doi:10.11887/j.cn.201803024 http://journal.nudt.edu.cn

不可能差分分析时间复杂度通用计算公式的改进*

刘 亚[1,2,3],刁倩倩[1],李 玮[4],刘志强[3],曾志强[5]

(1. 上海理工大学 光电信息与计算机工程学院,上海 200093;
2. 上海理工大学 光学仪器与系统教育部工程研究中心 上海市现代化光学系统重点实验室,上海 200093;
3. 上海交通大学 计算机科学与工程系,上海 200240;4. 东华大学 计算机科学与技术学院,上海 201620;
5. 信息保障技术重点实验室,北京 100072)

摘 要:研究Boura等和Derbez分别提出的不可能差分分析时间复杂度计算公式,根据实际攻击过程优化密钥排除的步骤,给出不可能差分分析实际攻击的时间复杂度计算的改进公式,进而利用两个分组密码算法模型将改进后公式计算的实际结果分别与Boura等的公式和Derbez的公式的计算结果进行对比,结果表明Boura等的公式计算结果既可能高于优化公式的实际分析计算的结果,也可能低于优化公式的实际分析计算的结果,而在轮子密钥独立时改进后公式的实际计算结果是Derbez公式的计算结果的$2^{-1.2}$倍。

关键词:分组密码;不可能差分分析;不可能差分链;时间复杂度

中图分类号:TN918.1 **文献标志码**:A **文章编号**:1001-2486(2018)03-153-06

Improved generic formula of time complexity on impossible differential attacks

LIU Ya[1,2,3], *DIAO Qianqian*[1], *LI Wei*[4], *LIU Zhiqiang*[3], *ZENG Zhiqiang*[5]

(1. School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China;
2. Shanghai Key Lab of Modern Optical System, Engineering Research Center of Optical Instrument and System, Ministry of Education, University of Shanghai for Science and Technology, Shanghai 200093, China;
3. Department of Computer Science and Engineering, Shanghai Jiao Tong University, Shanghai 200240, China;
4. School of Computer Science and Technology, Donghua University, Shanghai 201602, China;
5. Science and Technology on Assurance Laboratory, Beijing 100072, China)

Abstract: The previous formulas of the time complexity of impossible differential cryptanalysis proposed by Boura et al. and Derbez were researched respectively. By studying the filtration of round subkeys during the attacking procedure carefully, an improved formula estimated the real time complexity of impossible differential cryptanalysis was proposed. On this basis, the impossible differential attacks were mounted on two models of block ciphers and the time complexities by three formulas were calculated. The results show that the time complexity computed by Boura's formula can be higher or lower than the real time complexity, and the real time complexity is $2^{-1.2}$ times as big as the time complexity calculated by Derbez's formula if the round subkeys are independent of each other.

Key words: block ciphers; impossible differential attacks; impossible differentials; time complexity

Knudsen和Biham等分别独立提出了差分分析[1]的一种扩展方法——不可能差分分析[2-3],其基本思想是构造一条概率为零的差分链作为区分器剔除所有错误的密钥,最后留下唯一的密钥即为正确密钥。此后,Lü等提出了提早排除法[4],有效地提高了不可能差分分析的效率。截至目前,不可能差分分析被用来分析许多著名分组密码算法的安全性,如:AES(advanced encryption standard)、Camellia、CLEFIA、LBlock等[5-13]。

不可能差分分析的攻击过程非常复杂,受到多种因素的影响和制约,譬如:区分器中非零比特的位置、相关密钥猜测的顺序等。因此,研究者一直希望给出一个通用的复杂度的计算公式来估计不可能差分分析的时间复杂度。2014年,Boura等[14]在亚洲密码学年会(亚密)上给出了不可能差分攻击复杂度计算一般公式,并将其运用到

* **收稿日期**:2017-04-10
基金项目:国家自然科学基金资助项目(61402288,61672347,61472250,61302161);上海市自然科学基金资助项目(15ZR1400300);信息保障技术重点实验室开放基金资助项目(KJ-17-008)
作者简介:刘亚(1983—),女,安徽当涂人,讲师,博士,硕士生导师,E-mail:liuya@usst.edu.cn

CLEFIA – 128、Camellia、Simon 和 LBlock 的分析中,得到了非常好的攻击结果。随后,Derbez[15] 对一种类 AES 算法进行不可能差分分析,结果表明 Boura 公式计算的时间复杂度远低于实际的时间复杂度。本文进一步深入研究不可能差分分析时间复杂度计算公式,发现 Derbez 提出的不可能差分分析时间复杂度计算公式可以进一步优化,并给出了优化后新的计算公式。

