密码学报 ISSN 2095-7025 CN 10-1195/TN
Journal of Cryptologic Research, 2018, 5(4): 359–367

E-mail: jcr@cacrnet.org.cn
http://www.jcr.cacrnet.org.cn
Tel/Fax: +86-10-82789618

8 轮 Kiasu-BC 的多重不可能差分攻击*

蒋梓龙, 金晨辉

信息工程大学, 郑州 450002
通信作者: 蒋梓龙, E-mail: dracipher@126.com

摘 要: Jean 等人在 2014 年亚密会上提出可调密钥的算法框架, 并在 AES-128 基础上, 新增 64 比特调柄, 得到了新的可调分组密码——Kiasu-BC. 算法设计者声称 Kiasu-BC 相较于其它基于 AES 的可调分组密码而言, 算法结构更简洁、加密过程更高效, 并在 2014 年提交至 CAESAR 竞赛. 因此, 对可调分组密码的设计而言, 研究新增调柄的安全性, 具有极其重要的意义. 本文借鉴了调柄生成的非零差分会抵消攻击路径差分的思想, 提出了在单密钥模式下对 8 轮 Kiasu-BC 的多重不可能差分攻击. 利用构造的三条攻击路径, 可重复使用明文对轮密钥进行多次筛选, 从而提高轮密钥筛选效率. 此外, 我们综合运用了一系列技术如 "early abort" 技术、明文早夭技术、基于密钥扩展方案的轮密钥筛选技术等, 改进了 Kiasu-BC 算法不可能差分攻击的时间、数据和存储复杂度. 本文的时间、数据和存储复杂度分别为 $2^{115.5}$ 次 8 轮加密和 $2^{109.8}$ 次查表、2^{116} 选择明文和 $2^{97.6}$ 字节. 这是已知对 Kiasu-BC 最好的不可能差分攻击结果.

关键词: 多重不可能差分; 可调分组密码; Kiasu-BC; CAESAR 竞赛; 明文早夭技术

中图分类号: TP309.7 **文献标识码:** A DOI: 10.13868/j.cnki.jcr.000246

中文引用格式: 蒋梓龙, 金晨辉. 8 轮 Kiasu-BC 的多重不可能差分攻击[J]. 密码学报, 2018, 5(4): 359–367.

英文引用格式: JIANG Z L, JIN C H. Multiple impossible differentials cryptanalysis on 8-round Kiasu-BC[J]. Journal of Cryptologic Research, 2018, 5(4): 359–367.

Multiple Impossible Differentials Cryptanalysis on 8-round Kiasu-BC

JIANG Zi-Long, JIN Chen-Hui

Information Engineering University, Zhengzhou 450002, China
Corresponding author: JIANG Zi-Long, E-mail: dracipher@126.com

Abstract: At AsiaCrypt 2014, Jean et al. presented the TWEAKEY framework and a tweakable block cipher Kiasu-BC which was based on the AES-128 and added 64 bits tweak. The designers claimed that Kiasu-BC is more lightweight and faster than other tweakable block ciphers from AES, and submitted Kiasu-BC to CAESAR authenticated encryption competition in 2014. This shows that a cryptanalysis of the additional tweak is highly important for the design of tweakable block ciphers. This paper takes advantage of the idea that non-zero tweak difference may cancel the difference in the attack trails, and presents multiple impossible differentials cryptanalysis on 8-round Kiasu-BC in the single-key model. Utilizing constructed three attack trails, we can reuse the plaintexts and multiple sieve subkeys, so as to improve the efficiency of sieving subkey. Furthermore, we use a combination of various techniques, such as early abort technique, the new early abort technique, the master key

* 基金项目: 国家自然科学基金项目 (61772547, 61402523, 61272488)
Foundation: National Natural Science Foundation of China (61772547, 61402523, 61272488)
收稿日期: 2017-09-11 定稿日期: 2018-01-04

sieving technique based on key schedule algorithm, to improve the previous best impossible differential cryptanalysis on the time, data and memory complexities. The time, data, memory complexities are $2^{115.5}$ of 8-round Kiasu-BC encryptions and $2^{109.8}$ lookups, 2^{116} chosen plaintexts and $2^{97.6}$ bytes, respectively. This is so far the best result for impossible differential cryptanalysis of Kiasu-BC.

Key words: multiple impossible differentials cryptanalysis; tweakable block cipher; Kiasu-BC; CAESAR competition; new early abort technique

1 引言

分组密码算法是最受关注的密码算法之一, 是许多应用的安全基石, 常用于确保数据的保密性或真实性. 近几年, 可调分组密码的设计与分析受到了越来越多的关注. Schroeppel 等人 [1] 提出的算法 Hasty Pudding 已体现出可调分组密码的思想; 2002 年, Liskov 等人 [2] 正式提出了可调分组密码, 即允许使用者在明文和密钥之外, 额外多输入一个新的参数, 称之为调柄 (tweak), 调柄完全公开但是可以增加分组密码的随机性, 相较于更换密钥, 重新设置调柄更加经济方便.

在 2014 年亚密会上, Jean 等人 [3] 提出了可调密钥 (TWEAKEY) 的算法框架, 并基于 AES 算法轮函数, 给出了 3 个软件实现高效的可调分组密码算法, 分别是 Deoxys-BC, Joltik-BC, Kiasu-BC. 其中, Kiasu-BC 是基于 AES-128 的轮函数, 在轮密钥加变换之后的前两行模加 64 比特的调柄 T. 当 $T = 0$ 时, Kiasu-BC 就是 AES-128. 因此, Kiasu-BC 是一个简洁典型的可调分组密码, 且对 AES-128 的所有分析均可直接应用于 Kiasu-BC. 但是新增的调柄输入会给算法带来怎样的影响, 这是一个值得研究的问题.

不可能差分攻击 [4] 是传统差分攻击的拓展, 主要思想是构造一个或多个不可能差分区分器 (即概率为 0 的差分对应); 再利用区分器来实现对正确密钥的筛选. 不可能差分攻击过程具有极高的技巧性: Jiqiang Lu 等 [5] 提出密钥早幺技术, 通过分步攻击的方法, 有效降低时间复杂性; 张庆贵 [6] 基于快速排序技术, 提出了筛选明文对的改进算法, 可以减少筛选明文对过程中的时间复杂性; Li 等 [7,8] 提出了明文早夭技术, 使得在当前的轮密钥被判定为错误密钥时, 就停止遍历明密对, 而不必遍历所有的剩余明密对, 因此改进时间复杂度; Boura 等人 [9] 提出了状态检测技术, 可以改进筛选过程的复杂度. 因不可能差分攻击是一种强力有效的密码分析方法, 其被广泛应用于分组密码的分析中, 针对 AES 等 [10,11] 算法均得到了很好的分析结果.

