中国科学: 信息科学 2017 年 第 47 卷 第 10 期: 1395–1410
SCIENTIA SINICA Informationis
论文

对轻量级分组密码 MIBS 和 I-PRESENT 的非对称 Biclique 攻击

崔杰, 左海风, 仲红*

安徽大学计算机科学与技术学院, 合肥 230039
* 通信作者. E-mail: zhongh@ahu.edu.cn

收稿日期: 2017–01–15; 接受日期: 2017–03–23; 网络出版日期: 2017–08–30
国家自然科学基金 (批准号: 61502008, 61572001) 和安徽省自然科学基金 (批准号: 1508085QF132) 资助项目

摘要 安全评估在确定密码的安全边界方面一直扮演着关键的角色, 其中 Biclique 分析就是一种寻找安全边界的方法. 本文结合非对称 Biclique 结构和 early abort 技术提出了一种新的 Biclique 攻击技术, 运用该技术对 MIBS-80 和 I-PRESENT-128 进行攻击, 并且给出其安全边界. 复杂度分析表明, 攻击 MIBS-80 所需要的计算复杂度和数据复杂度分别为 $2^{78.62}$ 和 2^{64}, 攻击 I-PRESENT-128 所需的计算复杂度和数据复杂度分别为 $2^{127.07}$ 和 2^{64}, 与已有攻击方案对比表明, 本文两种方案的计算复杂度均是最优的. 由于攻击方案的总复杂度主要取决于计算复杂度, 因此本方案具有一定的优势. 此外, 本文也是首次运用非对称 Biclique 方案对全轮 I-PRESENT-128 进行攻击.

关键词 轻量级分组密码, Biclique 攻击, MIBS, I-PRESENT, 部分匹配

1 引言

最近几年, 随着射频识别标签 (RFID tags)、物联网 (Internet of things) 和无线传感节点 (wireless sensor nodes) 等低资源设备的发展, 轻量级密码技术的研究逐渐成为一种热门研究领域, 在这个领域中去寻找那些满足不同低资源设备安全目的的解决方案就显得越来越重要. 到目前为止, 有很多的分组密码都满足低资源设备的要求, 比如 PRESENT [1], the KATAN and KTANTAN families [2], LBLO-CK [3], LED [4], PRINCE [5] 和 the Simon and the Speck families [6].

MIBS 是由 Izadi 等 [7] 在 CANS 2009 上提出的一个轻量级分组密码算法, 具有资源占用量较少的优点, 主要适用于 RFID (radio frequency identification)、无线传感技术等设备资源和计算能力有限的设备和环境中. 该算法整体采用 Feistel 结构, 分组长度为 64 bit, 密钥长度可以为 64 bit 和 80 bit, 分别记作 MIBS-64 和 MIBS-80, 都迭代 32 轮. 目前针对 MIBS 的分析有差分分析、线性分析、不可能差分分析、积分分析、中间相遇分析以及相关密钥条件下的不可能差分分析等.

引用格式: 崔杰, 左海风, 仲红. 对轻量级分组密码 MIBS 和 I-PRESENT 的非对称 Biclique 攻击. 中国科学: 信息科学, 2017, 47: 1395–1410, doi: 10.1360/N112017-00015
Cui J, Zuo H F, Zhong H. Asymmetric Biclique cryptanalysis of lightweight block ciphers MIBS and I-PRESENT (in Chinese). Sci Sin Inform, 2017, 47: 1395–1410, doi: 10.1360/N112017-00015

表 1　MIBS-80 攻击方法的比较

Table 1　A comparison of attacks on MIBS-80

Attack	Rounds	Data complexity	Computational complexity	Method
Impossible differential	14	2^{54}	2^{56}	[11]
Biclique	12	2^{52}	$2^{77.13}$	[12]
Biclique	32(full)	2^{52}	$2^{78.98}$	[13]
Biclique	32(full)	2^{64}	$2^{78.62}$	Ours

文献 [8] 改进了关于 14 轮 MIBS-64 的差分分析结果, 需要的时间复杂度为 $2^{37.2}$ 次加密, 数据复杂度为 2^{40} 个选择明文; 对 MIBS 算法的抗线性分析的能力进行了估计, 结果显示对 18 轮 MIBS-80 的线性分析大体需要 $2^{60.9}$ 个已知明文和 $2^{76.1}$ 次加密; 给出了 12 轮 MIBS-80 的不可能差分分析. 随后, 文献 [9,10] 分别给出了 10 轮 MIBS-80 积分分析的结果. 2014 年, 文献 [11] 构造了相关密钥条件下的 10 轮的不可能差分特征, 并且对 14 轮的 MIBS-80 进行了攻击. 2015 年. 文献 [12] 对 MIBS 进行 12 轮的 Biclique 攻击. 2015 年, 文献 [13] 对 MIBS 进行了全轮的 Biclique 攻击.