1 不可能差分分析

1.1 分析方法简介

不可能差分分析将分组密码算法 E 分为三个部分:$E = E_3 \circ E_2 \circ E_1$,如图 1 所示。

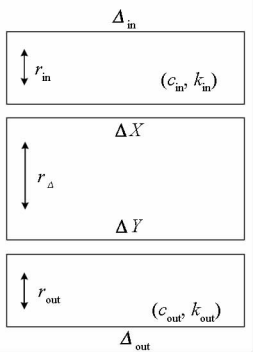

图 1 不可能差分攻击

Fig. 1 Impossible differential attacks

E_2 存在一条不可能差分链 $\Delta X \nrightarrow \Delta Y$,目前研究者已经给出了一系列不可能差分链搜索的算法[16-19]。E_1 和 E_3 分别是在不可能差分链前后两端连接 r_{in} 和 r_{out} 轮算法。ΔX 通过 E_1^{-1} 以概率为 1 扩展 r_{in} 轮得到明文输入差分(记为 Δ_{in}),ΔY 通过 E_3 以概率为 1 扩展 r_{out} 轮得到密文输出差分(记为 Δ_{out})。显然,差分特征 $\Delta_{in} \rightarrow \Delta X$ 应满足某一概率,记为 $2^{-c_{in}}$;同样地,差分特征 $\Delta Y \leftarrow \Delta_{out}$ 也满足某一概率,记为 $2^{-c_{out}}$。在不可能差分攻击实施中,需要猜测 E_1 和 E_3 部分相关的密钥,分别记为 k_{in} 和 k_{out},因此整个攻击中所需猜测的密钥为 $k_{in} \cup k_{out}$。利用提早排除法猜测候选密钥,来验证是否存在明密文对在某个猜测密钥加解密下得到了不可能差分链的输入差分 ΔX 和输出差分 ΔY。若存在,则此猜测密钥将被排除。

1.2 时间复杂度计算公式

Boura 等[14] 在 2014 年亚密上对不可能差分复杂度进行研究,提出了不可能差分分析复杂度计算的通用公式,表示如下:

1)数据复杂度:

$$C_N = \max\left\{\min_{\Delta \in \{\Delta_{in}, \Delta_{out}\}} \sqrt{N2^{n+1} - |\Delta|},\ N2^{n+1-|\Delta_{in}|-|\Delta_{out}|}\right\},$$

2)存储复杂度:N。

3)时间复杂度:

$$T_{com}^1 = C_N + (1 + 2^{|k_{in} \cup k_{out}| - c_{in} - c_{out}}) \cdot N \cdot C_{E'} + 2^{|K|} P \quad (1)$$

其中:n 为分组长度;N 是所需的明密文对数;$|K|$ 是恢复主密钥的长度;$C_{E'}$ 是每步攻击所需时间与整个加解密所需时间比,通常为攻击中活动 S 盒个数比整个 S 盒个数;P 为一个错误候选密钥被保留下来的概率,$P = (1 - 2^{-(c_{in}+c_{out})})^N \leqslant 2^{-|k_{in} \cup k_{out}|}$,若与穷搜时间复杂度折中,可保留一定数量错误密钥,此时 P 满足 $P \leqslant 2^{-1}$ 倍。

随后,Derbez[15] 给出了在不考虑穷搜和明密文对选取时间复杂度的情况下,将所有猜测密钥分为 $k_1, k_2, \cdots, k_b$,基于提前过滤技巧,其给出不可能差分分析的时间复杂度一般公式为:

$$T_{com}^2 = \sum_{1 \leqslant i \leqslant b} 2^{|k_1 \cup k_2 \cup \cdots \cup k_i| - \sum_{0 \leqslant j \leqslant i} r_j} \cdot N \cdot C_{E'} \quad (2)$$

式中,b 为猜测密钥的总步数,$r_j = \log_2 N_i$,N_i 为第 i 步猜测后明密文对被排除的数目。

Derbez 还构造了类 AES 算法模型解释这一结果。类 AES 算法如图 2 所示,记为 E^1,算法依次经过轮密钥加(Addtion Key, AK)、字节替换(S-Boxes, SB)、行移位(Shift Row, SR)、列混淆