算法设计者分析了 Kiasu-BC 的中间相遇攻击和在相关密钥、相关调柄模式下的差分攻击, 声称因保持了 AES-128 的轮函数和密钥扩展方案, 所以 Kiasu-BC 对抵抗各种分析方法的能力与 AES-128 相同. 然而, Dobraunig 等人 [12] 利用调柄生成的差分, 构造了 4 轮积分区分器, 得到了比 AES-128 复杂度更好的 7 轮积分攻击; 之后, Dobraunig 等人 [13] 利用调柄生成的差分与攻击路径的差分相抵消, 得到了 8 轮的不可能差分攻击和飞去来器攻击, 而对 AES-128 最好的分析结果只攻击到 7 轮. 这是已知对 Kiasu-BC 最好的不可能差分攻击结果.

Tsunoo 等人 [14] 提出了多重不可能差分攻击, 即构造多条不可能差分的攻击路径, 运用更多明文对去筛选轮密钥, 从而降低了对 CLEFIA 攻击的选择明文量和时间复杂度. 不同于之前的多重不可能差分, 本文提出的对 Kiasu-BC 的 8 轮多重不可能差分攻击, 先将有重合的密钥进行预处理, 计算出对应的明密对存储, 减少计算过程中的时间复杂性; 在筛选过程中, 固定位置相同的 8 字节公共轮密钥, 筛选剩余的 6 字节轮密钥, 之后运用密钥扩展方案再次对剩余轮密钥进行筛选, 提高密钥的筛选效率; 最后运用加密验证直至得到正确密钥. 结合密钥早夭技术 [5]、明文早夭技术 [7,8] 等, 改进了不可能差分攻击对 Kiasu-BC 的时间、数据和存储复杂度, 得到了已知对 Kiasu-BC 不可能差分攻击的最好结果. 本文攻击方案的复杂度结果与之前分析 Kiasu-BC 的结果比较如表1所示.

本文结构如下: 第2节给出了 Kiasu-BC 的算法描述和符号说明; 第 3 节构造了3个输入差分相同的不可能差分区分器; 第4节给出了具体攻击方案并计算了复杂度; 第5节总结全文.

表 1 Kiasu-BC 的分析的结果对比
Table 1 Summary of cryptanalysis on Kiasu-BC

分析方法	轮数	时间复杂度		数据复杂度	存储复杂度	参考文献
		加密轮数	查表次数			
积分攻击	7	2^{82}	-	2^{40}	2^{41}	[12]
积分攻击	7	$2^{48.5}$	-	$2^{43.6}$	$2^{41.7}$	[12]
矩阵攻击	7	2^{79}	2^{80}	2^{79}	2^{78}	[13]
飞去来器	7	2^{65}	$2^{66.6}$	2^{65}	2^{60}	[13]
飞去来器	8	$2^{103.1}$	2^{103}	$2^{103.1}$	2^{60}	[13]
不可能差分	8	2^{118}	$2^{120.2}$	2^{118}	2^{106}	[13]
不可能差分	8	$2^{115.5}$	$2^{109.8}$	2^{116}	$2^{97.6}$	本文

-: 未提及

2 Kiasu-BC 算法简介

Kiasu-BC 是可调分组密码算法, 分组长度是 128 比特, 可看作一个 16 字节的 4×4 矩阵, 每个字节都是有限域 GF(2^8) 上的值, Kiasu-BC 的轮函数由字节替换 SB、行移位 SR 、列混合 MC、轮密钥加 AK、调柄加 AT 这 5 种变换构成:

(1) 字节替换 SB: 由 16 个相同的可逆 S 盒并置而成, 对每个字节分别进行 S 盒变换.
(2) 行移位 SR: 对每一行进行循环左移, 第 i 行循环左移 i 字节 $(i = 0, 1, 2, 3)$.
(3) 列混合 MC : 在有限域 GF(2^8) 上, 根据相同的左乘矩阵, 对每列进行乘法运算.
(4) 轮密钥加 AK : 将中间状态与轮密钥按字节进行异或运算, 其中轮密钥由密钥扩展方案生成.
(5) 调柄加 AT : 将中间状态与调柄按字节进行异或运算, 其中调柄有 64 比特且每轮调柄值都相同.

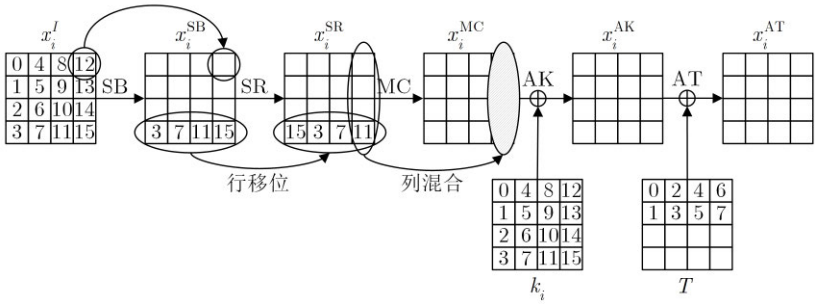

图 1 Kiasu-BC 的轮函数
Figure 1 Round function of Kiasu-BC

Kiasu-BC 算法最后一轮的列混合变换被省略且第一轮增加额外的轮密钥和调柄, 其轮密钥扩展方案与 AES-128 相同, 简述如下:

Kiasu-BC 需 11 个轮密钥, 每个轮密钥由 4 个字共 128 比特, 将所需的 44 个字定义为 $W[0, \cdots, 43]$, 前 4 个字直接取自初始密钥, 余下的轮密钥由以下公式生成:

$$W[i] = \begin{cases} W[i-4] \oplus W[i-1], & \text{if } i \bmod 4 \neq 0 \\ W[i-4] \oplus \mathrm{SB}(W[i-1] \lll 8) \oplus \mathrm{RCON}[\frac{i}{4}], & \text{if } i \bmod 4 = 0 \end{cases}$$

其中 SB 为字节替换变换, 对每个字中的 4 字节分别进行 S 盒变换; $\lll 8$ 表示循环左移 8 比特; RCON$[\frac{i}{4}]$ 是提前设置的轮常数.

