

改进的 Camellia-256 高阶中间相遇攻击

张丽 卫宏儒

(北京科技大学数理学院 北京 100083)

摘要 Camellia 是一种具有 Feistel 结构的迭代型分组密码。Camellia 算法的分组长度为 128 比特,密钥长度为 128 比特、192 比特或 256 比特,其中密钥长度为 128 比特时迭代轮数为 18 轮,当密钥长度为 192 比特或 256 比特时,迭代轮数为 24 轮。目前,对 Camellia 算法的安全性分析一直是研究的热点。文中根据 Camellia 的密钥扩展算法和密钥相关性,分析了轮密钥之间的关系,并借助密钥桥找到了猜测密钥的 8 条关系。因此在对 16 轮 Camellia-256 进行高阶中间相遇攻击时,减少了在计算相关值时所需的子密钥数量,使得时间复杂度减少了 2^8 。这个结果比之前任何不带函数和白化层的 Camellia 密码分析的结果都要好。

关键词 Camellia 算法,高阶中间相遇攻击,密钥相关性,中间相遇攻击,密钥扩展算法

中图法分类号 TP309 文献标识码 A DOI 10.11896/j.sjkx.180901786

Improved Higher-order Meet-in-the-Middle Attack on Camellia-256

ZHANG Li WEI Hong-ru

(School of Mathematics and Physics, University of Science and Technology Beijing, Beijing 100083, China)

Abstract Camellia is an iterated block cipher with Feistel structure. The block length of Camellia is 128 bits, and the key length is 128 bits, 192 bits or 256 bits, which employs a total of 18 rounds for a 128-bit key and 24 rounds for a 192-bit or 256-bit key. At present, the security analysis of Camellia is a research hotspot. According to the key schedule and relation, this paper analyzed the relation between the round keys and found 8 relations of the guessing keys in total by means of the key-bridge technology. Therefore, when 16 rounds Camellia-256 against higher-order meet-in-the-middle attack, the number of subkeys required to compute the relevant values is reduced. The time complexity is reduced by 2^8 . This result is better than any previously published cryptanalytic results on Camellia without FL/FL^{-1} functions and whitening layers.

Keywords Camellia, Higher-order meet-in-the-middle attack, Key relation, Meet-in-the-middle attack, Key schedule

1 引言

Camellia^[1]是由 NTT 和 Mitsubishi 电子公司联合提交的一个分组密码,它最早公布于 2000 年的 SAC 会议上。Camellia 算法的分组长度为 128 比特,密钥长度为 128 比特、192 比特或 256 比特,128 比特密钥的 Camellia 使用 18 轮的 Feistel^[2]结构,192 比特和 256 比特的 Camellia 则使用 24 轮的 Feistel 结构,而且每 6 轮加入另外的输入/输出白化和逻辑函数 FL/FL^{-1} 。

近年来,国内外学者用各种方法对 Camellia 算法的安全性进行分析,包括差分密码分析、截断差分密码分析^[3]、高阶差分密码分析^[4]、不可能差分密码分析^[5-10]、线性密码分析、Square 攻击^[11-12]、碰撞攻击、相关密钥攻击、中间相遇攻击^[13-14]、高阶中间相遇攻击^[15]、代数攻击、零相关线性分析^[16]等,而且已经获得了许多研究成果。

中间相遇攻击是分析分组密码安全性的方法,高阶中间

相遇攻击是中间相遇攻击的扩展。高阶中间相遇攻击的核心思想是在构建“中间值”的基本单元时,使用多重明文来取消一些依赖于密钥的组件或参数。本文基于文献[15]中对 16 轮不带函数和白化层的 Camellia-256 的攻击,根据 Camellia 算法的密钥扩展算法及密钥搭桥技术^[17]对 Camellia-256 的高阶中间相遇攻击进行改进,找到了猜测密钥的相关关系,因此可以减少在计算相关值时所需的子密钥数量,从而减少时间复杂度。

