TWINE 算法的相关密钥不可能飞来去器攻击

谢敏，田峰，李嘉琪
（西安电子科技大学综合业务网理论及关键技术国家重点实验室，陕西 西安 710071）

摘 要：为了评估轻量级分组密码算法 TWINE 的安全性，利用相关密钥不可能飞来去器的方法对其进行了分析。构造了由 16 轮和 17 轮两条路径组成的相关密钥不可能飞来去器区分器，并将 16 轮和 17 轮的路径向前扩展 4 轮、向后分别扩展 3 轮和 2 轮，完成对 23 轮 TWINE 密码算法（80 bit 密钥）的攻击。实验结果表明，该攻击的数据复杂度为 $2^{62.05}$ 个明文，时间复杂度为 $2^{70.49}$ 次 23 轮加密，与现有算法相比有明显优势。

关键词：TWINE 算法；轻量级分组密码；不可能飞来去器；相关密钥
中图分类号：TN918.1
文献标识码：A
doi: 10.11959/j.issn.1000−436x.2019152

Related-key impossible boomerang cryptanalysis on TWINE

XIE Min, TIAN Feng, LI Jiaqi
State Key Laboratory of Integrated Services Networks, Xidian University, Xi’an 710071, China

Abstract: In order to evaluate the security of the lightweight block cipher TWINE, the method of related-key impossible boomerang cryptanalysis was applied and a related-key impossible boomerang distinguisher consisting of 16-round and 17-round paths was constructed. Based on this new distinguisher, an attack on 23-round TWINE was mounted successfully by concatenating 4-round to the beginning and 2-round for the 17-round path and 3-round for the 16-round path to the end respectively. The attack on 23-round TWINE required data complexity of only $2^{62.05}$ plaintexts and computational complexity of about $2^{70.49}$ 23-round encryptions. Compared with published cryptanalysis results, the proposed attack has obvious advantages.

Key words: TWINE algorithm, lightweight block cipher, impossible boomerang, related-key

1 引言

随着电子信息技术的迅猛发展，物联网、射频识别等技术被广泛应用，这使适用于资源受限设备的轻量级分组密码迅速成为研究热点。与传统分组密码相比，轻量级分组密码具有占用资源少、功耗低、效率高和易于实现等优势。从早期的 HIGHT[1]、PRESENT[2]和 MIBS[3]，到后来的 LBlock[4]、PRINCE[5]和 Piccolo[6]等多种算法的提出，轻量级分组密码设计和分析的发展已经愈显成熟。

TWINE 分组密码算法是 Suzaki 等[7]在 Selected Areas in Cryptography 2012 上提出的一种轻量级分组密码算法，可以在计算资源受限的硬件和微型控制器上实现。TWINE 分组密码算法的设计采用了广义 Feistel 结构，分组长度为 64 bit，密钥长度分为 80 bit 和 128 bit 这 2 种版本。算法的提出者对 TWINE 进行了安全性分析，提出了 15 轮的不可能

收稿日期：2019–01–26；**修回日期**：2019–05–22
基金项目：国家重点研发计划基金资助项目（No.2016YFB0800601）；国家自然科学基金资助项目（No.U1636209）；“十三五”国家密码发展基金资助项目（No.MMJJ20180219）
Foundation Items: The National Key Research and Development Program of China (No.2016YFB0800601), The National Natural Science Foundation of China (No.U1636209), The National Cryptography Development Fund of the 13th Five-Year Plan (No. MMJJ20180219)

差分路径，完成了对 23 轮 TWINE-80 和 24 轮 TWINE-128 的不可能差分分析；Zheng 等[8]对 Suzaki 等在分析中关于计算复杂度上存在的一些漏洞进行了更正与补充，提出了更严谨的不可能差分分析；此后 Wang 等[9]利用零相关线性分析的方法，对 23 轮的 TWINE 进行了分析，结论较已有分析有所改进；Coban 等[10]和 Mohamed 等[11]对 36 轮的 TWINE 分别进行了 Biclique 分析和中间相遇攻击，但其计算复杂度都接近穷举搜索；2017 年，Wei 等[12]对 TWINE 进行了相关密钥不可能差分分析，并提出了 TWINE 的等价算法，该算法描述简洁直观，更加有利于分析，他们构造了一条 15 轮的相关密钥不可能区分器，并向上扩展 4 轮，向下扩展 5 轮，首次对 24 轮的 TWINE 进行了攻击，但在构造文章所述的明文对时，结构数 n 最大只能取到 16，这会导致能恢复的密钥比特很少且无实际价值。

相关密钥不可能飞来去器[13]是近年来提出的一种新的分析方法，它结合了 3 种不同分析方法的优势，对于轻量级的分组密码算法如 LBlock 等已有较好的分析结果[14]。对 TWINE 而言，引入相关密钥和飞来去器的方法可以使路径的选择变得更加灵活，本文采用相关密钥不可能差分飞来去器的方法对 23 轮 TWINE-80 算法进行了攻击，获得了较优的分析结果。

2　TWINE 分组密码介绍

2.1　TWINE 加密算法

TWINE 算法的分组长度为 64 bit，密钥长度分为 80 bit 和 128 bit 这 2 种，明文经过 36 轮迭代得到密文。其中，轮函数采用了广义 Feistel 结构，如图 1 所示，结构中的 S 盒如表 1 所示。

表 1　TWINE 的 S 盒

x	$S(x)$	x	$S(x)$
0	C	8	8
1	0	9	3
2	F	10	D
3	A	11	7
4	2	12	1
5	B	13	E
6	9	14	6
7	5	15	4

2.2　TWINE 的等价算法

Wei 等[12]将 TWINE 算法描述为等价的 TWINE*算法，并对 2 种算法的等价性进行了证明。TWINE*算法更加直观地体现了 TWINE 算法的结构特点，便于更好地展开分析。本文将在 TWINE*算法的基础上进行相关密钥不可能飞来去器分析，算法的描述如下。

