0,0,v_2)\rightarrow(v_3,0,0,0)$	$(0,0,0,v_2)\rightarrow(v_1,0,0,0)$
$(0,0,0,v_3)\rightarrow(v_2,0,0,0)$	$(0,0,0,v_3)\rightarrow(v_4,0,0,0)$	$(0,0,0,v_4)\rightarrow(v_3,0,0,0)$
$(0,0,0,v_4)\rightarrow(v_5,0,0,0)$	$(0,0,0,v_5)\rightarrow(v_4,0,0,0)$	$(0,0,0,v_5)\rightarrow(v_6,0,0,0)$
$(0,0,0,v_6)\rightarrow(v_5,0,0,0)$	$(0,0,0,v_6)\rightarrow(v_7,0,0,0)$	$(0,0,0,v_7)\rightarrow(0,v_0,0,0)$
$(0,0,0,v_7)\rightarrow(v_6,0,0,0)$	$(0,0,v_0,0)\rightarrow(0,v_1,0,0)$	$(0,0,v_0,0)\rightarrow(v_7,0,0,0)$
$(0,0,v_1,0)\rightarrow(0,v_0,0,0)$	$(0,0,v_1,0)\rightarrow(0,v_2,0,0)$	$(0,0,v_2,0)\rightarrow(0,v_1,0,0)$
$(0,0,v_2,0)\rightarrow(0,v_3,0,0)$	$(0,0,v_3,0)\rightarrow(0,v_2,0,0)$	$(0,0,v_3,0)\rightarrow(0,v_4,0,0)$
$(0,0,v_4,0)\rightarrow(0,v_3,0,0)$	$(0,0,v_4,0)\rightarrow(0,v_5,0,0)$	$(0,0,v_5,0)\rightarrow(0,v_4,0,0)$
$(0,0,v_5,0)\rightarrow(0,v_6,0,0)$	$(0,0,v_6,0)\rightarrow(0,v_5,0,0)$	$(0,0,v_6,0)\rightarrow(0,v_7,0,0)$
$(0,0,v_7,0)\rightarrow(0,v_6,0,0)$	$(0,0,v_7,0)\rightarrow(v_0,0,0,0)$	–

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.

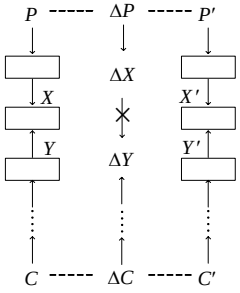

Fig.2 Schematic diagram of miss-in-the-middle

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$(0,0,0,v_7)\rightarrow(v_6,0,0,0)$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(0,0,0,0,0,1,?,?,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,?,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,?,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,?,?,0,0,0,0,1,?,?)
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,?,0,0,0,0,0,0,1)
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:

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

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
1   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
2   for the given input mask Δx_i∈Δ do
3   |  for the given output mask Δy_i∈Γ do
4   |  |  Modify constraints on the fixed input
    |  |  and output masks of model.cvc
5   |  |  m=dispose(model.cvc)
6   |  |  if m==Invalid then
    |  |     //输出零相关路径
7   |  |     print input and output mask
8   |  |  else then
9   |  |     print nothing
10  |  end
11 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		
$(0,v_0,0,0)\rightarrow(0,0,0,v_7)$	$(0,v_0,0,0)\rightarrow(0,0,v_1,0)$	$(0,v_1,0,0)\rightarrow(0,0,v_0,0)$
$(0,v_1,0,0)\rightarrow(0,0,v_2,0)$	$(0,v_2,0,0)\rightarrow(0,0,v_1,0)$	$(0,v_2,0,0)\rightarrow(0,0,v_3,0)$
$(0,v_3,0,0)\rightarrow(0,0,v_2,0)$	$(0,v_3,0,0)\rightarrow(0,0,v_4,0)$	$(0,v_4,0,0)\rightarrow(0,0,v_3,0)$
$(0,v_4,0,0)\rightarrow(0,0,v_5,0)$	$(0,v_5,0,0)\rightarrow(0,0,v_4,0)$	$(0,v_5,0,0)\rightarrow(0,0,v_6,0)$
$(0,v_6,0,0)\rightarrow(0,0,v_5,0)$	$(0,v_6,0,0)\rightarrow(0,0,v_7,0)$	$(0,v_7,0,0)\rightarrow(0,0,0,v_0)$
$(0,v_7,0,0)\rightarrow(0,0,v_6,0)$	$(v_0,0,0,0)\rightarrow(0,0,0,v_1)$	$(v_0,0,0,0)\rightarrow(0,0,v_7,0)$
$(v_1,0,0,0)\rightarrow(0,0,0,v_0)$	$(v_1,0,0,0)\rightarrow(0,0,0,v_2)$	$(v_2,0,0,0)\rightarrow(0,0,0,v_1)$
$(v_2,0,0,0)\rightarrow(0,0,0,v_3)$	$(v_3,0,0,0)\rightarrow(0,0,0,v_2)$	$(v_3,0,0,0)\rightarrow(0,0,0,v_4)$
$(v_4,0,0,0)\rightarrow(0,0,0,v_3)$	$(v_4,0,0,0)\rightarrow(0,0,0,v_5)$	$(v_5,0,0,0)\rightarrow(0,0,0,v_4)$
$(v_5,0,0,0)\rightarrow(0,0,0,v_6)$	$(v_6,0,0,0)\rightarrow(0,0,0,v_5)$	$(v_6,0,0,0)\rightarrow(0,0,0,v_7)$
$(v_7,0,0,0)\rightarrow(0,0,0,v_6)$	$(v_7,0,0,0)\rightarrow(0,0,v_0,0)$	–

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.