本文第 2 节描述了符号和 Camellia 算法;第 3 节描述了高阶中间相遇攻击;第 4 节展示了 Camellia 密钥相关关系;第 5 节给出了 Camellia 的攻击结果和复杂度计算;最后总结全文。

2 Camellia 算法

2.1 符号说明

为了描述方便,首先定义下列符号和运算。

$P_L \parallel P_R$: 明文; $C_L \parallel C_R$: 密文; X_L^r : 第 r 轮输出的左边 64

到稿日期:2018-09-22 返修日期:2019-01-15 本文受国家自然科学基金(61672509, U1603116), 内蒙古自治区科技创新引导奖励资金项目资助。

张丽(1994—),女,硕士生,主要研究方向为密码学与信息安全,E-mail:ZhangLiAa@163.com;卫宏儒(1963—),男,副教授,硕士生导师,主要研究方向为数学、信息安全与密码学、物联网关键技术,E-mail:weihr@ustb.edu.cn(通信作者)。

比特; X_r^r : 第 r 轮输出的右边 64 比特; K_r : 第 r 轮子密钥; $K_r[m]$: 第 r 轮子密钥的第 m 比特; $X^{(r,i)}$: 第 r 轮输出的第 i 字节; K_r^i : 第 r 轮子密钥的第 i 字节; $X_{(n)}$: 下标表示 X 的比特长度为 n ; \oplus : 逐比特异或运算; \parallel : 操作数串接符号; $<\!\!<\!\!<\!\!n$: 操作数左移 n 比特; $>\!\!>\!\!n$: 操作数右移 n 比特。

2.2 Camellia 算法描述

Camellia 的分组长度为 128 比特, 密钥长度为 128 比特、192 比特或 256 比特。依据密钥长度的不同, 128 比特密钥的 Camellia 使用 18 轮的 Feistel 结构, 192 比特和 256 比特的 Camellia 则使用 24 轮的 Feistel 结构, 而且每 6 轮加了另外的输入/输出白化和逻辑函数 FL 和 FL^{-1} 。Camellia 的基本结构中的 F 函数如下所示:

$$F: L \times L \rightarrow L$$

$$(X_{(64)}, K_{(64)}) \mapsto Y_{(64)} = P(S(X_{(64)} \oplus K_{(64)}))$$

F 函数^[18]采用 SPN 结构, 是 Camellia 算法的核心函数, 在密钥扩展、加密和解密过程中均有使用。 F 函数由轮密钥加、非线性层 S 函数和线性层 P 函数构成。其中, S 函数由 4 个不同的 8 比特 S 盒 s_1, s_2, s_3, s_4 组成, 它们都仿射等价于有限域中的求逆函数。 s_1, s_2 和 s_4 可以由表(请参见文献[14])得到。 F 函数的具体描述如图 1 所示。

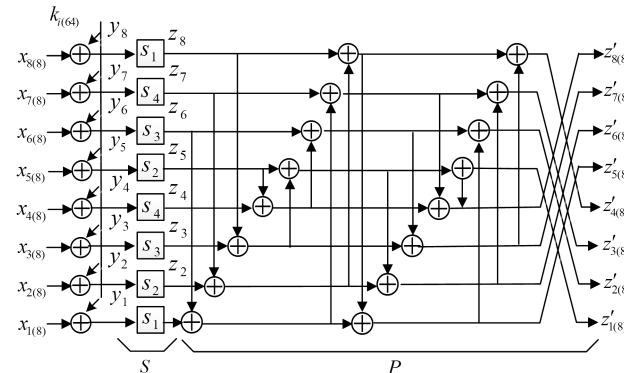


图 1 Camellia 的轮函数

Fig. 1 Round function of Camellia

P 函数记为 (z_0, \dots, z_7) 到 (z'_0, \dots, z'_7) 的映射, 具体如下所示:

$$\begin{aligned} z_0' &= z_0 \oplus z_2 \oplus z_3 \oplus z_5 \oplus z_6 \oplus z_7 \\ z_1' &= z_0 \oplus z_1 \oplus z_3 \oplus z_4 \oplus z_6 \oplus z_7 \\ z_2' &= z_0 \oplus z_1 \oplus z_2 \oplus z_4 \oplus z_5 \oplus z_7 \\ z_3' &= z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \\ z_4' &= z_0 \oplus z_1 \oplus z_5 \oplus z_6 \oplus z_7 \\ z_5' &= z_1 \oplus z_2 \oplus z_4 \oplus z_6 \oplus z_7 \\ z_6' &= z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_7 \\ z_7' &= z_0 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6 \end{aligned}$$

3 高阶中间相遇攻击

文献[15]提出了高阶中间相遇攻击, 它的基本思想是使用多重明文构建中间相遇攻击中的一个中间值, 即假设 $\{P_1, P_2, \dots, P_l\}$ 是一组选择明文集合, $\{C_1, C_2, \dots, C_l\}$ 是对应的密文集合, 加密过程 E 分解为 E_a 和 E_b 两部分, 两部分的密钥分别用 K_a 和 K_b 表示。给定子密钥 (K_a, K_b) 的猜测密钥值 (K_a^*, K_b^*) , 对于函数 $f: \{0,1\}^{n \times l} \rightarrow \{0,1\}^m$, 选择明文集和子密钥 K_a^* 进行加密运算得到 $f(E_{K_a^*}(P_1), E_{K_a^*}(P_2), \dots,$

$E_{K_a^*}(P_l))$, 将结果存储起来, 再将选择密文集用所猜测的密钥 K_b^* 进行解密, 得到 $f((E_{K_b^*}^b)^{-1}(C_1), (E_{K_b^*}^b)^{-1}(C_2), \dots, (E_{K_b^*}^b)^{-1}(C_l))$, 检验是否 $f(E_{K_a^*}(P_1), E_{K_a^*}(P_2), \dots, E_{K_a^*}(P_l)) = f((E_{K_b^*}^b)^{-1}(C_1), (E_{K_b^*}^b)^{-1}(C_2), \dots, (E_{K_b^*}^b)^{-1}(C_l))$ 。如果相等, 那么猜测密钥 (K_a^*, K_b^*) 可能是正确的; 否则, 这个猜测一定是不正确的, 将被淘汰。

文献[15]将 7 轮的高阶中间相遇攻击的性质用在 14 轮不带 FL/FL^{-1} 函数的 Camellia-192 的 5~11 轮上, 得到了较好的结果(具体分析见文献[15]); 之后将 8 轮的高阶中间相遇攻击的性质用于攻击 16 轮不带 FL/FL^{-1} 函数的 Camellia-256, 将其作用于 4~11 轮。攻击需要至多 2^{120} 选择明文, 总的时间复杂度为 2^{252} 。具体分析如下:首先, 猜测密钥可以表示为 $(K_1, K_{2,1}, K_{2,2}, K_{2,3}, K_{2,5}, K_{2,8}, K_{3,1}, \delta, K_{12,6}, K_{13,3}, K_{13,5}, K_{13,7}, K_{13,8}, K_{14}, K_{15}, K_{16})$, 其中添加了一个 8 比特的参数 δ , 定义如下: $\delta = \gamma_1 \oplus \gamma_2 \oplus \gamma_3 \oplus S_4(\gamma_4 \oplus K_{3,4}) \oplus S_6(\gamma_5 \oplus K_{3,6}) \oplus S_7(\gamma_6 \oplus K_{3,7})$, 其中 $\gamma_1, \gamma_2, \dots, \gamma_6$ 是 6 个随机选择的 8 比特常量值。以此对密钥恢复阶段的计算序列进行排序。28 个参数 $c_1', c_2', \dots, c_{28}'$ 的每一个可能的值按一定顺序存储在预算算表 $\psi_{c_1', c_2', \dots, c_{28}'}(0, z)$ 中, 其中 $z=1, 2, \dots, 63$ 。然后选择明文, 进行高阶中间相遇攻击, 如果得到的是正确密钥, 那么便可以继续进行密钥恢复工作。