1) 第一轮进行置换 IP，如表 2 所示，置换后的明文分为左 32 bit 和右 32 bit。

2) 按图 2 所示加密结构进行迭代计算，其中 P_1 和 P_2 置换如表 3 和表 4 所示。

3) 对最后一轮的轮函数输出进行置换 FP，如表 5 所示。

表 2　置换 IP

x	IP(x)	x	IP(x)
0	0	8	4
1	8	9	12
2	1	10	5
3	9	11	13
4	2	12	6
5	10	13	14
6	3	14	7
7	11	15	15

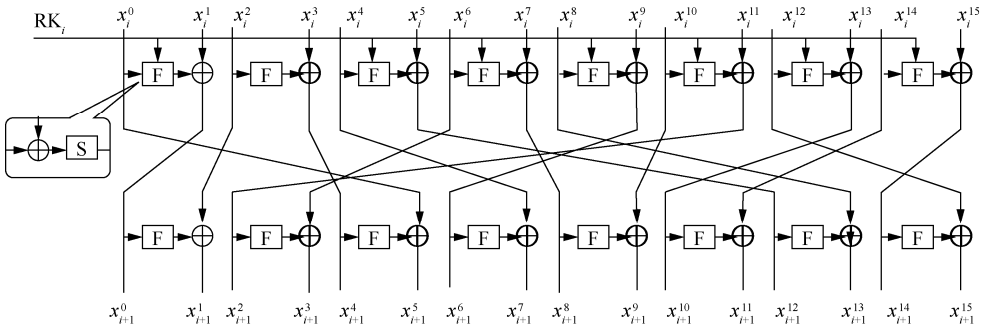


图 1　TWINE 算法的轮函数

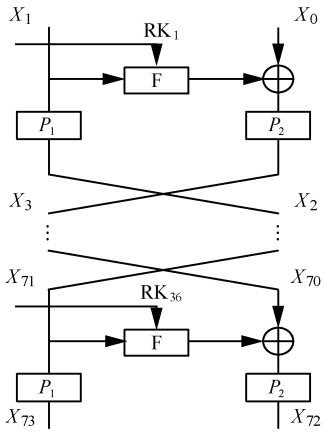


图 2　TWINE*的加密结构

表 3　　P_1 置换

x	$P_1(x)$
0	2
1	0
2	3
3	1
4	6
5	4
6	7
7	5

表 4　　P_2 置换

x	$P_2(x)$
0	0
1	2
2	6
3	4
4	3
5	1
6	5
7	7

表 5　　置换 FP

x	FP(x)	x	FP(x)
0	0	8	1
1	2	9	3
2	4	10	5
3	6	11	7
4	8	12	9
5	10	13	11
6	12	14	13
7	14	15	15

2.3　TWINE-80 的密钥编排算法

TWINE-80 算法的密钥编排算法为

$$\mathrm{WK}^0\|\mathrm{WK}^1\|\cdots\|\mathrm{WK}^{18}\|\mathrm{WK}^{19} \leftarrow K$$

其中，K 为 80 bit 主密钥，$\mathrm{WK}^i(0\leqslant i\leqslant 19)$ 为半字节块。

for　$r \leftarrow 1$ to 35

$$\text{do}\begin{cases}\mathrm{RK}_{r(32\,\mathrm{bit})} \leftarrow \mathrm{WK}^1\|\mathrm{WK}^3\|\mathrm{WK}^4\|\mathrm{WK}^6\| \\ \|\mathrm{WK}^{13}\|\mathrm{WK}^{14}\|\mathrm{WK}^{15}\|\mathrm{WK}^{16}\| \\ \mathrm{WK}^1 \leftarrow \mathrm{WK}^1 \oplus S(\mathrm{WK}^0) \\ \mathrm{WK}^4 \leftarrow \mathrm{WK}^4 \oplus S(\mathrm{WK}^{16}) \\ \mathrm{WK}^7 \leftarrow \mathrm{WK}^7 \oplus 0\|\mathrm{CON}_r^H \\ \mathrm{WK}^{19} \leftarrow \mathrm{WK}^{19} \oplus 0\|\mathrm{CON}_r^L \\ \mathrm{WK}^0\|\mathrm{WK}^1\|\mathrm{WK}^2\|\mathrm{WK}^3 \leftarrow \\ \mathrm{Rot4}(\mathrm{WK}^0\|\mathrm{WK}^1\|\mathrm{WK}^2\|\mathrm{WK}^3) \\ \mathrm{WK}^0\|\mathrm{WK}^1\|\mathrm{WK}^2\|\cdots\|\mathrm{WK}^{19} \leftarrow \\ \mathrm{Rot16}(\|\mathrm{WK}^0\|\mathrm{WK}^1\|\mathrm{WK}^2\|\cdots\|\mathrm{PWK}^{19})\end{cases}$$

$$\mathrm{RK}_{36(32\,\mathrm{bit})} \leftarrow \mathrm{WK}^1\|\mathrm{WK}^3\|\mathrm{WK}^4\|\mathrm{WK}^6\|\mathrm{WK}^{13}\|\mathrm{WK}^{14}\|\mathrm{WK}^{15}\|\mathrm{WK}^{16}$$

$$\mathrm{RK} \leftarrow \mathrm{RK}_1\|\mathrm{RK}_2\|\mathrm{RK}_3\|\cdots\|\mathrm{RK}_{34}\|\mathrm{RK}_{35}\|\mathrm{RK}_{36}$$