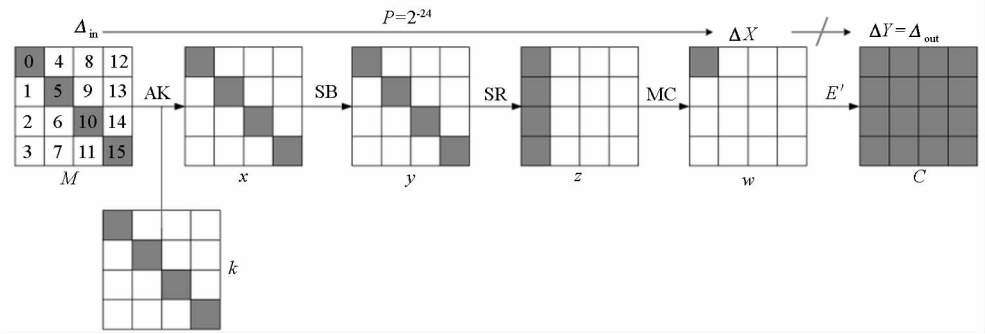

图 2 类 AES 模型

Fig. 2 AES-like model

(Mix Column, MC)运算,最后再接连一个密码分组长度为 128 bit 的密码算法 E',即 $E^1 = E' \circ MC \circ SR \circ SB \circ AK$,其中轮密钥加、字节替换、行移位、列混淆定义如 AES 算法,令 M, k, C 表示明文、轮密钥和密文,$x、y、z、w$ 分别表示 AK、SB、SR、MC 后的状态值,$\Delta x、\Delta y、\Delta z、\Delta w$ 分别表示 AK、SB、SR、MC 后的状态值的异或值。假设在 E'加密部分存在一条不可能差分链 $\Delta X \nrightarrow \Delta Y$,其中 ΔX 只有一个字节是非零差分,ΔY 中 16 个字节都为非零差分。在不可能差分链前端增加一轮,对分组密码算法模型 E^1 进行不可能差分分析,结果表明攻击的实际复杂度为 Boura 等提出通用公式所计算复杂度的 $2^{5.7}$倍。

2　时间复杂度通用计算公式的改进

2.1　Derbez 时间复杂度一般公式的改进

改进思路: Derbez 进行不可能差分分析时,最后一步为猜测密钥 k_b,并对所有剩余的明密文对加解密,最后排除错误的密钥。而事实上,通常最后一步是依次利用明密文对来验证猜测密钥是否是错误密钥,如果存在某个明密文对在密钥猜测下加解密得到不可能差分链,则此猜测密钥即为错误的,被排除,后续的明密文对不需要继续验证,这样可以在一定程度上降低攻击的复杂度。

此时,不可能差分分析的时间复杂度的一般公式计算如下:

设 $2^{-r_1}, 2^{-r_2}, \cdots, 2^{-r_b}$为每一步猜测密钥时明密文对被排除的概率。$S_{E'}$为每一步参与运算的 S 盒个数与整个 S 盒总数比。因为在类 AES 算法中,S 盒运算占主导地位,其他可以忽略,因此可用 $S_{E'}$近似表示 $C_{E'}$。在不考虑数据对选取和穷搜的时间复杂度的情况下,攻击的时间复杂度可以表示为:

$$\begin{aligned} T_{\text{com}}^3 &= \{2N \cdot \sum_{1 \leqslant i \leqslant b-1} 2^{|k_1 \cup \cdots \cup k_i| - \sum_{0 \leqslant j \leqslant i} r_j} + \\ &\quad 2^{|k_{\text{in}} \cup k_{\text{out}}|+1}[1 + (1-2^{-r_b}) + \cdots + \\ &\quad (1-2^{-r_b})^{N \cdot 2^{-r_1-\cdots-r_{b-1}}}]\} S_{E'} \\ &= \{2N \cdot \sum_{1 \leqslant i \leqslant b-1} 2^{|k_1 \cup \cdots \cup k_i| - \sum_{0 \leqslant j \leqslant i} r_j} + \\ &\quad 2^{|k_{\text{in}} \cup k_{\text{out}}|+1}\left[\frac{1-(1-2^{-r_b})^{N \cdot 2^{-r_1-\cdots-r_{b-1}}}}{1-(1-2^{-r_b})}\right]\} S_{E'} \end{aligned}$$

因为 $2^{-r_1-\cdots-r_b} = 2^{-(c_{\text{in}}+c_{\text{out}})}$,令 $P = (1-2^{-r_b})^{N \cdot 2^{-r_1-\cdots-r_{b-1}}} = (1-2^{-(c_{\text{in}}+c_{\text{out}})})^N \approx e^{-N \cdot 2^{-(c_{\text{in}}+c_{\text{out}})}}$,则时间复杂度可化简为:

$$\begin{aligned} T_{\text{com}}^3 &= [2N \cdot \sum_{1 \leqslant i \leqslant b-1} 2^{|k_1 \cup \cdots \cup k_i| - \sum_{0 \leqslant j \leqslant i} r_j} + \\ &\quad 2 \cdot 2^{|k_{\text{in}} \cup k_{\text{out}}|} \cdot 2^{r_b} \cdot (1-P)] \cdot S_{E'} \end{aligned} \quad (3)$$