下面给出本文符号说明:

P、C、T: 明文、密文、调柄.

$x^{I}_{i,(p,\cdots,r)}$、$x^{\mathrm{SB}}_{i,(p,\cdots,r)}$、$x^{\mathrm{SR}}_{i,(p,\cdots,r)}$、$x^{\mathrm{MC}}_{i,(p,\cdots,r)}$、$x^{\mathrm{AK}}_{i,(p,\cdots,r)}$、$x^{\mathrm{AT}}_{i,(p,\cdots,r)}$: 第 i 轮输入/字节替换/行移位/列混合/轮密钥加/调柄加变换后的第 $(p,\cdots,r)$ 字节的值.

$\mathrm{col}(j)$、$\mathrm{SR}[\mathrm{col}(j)]$: 状态中第 j 列的对应字节、状态中第 j 列经行移位变换后的对应字节.

Δx: x 的差分值.

$k_{i,(p,\cdots,r)}$: 第 i 轮密钥 k_i 的第 $(p,\cdots,r)$ 字节的值.

3 Kiasu-BC 的 4 轮不可能差分区分器

本文运用的区分器与文献 [13] 的区分器相同, 也考虑调柄引入的差分值, 文中引入的调柄在第零字节差分非零, 其余字节差分值为 0. 构造 3 个输入差均为 $x^{I}_{3,(0)}$, 但输出差不同的不可能差分区分器, 其中 3 个输出差分别在 $x^{\mathrm{SR}}_{6,(0,1,3)}$ 或 $x^{\mathrm{SR}}_{6,(0,2,3)}$ 或 $x^{\mathrm{SR}}_{6,(0,1,2)}$ 差分值非零, 其余字节差分值为 0. 三个区分器输出差的特点是: 仅在第 0 列有且只有三个字节差分非零, 其余字节差分值为 0.

如图2所示, 本文可将区分器分为两段: 按照加密方向, 保证第四轮输出差在第 1、2 和 3 列差分值非零; 按解密方向, 保证第五轮输入差在 $x^{I}_{5,\mathrm{SR}^{-1}[\mathrm{col}(2)]}$ 或 $x^{I}_{5,\mathrm{SR}^{-1}[\mathrm{col}(1)]}$ 或 $x^{I}_{5,\mathrm{SR}^{-1}[\mathrm{col}(3)]}$ 差分值为 0, 故在中间产生矛盾, 从而构成 4 轮不可能差分.

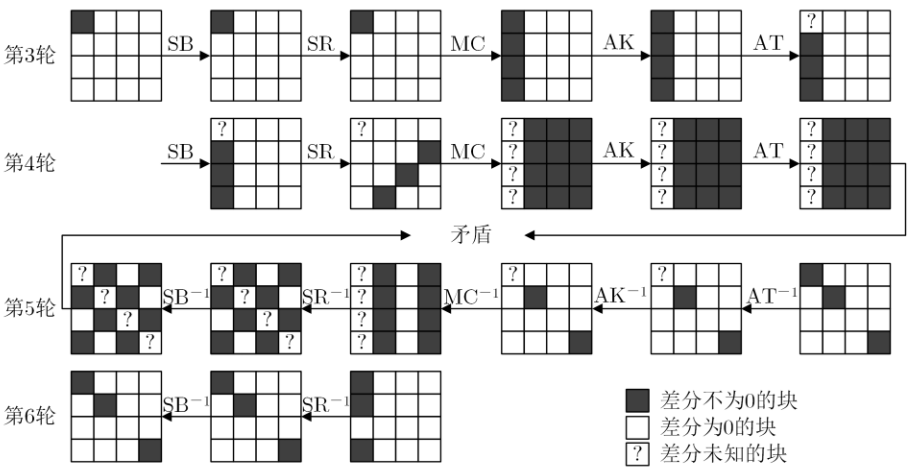

图 2 一个 4 轮的不可能差分区器样例

Figure 2 One sample of 4-round impossible differentials

4 8 轮 Kiasu-BC 的多重不可能差分攻击

根据第3节的不可能差分区分器, 利用调柄在第零字节差分非零的特点, 在攻击路径的第一轮中, 构造差分碰撞, 即调柄第零字节的非零差分可以抵消攻击路径中的差分 $x^{\mathrm{AK}}_{1,(0)}$, 从而能在区分器前扩展两轮; 再根据区分器的输出差分, 经第 6 轮列混合变换后, 分别在 $x^{\mathrm{SR}}_{6,(0,13)}$ 或 $x^{\mathrm{SR}}_{6,(0,10)}$ 或 $x^{\mathrm{SR}}_{6,(0,7)}$ 差分值非零, 其余字节差分值为 0. 然后以概率为 1 向后拓展两轮, 构造了三条攻击路径. 本文结合早夭技术 [5]、明文早夭技术 [7] 、基于密钥扩展方案的轮密钥筛选技术 [10]、基于快速排序方法的明文对筛选技术 [6] 等, 提出了对 Kiasu-BC 的多重不可能差分攻击.

如图3所示, 需攻击 14 字节的轮密钥 ($k_{0,(0,5,10,15)}$, $k'_{7,(0,13)}$, $k_{8,\mathrm{SR[col(0,3)]}}$), 其中第 6 轮和第 7 轮调整了密钥加变换与列混合变换的顺序, 分析得出的是等效密钥 (记作 k'). 其余的两个路径也需攻击 14 字节轮密钥, 具体的轮密钥字节分别为 ($k_{0,(0,5,10,15)}$, $k'_{7,(0,10)}$, $k_{8,\mathrm{SR[col(0,2)]}}$) 和 ($k_{0,(0,5,10,15)}$, $k'_{7,(0,7)}$, $k_{8,\mathrm{SR[col(0,1)]}}$). 可以看出, 在 3 条攻击路径中, 有 9 字节公共轮密钥 ($k_{0,(0,5,10,15)}$, $k'_{7,(0)}$, $k_{8,\mathrm{SR[col(0)]}}$), 其字节位置相同. 本文先固定 8 字节密钥 ($k_{0,(0,5,10,15)}$, $k_{8,\mathrm{SR[col(0)]}}$) 对其余 6 字节密钥进行筛选, 再利用轮密钥 $k'_{7,(0)}$ 进行对比验证, 这样不仅可以提高密钥筛选效率, 还可以降低了在线攻击阶段的时间复杂度. 同时结合一系列不可能差分技术, 本文得到了对 8 轮 Kiasu-BC 不可能差分攻击的最好结果.