其中，$\mathrm{CON}_i^{(6)} = \mathrm{CON}_i^{H(3)}\|\mathrm{CON}_i^{L(3)}, i = 1,\cdots,35$，$\mathrm{CON}_i$ 的值如表 6 所示。根据密钥编排算法的特点可知，每轮只有 2 个半字节密钥 WK^i 进入 S 盒，2 个半字节密钥与 CON 值异或。引入相关密钥后，主密钥与 CON 值的异或并不会影响其本身的差分。合理利用密钥编排算法这一弱点，选择合适的主密钥差分，可以得到较好的分析路径。

表 6　　CON_i 的值

i	CON_i	i	CON_i
1	1	19	0F
2	2	20	1E
3	4	21	3C
4	8	22	3B
5	10	23	35
6	20	24	29
7	3	25	11
8	6	26	22
9	0C	27	7
10	18	28	0E
11	30	29	1C
12	23	30	38
13	5	31	33
14	0A	32	25
15	14	33	9
16	28	34	12
17	13	35	24
18	26	—	—

3　相关密钥不可能飞来去器攻击介绍

相关密钥[15]、不可能差分[16]和飞来去器[17]都是被广泛应用的分组密码攻击方法，其中相关密钥利用了密钥编排算法的弱点，构造特定的密钥差分影响算法的加解密，从而构造路径恢复密钥；不可能差分攻击是用一条概率为 0 的差分路径来淘汰符合这条路径的错误密钥；飞来去器则灵活地应用差分的特点将算法分为两部分进行分析，以寻找更好的路径。近年来，很多研究者倾向于将多种分析方法相结合，以期对算法安全性做出更好的研究[18-20]。

相关密钥不可能飞来去器攻击结合了以上 3 种分析方法的思想。利用飞来去器和相关密钥的方法，可以在算法上下两部分做不同的密钥差分，有助于扩展攻击轮数；利用不可能差分，配合相关密钥对算法分析给出更多的可能途径，以便寻找到更好的分析路径。相关密钥不可能飞来去器的攻击方法如图 3 所示。

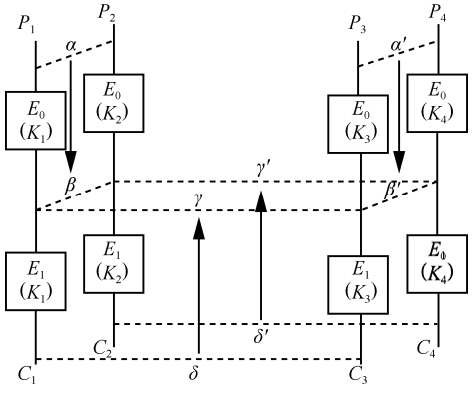


图 3　相关密钥不可能飞来去器的攻击方法

算法分析过程中，加密算法 E 被分为 2 种算法（E_0 和 E_1）的组合。P_1、P_2、P_3、P_4 经对应密钥 K_1、K_2、K_3、K_4 加密分别得到(C_1、C_2、C_3、C_4)，其中 4 个密钥满足 $K_1 \oplus K_2 = K_3 \oplus K_4 = \Delta K_1$，并且 $K_1 \oplus K_3 = K_2 \oplus K_4 = \Delta K_2$。图 3 中 α、β、γ、δ、α'、β'、γ'、δ' 均代表差分，$\alpha \to \beta$ 和 $\alpha' \to \beta'$ 是 E_0 中 2 条概率为 1 的差分路径，$\delta \to \gamma$ 和 $\delta' \to \gamma'$ 是 E_1^{-1} 中 2 条概率为 1 的差分路径。在中间轮相遇时，β、β'、γ、γ' 满足 $\beta \oplus \beta' \oplus \gamma \oplus \gamma' \neq 0$。

4　TWINE-80 的相关密钥不可能飞来去器攻击

4.1　路径构造

根据 2.2 节 TWINE 算法的等价算法 TWINE*的描述，利用相关密钥不可能飞来去器的分析方法，构造出一个由 16 轮和 17 轮 2 条路径组成的相关密钥不可能飞来去器区分器。并将其向上扩展 4 轮，向下将 2 条差分路径分别扩展 3 轮和 2 轮，完成了对 23 轮 TWINE 算法的分析。除特别声明外，下文符号“*”表示非零差分，“？”表示不确定的差分。

通过对 TWINE 密钥编排算法的研究，发现对于每轮的密钥更新算法，有 2 个半字节的主密钥会进入 S 盒并参与异或运算，从而实现非零密钥差分的快速扩散。在相关密钥不可能飞来去器的构造中，选择区分器上半部分主密钥的特定半字节差分 $\Delta WK^i \neq 0$，其中 WK^i 在差分路径 $\alpha \to \beta$、$\alpha' \to \beta'$ 中不会进入 S 盒，这样可以使非零差分的扩散变慢，同时区分器的长度增加。经过分析对比，并同时考虑到密钥恢复算法的计算复杂度，本文在本次攻击中选取了主密钥差分 $\Delta WK = 00000000000000020000$，即 $\Delta WK^{15} = 2$，由此决定的轮密钥差分如表 7 所示。

表 7　　轮密钥差分

轮数	轮密钥差分	轮数	轮密钥差分
1	00000020	8	00020000
2	00000000	9	00000000
3	00000000	10	00000000
4	02000000	11	00002000
5	00000000	12	00000000
6	00000200	13	00000000
7	00000000	14	20000000

由主密钥差分可推知，第 6 轮、第 7 轮和第 8 轮的轮密钥差分分别为 00000200、00000000 和 00020000（如表 7 所示），若令第 5 轮的输入差分为（00000000，00000020），经过两轮加密之后，第 8 轮的输入差分为（00020000，00000000），易知这种构造可使得区分器的活跃 S 盒数目大大降低，从而可以获得更长轮数的路径。因此，选取第 5 轮的输入差分 α 和 α' 均为(00000000,00000020)。在区分器的下半部分，本文选择 2 条不同的差分路径，结合不可能差分分析的思想，经过大量分析对比后确定了输出差分：一条差分路径中，选取第 20 轮的输出差分 δ 为（00000200，00000000）；另一条差分路径中，选取第 21 轮的输出差分 δ' 为（20000000，00000000）。在此基础上根据相关密钥不可能差分飞来去器的分析方法构造了不可能差分路径，分别如图 4 和图 5 所示。