为了方便计算,将错误密钥被保留下来的概率 P 进行约束,同时给出不可能差分分析过程中所需要的明密文对数(存储复杂度)的简化公式。与文献[15]一样,假定不考虑穷搜和数据对选取时的复杂度计算,所以在计算完所有明密文对后,可以确定唯一正确的密钥。假设令 $P = 2^{-2^m}(m \geqslant 0)$,因为 $2^{|k_{\text{in}} \cup k_{\text{out}}|}(1-2^{-r_b})^{N \cdot 2^{-r_1-\cdots-r_{b-1}}} = 2^{|k_{\text{in}} \cup k_{\text{out}}|} P \leqslant 1$,则 $P \leqslant 2^{-|k_{\text{in}} \cup k_{\text{out}}|}$,故 $m \geqslant \log_2 |k_{\text{in}} \cup k_{\text{out}}|$。又因为 $2^{-2^m} = e^{-2^m \cdot \ln 2}$,且 $P \approx e^{-N \cdot 2^{-(c_{\text{in}}+c_{\text{out}})}}$,所以 $N \cdot 2^{-(c_{\text{in}}+c_{\text{out}})} = 2^m \cdot \ln 2$。因此存储复杂度可以化简为:$N = 2^{c_{\text{in}}+c_{\text{out}}+m} \cdot \ln 2$。

2.2　类 AES 算法不可能差分分析的改进

文献[15]中类 AES 模型只涉及一轮密钥猜测,即 k_0, k_5, k_{10}, k_{15}。因为 $\Pr(\Delta_{\text{in}} \rightarrow \Delta X) = 2^{-24}$,即一个候选密钥被排除的概率为 2^{-24},则 $c_{\text{in}} + c_{\text{out}} = 24$,$N = 2^{c_{\text{in}}+c_{\text{out}}+m} \cdot \ln 2 = 2^{24+m} \cdot \ln 2$。此外,文献[15]在计算时间复杂度时,将一对明密文对的复杂度当作一个明文加密来计算,所以文献[15]所计算的复杂度应乘以 2。利用改进思路,接下来分类讨论时间复杂度。

1) k_0, k_5, k_{10}, k_{15} 相互独立,即 $|k_0 \cup k_5 \cup k_{10} \cup k_{15}| = 32$:

步骤 1:猜测 k_0。对所有明密文对,计算 Δz_0。由于 $\Delta w_1 = \Delta w_2 = \Delta w_3 = 0$,根据 MC 定义,计算 $\Delta z_1、\Delta z_2、\Delta z_3$,即 $\Delta y_5、\Delta y_{10}、\Delta y_{15}$可知。又因为 S 盒具有如下特性:已知 S 盒的输出差分,其输入差分有 2^7 种可能性,故明密文对在 $x_5、x_{10}、x_{15}$处的差分平均分别有 2^7 种被留下,因此一个明密文对留下的概率为 2^{-3}。

步骤 2:猜测 k_5。对剩下的明密文对,计算 Δy_5。若加密某个明密文对得到的 Δy_5 的值等于步骤 1 中计算的 Δy_5,则此明密文对将被留下,故一个明密文对留下的概率为 2^{-7}。

步骤 3:猜测 k_{10}。此步与步骤 2 类似,对剩下的明密文对计算 Δy_{10},若与步骤 1 中所计算的 Δy_{10}相等,则此明密文对将被留下。此时,一个明密文对被留下的概率为 2^{-7}。

步骤 4:猜测 k_{15}。依次加密剩余的明密文,若对某个明密文对加密得到不可能差分链,则此 k_{15} 的猜测值与之前 $k_0、k_5、k_{10}$的猜测值一起被排除。接下来,重新猜测 k_{15},重复上述操作直到所有错误的密钥被排除。此时,猜测密钥被排除的概率为 2^{-7}。

因此攻击过程的时间复杂度为:

$$T^3_{\text{com}} = 2N(2^8 + 2^{8+8-3} + 2^{8+8+8-3-7})S_{E'} + 2 \cdot 2^{32} \cdot 2^7 \cdot (1-P)S_{E'} \approx 2^{39.6+m} \cdot \ln 2 \cdot S_{E'} + 2^{40}(1-P)S_{E'}$$

若按文献[15]的复杂度公式计算,则攻击过程的时间复杂度为:

$$T^2_{\text{com}} = N \cdot (2^8 + 2^{8+8-3} + 2^{8+8+8-3-7} + 2^{8+8+8+8-3-7-7})S_{E'} \approx 2^{39.8+m} \cdot \ln 2 \cdot S_{E'}$$