4 Camellia 密钥相关性分析

4.1 Camellia 密钥扩展算法

密钥扩展算法通过种子密钥 K 生成用于输入/输出白化的 64 比特子密钥、轮函数的子密钥和函数的子密钥, 其中用 r 表示轮数。两个 128 比特的变量 K_L 和 K_R , 与 4 个 64 比特的变量 K_{LL}, K_{LR}, K_{RL} 和 K_{RR} 的定义如下:

$$K_{(128)} = K_{L(128)}, K_{R(128)} = 0$$

$$K_{(192)} = K_{L(128)} \parallel K_{RL(64)}, K_{RR(64)} = \overline{K_{RL(64)}}$$

$$K_{(256)} = K_{L(128)} \parallel K_{R(128)}$$

$$K_{L(128)} = K_{LL(64)} \parallel K_{LR(64)}$$

$$K_{R(128)} = K_{RL(64)} \parallel K_{RR(64)}$$

Camellia 的密钥扩展算法采用 Feistel 结构(见图 2)。

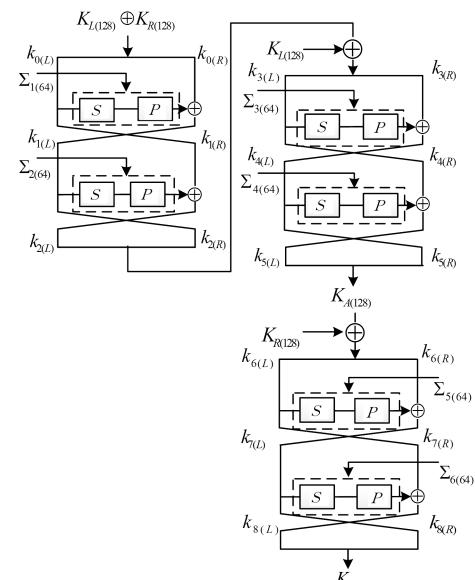


图 2 Camellia 的密钥扩展算法

Fig. 2 Key extending schedule of Camellia

第 $r+1$ 轮结构可按如下表达式给出:

$$K_L \oplus K_R = k_{0(L)} \parallel k_{0(R)}$$

$$k_{i+1(R)} = k_{i(L)}$$

$$k_{i+1(L)} = k_{i(R)} \oplus P(S(k_{i(L)}))$$

$$k_{3(L)} \parallel k_{3(R)} = k_{2(L)} \oplus K_{LL} \parallel k_{2(R)} \oplus K_{LR}$$

$$k_{6(L)} \parallel k_{6(R)} = k_{5(L)} \oplus K_{RL} \parallel k_{5(R)} \oplus K_{RR}$$

$$k_{6(L)} \parallel k_{6(R)} = K_B, i=0,1,3,4,6,7$$

需要注意的是: K_B 只用于密钥长度为 192 比特或 256 比特的情况。64 比特的常数 Σ_i ($i=1,2,\dots,6$) 在 Feistel 结构中被用作“密钥”。子密钥通过 K_L, K_R, K_A 和 K_B 的循环移位及它们的左半部分或右半部分生成。

4.2 符号描述

以下是本文定义的新符号: k_i^n : 第 i 轮的第 n 字节; SK : S 盒的输出; $S(K)[m]$: 输入 K 经过 S 盒的输出的第 m 比特; K_{0i0j0k} : 第 i 轮密钥的第 j 个字节的第 k 个比特; $K_{R000m0n}$: K_R 的第 m 个字节的第 n 个比特。