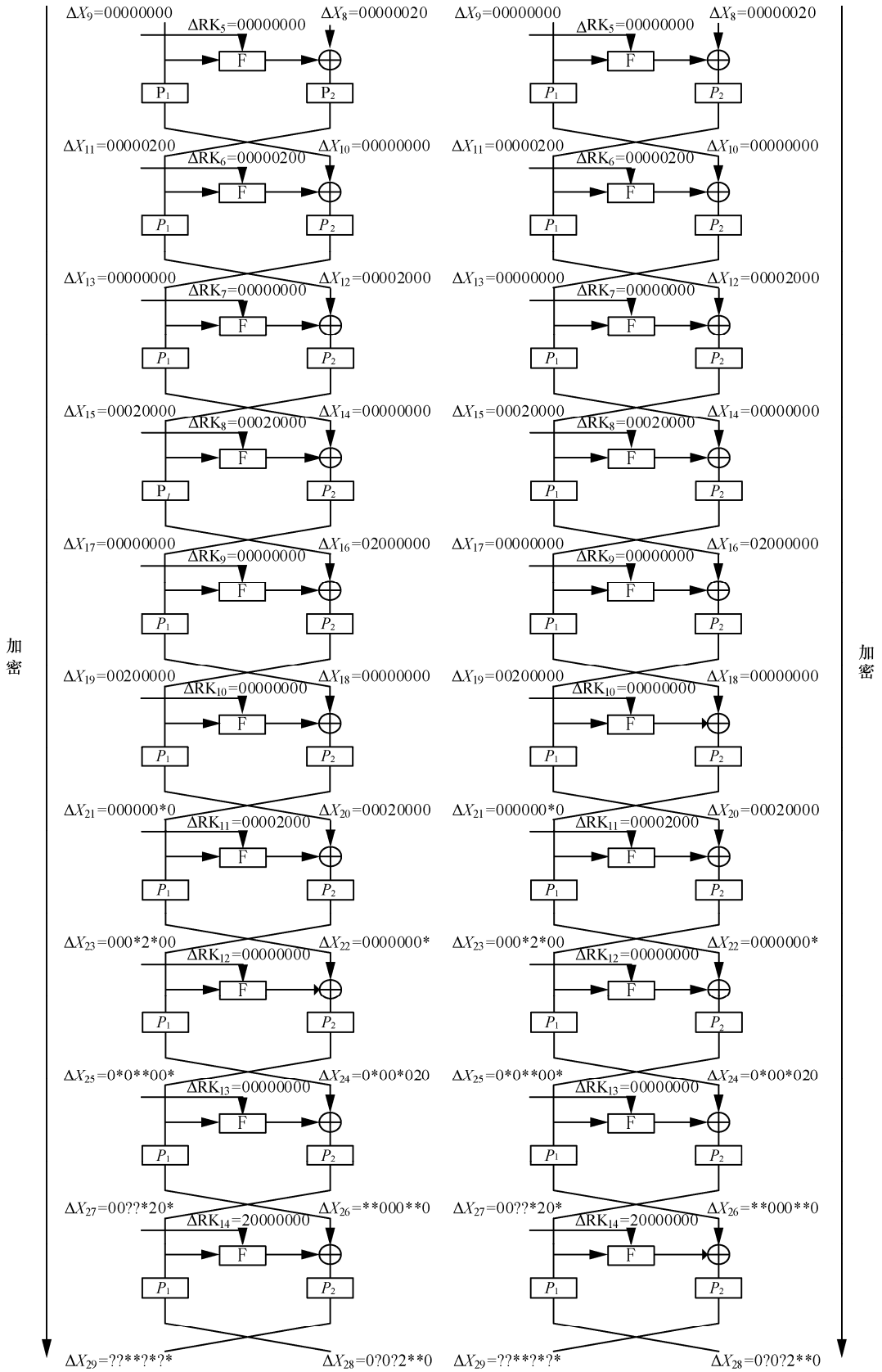

加密
ΔX9=00000000
ΔRK5=00000000
ΔX8=00000020
ΔX11=00000200
ΔRK6=00000200
ΔX10=00000000
ΔX13=00000000
ΔRK7=00000000
ΔX12=00002000
ΔX15=00020000
ΔRK8=00020000
ΔX14=00000000
ΔX17=00000000
ΔRK9=00000000
ΔX16=02000000
ΔX19=00200000
ΔRK10=00000000
ΔX18=00000000
ΔX21=000000*0
ΔRK11=00002000
ΔX20=00020000
ΔX23=000*2*00
ΔRK12=00000000
ΔX22=0000000*
ΔX25=0*0**00*
ΔRK13=00000000
ΔX24=0*00*020
ΔX27=00??*20*
ΔRK14=20000000
ΔX26=**000**0
ΔX29=??**?*?*
ΔX28=0?0?2**0
F
P1
P2
加密