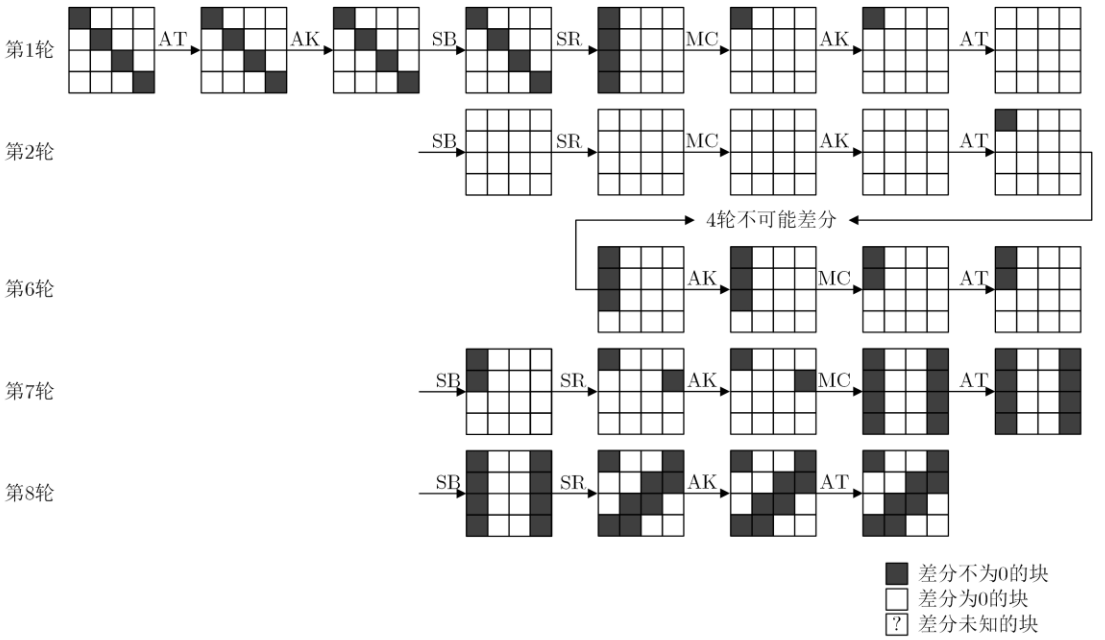

图 3 一个 Kiasu-BC 的不可能差分攻击路径
Figure 3 One of impossible differential attack trails on Kiasu-BC

4.1 攻击过程

本文攻击步骤包括数据处理阶段、预计算阶段和在线攻击阶段三个部分.

数据处理阶段 明文在 $(1,2,3,4,6,7,8,9,11,12,13,14)$ 这 12 字节位置上的取固定值, 在剩余的 4 字节位置上遍历所有的可能值, 同时在调柄的第零字节取所有值, 其余字节取固定值, 将这样的 2^{40} 个明文-调柄称之为一个结构. 得到 8 轮加密后对应的 2^{40} 个密文, 运用张庆贵提出的基于快速排序方法的明文对筛选技术 [6], 得到密文在 8 字节处 SR[col(1,2)] 差分值为 0 的密文对, 则有 $[2^{40}\times(2^8-1)^5/2]\times 2^{-64}\approx 2^{15}$ 个明密对符合结构要求. 本文选取 2^n 个明文结构, 则选择明文量为 2^{n+40}, 可以得到 2^{n+15} 个明文-调柄-密文对, 记作 $(P_iT_iC_i, P_jT_jC_j)$, 并将 $(0,5,10,15)$ 存储在表 Ω_1 中, 即只需存储差分非零的字节, 以调柄差分值为 0 的字节作为索引. 注意到选择的明文对在 4 字节和调柄对在第零字节应差分非零, 存在差分值为 0 的概率是 $(1-2^{-8})^5\approx 2^{-0.02}$, 对有效明密对的影响可忽略不计.

对另外两类攻击路径, 用类似的方法, 分别筛选得到在 8 字节位置上 SR[col(2,3)] 和 SR[col(1,3)] 差分值为 0 的密文对, 并将对应的 2^{n+15} 个明文-调柄-密文对分别存入表 Ω_2 和 Ω_3 中.

预计算阶段 S 盒的差分性质 [15]: 对 AES 的可逆 S 盒, 在给定非零输入差 Δ_{in} 和非零输出差 Δ_{out} 时, 方程 $S(x)\oplus S(x\oplus\Delta_{\mathrm{in}})=\Delta_{\mathrm{out}}$ 平均求得一个解, 构造表 H, 索引为 $(2^8-1)^2$ 个非零差分 $(\Delta_{\mathrm{in}},\Delta_{\mathrm{out}})$, 每个 $(\Delta_{\mathrm{in}},\Delta_{\mathrm{out}})$ 存储对应的输入值 x, 存储复杂度为 2^{16} 字节.

为降低筛选过程中的计算复杂度, 本文先将在三类攻击路径下, 经共同的 4 字节密钥 $k_{0,(0,5,10,15)}$ 筛选后符合要求的密文对提前预计算并存储, 具体过程如下.

求解 $k_{0,(0,5,10,15)}$: 对每个明文-调柄对 (P_iT_i, P_jT_j), 可得 1 个差分 $\Delta x^{\mathrm{AK}}_{0,(0,5,10,15)}$, 需构造调柄差分与第一轮路径差分碰撞, 故由当前的调柄对, 可得 1 个差分 $\Delta x^{\mathrm{MC}}_{1,(0)} = T_i[0] \oplus T_j[0]$, 由列混合、行移位逆变换可得 $\Delta x^{\mathrm{SB}}_{1,(0,5,10,15)}$, 由字节替换前后差分为索引查表 H, 可得 $x^{\mathrm{AK}}_{0,(0,5,10,15)}$, 与当前的明文和调柄模加后可得 $k_{0,(0,5,10,15)}$, 共可得 2^{n+15} 个 $k_{0,(0,5,10,15)}$, 以 $k_{0,(0,5,10,15)}$ 为索引将对应的密文-调柄对 $(C_{i,\mathrm{SR}[\mathrm{col}(0,3)]}T_i, C_{j,\mathrm{SR}[\mathrm{col}(0,3)]}T_j)$ 存入表 Ω_1, 平均每个 $k_{0,(0,5,10,15)}$ 有 2^{n-17} 个密文-调柄对.