I-PRESENT [14] 算法是一种代换置换网络型对合的轻量级分组密码, 同时也是对 PRESENT 算法的改进. I-PRESENT 的主要优点是使用了对合函数, 使得加密电路和解密电路完全相同, 另外还可以使密码的混淆扩散速度更快. 这对于需要两种电路实现的环境来说是一个比较大的优势. I-PRESENT 明文分组长度为 64 位, 支持密钥的长度为 80 位和 128 位两种, 这两个版本的分组密码分别叫做 I-PRESENT-80 和 I-PRESENT-128. 主密钥作为密钥扩展算法的输入, 然后通过密钥扩展算法生成 30 个 64 位的轮密钥. 明文通过 15 轮的轮函数之后执行对合操作, 接着再进行 15 轮的逆轮函数从而产生密文. I-PRESENT 轻量级分组密码共需要 30 轮的轮函数. 利用本文提出的方案, 我们将对 I-PRESENT 进行攻击.

Biclique 攻击方法首次是由 Khovratovich 等 [15] 在 2011 年提出来的. 相对来说 Biclique 攻击是比较新的技术. 一个 Biclique 结构就是一个完全二部图, 其中起始状态的每一条边都和结束状态的一条边相连. 另外, Biclique 结构中的每条路径都是通过唯一的密钥相连. 如果路径中没有共享活动的非线性加密单元, 则通过 Biclique 结构敌手就可以高效地测试一系列的候选密钥. 这样的话, 攻击的开销就会降低, 或者说是可以增加中间相遇攻击以及其他攻击的轮数. Biclique 攻击方法在对分组密码的密钥恢复上有着比较强的适用能力. 2011 年, Bogdanov 等 [16] 对 AES 进行了 Biclique 攻击后, 他们的工作就受到了广泛的关注, 因为这是第一次针对单密钥模型分组密码的全轮攻击. 自那之后, 基于 Biclique 结构的密钥恢复攻击成功地应用到一系列的分组密码中, 其中包括 3D 分组密码 [17], SQUARE [18], HIGHT [19], Piccolo [20], LBlock [21], TWINE [22], KLEIN [23] 和 mCrypton [24], 所有的这些工作, 都是第一次对全轮密码的攻击.

本文对 MIBS-80 和 I-PRESENT-128 分组密码分别进行了全轮的 Biclique 攻击, 并且把对 MIBS-80 的攻击结果和文献 [11~13] 作比较, 结果如表 1. 因本文是首次运用非对称 Biclique 技术对 I-PRESENT-128 进行攻击, 所以只列出复杂度分析的结果.

本文其余部分组织如下: 第 2 节介绍使用 early abort 技术 [25] 的非对称 Biclique 攻击技术; 第 3 节介绍 MIBS 算法; 第 4 节给出 MIBS-80 的 Biclique 攻击过程和结果; 第 5 节介绍 I-PRESENT 算法; 第 6 节给出 I-PRESENT-128 的 Biclique 攻击过程和结果; 第 7 节对全文进行总结.

2 结合 early abort 技术的非对称 Biclique 攻击技术

结合 early abort 技术的非对称 Biclique 攻击技术由密钥空间的划分、构造 Biclique、部分匹配和重新检测候选密钥 4 个步骤组成, 下面给出详细的实施过程.

2.1 密钥空间的划分

首先把主密钥 K 划分为 4 个集合, 分别叫做 K^f, K^{b_1}, K^{b_2} 和 K^g, 各占 d, d, d 和 $n-3d$ 位. 可知, 对于任意固定的密钥 K^g 来说, 都可以找到一组不同的密钥值 K^f, K^{b_1} 和 K^{b_2}. 组内的密钥值都可以表示为 $K[i, j_1, j_2]$, 其中 $K^f = i$, $K^{b_1} = j_1$ 和 $K^{b_2} = j_2$, $0 \leqslant i, j_1, j_2 \leqslant 2^d - 1$. 差分定义如下:

$$\begin{aligned}
\Delta_i^K &= K[0,0,0] + K[i,0,0];\\
\nabla_j^K &= K[0,0,0] + K[0,j_1,j_2];\\
\nabla_{j_1}^K &= K[0,0,0] + K[0,j_1,0];\\
\nabla_{j_2}^K &= K[0,0,0] + K[0,0,j_2].
\end{aligned}$$

2.2 构造 Biclique

如果对于 $\forall i, j_1, j_2 \in \{0, 1, \ldots, 2^d - 1\}$, 公式 $S_{j_1,j_2} \xleftarrow{K[i,j_1,j_2]} C_i$ 成立, 那么一个 $(d, 2d)$ 维的 Biclique 结构就可以用三元组 $[\{C_i, \{S_{j_1}, j_2\}, \{K[i, j_1, j_2]\}]$ 表示, 其中 C_i 表示包含 2^d 个密文的集合, S_{j_1}, j_2 表示包含 2^{2d} 个中间状态的集合.