在此公式中,作者忽略了每次是一对明密文对进行计算,因此文献[15]中正确的时间复杂度应为 $T^2_{\text{com}} = 2^{40.8+m} \cdot \ln 2 \cdot S_{E'}$。其中 $m \geqslant \log_2 32 = 5$,故 $T^2_{\text{com}}/T^3_{\text{com}} \approx 2^{1.12}$。当 m 取值尽可能大时,T^3_{com} 中第二部分值可忽略不计,此时 $\max\{T^2_{\text{com}}/T^3_{\text{com}}\} \approx 2^{1.2}$,所以 Derbez 计算的复杂度是实际复杂度的 $2^{1.2}$ 倍。

2) k_0, k_5, k_{10}, k_{15} 具有某个线性关系,此时 $|k_0 \cup k_5 \cup k_{10} \cup k_{15}| = 2^{24}$。假设密钥猜测顺序为 $(k_0, k_5, k_{10}, k_{15})$,攻击过程的时间复杂度应该为:

$$T^3_{\text{com}} = 2N(2^8 + 2^{8+8-3} + 2^{8+8+8-3-7})S_{E'} + 2 \cdot 2^{24} \cdot 2^7 \cdot (1-P)S_{E'} \approx 2^{39.6+m} \cdot \ln 2 \cdot S_{E'} + 2^{32}S_{E'}$$

按照 Derbez 的复杂度公式,攻击过程的时间复杂度为:

$$T^2_{\text{com}} = 2N \cdot (2^8 + 2^{8+8-3} + 2^{8+8+8-3-7} + 2^{8+8+8-3-7-7})S_{E'} \approx 2^{39.6+m} \cdot \ln 2 \cdot S_{E'}$$

因为 $m \geqslant \log_2 24 = 4.6$,故 $T^2_{\text{com}}/T^3_{\text{com}} \approx 1$。此时作者计算的复杂度和实际复杂度相等。同样地,当 $|k_0 \cup k_5 \cup k_{10} \cup k_{15}| = 2^{16}$ 或者当 $|k_0 \cup k_5 \cup k_{10} \cup k_{15}| = 2^8$ 时,此时 $T^2_{\text{com}}/T^3_{\text{com}} \approx 1$。

将本文的公式的计算结果和文献[15]对比,见表1。根据结果发现,当密钥之间相互独立时,Derbez 所计算的复杂度 T^2_{com} 是真实时间复杂度 T^3_{com} 的 $2^{1.2}$ 倍。当密钥之间存在线性关系时,真实时间复杂度基本等于公式计算时间复杂度。

表1 模型 E^1 不可能差分时间复杂度对比

Tab. 1 Comparison of time complexity of impossible differential attacks on E^1

密钥关系	时间复杂度(参考文献)	$\frac{T^2_{\text{com}}}{T^3_{\text{com}}}$
$\lvert k_0 \cup \cdots \cup k_{15} \rvert = 32$	$\frac{2^{40.8+m} \cdot \ln 2 \cdot S_{E'}([15])}{(2^{39.6+m} \cdot \ln 2 + 2^{40}) \cdot S_{E'}}$ (本文)	$2^{1.2}$
$\lvert k_0 \cup \cdots \cup k_{15} \rvert = 2^{24}$	$\frac{2^{39.6+m} \cdot \ln 2 \cdot S_{E'}([15])}{(2^{39.6+m} \cdot \ln 2 + 2^{32}) \cdot S_{E'}}$ (本文)	1

2.3 类 AES 新 SPN 模型不可能差分分析

S 盒的大小直接影响着不可能差分分析效率,而4 bit 的 S 盒经常被用在轻量级分组密码构造中,因此本节构造了一种新的代换置换(Substitution Permutation Network, SPN)模型,其中 S 盒的大小为4 bit,记为 E^2,如图3所示,接下来将基于此模型研究不可能差分分析时间复杂度计算公式。