对另外两类路径也做类似的预计算, 并对应更新表 Ω_2 和 Ω_3 的索引与存储内容.

在线攻击阶段 将在线攻击步骤归纳总结如下: 第 1、2 步采取早夭技术筛选符合攻击路径的密文对. 第 3 步利用明文早夭技术, 排除错误轮密钥. 第 4、5 步利用另外两条攻击路径, 再次筛选错误轮密钥, 并利用公共的 9 字节轮密钥提高筛选效率. 这里需指出本文的多重不可能差分攻击与文献 [14] 的不同之处: 本文先运用明文早夭技术, 对第 7 轮的两字节密钥进行筛选; 之后固定 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0)]})$, 对其余 6 字节密钥进行筛选. 这样对筛选掉的错误轮密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0)]})$ 就不用再次检验, 减少计算复杂性. 第 6 步利用主密钥恢复算法, 本文借鉴了文献 [10] 的思想并做出了改进, 在构造攻击路径时, 使三条路径都有相同字节位置的等效密钥 $k'_{7,(0)}$, 在恢复主密钥之前, 可以提前对比验证, 即判断 $k'_{7,(0)}$ 的值是否相同, 不同的则为错误密钥予以排除, 而不必像文献 [10] 对全部的剩余轮密钥都需要生成主密钥, 从而降低了计算过程的时间复杂性, 也可提高对错误轮密钥的筛选率; 最后对剩下的主密钥进行加密检验, 直至得到正确主密钥. 在线攻击的具体步骤如下:

1. 由 $k_{0,(0,5,10,15)}$ 的当前值, 攻击 $k_{8,\mathrm{SR}[\mathrm{col}(0)]}$.
   查表 Ω_1 可得 2^{n-17} 个 $(C_{i,\mathrm{SR}[\mathrm{col}(0,3)]}T_i, C_{j,\mathrm{SR}[\mathrm{col}(0,3)]}T_j)$, 对每个密文-调柄对穷举 2^8 个差分 $\Delta x^{\mathrm{AK}}_{7,(0)}$, 经列混合、调柄加变换后可得 2^8 个 $\Delta x^{\mathrm{AT}}_{7,\mathrm{col}(0)}$; 每个密文-调柄对可得 1 个 $\Delta x^{\mathrm{AT}}_{8,\mathrm{SR}[\mathrm{col}(0)]}$, 经调柄加、密钥加、行移位的逆变换后, 可得 1 个 $\Delta x^{\mathrm{SB}}_{8,\mathrm{col}(0)}$. 查表 H, 每个密文对可得 2^8 个 $x^{\mathrm{SB}}_{8,\mathrm{col}(0)}$, 经行移位变换、调柄模加、密文模加后可得 2^8 个 $k_{8,\mathrm{SR}[\mathrm{col}(0)]}$, 总共可得 2^{n-9} 个 $k_{8,\mathrm{SR}[\mathrm{col}(0)]}$, 以 $k_{8,\mathrm{SR}[\mathrm{col}(0)]}$ 为索引将 $(C_{i,\mathrm{SR}[\mathrm{col}(3)]}T_i, C_{j,\mathrm{SR}[\mathrm{col}(3)]}T_j)$ 和 $(x^{\mathrm{AK}}_{7,(0)}, x'^{\mathrm{AK}}_{7,(0)})$ 存入 $T^{(1)}$, 平均每个索引有 2^{n-41} 个密文-调柄对和 $(x^{\mathrm{AK}}_{7,(0)}, x'^{\mathrm{AK}}_{7,(0)})$.
2. 由当前的 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0)]})$, 攻击 $k_{8,\mathrm{SR}[\mathrm{col}(3)]}$.
   查表 $T^{(1)}$ 可得 2^{n-41} 个 $(C_{i,\mathrm{SR}[\mathrm{col}(3)]}T_i, C_{j,\mathrm{SR}[\mathrm{col}(3)]}T_j)$, 对每个密文-调柄对穷举 2^8 个差分 $\Delta x^{\mathrm{AK}}_{7,(13)}$, 经列混合、调柄加变换后可得 2^8 个 $\Delta x^{\mathrm{AT}}_{7,\mathrm{col}(3)}$; 每个密文-调柄对可得 1 个 $\Delta x^{\mathrm{AT}}_{8,\mathrm{SR}[\mathrm{col}(3)]}$, 经调柄加、密钥加、行移位的逆变换后, 可得 1 个 $\Delta x^{\mathrm{SB}}_{8,\mathrm{col}(3)}$. 查表 H, 每个密文对可得 2^8 个 $x^{\mathrm{SB}}_{8,\mathrm{col}(3)}$, 经行移位变换、调柄模加、密文模加后可得 2^8 个 $k_{8,\mathrm{SR}[\mathrm{col}(3)]}$, 总共可得 2^{n-33} 个 $k_{8,\mathrm{SR}[\mathrm{col}(3)]}$, 以 $k_{8,\mathrm{SR}[\mathrm{col}(3)]}$ 为索引将 $(x^{\mathrm{AK}}_{7,(0,13)}, x'^{\mathrm{AK}}_{7,(0,13)})$ 存入 $T^{(2)}$, 平均每个索引有 2^{n-65} 个 $(x^{\mathrm{AK}}_{7,(0,13)}, x'^{AK}_{7,(0,13)})$.
3. 由当前公共的 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0)]})$, 筛选 $(k'_{7,(0,13)}, k_{8,\mathrm{SR}[\mathrm{col}(3)]})$.
   运用明文早夭技术 [13], 构造表 S_1, 有 2^{16} 个地址且存放的内容为 1 或 0, 每个地址对应 2 字节密钥 $k'_{7,(0,13)}$ 具体值, 初始化表 S_1 内的所有值, 即对所有地址内容均设置为 0, 并设置计数器 F_1, 其初始值也为 0.
   穷举区分器的 3 种输出差分, 共有 $3 \times (2^8-1)^3 \approx 3 \times 2^{24}$ 种情况, 经列混合变换, 差分路径要求在 $\Delta x^{\mathrm{MC}}_{6,(0,1)}$ 两字节差分非零, 两字节差分值为 0, 故可得 3×2^8 个 $\Delta x^{\mathrm{MC}}_{6,(0,1)}$, 经调柄加变换后可得 3×2^8 个 $\Delta x^{\mathrm{AT}}_{6,(0,1)}$; 查表 $T^{(2)}$ 可得 $(x^{\mathrm{AK}}_{7,(0,13)}, x'^{\mathrm{AK}}_{7,(0,13)})$, 经行移位的逆变换可得 $\Delta x^{\mathrm{SB}}_{7,(0,1)}$, 查表 H 可得 $x^{\mathrm{SB}}_{7,(0,1)}$, 经行移位与 $x^{\mathrm{AK}}_{7,(0,13)}$ 模加后可得等效轮密钥 $k'_{7,(0,13)}$. 遍历表 $T^{(2)}$ 中的每个值, 对每个求解得到的等效密钥 $k'_{7,(0,13)}$, 查表 S_1 对应地址的值, 若为 0 则将其更新为 1, 并将计数器 F_1 的值增加 1. 若遍历完 $T^{(2)}$ 中的所有值后, 仍有 $F_1 < 2^{16}$, 则存储对应地址内容为零的轮密钥, 继续筛选密钥. 若 $F_1 = 2^{16}$, 则判定当前的 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0,3)]})$ 为错误密钥, 予以排除, 并固定当前 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0)]})$ 检查下一个轮密钥 $k_{8,\mathrm{SR}[\mathrm{col}(3)]}$, 在遍历完 6 字节密钥 $(k'_{7,(0,13)}, k_{8,\mathrm{SR}[\mathrm{col}(3)]})$ 后, 将通过检测的 6 字节密钥 $(k'_{7,(0,13)}, k_{8,\mathrm{SR}[\mathrm{col}(3)]})$ 存入表 M_1.
4. 由当前公共的 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR}[\mathrm{col}(0)]})$, 筛选 $(k'_{7,(0,10)}, k_{8,\mathrm{SR}[\mathrm{col}(2)]})$.
   (1) 由当前的 $k_{0,(0,5,10,15)}$ 查表 Ω_2, 可得对应的密文-调柄对, 类似第 1 步的筛选方式, 以