这里使用最通常的 Biclique 的构造方法, 步骤如下:

步骤 1. 对于所有的 $j_1, j_2 \in \{0, 1, \ldots, 2^d - 1\}$ 来说, 选择一个随机的密文 C_0 然后按公式计算 S_{j_1,j_2}:

$$S_{j_1,j_2} \xleftarrow{K[0,j_1,j_2]} C_0.$$

步骤 2. 对于所有的 $i \in \{0, 1, \ldots, 2^d - 1\}$ 来说, 然后按如下公式计算 C_i:

$$S_0 \xrightarrow{K[i,0]} C_i.$$

如果 Δ_i^K 的相关密钥差分特征在前向计算过程中没有共享后向计算过程 ∇_j^K 中任意的相关密钥差分特征, 那么就可以构造一个 Biclique 结构.

2.3 使用 early abort 技术的部分匹配

为了攻击密码除了 Biclique 结构所在的剩余轮数, 我们使用了预计算和重计算 [16] 的部分匹配技术. 为了方便 Biclique 攻击, 中间的匹配变量 V 应选择在匹配阶段的首轮和末轮的合适位置. 但是为了结合 early abort 技术, 我们在合适的位置选择两个更小的中间变量, 分别叫做 $V^{(1)}$ 和 $V^{(2)}$.

接着, 使用密钥 $K[0, j_1, j_2]$ 在后向计算 $\overleftarrow{V_{0,j_1,j_2}^{(1)}}$ 中部分解密 S_{j_1,j_2} 到第一个匹配变量的位置, 然后存储涉及到的所有中间状态. 在前向计算 $\overrightarrow{V_{0,j_1,j_2}^{(1)}}$ 中, 相似地使用密钥 $K[i, 0, 0]$ 部分加密 P_i 到第一个匹配变量的位置, 同样地存储涉及到的所有中间状态. 下面就要筛选错误轮密钥, 为了这个目的, 我们按照以下程序检测每组中的每一个密钥值 $K[i, j_1, j_2]$.

后向计算过程中, 当 $i \neq 0$ 时, 为了使用密钥 $K[i, j_1, j_2]$ 解密 S_{j_1,j_2} 找到匹配变量 $\overleftarrow{V_{i,j_1,j_2}^{(1)}}$, 我们仅需要重新计算 K^f 中受 i 改变的影响的那些位, 其余的比特位不需要重新计算. 相似地, 前向计算过程

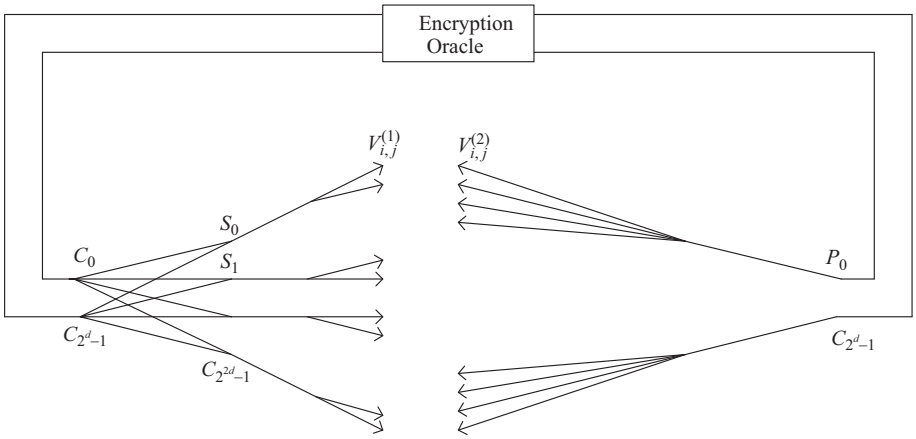


图 1　非对称 Biclique 攻击

Figure 1　Asymmetric Biclique cryptanalysis

中, 当 $j_1, j_2 \neq 0$ 时, 为了使用密钥 $K[i, j_1, j_2]$ 加密 P_i 找到匹配变量 $\overrightarrow{V_i, j_1, {j_2}^{(1)}}$, 我们仅需要重新计算 K^f 中受 j_1 或者 j_2 改变的影响的那些位, 其余的比特位不需要重新计算. 需要注意的是, 这些位置只是受 K^{b_1} 或者 K^{b_2} 其中之一的影响.