图4　加密方向差分路径

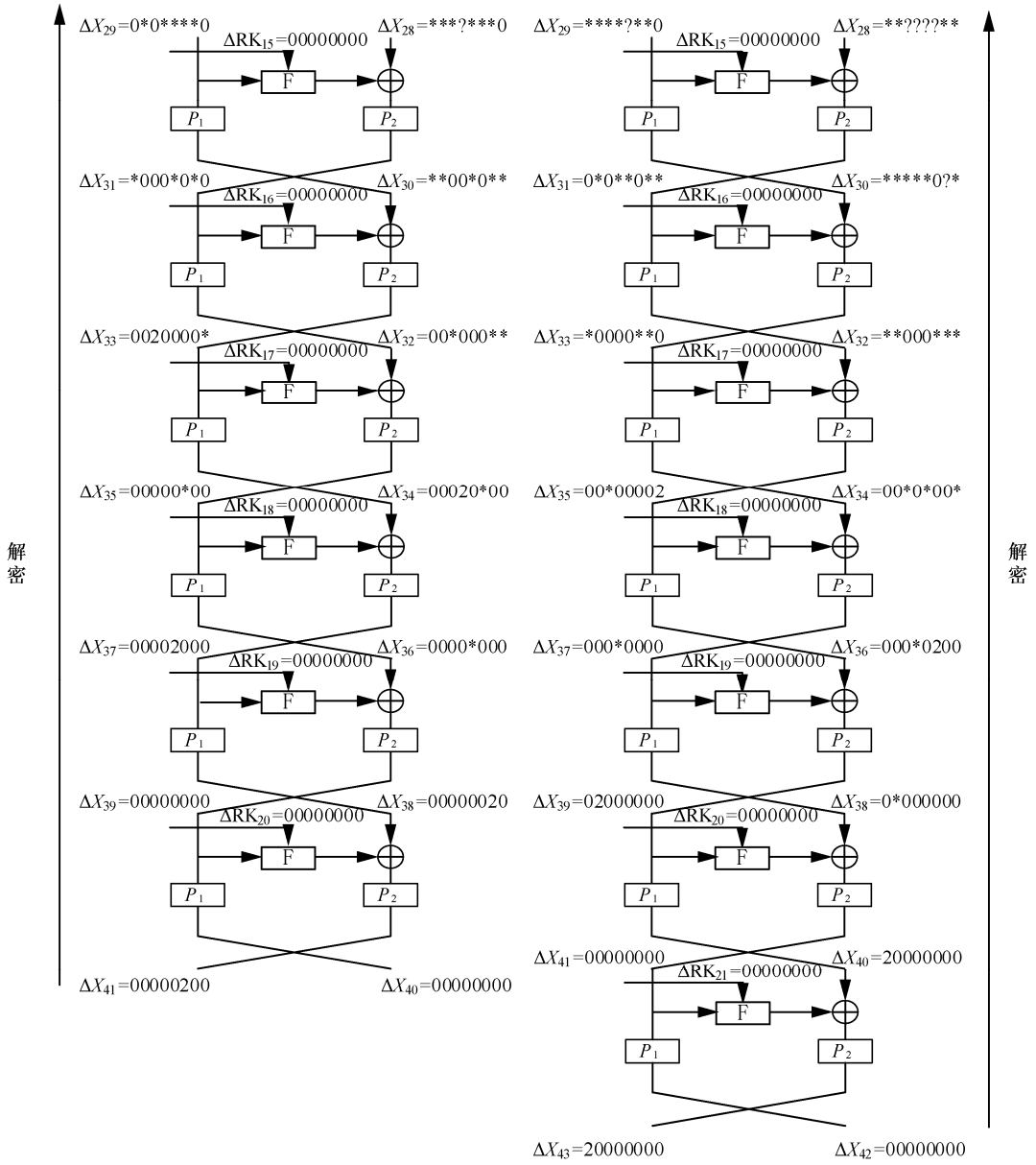


图 5　解密方向差分路径

令 E_0 表示 5~14 轮，E_1 表示 15~20（21）轮。区分器的密钥关系为 $K_1=K_3$，$K_2=K_4$，$K_1\oplus K_2=K_3\oplus K_4$=00000000000000020000。$E_0$ 的 2 条差分路径均为 (00000000,00000020) →(??**?*?*,0?0?2**0)，长度为 10 轮。E_1^{-1} 的一条差分路径为 (00000200,00000000) → (0*0****0,***?***0)，长度为 6 轮；另一条差分路径为：(20000000,00000000) →(**** ?**0,**?????*)，长度为 7 轮；2 条路径的密钥差分均为 0。E_0 的 2 条加密路径在第 15 轮的输入差分分别为 (??**?*?*,0?0?2**0),(??**?*?*,0?0?2**0)，E_1^{-1} 的 2 条解密路径在第 15 轮的输入差分分别为 (0*0****0,***?***0),(****?**0,**????**)，其中下划线标识的 4 个半做字节做异或运算一定不为 0，满足不可能差分的性质。

在路径的下半段，为使区分器中差分路径尽可能长，本文采用 2 条不同长度的差分路径（6 轮和 7 轮），这种设计不但不会影响不可能差分的性质，而且还会降低密钥恢复算法的计算复杂度。事实上，由图 3 可知，2 对向下加密的路径和 2 对向上解密的路径分别加密解密至某相同轮数，对应差分 γ、γ' 与 β、β' 只要满足 $\beta\oplus\beta'\oplus\gamma\oplus\gamma'\neq 0$ 就满足了不可能差分的要求，而本文设计的不同长度的

差分路径是满足该要求的；在此基础上，为完成对 23 轮 TWINE 算法的分析，只需要分别向下扩展 3 轮和 2 轮，故而密钥恢复算法的计算复杂度也因此有所降低。

4.2 扩展路径

Suzaki 等[7]提出 TWINE 算法时，对其 S 盒的差分特征给出了如下性质：满足 S 盒差分特征（$\alpha \to \beta$）的输入对的平均对数为 $\frac{16}{7}$，即给定密钥 RK 使 $\alpha \to \beta$ 成立的概率为 $\frac{1}{7}$。利用这个性质，在路径扩展时可以筛除掉多余的明密文对，使算法的计算复杂度大大降低。