$k_{8,\mathrm{SR[col(0)]}}$ 为索引将 $(C_{i,\mathrm{SR[col(2)]}}T_i, C_{j,\mathrm{SR[col(2)]}}T_j)$ 存入 $T^{(3)}$, 平均每个索引有 2^{n-41} 个密文-调柄对和 $(x^{\mathrm{AK}}_{7,(0)}, x'^{\mathrm{AK}}_{7,(0)})$.

(2) 类似第 2 步求 $k_{8,\mathrm{SR[col(2)]}}$. 以 $k_{8,\mathrm{SR[col(2)]}}$ 为索引将 $(x^{\mathrm{AK}}_{7,(0,10)}, x'^{\mathrm{AK}}_{7,(0,10)})$ 存入 $T^{(4)}$, 平均每个索引有 2^{n-65} 个 $(x^{\mathrm{AK}}_{7,(0,10)}, x'^{\mathrm{AK}}_{7,(0,10)})$.

(3) 固定当前 8 字节密钥值 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$, 类似第 3 步, 运用明文早夭技术造表筛选 2 字节等效密钥 $x'^{\mathrm{AK}}_{7,(0,10)}$, 然后进一步筛选 6 字节密钥 $(x'^{\mathrm{AK}}_{7,(0,10)}, k_{8,\mathrm{SR[col(2)]}})$, 将通过检测的 6 字节密钥 $(k'_{7,(0,10)}, k_{8,\mathrm{SR[col(2)]}})$ 存入表 M_2.

5. 由当前公共的 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$, 筛选 $(k'_{7,(0,7)}, k_{8,\mathrm{SR[col(1)]}})$.
利用第三类路径筛选密钥, 其具体的筛选过程与第 4 步类似, 最后筛选 6 字节密钥 $(k'_{7,(0,7)}, k_{8,\mathrm{SR[col(1)]}})$, 将通过检测的 6 字节密钥 $(k'_{7,(0,7)}, k_{8,\mathrm{SR[col(1)]}})$ 存入表 M_3.

6. 由当前的 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$, 查表 M_1、M_2 和 M_3 可得 $(k'_{7,(0,7,10,13)}, k_{8,\mathrm{SR[col(1,2,3)]}})$.
注意到每个表中都有等效密钥字节 $k'_{7,(0)}$, 先判断三个表中 $k'_{7,(0)}$ 的值是否一致, 一致的轮密钥组合 $(k'_{7,(0,7,10,13)}, k_{8,\mathrm{SR[col(1,2,3)]}})$ 判定为候选密钥; 再根据得到的第 8 轮密钥 k_8, 运用密钥扩展方案得到等效密钥 $k'_{7,(0,5,10,15)}$ 和轮密钥 $k_{0,(0,5,10,15)}$, 与表中对应的轮密钥进行对比验证, 若不一致则判定当前密钥 $(k_{0,(0,5,10,15)}, k'_{7,(0,7,10,13)}, k_8)$ 错误并予以排除, 若一致则判定为候选密钥; 最后, 对所有剩余的候选密钥进行加密验证, 直至得到正确的主密钥. 具体过程如下:

(1) 每个表 $M_i(i=1,2,3)$ 均有等效密钥 $k'_{7,(0)}$, 若为正确密钥, 则 3 个表中的共同密钥字节值应相等, 挑选出 $k'_{7,(0)}$ 值相同的密钥组合 $(k'_{7,(0,7,10,13)}, k_{8,\mathrm{SR[col(1,2,3)]}})$, 因表 $M_i(i=1,2,3)$ 中的三个密钥 $k'_{7,(0)}$ 值相互独立且近似满足均匀分布, 可得通过率为 2^{-16}.

(2) 根据 AES-128 的密钥扩展方案, 由第 8 轮密钥 k_8 计算出 k_7, 其中等效密钥 $k'_{7,(0,7,10,13)}$ 可由第 7 轮密钥经列混合逆变换计算得出, 验证得到的等效密钥是否与表中的一致, 若不一致则判定当前密钥 $(k_{0,(0,5,10,15)}, k'_{7,(0,7,10,13)}, k_8)$ 错误并予以排除, 通过率为 2^{-32}. 若表 $M_i(i=1,2,3)$ 中的密钥均未通过检测, 则对应的所有轮密钥组合 $(k'_{7,(0,7,10,13)}, k_{8,\mathrm{SR[col(1,2,3)]}})$ 均是错误密钥, 故可判定当前密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$ 错误予以排除, 并检测下一个密钥; 否则进行下一步.