现在使用 early abort 技术使攻击中的计算复杂度得到改善. 对于密钥 $K[i, j_1, j_2]$ 来说, 如果检测出 $\overrightarrow{V_i, j_1, {j_2}^{(1)}} \neq \overleftarrow{V_i, j_1, {j_2}^{(1)}}$, 那么就要停止检测; 如果相等的话, 就按如下步骤继续检测. 后向计算过程中, 继续解密和重计算 $\overleftarrow{V_i, j_1, {j_2}^{(2)}}$ 中独立的部分, 前向计算过程中, 继续解密和重计算 $\overrightarrow{V_i, j_1, {j_2}^{(2)}}$ 中独立的部分. 如果 $\overrightarrow{V_i, j_1, {j_2}^{(2)}} = \overleftarrow{V_i, j_1, {j_2}^{(2)}}$, 那么密钥 $K[i, j_1, j_2]$ 就为候选密钥.

2.4　重新检测候选密钥

最后, 为了筛选出错误密钥, 我们就要通过明密文对 (P, C) 来测试候选密钥. 图 1 表示的是改善的非对称 Biclique 攻击的示意图.

3　MIBS 算法介绍

3.1　符号说明

K: 主密钥.

$K[i]$: 主密钥的第 i bit.

$K[i-j]$: 主密钥中第 j 到第 i bit (共 $i-j+1$ bit).

k^i: 第 i 轮的轮密钥.

x_i, y_i: 中间状态的第 i 个连续的 4 bit.

L_i: 第 i 轮输入的左 32 bit.

R_i: 第 i 轮输入的右 32 bit.

$>>> n$: 循序右移 n bit.

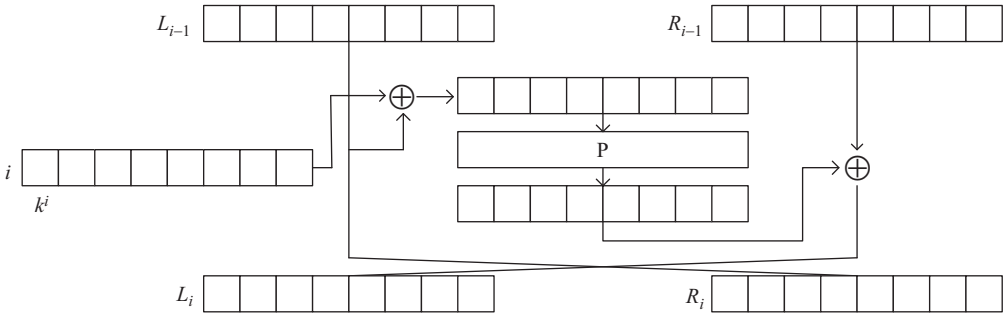


图 2 MIBS 算法第 i 轮结构

Figure 2 The i-th round construction of MIBS

3.2 MIBS 算法

MIBS 分组长度为 64 bit, 密钥长度可以为 64 bit 和 80 bit, 分别记作 MIBS-64 和 MIBS-80, 都迭代 32 轮 (这两种算法轮函数是一样的, 只是在密钥扩展算法上不同). 每轮的 F 函数包括轮子密钥变换, 非线性 S 盒变换和线性 P 盒变换. 第 i 轮的结构如图 2 所示.

设 64 bit 明文为 $L_0||R_0$ 约定从左至右为高比特到低比特的排列, 加密得到密文 $L_{32}||R_{32}$ 过程如下. 对 $1 \leqslant i \leqslant 32$, $L_i = F(L_{i-1}, k^i) \oplus R_{i-1}$, $R_i = L_{i-1} \circ F(L_{i-1}, k^i)$ 定义如下:

(1) 密钥加变换. $X = L_{i-1} \oplus k^i$.

(2) 非线性 S 盒变换. 令 $X = x_8||x_7||x_6||x_5||x_4||x_3||x_2||x_1$, $y_i = S(x_i)$ $(i = 1, \ldots, 8)$.

(3) 线性 P 盒变换.

$$
\begin{aligned}
y'_1 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_7 \oplus y_8;\\
y'_2 &= y_2 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_6 \oplus y_7;\\
y'_3 &= y_1 \oplus y_2 \oplus y_3 \oplus y_5 \oplus y_6 \oplus y_8;\\
y'_4 &= y_2 \oplus y_3 \oplus y_4 \oplus y_7 \oplus y_8;\\
y'_5 &= y_1 \oplus y_3 \oplus y_4 \oplus y_5 \oplus y_8;\\
y'_6 &= y_1 \oplus y_2 \oplus y_4 \oplus y_5 \oplus y_6;\\
y'_7 &= y_1 \oplus y_2 \oplus y_3 \oplus y_6 \oplus y_7;\\
y'_8 &= y_1 \oplus y_3 \oplus y_4 \oplus y_6 \oplus y_7 \oplus y_8.
\end{aligned}
$$

$F(L_{i-1}, k^i)$ 的输出即为 $y'_8||y'_7||y'_6||y'_5||y'_4||y'_3||y'_2||y'_1$.