本文对不可能差分路径向两端扩展，向上扩展 4 轮，如图 6 所示，其中，$\alpha_1 \in \Delta S(2)$，$\alpha_2 \in \Delta S(\alpha_1)$，$\alpha_3 \in \Delta S(\alpha_2), \alpha_4 \in \Delta S(\alpha_3), \alpha_4' \in \Delta S(\alpha_3 \oplus 2)$ ，$\alpha_2''' \in \Delta S(\alpha_1)$，$\alpha_1' \in \Delta S(2), \alpha_2' \in \Delta S(\alpha_1' \oplus 2)$，$\alpha_3' \in \Delta S(\alpha_2'), \alpha_2'' \in \Delta S(\alpha_1')$；向下分别扩展 2 轮和 3 轮，如图 7 所示，其中，$\gamma_1 \in \Delta S(2), \gamma_2 \in \Delta S(\gamma_1)$，$\gamma_3 \in \Delta S(\gamma_2), \gamma_1' \in \Delta S(2)$，$\beta_1 \in \Delta S(2), \beta_2 \in \Delta S(\beta_1)$。在此基础上最终完成对 TWINE 算法的 23 轮相关密钥不可能差分飞来去器攻击。符号 $\Delta S(\alpha)$ 表示 S 盒输入差分为 α 时，其输出差分所有可能取值的集合。

4.3 密钥恢复算法

根据图 6 和图 7 的扩展差分路径，本文对算法进行密钥恢复。具体的过程如下。

步骤 1 按照图 6 中明文差分的输入结构，选取 2^n 个明文结构，每个结构包含 2^{40} 个明文，它们可以构成 2^{n+79} 个明文对，记为 (P_1, P_2)，再选择 2^{n+79} 个这样的明文对 (P_3, P_4)，它们组成 2^{2n+158} 个四元组 (P_1, P_2, P_3, P_4)。

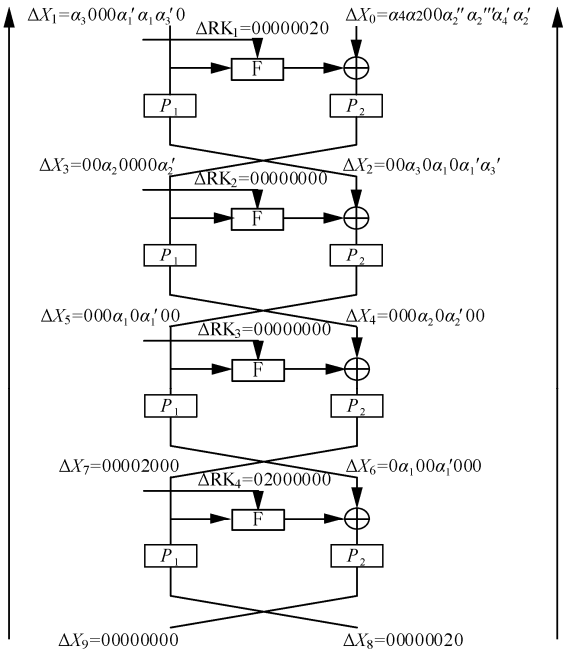


图 6 向上扩展的差分路径

步骤 2 将四元组中的 2 个明文对分别在密钥差分为 0000000000000020000 的密钥对下加密 23 轮，得到对应的密文四元组 (C_1, C_2, C_3, C_4)。按照图 7 中密文差分的结构，分别筛除密文差分不满足 $C_1 \oplus C_3 = (*000*0*0, 020*0000)$ 和 $C_2 \oplus C_4 = (*0000020, 00*00000)$ 的四元组。经过筛选后，剩余的四元组数为 $2^{158+2n} \times 2^{-104} = 2^{54+2n}$。利用 4.2 节

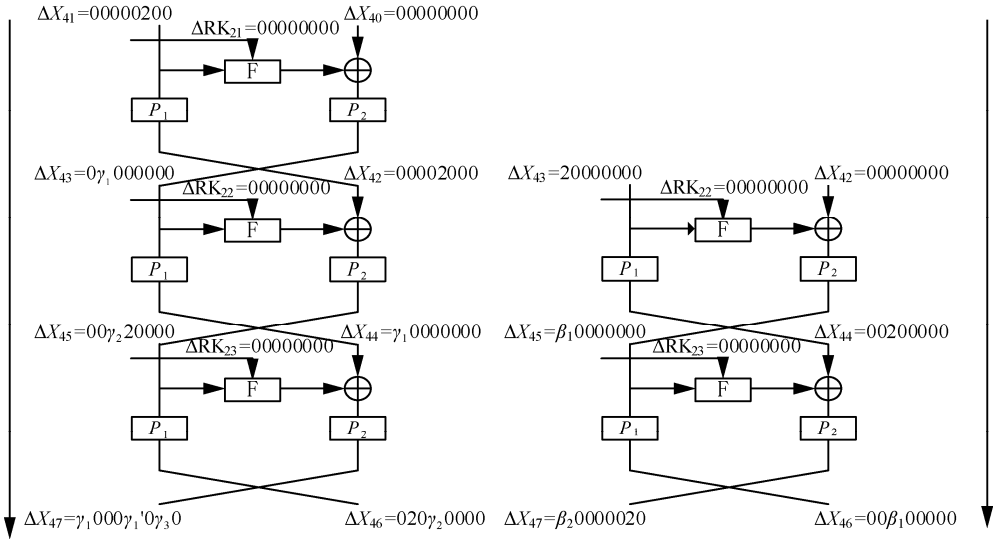


图 7 向下扩展的差分路径

中 S 盒的性质，可以对剩余四元组进行再次筛选。再次筛选后剩余四元组数为 $2^{54+2n}\times\left(\frac{7}{16}\right)^{20}\times\left(\frac{7}{16}\right)^{6}\approx 2^{54+2n}\times 2^{-31.01}=2^{2n+22.99}$。