(3) AES-128 的密钥扩展方案, 由第 8 轮密钥 k_8 计算出 $k_{0,(0,5,10,15)}$, 若得到的值与当前值不一致, 则判定 $(k_{0,(0,5,10,15)}, k'_{7,(0,7,10,13)}, k_8)$ 为错误密钥并予以排除, 通过率为 2^{-32}. 若表 $M_i(i=1,2,3)$ 中的密钥均未通过检测, 则判定当前密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$ 错误并排除, 并检测下一个密钥; 否则运用 k_8 生成所有的轮密钥进行加密验证, 直至得到正确的主密钥.

4.2 复杂度分析

数据处理阶段: 需对 2^{n+40} 个密文进行查找与存储, 其时间复杂度为快速排序时间复杂度, 为 $2^n \times 2^{40}\log_2 2^{40} \approx 2^{n+45.3}$ 次查表, 由文献 [16] 可知一轮 AES 加密的时间复杂度约为 20 次查表, 且需对 3 类路径均进行处理, 则其时间复杂度约为 $3 \times 2^{n+45.3}/(20 \times 8) \approx 2^{n+39.5}$ 次 8 轮加密; 存储复杂度为 $3 \times 2^{n+15} \times 2 \times (4+1+8) \approx 2^{n+21.3}$ 字节.

预计算阶段: 构造表 H 的复杂度可以忽略不计, 构造表 $\Omega_i(i=1,2,3)$ 需 $3 \times 2^{n+15}$ 次查表, 存储复杂度为 $3 \times 2^{32} \times 2^{n-17} \times 2 \times (8+8) \approx 2^{n+21.6}$ 字节.

下面分析在线攻击阶段复杂度:

第 1 步的时间复杂度是 $2^{32} \times 2^{n-17} \times 2^8 = 2^{n+23}$ 次查表, 存储量是 $2^{32} \times 2^{n-41} \times 2 \times (4+8+1) \approx 2^{n-4.3}$ 字节.

第 2 步的时间复杂度是 $2^{64} \times 2^{n-41} \times 2^8 = 2^{n+31}$ 次查表, 存储量是 $2^{32} \times 2^{n-64} \times 2 \times 2 = 2^{n-30}$ 字节.

第 3 步运用明文早夭技术, 一个错误轮密钥通过 1 对明文检测的概率是 $1 - 3 \times 2^{-8} \approx 1 - 2^{-6.4}$, 2^{16} 个等效密钥 $k'_{7,(0,13)}$ 均不通过 $2^{6.4}$ 次独立检验的概率是 $[1-(1-2^{-6.4})^{2^{6.4}}]^{2^{16}} \approx e^{-2^{16-1.4425}}$; 则 2^{16} 个 $k'_{7,(0,13)}$ 能通过 $2^{6.4}d$ 个明文对检测但不能通过 $2^{6.4}(d+1)$ 个明文对检测的概率为 $p_d =$

$e^{-2^{16-1.4425(d+1)}} - e^{-2^{16-1.4425d}}$, 故 d 的数学期望为

$$E(d) = \sum_{d=1}^{\infty} dp_d = \sum_{d=1}^{\infty} d[e^{-2^{16-1.4425(d+1)}} - e^{-2^{16-1.4425d}}]$$
$$\approx \sum_{d=1}^{\infty} d(e^{-2^{16-1.4425\times(d+1)}} - e^{-2^{16-1.4425\times d}}) \approx 11.17 \approx 2^{3.5}$$

则第 3 步时间复杂度为 $2^{32} \times 2^{64} \times 2^{6.4+3.5} = 2^{105.9}$ 次查表. 而此时对错误轮密钥的通过率为 $P_1 = (1-2^{-6.4})^{2^{n-65}} \approx e^{-2^{n-71.4}}$, 故表 M_1 中存储了 $2^{48} \times P_1$ 个轮密钥 $(k'_{7,(0,13)}, k_{8,\mathrm{SR[col(3)]}})$. 若不采取明文早夭技术, 则需遍历所有剩余的明密对, 其时间复杂度为 $2^{32} \times 2^{64} \times 2^{n-65} \times 3 \times 2^8 = 2^{n+40.6}$ 次查表.

下面分析第 4 步: 4.1 步的复杂度与第 1 步相同; 在 4.2, 4.3 步的时间复杂度需考虑对共同 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$ 的通过率, 在第 3 步中若 6 字节密钥 $(k'_{7,(0,13)}, k_{8,\mathrm{SR[col(3)]}})$ 均是错误密钥, 则当前的 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$ 为错误密钥, 其通过率为 $P_2 = 1 - [1-(1-2^{-6.4})^{2^{n-65}}]^{2^{48}}$, 则 4.2 步时间复杂度为 $2^{n+31} \times P_2$, 4.3 步的时间复杂度为 $2^{105.9} \times P_2$.

第 5 步与第 4 步类似, 5.1 步的复杂度与第 1 步相同, 5.2, 5.3 步的时间复杂度分别为 $2^{n+31} \times {P_2}^2$、$2^{105.9} \times {P_2}^2$.

本文取 $n = 76$, 可得 $P_1 = 2^{-35}$, $P_2 \approx 1$. 故 4, 5 步对 8 字节共同密钥的筛选可忽略不计, $M_i(i = 1, 2, 3)$ 中的密钥个数为 $2^{48} \times 2^{-35} = 2^{13}$; 则在第 6 步的筛选过程中, 对当前共同的 8 字节密钥 $(k_{0,(0,5,10,15)}, k_{8,\mathrm{SR[col(0)]}})$, 可以得到 $(2^{13})^3 \approx 2^{39}$ 个 $(k'_{7,(0,5,10,15)}, k_{8,\mathrm{SR[col(1,2,3)]}})$, 因第 6 步先运用表中共有的等效密钥 $k'_{7,(0)}$ 进行对比筛选, 故时间复杂度为 $2^{64} \times 2^{39} = 2^{103}$ 次对比; 之后运用生成的轮密钥与当前表 $M_i(i = 1, 2, 3)$ 中的轮密钥对比筛选, 剩余 $2^{103} \times 2^{-16} \times 2^{-32} \times 2^{-32} = 2^{23}$ 个主密钥, 对其进行加密验证的复杂性, 相较于之前攻击的复杂性可忽略不计. 综上, 时间复杂性分为两部分: 数据处理阶段, 所需时间复杂度为 $2^{115.5}$ 次加密; 在线攻击阶段, 所需时间复杂为各步总和, 约为 $3 \times 2^{108.2} + 3 \times 2^{105.9} + 2^{103} \approx 2^{109.8}$ 次查表. 存储复杂度最大的在预计算阶段, 需存储 $2^{97.6}$ 字节. 选择明文量为 2^{116}.