本文工作只针对 MIBS-80, 这里只介绍 MIBS-80 的密钥扩展算法. 设 $K = K[79, 78, \ldots, 0]$ 为长度为 80 bit 的主密钥, $\text{state}^{-1} \leftarrow K$, 则由主密钥生成 32 个 32 bit 的轮密钥 k^i $(0 \leqslant i \leqslant 31)$ 的过程如下:

(1) $\text{state}^i \leftarrow \text{state}^{i-1} >>> 19$;

(2) $\text{state}^i \leftarrow S(\text{state}^i_{[79\sim76]})||S(\text{state}^i_{[75\sim72]})||\text{state}^i_{[71\sim0]}$;

(3) $\text{state}^i \leftarrow \text{state}^i_{[79\sim19]}||\text{state}^i_{[18\sim14]} \oplus \text{RC}||\text{state}^i_{[13\sim0]}$;

(4) $k^i \leftarrow \text{state}^i_{[79\sim48]}$.

其中 S 盒与加密算法中的 S 盒一样, RC 表示轮常数.

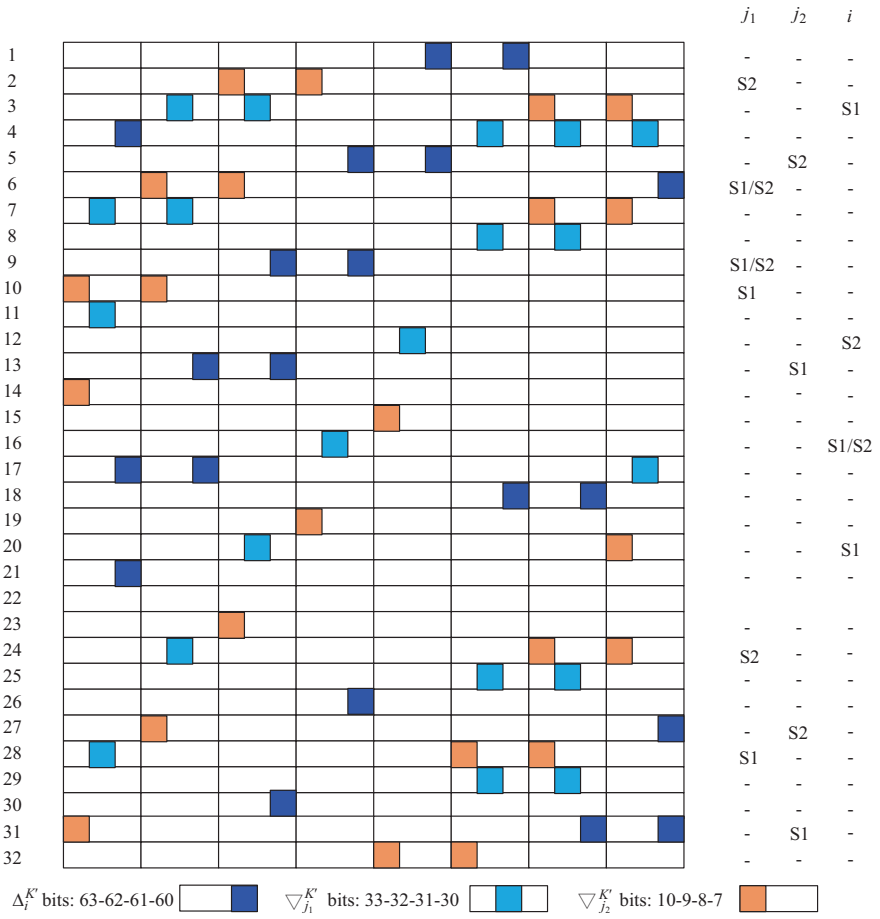


图 3 (网络版彩图) MIBS-80 的密钥扩展方案

Figure 3 (Color online) Key schedule of MIBS-80

4 MIBS-80 的非对称 Biclique 攻击

4.1 攻击方案

我们利用密钥扩展中后向混淆中的弱密钥性来提高 Biclique 的攻击效果, 以此降低攻击的计算复杂度. 假设 K' 是 22 轮中主密钥状态, 定义 $K'^f = K'[63-60]$, $K'^{b_1} = K'[33-30]$ 和 $K'^{b2} = K'[10-7]$ (如图 3).

图 3 中可以看出在密钥扩展阶段, 任意的 $\Delta_i^{K'}, \nabla_{j_1}^{K'}$ 和 $\nabla_{j_2}^{K'}$ 差分没用共享活动的 S 盒. 因此, 可以忽略密钥分发阶段的计算复杂度. 在 MIBS-80 的 23~32 轮可以构造 10 轮的 $(d, 2d)$ 维的 Biclique 结 (如图 4). 另外, 12 轮的 R_{12} 中第一和第六个 4 位值分别作为匹配变量 $V_{i,j_1,j_2}^{(1)}$ 和 $V_{i,j_1,j_2}^{(2)}$ (如图 5 和 6).