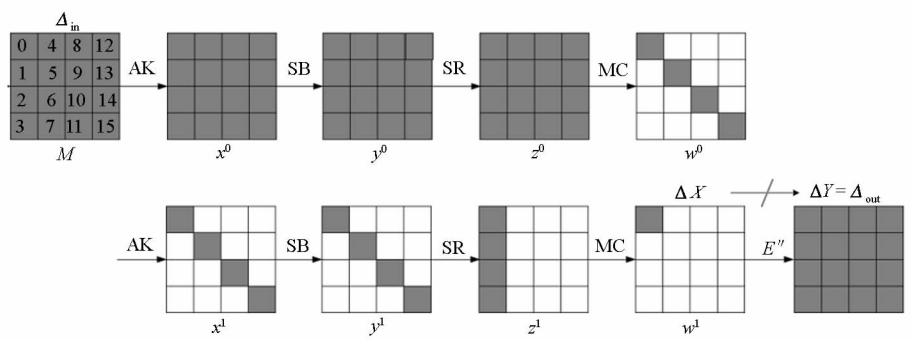

图3 SPN 模型

Fig. 3 SPN model

模型 E^2 加密过程和类 AES 模型类似,经过两轮轮密钥加、字节替换、行移位、列混淆运算,算法表示为 $E^2 = E'' \circ MC \circ SR \circ SB \circ AK \circ MC \circ SR \circ SB \circ AK$,其中 E''是密码分组长度为64 bit 的密码算法,字节替换运用 Midori[20] 的 4×4 的 S 盒,列混淆中使用有限域 $GF(2^4)$ 上的 MDS(maximum distance separable)矩阵,轮密钥加和行移位与类 AES 模型一致。假设在 E''部分存在不可能差分链 $\Delta X \nrightarrow \Delta Y$,其中 ΔX 只有一个块是非零差分,ΔY 所有块均为非零差分。在不可能差分链前端增加两轮,构成对模型 E^2 不可能差分分析。

分组长度为64 bit 的 E^2 模型不可能差分分

析包含两轮密钥猜测,即(k_0^0, k_1^0, …, k_{15}^0, k_0^1, k_5^1, k_{10}^1, k_{15}^1)。$\Pr(\Delta_{in}\rightarrow\Delta X)=2^{-3\times5\times4}$,即一个候选密钥被排除的概率为 2^{-60}。因此,$c_{in}+c_{out}=60$,$N=2^{c_{in}+c_{out}+m}\cdot\ln2=2^{60+m}\cdot\ln2$,$m\geqslant\log_2|k_{in}\cup k_{out}|$。接下来分类讨论时间复杂度。

1) k_0^0, k_1^0, …, k_{15}^0, k_0^1, k_5^1, k_{10}^1, k_{15}^1 相互独立,$|k_0^0\cup k_1^0\cup\cdots\cup k_{15}^1|=80$:

步骤 1:猜测 k_0^0。对所有明密文对,计算 Δz_0^0。由于 $\Delta w_1^0=\Delta w_2^0=\Delta w_3^0=0$,根据 MC 定义,计算 Δz_1^0、Δz_2^0、Δz_3^0,即得到 Δy_5^0、Δy_{10}^0、Δy_{15}^0。若 Midori 的 S 盒的输出差分固定,则其输入差分有 8 种可能。因此加密某一明密文对得到 Δx_5^0、Δx_{10}^0、Δx_{15}^0 均属于这 8 种情况,将被留下,否则被排除,此时一对明密文对被留下的概率为 $(8/16)^3$。接下来,依次猜测(k_5^0,k_{10}^0,k_{15}^0),部分加密剩余明密文对,将不符合不可能差分的明密文对排除,故明密文对被留下的概率为 2^{-3}。

步骤 2:与步骤 1 类似,依次猜测(k_4^0,k_9^0,k_{14}^0,k_3^0),(k_8^0,k_{13}^0,k_2^0,k_7^0),(k_{12}^0,k_1^0,k_6^0,k_{11}^0)。

步骤 3:猜测(k_0^1,k_5^1,k_{10}^1,k_{15}^1)。将符合不可能差分链的猜测密钥 k_{15}^1 以及之前猜测的密钥(k_0^0,k_1^0,…,k_{10}^1)一并排除,最后留下唯一正确的密钥。最后通过穷举搜索来恢复主密钥。时间复杂度计算见表 2。

表 2　模型 E^2 不可能差分分析时间复杂度计算

Tab. 2　Time complexity of impossible differential attacks on E^2

步骤	时间复杂度
1	$2N(2^4+2^{8-3}+2^{12-3-3}+2^{16-9})\approx2^{8.91}N$
2	$2N(2^{20-12}+2^{24-15}+2^{28-18}+2^{32-21}+2^{36-24}+2^{40-27}+2^{44-30}+2^{48-33}+2^{52-36}+2^{56-39}+2^{60-42}+2^{64-45})\approx(2^{12.91}+2^{16.91}+2^{20.91})N$
3	$2N(2^{68-48}+2^{72-51}+2^{76-54})+2\cdot2^{80}\cdot8(1-P)\approx2^{23.81}N+2^{84}(1-P)$

所以实际攻击过程的时间复杂度为:

$$T_{com}^3=[(2^{8.91}+2^{12.91}+2^{16.91}+2^{20.91}+2^{23.81})N+2^{84}(1-P)]S_{E'}\approx(2^{84+m}\cdot\ln2+2^{84})S_{E'}$$

按照 Derbez 的复杂度计算方法,攻击过程的时间复杂度为:

$$T_{com}^2=(2^{8.91}+2^{12.91}+2^{16.91}+2^{20.91}+2^{23.91})\cdot N\cdot S_{E'}\approx2^{85+m}\cdot\ln2\cdot S_{E'}$$