4.3 高阶中间相遇攻击中新的密钥关系

由 Camellia 密钥扩展算法和轮密钥的移位操作可知, 已知 $(K_1, K_{3,1}, K_{2,2}, K_{3,3}, K_{2,5}, K_{2,8}, K_{3,1})$, 则 $(K_{12,6}, K_{13,2}, K_{13,3}, K_{13,5}, K_{13,7}, K_{13,8}, K_{14}, K_{15}, K_{16})$ 仅有 128 比特的未知密钥, 这是因为它们之间存在着共同比特。根据 Camellia 密钥编排算法和密钥相关性, 找到了相较于公共比特更加复杂的比特关系, 共得到 8 条猜测密钥的相关关系, 大大减少了子密钥的计算量, 减少的时间复杂度为 2^8 。由 Camellia 的密钥扩展算法可知:

$$k_{8(R)} = k_{7(L)}$$

$$k_{5(L)} \oplus K_{R(L)} = k_{6(L)}$$

$$k_{6(L)} = k_{7(R)}$$

$$k_{7(R)} \oplus P(S(k_{7(L)})) = k_{8(L)}$$

整理可得:

$$k_{5(L)} \oplus K_{R(L)} \oplus P(S(k_{7(L)})) = k_{8(L)}$$

推导密钥相关关系可得下列 8 条密钥关系:

第 1 条密钥关系:

$$\begin{aligned} KR000304 &\Leftarrow K050304 \oplus K080304 \oplus SK070104 \oplus \\ SK070204 \oplus SK070304 \oplus SK070404 \oplus SK070504 \oplus \\ SK070604 \end{aligned}$$

其余 7 条密钥关系:

$$\begin{aligned} KR00030m &\Leftarrow K05030m \oplus K08030m \oplus SK07010m \oplus \\ SK07020m \oplus SK07030m \oplus SK07040m \oplus SK07050m \oplus \\ SK07060m (m=0,1,2,3) \end{aligned}$$

$$\begin{aligned} KR00020n &\Leftarrow K05020n \oplus K08020n \oplus SK07000n \oplus \\ SK07010n \oplus SK07020n \oplus SK07040n \oplus SK07050n \oplus \\ SK07070n (n=5,6,7) \end{aligned}$$

以第 1 条密钥关系为例, 进行模 2 加法运算、 S 盒变换和 P 置换得到 $KR000304$ 。若已知 S 盒的输入, 则可通过复杂的 S 盒和 P 置换求得相应的输出。

如图 3 所示, 在第 1 条猜测密钥关系中只需要 P 置换中的一条 $z'_3 = z_1 \oplus z_2 \oplus z_3 \oplus z_4 \oplus z_5 \oplus z_6$ 便可得到对应的输出。因此可求得第 1 条猜测密钥关系 $SK070104$,

$SK070204, SK070304, SK070404, SK070504, SK070604$ 。即将第 7 轮密钥的第 3 字节的第 4 比特输出记作: $SK070104 \oplus SK070204 \oplus SK070304 \oplus SK070404 \oplus SK070504 \oplus SK070604$ 。另外 7 条密钥关系同理可得。