4.2 复杂度分析

图 4 中可以看出, 对于每个 Biclique 来说, 都有 16 个活动的 4 位比特值, 所以攻击的数据复杂度为 2^{64}.

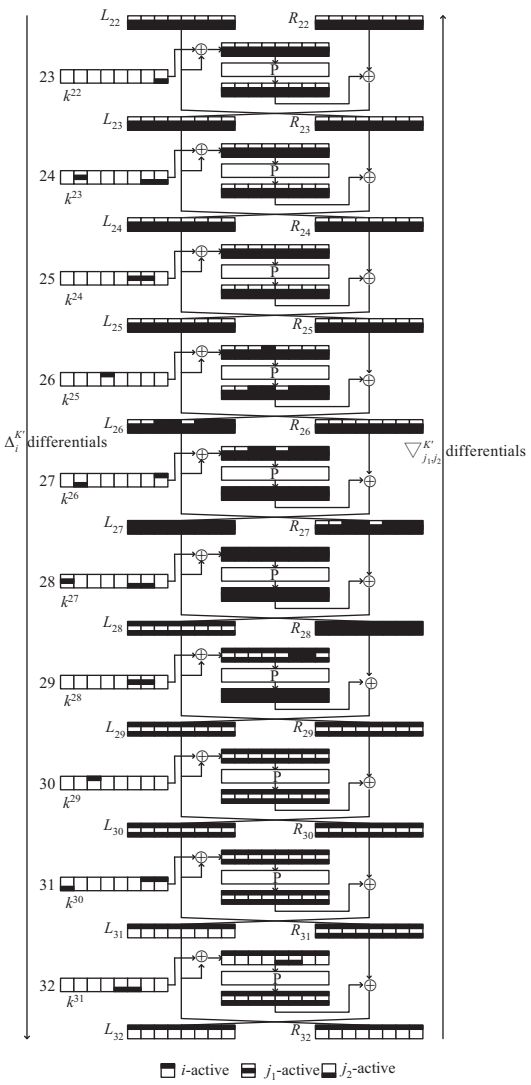


图 4 MIBS-80 的 10 轮 Bicilque 结构

Figure 4 10 rounds Biclique of MIBS-80

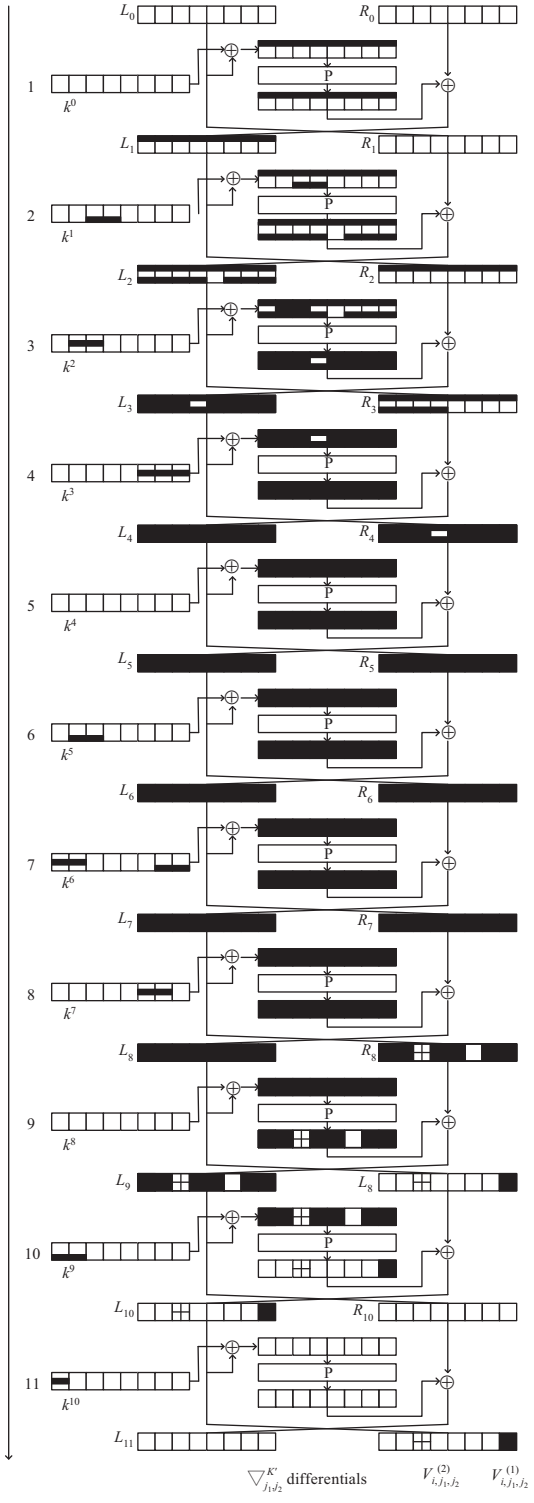


图 5 MIBS-80 的前向部分匹配

Figure 5 Forward partial matching of MIBS-80

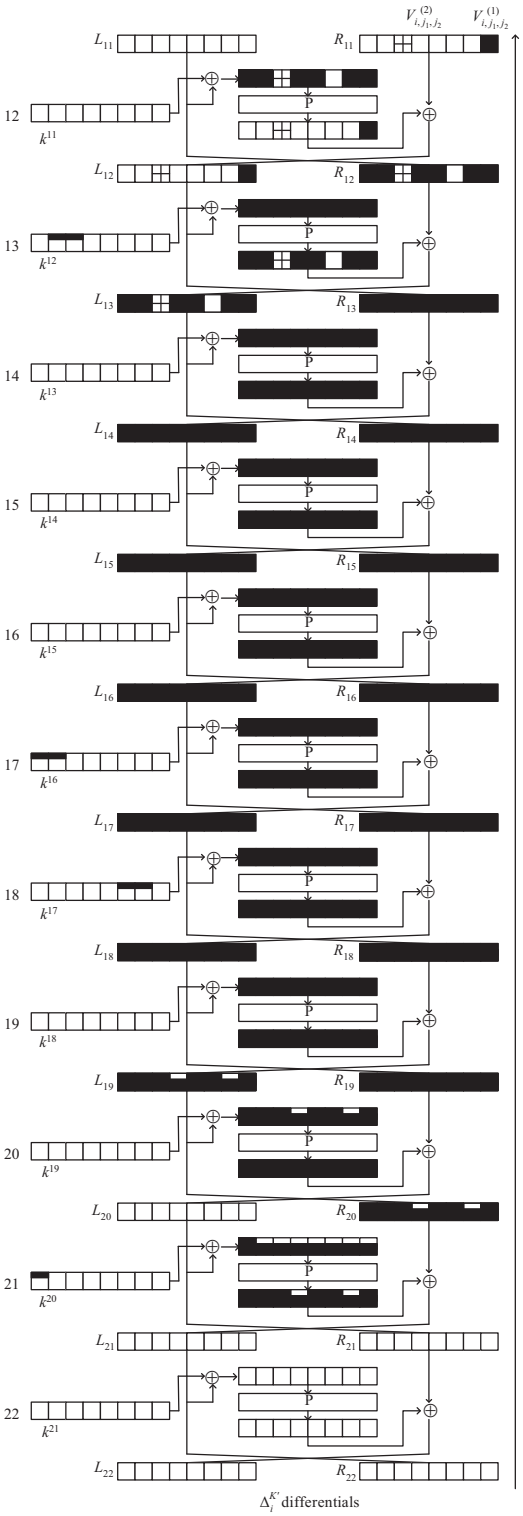


图 6　MIBS-80 的后向部分匹配

Figure 6　Backward partial matching of MIBS-80

考虑到攻击的计算复杂度相对于其他线性单元来说, 主要是受 S 盒的影响, 所以我们要算出攻击涉及到的 S 盒的总数. MIBS-80 在加密阶段有 32×8=256 个 S 盒, 以及密钥扩展阶段的 31×2=62 个 S 盒. 因此, 32 轮的 MIBS-80 共有 318 个 S 盒要计算.

在 Biclique 构造部分, 有 6 个 S 盒需要计算一次, 16 个 S 盒需要计算 2^4 次以及 58 个 S 盒需要计算 2^8 次. 因此, Biclique 构造所需的计算复杂度为

$$C_{\text{Biclique}} = \frac{6 + 16 \times 2^4 + 58 \times 2^8}{318} = 2^{5.57}.$$