步骤 3　猜测 RK_1^0、RK_1^4、RK_1^5、RK_1^6，对剩余四元组部分加密一轮，检查输出的四元组中左半部分的第 0、1、3、5 个半字节的差分是否为 0，若不为 0 则筛除相应的四元组。该步操作后剩余 $2^{2n+22.99}\times\left(\frac{1}{7}\right)^{2\times 4}=2^{2n+0.51}$ 个四元组。该步的计算复杂度为 $(2^{2n+22.99}\times 2^4+2^{2n+17.37}\times 2^8+2^{2n+11.75}\times 2^{12}+2^{2n+6.13}\times 2^{16})\times\frac{1}{8}\times\frac{1}{23}=2^{2n+20.01}$。

步骤 4　猜测 RK_{23}^2、RK_{23}^3，对剩余四元组的 (C_1,C_3) 部分解密一轮，检查 (C_1,C_3) 对应输出左半部分的第 2、3 个半字节的差分是否为 0，若不是则筛除相应的四元组。该步操作后剩余 $2^{2n-16.35}$ 个四元组。该步的计算复杂度为 $2^{2n+23.00}$。

步骤 5　猜测 RK_2^2、RK_2^7、RK_1^1、RK_1^7，对剩余四元组部分加密 2 轮，检查输出的四元组中左半部分的第 6、7 个半字节的差分是否为 0，若不为 0 则筛除相应的四元组。该步操作后剩余 $2^{2n-16.35}$ 个四元组。该步的计算复杂度为 $2^{2n+23.00}$。

步骤 6　猜测 RK_3^3、RK_3^5、RK_2^4、RK_2^6、RK_1^2、RK_1^3，对剩余四元组部分加密 3 轮，其中 $\mathrm{RK}_3^3=\mathrm{RK}_1^5$，$\mathrm{RK}_3^5=\mathrm{RK}_1^1$ 在步骤 3 和步骤 5 已猜测。检查输出的四元组中左半部分的第 1、4 个半字节的差分是否为 0，若不为 0 则筛除相应的四元组。该步操作后剩余 $2^{2n-27.59}$ 个四元组。该步的计算复杂度为 $2^{2n+28.33}$。

步骤 7　猜测 RK_4^1、RK_4^4、RK_3^3、RK_3^5、RK_1^1、RK_1^7，对剩余四元组部分加密 4 轮，其中 X_5^5、X_5^3 已经在步骤 6 中计算得到，$\mathrm{RK}_4^1=\mathrm{RK}_1^6\oplus C_3^H$、$\mathrm{RK}_4^4=\mathrm{RK}_1^3$、$\mathrm{RK}_3^3$、$\mathrm{RK}_1^1$、$\mathrm{RK}_3^5$、$\mathrm{RK}_1^7$ 在步骤 3、步骤 5 和步骤 6 已猜测，不需要再猜测。检查输出的四元组中左半部分的第 2、3 个半字节的差分是否为 0，若不为 0 则筛除相应的四元组。该步操作后剩余 $2^{2n-38.83}$ 个四元组。该步的计算复杂度为 $2^{2n+22.65}$。

步骤 8　猜测 RK_{22}^1、RK_{23}^0，对剩余四元组其中的 (C_1,C_3) 部分解密一轮，检查 (C_1,C_3) 对应输出左半部分的第一个半字节的差分是否为 0，若不为 0 则筛除相应的四元组。对剩余四元组其中的 (C_2,C_4) 部分解密一轮，检查 (C_2,C_4) 对应输出左半部分的第 0 个半字节的差分是否为 0，若不为 0 则筛除相应的四元组。该步操作后剩余 $2^{2n-44.45}$ 个四元组。该步的计算复杂度为 $2^{2n+18.74}$。

步骤 9　对 (C_1,C_3)，猜测 X_{41}^5，共有 16 种可能，对剩余四元组进行第 3 轮解密，利用 $F(\Delta X_{41}^5\oplus\Delta RK_{21}^5)\oplus\gamma_1=0$ 完成筛选，筛选后剩余四元组个数为 $2^{2n-44.45}\times 2^4\times\left(\frac{1}{7}\right)=2^{2n-43.26}$；对 (C_2,C_4)，猜测 X_{43}^0，共有 16 种可能，对剩余四元组进行第 2 轮解密，利用 $F(\Delta X_{43}^0\oplus\Delta RK_{22}^0)\oplus\beta_1=0$ 完成筛选，筛选后剩余四元组个数为 $2^{2n-43.26}\times 2^4\times\left(\frac{1}{7}\right)=2^{2n-42.07}$。该步的计算复杂度为 $2^{2n+12.02}+2^{2n+17.21}$。

若在步骤 1 中取 $n=21.05$，则步骤 9 中剩余四元组个数为 $2^{2n-42.07}=2^{0.03}>1$，恰好可以剔除错误密钥，恢复出正确的密钥。

综上，本次 23 轮 TWINE 的相关密钥不可能飞来去器攻击共可以恢复出 68 bit 密钥，需要的明文数为 $2^{n+40+1}=2^{62.05}$，计算复杂度为 $2^{2n+20.01}+2^{2n+14.69}+2^{2n+23.00}+2^{2n+28.33}+2^{2n+22.65}+2^{2n+18.74}+2^{2n+12.02}+2^{2n+17.21}=2^{2n+28.39}=2^{70.49}$。与 TWINE 算法已有分析结果相比，本文结果在数据复杂度和时间复杂度上都具有一定优势，说明相关密钥不可能飞来去器分析对 TWINE 算法具有较好的攻击效果。具体分析结果对比如表 8 所示。