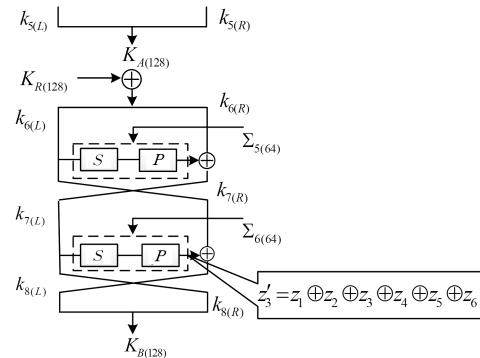


图 3 Camellia 的部分密钥扩展算法

Fig. 3 Partial key Schedule of Camellia

4.4 高阶中间相遇攻击中密钥关系的描述

根据 Camellia 轮密钥表可知 16 轮 Camellia-256 高阶中间相遇攻击中的猜测密钥对应表如表 1 所列。

表 1 Camellia-256 的轮密钥表

Table 1 Round keys of Camellia-256

密钥	值	密钥	值
$K_{1(64)}$	$(K_B \lll 0)_{L(64)}$	$K_{13(64)}$	$(K_R \lll 60)_{L(64)}$
$K_{2(64)}$	$(K_B \lll 0)_{R(64)}$	$K_{14(64)}$	$(K_R \lll 60)_{R(64)}$
$K_{3(64)}$	$(K_R \lll 15)_{L(64)}$	$K_{15(64)}$	$(K_B \lll 60)_{L(64)}$
$K_{12(64)}$	$(K_A \lll 45)_{R(64)}$	$K_{16(64)}$	$(K_B \lll 60)_{R(64)}$

将第 1 条密钥相关关系的推导转化为猜测密钥中的已知密钥可得表 2。

表 2 Camellia-256 的猜测密钥

Table 2 Guessing keys of Camellia-256

密钥标记	猜测密钥	密钥标记	猜测密钥
$KR000304$	$K_{14}[33]$	k_8^{11}	$K_{15}[29-36]$
$K050304$	$K_{12}[48]$	k_8^{12}	$K_2[33-40]$
$K080304$	$K_1[29]$	k_8^{13}	$K_{15}[45-52]$
	k_8^9	$K_2[9-16]$	k_8^{14}
	k_8^{10}	$K_2[17-24]$	$K_{15}[53-60]$

由此, 可得到猜测密钥关系为:

$$\begin{aligned} K_{14}[33] &\Leftarrow K_{12}[48] \oplus K_1[29] \oplus S(K_2[9 \sim 16])[4] \oplus \\ &S(K_2[17 \sim 24])[4] \oplus S(K_{15}[29 \sim 36])[4] \oplus \\ &S(K_2[33 \sim 40])[4] \oplus S(K_{15}[45 \sim 52])[4] \oplus \\ &S(K_{15}[53 \sim 60])[4] \end{aligned}$$

同理, 可得另外 7 组猜测密钥关系。

5 计算复杂度

对于 16 轮 Camellia-256 的高阶中间相遇攻击, 已有研究只分析了由密钥扩展算法和移位操作得到的猜测密钥的公共比特关系, 即给定猜测密钥 $(K_1, K_{2,1}, K_{2,2}, K_{2,3}, K_{2,5}, K_{2,8}, K_{3,1})$, 则可以得到 112 个公共比特, 那么 $(K_{12,6}, K_{13,2}, K_{13,3}, K_{13,5}, K_{13,7}, K_{13,8}, K_{14}, K_{15}, K_{16})$ 仅有 128 比特的未知密钥。所求总的时间复杂度为 2^{252} 。而本文分析了除公共比特外更复杂的密钥相关关系, 减少了时间复杂度。由密钥相关性可

知,根据猜测密钥 $K_1, K_{1,2}, K_{2,2}, K_{2,3}, K_{2,5}, K_{2,8}, K_{3,1}, K_{12,6}, K_{13,3}, K_{13,5}, K_{13,7}, K_{13,8}, K_{14}, K_{15}, K_{16}$ 得到 8 组相关关系。对于存储在预算表中的 $c'_1, c'_2, \dots, c'_{28}$ 来说,一次性的预算算表需要 $2^{28 \times 8} \times 63 \approx 2^{230}$ 字节的存储空间,时间复杂度为 $2^{224} \times 64 \times 5 \times 16^{-1} \approx 2^{228.4}$ 。在 16 轮 Camellia-256 的时间计算中, $\psi_{c'_1, c'_2, \dots, c'_{28}}$ 等于 5 个单轮 Camellia-256 加密,加上一个一次性计算。因此时间复杂度为:

$$2^{120+128-8} \times 64 \times \frac{8+8+8+5+1}{8 \times 16} \approx 2^{244}$$

由此可知,分析了 Camellia-256 的密钥扩展算法和密钥相关关系后的时间复杂度比之前的时间复杂度减少了 2^8 。

结束语 本文描述了高阶中间相遇攻击,并分析了新的密钥相关性,找到了除公共比特外更复杂的猜测密钥之间的相关关系,进而改进了对 16 轮的 Camellia-256 的高阶中间相遇攻击。新的密钥相关关系减少了攻击的时间复杂度,这是目前得到的最好结果。