部分匹配的前向计算 (1∼11 轮) 中, 对每个明文 P_i 来说, 为了获得第一个匹配变量 $\overrightarrow{V^{(1)}_{i,j_1,j_2}}$, 15 个 S 盒需要计算一次, 8 个 S 盒需要计算 2^4 次以及 55 个 S 盒需要计算 2^8 次. 同样地, 对于后向计算 (12∼22 轮) 中每个中间变量 S_j 来说, 为了获得第一个匹配变量 $\overleftarrow{V^{(1)}_{i,j_1,j_2}}$, 有 9 个 S 盒需要计算一次, 61 个 S 盒需要计算 2^4 次. 如果 $\overrightarrow{V^{(1)}_{i,j_1,j_2}} = \overleftarrow{V^{(1)}_{i,j_1,j_2}}$, 就还要获得 $\overrightarrow{V^{(2)}_{i,j_1,j_2}}$ 和 $\overleftarrow{V^{(2)}_{i,j_1,j_2}}$, 计算过程中, 在前向计算有 2 个 S 盒需要计算 2^4 次; 后向计算中 2 个 S 盒需要计算 2^8 次. 对于每一个错误的猜测密钥来说, 每组密钥中都有 2^{-4} 的概率出现 $\overrightarrow{V^{(1)}_{i,j_1,j_2}} = \overleftarrow{V^{(1)}_{i,j_1,j_2}}$ 的情况, 所以, 需要额外的计算 S 盒 $2^{12} \times 2^{-4} = 2^8$ 次. 因此, 检测 MIBS-80 匹配阶段所有密钥的计算复杂度为 $C_{\text{match}} = C_{\text{forward}} + C_{\text{backward}}$, 其中