表 8　**TWINE 的部分分析结果**

攻击方式	轮数	数据复杂度	时间复杂度	算法
饱和攻击	22	2^{62}	$2^{68.43}$	文献[7]
不可能差分	23	$2^{57.85}$	$2^{79.09}$	文献[8]
零相关线性	23	$2^{62.1}$	$2^{72.15}$	文献[9]
相关密钥不可能飞来去器	23	$2^{62.05}$	$2^{70.49}$	本文算法
Biclique attack	36	2^{60}	$2^{79.10}$	文献[10]
generalized MITM	36	2	$2^{78.74}$	文献[11]

5　结束语

本文利用 TWINE 密钥编排算法的弱点，采用了相关密钥、不可能差分和飞来去器三者结合的手段对其进行了攻击。充分利用了密钥差分对路径的影响，应用飞来去器的方法构造出一条尽可能长的差分分析路径，完成了对 23 轮 TWINE 的相关密钥

不可能差分飞来去器攻击。该攻击需要的数据复杂度为 $2^{62.05}$，时间复杂度为 $2^{70.49}$，与已有分析结果相比具有一定优势。这种将多种分析方法相结合的攻击充分利用了各种分析方法的优势，有利于达到更高轮数的攻击，对于其他分组密码算法的安全性分析也是一种新思路。

参考文献：

[1] HONG D, SUNG J, HONG S, et al. HIGHT: a new block cipher suitable for low-resource device[C] // International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2006: 46-59.

[2] BOGDANOV A, KNUDSEN L R, LEANDER G, et al. PRESENT: an ultra-lightweight block cipher[C]//International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2007:450-466.

[3] IZADI M, SADEGHIYAN B, SADEGHIAN S S, et al. MIBS: a new lightweight block cipher[C]//8th International Conference on Cryptology and Network Security. Springer, 2009: 334-348.

[4] WU W L, ZHANG L. LBlock: a lightweight block cipher[C]//9th International Conference on Applied Cryptography and Network Security. Springer, 2011: 327-344.

[5] BORGHOFF J,CANTEAUT A, GÜNEYSU T, et al. PRINCE – a low-latency block cipher for pervasive computing applications[C]// 18th International Conference on the Theory and Application of Cryptology and Information Security. Springer, 2012:208-225.

[6] SHIBUTANI K,ISODE T,HIWATARI H, et al. Piccolo: an ultra-lightweight blockcipher[C]//13th International Workshop on Cryptographic Hardware and Embedded Systems. Springer, 2011:342-357.

[7] SUZAKI T, MINEMATSU K, SORIOKA S, et al. TWINE: a lightweight block cipher for multiple platforms[C]// 19th International Conference on Selected Areas in Cryptography. Springer, 2012:339-354.

[8] ZHENG X X, JIA K T. Impossible differential attack on reduced-round TWINE[C]// 16th International Conference on Information Security and Cryptology. Springer, 2013: 123-143.

[9] WANG Y F,WU W L. Improved multidimensional zero-correlation linear cryptanalysis and applications to LBlock and TWINE[C]// 19th Australasian Conference on Information Security and Privacy. Springer, 2014: 1-16.

[10] COBAN M, KARAKOC F, ÖZKAN B, et al. Biclique cryptanalysis of TWINE[C]// 11th International Conference on Cryptology and Network Security. Springer, 2012: 43-55.

[11] MOHAMED T, YOUSSEF A. Generalized MitM attacks on full TWINE[J]. Information Processing Letters, 2016,116(2):128-135.

[12] WEI Y C, XU P,RONG Y S. Related-key impossible differential cryptanalysis on lightweight cipher TWINE[J]. Journal of Ambient Intelligence and Humanized Computing, 2019,10(2) :509-517.

[13] LU J Q. Cryptanalysis of block cipher[R]. London: University of London, 2016.

[14] 谢敏，牟彦利. LBlock 算法的相关密钥不可能飞来去器分析[J]. 通信学报, 2017, 38(5): 66-71.
XIE M, MU Y L. Related-key impossible boomerang cryptanalysis on LBlock[J]. Journal on Communications, 2017, 38(5): 66-71.

[15] BIHAM E. New types of cryptanalytic attacks using related key[J]. Journal of Cryptology, 1994, 7(4): 229-246.

[16] BIHAM E, BIRUUKOV A, SHAMIR A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials[C]// International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 1999: 12-23.

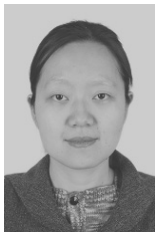
[17] WAGNER D. The boomerang attack[C]// 6th International Workshop on Fast Software Encryption. Springer, 1999: 156-170.

[18] 陈平, 廖福成, 卫宏儒. 对轻量级密码算法 MIBS 的相关密钥不可能差分攻击[J]. 通信学报, 2014, 35(2): 190-193.
CHEN P, LIAO F C, WEI H R. Related-key impossible differential attack on a lightweight block cipher[J]. Journal on Communications, 2014, 35(2): 190-193.

[19] MA X S, QIAO K X. Related-key rectangle attack on round-reduced Khudra block cipher[C]// The 9th International Conference on Network and System Security. Springer, 2015: 331-344.

[20] SASAKI Y. Related-key boomerang attacks on full ANU lightweight block cipher[C]// 16th International Conference on Applied Cryptography and Network Security. Springer, 2018: 421-439.

[作者简介]



谢敏（1976− ），女，湖南桃源人，博士，西安电子科技大学副教授，主要研究方向为编码与密码。

田峰（1995− ），男，河南安阳人，西安电子科技大学硕士生，主要研究方向为分组密码算法的分析。

李嘉琪（1993− ），男，陕西榆林人，西安电子科技大学硕士生，主要研究方向为分组密码算法的分析。