按照 Boura 等的通用计算公式,攻击过程的时间复杂度为:

$$T_{com}^1=(1+2^{|k_{in}\cup k_{out}|-(c_{in}+c_{out})})\cdot N\cdot C_{E'}=(2^{c_{in}+c_{out}}+2^{|k_{in}\cup k_{out}|})\cdot2^m\cdot\ln2\cdot20\cdot S_{E'}=(2^{60}+2^{80})\cdot2^m\cdot\ln2\cdot20\cdot S_{E'}=2^{m+84.32}\cdot\ln2\cdot S_{E'}$$

因为 $m\geqslant\log_280=6.32$。此时,$T_{com}^2/T_{com}^3\approx2$。所以,Derbez 计算的复杂度是实际复杂度的 2 倍。同时,将实际复杂度计算结果与 Boura 等的通用计算公式的结果对比后发现,Boura 等的通用公式所计算的复杂度要略高于实际时间复杂度,且不可能差分攻击的轮数越多,Boura 等提出的时间复杂度的计算结果高于实际时间复杂度也越多。

2) k_0^0, k_1^0, …, k_{10}^1, k_{15}^1 存在线性关系:不妨设密钥关系 $k_0^0=k_0^1$, $k_5^0=k_5^1$, $k_{10}^0=k_{10}^1$, $k_{15}^0=k_{15}^1$,则 $|k_0^0\cup\cdots\cup k_{15}^1|=64$,密钥恢复过程与 1) 相似,因为密钥之前的线性关系,第二轮的密码不需要猜测。所以实际攻击过程的时间复杂度为:

$$T_{com}^3=[(2^{8.91}+2^{12.91}+2^{16.91}+2^{20.91}+2^{17.2})\cdot N+2^{68}(1-P)]S_{E'}\approx(2^{81+m}\cdot\ln2+2^{68})S_{E'}$$

按照 Derbez 的复杂度计算方法,攻击过程的时间复杂度为:

$$T_{com}^2=(2^{8.91}+2^{12.91}+2^{16.91}+2^{20.91}+2^{17.2})\cdot N\cdot S_{E'}\approx2^{81+m}\cdot\ln2\cdot S_{E'}$$

用 Boura 等的复杂度通用公式,攻击过程的时间复杂度为:

$$T_{com}^1=(1+2^{|k_{in}\cup k_{out}|-(c_{in}+c_{out})})\cdot N\cdot C_{E'}=(2^{c_{in}+c_{out}}+2^{|k_{in}\cup k_{out}|})\cdot2^m\cdot\ln2\cdot20\cdot S_{E'}=(2^{60}+2^{64})\cdot2^m\cdot\ln2\cdot20\cdot S_{E'}=2^{m+68.42}\cdot\ln2\cdot S_{E'}$$

因为 $m\geqslant\log_264=6$,所以 $T_{com}^2/T_{com}^3\approx1$。此时,实际复杂度与 Derbez 计算的复杂度相近。同时,将实际复杂度计算结果与 Boura 等的时间复杂度通用公式的计算结果对比后发现 $T_{com}^1/T_{com}^3\approx2^{-12.58}$,即 Boura 等提出的时间复杂度通用公式计算的结果比实际复杂度要低。表 3 列出了本文的计算结果和文献[14]Boura、文献[15]Derbez 计算结果的对比情况。

表3 模型 E^2 不可能差分时间复杂度对比

Tab. 3 Comparison of time complexity of impossible differential attacks on E^2

密钥关系	时间复杂度(参考文献)	$\frac{T^1_{com}}{T^3_{com}}$	$\frac{T^2_{com}}{T^3_{com}}$
$\lvert k_0^0 \cup \cdots \cup k_{15}^1 \rvert = 80$	$2^{m+84.32} \cdot \ln 2 S_{E'}$ ([14]) $2^{85+m} \cdot \ln 2 \cdot S_{E'}$ ([15]) $(2^{84+m} \cdot \ln 2 + 2^{84}) \cdot S_{E'}$ (本文)	$2^{0.32}$	2
$\lvert k_0^0 \cup \cdots \cup k_{15}^1 \rvert = 64$	$2^{m+68.42} \cdot \ln 2 S_{E'}$ ([14]) $2^{81+m} \cdot \ln 2 \cdot {}_{E'}$ ([15]) $(2^{81+m} \cdot \ln 2 + 2^{68}) \cdot S_{E'}$ (本文)	$\frac{1}{2^{12.58}}$	1

3 结论

本文改进了文献[15]中 Derbez 提出的时间复杂度计算的通用公式,并给出了一个新的时间复杂度计算的通用公式。对两个类 AES 算法模型进行不可能差分分析,结果表明,在轮子密钥独立的情形下,利用改进的时间复杂度的公式得到的结果是 Derbez 公式计算结果的 $2^{-1.2}$ 倍,即实际的时间复杂度比 Derbez 预计的要低。而 Boura 等提出的时间复杂度公式计算结果不仅可能低于实际分析计算的结果,也可能高于实际分析计算的结果。

参考文献(References)

[1] Biham E, Shami A. Differential cryptanalysis of DES-like cryptosystems [J]. Journal of Cryptology, 1991, 4(1): 3 – 72.