参 考 文 献

- [1] AOKI K, ICHIKAWA T, KAND M, et al. Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms-Design and Analysis[C] // Selected Areas in Cryptography. Berlin: Springer, 2001:39-56.
- [2] KUWAKADO H, MORII M. Quantum distinguisher between the 3-round Feistel cipher and the random permutation[C] // Proceedings of IEEE International Symposium on Information Theory. New York: IEEE Press, 2010:2682-2685.
- [3] LEE S, HONG S H, LEE S, et al. Truncated differential cryptanalysis of Camellia[C] // Information Security and Cryptology. Berlin: Springer, 2002:32-38.
- [4] HATANO Y, SEKINE H, KANEKO T. Higher Order Differential Attack of Camellia(II)[C] // Selected Areas in Cryptography. Berlin: Springer, 2003:129-146.
- [5] CHEN J Z, JIA K T, YU H B, et al. New Impossible Differential Attacks of Reduced-Round Camellia-192 and Camellia-256[C] // Information Security and Privacy. Berlin: Springer, 2011:16-33.
- [6] MALA H, SHAKIBA M, DAKHILALIAN M, et al. New Results on Impossible Differential Cryptanalysis of Reduced-Round Camellia-128[C] // Selected Areas in Cryptography. Berlin: Springer, 2009:281-294.
- [7] LU J Q, WEI Y Z, KIM J, et al. The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher [J]. Theoretical Computer Science, 2014, 527(27):102-122.
- [8] LIU Y, LI L, GU D, et al. New Observations on Impossible Differential Cryptanalysis of Reduced-Round Camellia[C] // Fast Software Encryption. Berlin: Springer, 2012:90-109.
- [9] BAI D X, LI L B. New Impossible Differential Attacks on Camellia[C] // Information Security Practice and Experience. Berlin: Springer, 2012:80-96.
- [10] MALA H, DAKHILALIAN M, SHAKIBA M. Impossible differential cryptanalysis of reduced-round Camellia-256 [J]. IET-Information Security, 2011, 5(3):129-134.
- [11] LEI D, LI C, FENG K. Square Like Attack on Camellia[C] // Information and Communications Security. Berlin: Springer, 2007: 269-283.
- [12] LEI D, LI C, FENG K. New Observation on Camellia [C] // Selected Areas in Cryptography. Berlin: Springer, 2006:51-64.
- [13] LU J Q, WEI Y Z, PASALIC E, et al. Meet-in-the-Middle Attack on Reduced Versions of the the Camellia Block Cipher[C] // Advances in Information and Computer Security. Berlin: Springer, 2012:197-215.
- [14] CHEN J Z, LI L B. Low Data Complexity Attack on Reduced Camellia-256[C] // Information Security and Privacy. Berlin: Springer, 2012:101-114.
- [15] LU J Q, WEI Y Z, KIM J, et al. The Higher-Order Meet-in-the-Middle Attack and Its Application to the Camellia Block Cipher [J]. Theoretical Computer Science, 2014, 527(27):102-122.
- [16] BOGDANOV A, GENG H, WANG M, et al. Zero-Correlation Linear Cryptanalysis with FFT and Improved Attacks on ISO Standards Camellia and CLEFIA[C] // Selected Areas in Cryptography. Berlin: Springer, 2011:306-323.
- [17] LI L, WU W L, ZHENG Y F. Automatic Search for Key-Bridging Technique: Applications to LBlock and TWINE[C] // Fast Software Encryption. Berlin: Springer, 2016:247-267.
- [18] 吴文玲, 冯登国, 张文涛. 分组密码的设计与分析(第二版) [M]. 北京: 清华大学出版社, 2009:34-46.