5 总结

本文提出了对 Kiasu-BC 的 8 轮多重不可能差分攻击, 根据三条攻击路径有相同密钥字节的特点, 调整攻击方案, 在固定相同的密钥字节的情况下, 对轮密钥进行反复筛选, 从而可以提高轮密钥的筛选效率; 此外, 在攻击过程中结合一系列不可能差分攻击的技术, 如明文早夭技术等, 并改进了基于密钥扩展方案的轮密钥筛选技术, 从而进一步降低了复杂性, 得到了已知对 Kiasu-BC 不可能差分攻击的最好结果.

References

[1] SCHROEPPEL R, ORMAN H. The hasty pudding cipher[C]. AES candidate submitted to NIST, 1998: M1.

[2] LISKOV M, RIVEST R L, WAGNER D. Tweakable block ciphers[C]. In: Advances in Cryptology—CRYPTO 2002. Springer Berlin Heidelberg, 2002: 31–46. [DOI: 10.1007/3-540-45708-9_3]

[3] JEAN J, NIKOLIĆ I, PEYRIN T. Tweaks and keys for block ciphers: The TWEAKEY framework[C]. In: Advances in Cryptology—ASIACRYPT 2014. Springer Berlin Heidelberg, 2014: 274–288. [DOI: 10.1007/978-3-662-45608-8_15]

[4] BIHAM E, BIRYUKOV A, SHAMIR A. Cryptanalysis of Skipjack reduced to 31 rounds using impossible differentials[C]. In: Advances in Cryptology—EUROCRYPT 1999. Springer Berlin Heidelberg, 1999: 12–23. [DOI: 10.1007/3-540-48910-X_2]

[5] LU J, KIM J, KELLER N, et al. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1[C]. In: Topics in Cryptology—CT-RSA 2008. Springer Berlin Heidelberg, 2008: 370–386. [DOI: 10.1007/978-3-540-79263-5_24]

[6] ZHANG Q G. Plaintext pair sieve methods in impossible differential attack[J]. Computer Engineering, 2010, 36(2): 127–129. [DOI: 10.3969/j.issn.1000-3428.2010.02.045]

张庆贵. 不可能差分攻击中的明文对筛选方法 [J]. 计算机工程, 2010, 36(2): 127–129. [DOI: 10.3969/j.issn.1000-3428.2010.02.045]

[7] LI X R, FU F W, GUANG X. Multiple impossible differential cryptanalysis on reduced FOX[J]. IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2015, 98(3): 906–911. [DOI: 10.1587/transfun.E98.A.906]

[8] LI X R, JIN C H, FU F W. Improved results of impossible differential cryptanalysis on reduced FOX[J]. The Computer Journal, 2015, 59(4): 541–548. [DOI: 10.1093/comjnl/bxv073]

[9] BOURA C, NAYA-PLASENCIA M, SUDER V. Scrutinizing and improving impossible differential attacks: Applications to CLEFIA, Camellia, LBlock and Simon[C]. In: Advances in Cryptology—ASIACRYPT 2014, Part I. Springer Berlin Heidelberg, 2014: 179–199. [DOI:10.1007/978-3-662-45611-8_10]

[10] HU H J, JIN C H, LI X R. Improved impossible differential attack on 7-round AES-128. Journal of Cryptologic Research, 2015, 2(1): 92–100. [DOI: 10.13868/j.cnki.jcr.000063]
胡弘坚, 金晨辉, 李信然. 改进的 7 轮 AES-128 的不可能差分攻击 [J]. 密码学报, 2015, 2(1): 92–100. [DOI: 10.13868/j.cnki.jcr.000063]

[11] LIU Y, GU D, LIU Z, et al. New improved impossible differential attack on reduced-round AES-128[C]. In: Computer Science and Convergence. Springer Dordrecht, 2012: 453–461. [DOI:10.1007/978-94-007-2792-2_43]

[12] DOBRAUNIG C, EICHLSEDER M, MENDEL F. Square attack on 7-round Kiasu-BC[C]. In: Applied Cryptography and Network Security—ACNS 2016. Springer Cham, 2016: 500–517. [DOI:10.1007/978-3-319-39555-5_27]

[13] DOBRAUNIG C, LIST E. Impossible-differential and boomerang cryptanalysis of round-reduced KIASU-BC[C]. In: Topics in Cryptology—CT-RSA 2017. Springer Cham, 2017: 207–222. [DOI: 10.1007/978-3-319-52153-4_12]

[14] TSUNOO Y, TSUJIHARA E, SHIGERI M, et al. Cryptanalysis of CLEFIA using multiple impossible differentials[C]. In: 2008 International Symposium on Information Theory and Its Applications—ISITA 2008. IEEE, 2008: 1–6. [DOI: 10.1109/ISITA.2008.4895639]

[15] TOLBA M, ABDELKHALEK A, YOUSSEF A M. Impossible differential cryptanalysis of reduced-round skinny[C]. In: Progress in Cryptology—AFRICACRYPT 2017. Springer Cham, 2017: 117–134. [DOI: 10.1007/978-3-319-57339-7_7]

[16] LU J, DUNKELMAN O, KELLER N, et al. New impossible differential attacks on AES[C]. In: Progress in Cryptology—INDOCRYPT 2008. Springer Berlin Heidelberg, 2008: 279–293. [DOI: 10.1007/978-3-540-89754-5_22]

作者信息

蒋梓龙 (1992–), 江苏南通人, 在读硕士研究生. 主要研究领域为分组密码的设计与分析.
dracipher@126.com

金晨辉 (1965–), 河南扶沟人, 教授, 博士生导师. 主要研究领域为密码学和信息安全.
jinchenhui@126.com