[2] Knudsen L R. DEAL—a 128-bit block cipher: technical report 151[R]. Bergen, Norway: Department of Informatics, University of Bergen, 1998.

[3] Biham E, Biryukov A, Shamir A. Cryptanalysis of skipjack reduced to 31 rounds using impossible differentials [C]// Proceedings of Advances in Cryptology: EUROCRYPT'99, 1999: 12 – 23.

[4] Lü J Q, Kim J, Keller N, et al. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1[C] //Proceedings of the Cryptopgraphers' Track at the RSA Conference on Topics in Cryptology, 2008: 370 – 386.

[5] Phan R C W. Impossible differential cryptanalysis of 7-round advanced encryption standard (AES) [J]. Information Processing Letters, 2004, 91(1): 33 – 38.

[6] Liu Y, Gu D W, Liu Z Q, et al. Improved results on impossible differential cryptanalysis of reduced-round Camellia-192/256 [J]. Journal of Systems and Software, 2012, 85(11): 2451 – 2458.

[7] Liu Y, Li L B, Gu D W, et al. New observations on impossible differential cryptanalysis of reduced-round Camellia[C]// Proceedings of the 19th International Conference on Fast Software Encryption, 2012: 90 – 109.

[8] Liu Y, Yang A R, Liu Z Q, et al. Improved impossible differential attack on reduced version of Camellia with FL/FL – 1 functions [J]. IET Information Security, 2016, 10(6): 425 – 432.

[9] Wu W L, Zhang L, Zhang W T. Improved impossible differential cryptanalysis of reduced-round Camellia [C]// Proceedings of Selected Areas in Cryptography, 15th International Workshop, 2009: 442 – 456.

[10] Zhang W Y, Han J. Impossible differential analysis of reduced round CLEFIA [C]// Proceedings of Information Security and Cryptology, 4th International Conference, 2008: 181 – 191.

[11] Liu Y, Gu D W, Liu Z Q, et al. Impossible differential attacks on reduced-round LBlock [C]// Proceedings of International Conference on Information Security Practice and Experience, 2012: 97 – 108.

[12] 孙兵, 张鹏, 李超. Zodiac 算法的不可能差分和积分攻击[J]. 软件学报, 2011, 22(8): 1911 – 1917.
SUN Bing, ZHANG Peng, LI Chao. Impossible differential and integral cryptanalysis of Zodiac [J]. Journal of Software, 2011, 22(8): 1911 – 1917. (in Chinese)

[13] 李超, 魏悦川. Zodiac 算法新的不可能差分攻击 [J]. 国防科技大学学报, 2012, 34(5): 132 – 136.
LI Chao, WEI Yuechuan. New impossible differential cryptanalysis of Zodiac [J]. Journal of National University of Defense Technology, 2012, 34(5): 132 – 136. (in Chinese)

[14] Boura C, Naya-Plasencia M, Suder V. Scrutinizing and improving impossible differential attacks: applications to CLEFIA, Camellia, LBlock and SIMON [C]// Proceedings of Advances in Cryptology-ASIACRYPT, 2014: 179 – 199.

[15] Derbez P. Note on impossible differential attacks [C] // Proceedings of Fast Software Encryption, 2016: 416 – 427.

[16] Kim J, Hong S, Sung J, et al. Impossible differential cryptanalysis for block cipher structures[C]// Proceedings of International Conference on Cryptology in India, 2003: 82 – 96.

[17] Wei Y C, Li P, Sun B, et al. Impossible differential cryptanalysis on feistel ciphers with SP and SPS round functions [C]// Proceedings of Applied Cryptography and Network Security (ACNS), 2010: 105 – 122.

[18] Li R L, Sun B, Li C. Impossible differential cryptanalysis of SPN ciphers [J]. IET Information Security, 2011, 5(2): 111 – 120.

[19] Luo Y Y, Wu Z M, Lai X J, et al. A unified method for finding impossible differentials of block cipher structures [J]. Information Science, 2014, 263: 211 – 220.

[20] Banik S, Bogdanov A, Isobe T, et al. Midori: a block cipher for low energy[C]// Proceedings of Advances in Cryptology-ASIACRYPT, 2015: 411 – 436.