$$C_{\text{forward}} = \frac{2^4 \times (15 + 8 \times 2^4 + 55 \times 2^8) + 2 \times 2^4}{318} = 2^{9.48},$$
$$C_{\text{backward}} = \frac{2^8 \times (9 + 61 \times 2^4) + 2 \times 2^8}{318} = 2^{9.63}.$$

因此, $C_{\text{match}} = 2^{10.56}$.

使用两个 4 位的匹配变量中接受到错误密钥的概率为 2^{-8}, 另外, 每组中需要检测的密钥数为 2^{12} 个, 因此, 重新检测错误密钥的计算复杂度为 $C_{\text{recheck}} = 2^{12} \times 2^{-8} = 2^4$.

综上所述, 攻击所需的总的计算复杂度为

$$C_{\text{total}} = 2^{68} \times (C_{\text{Biclique}} + C_{\text{match}} + C_{\text{recheck}}) = 2^{68} \times (2^{5.57} + 2^{10.56} + 2^4) = 2^{78.62}.$$

5 I-PRESENT 算法介绍

5.1 符号说明

K: 主密钥.
$K[i]$: 主密钥的第 i bit.
$K[i-j]$: 主密钥中第 j 到第 i bit (共 $i-j+1$ bit).
k^i: 第 i 轮的轮密钥.
X_i: 第 i 轮的输入.
$<<< n$: 循序左移 n bit.

5.2 I-PRESENT 算法

I-PRESENT 分组长度为 64 bit, 密钥长度可以为 80 bit 和 128 bit, 分别记作 I-PRESENT-80 和 I-PRESENT-128, 都迭代 30 轮 (这两种算法轮函数是一样的, 只是在密钥扩展算法上不同). 每轮的 F

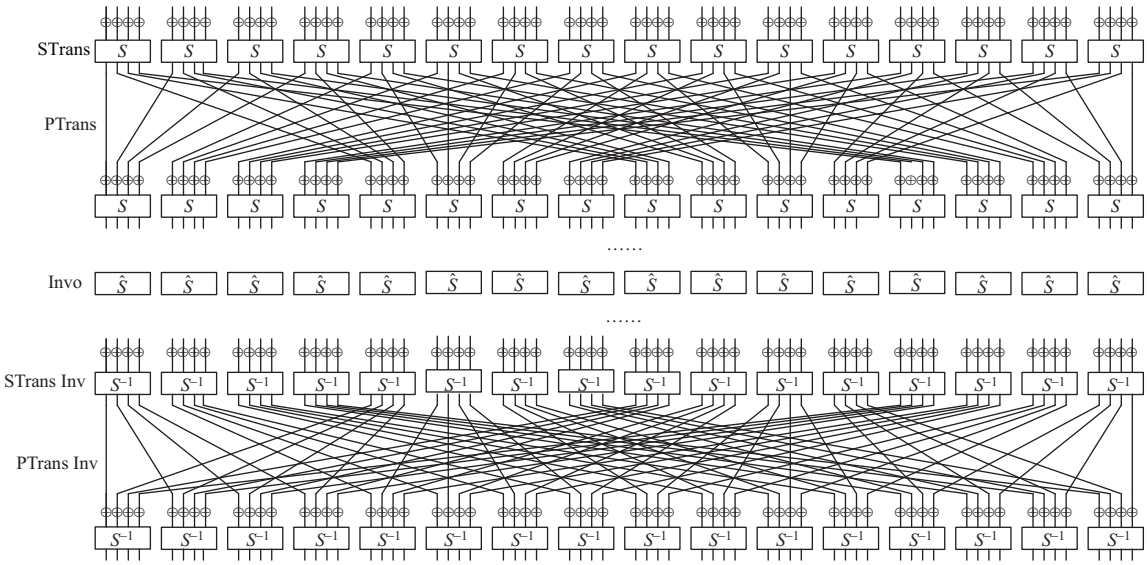


图 7 I-PRESENT 算法的结构

Figure 7 The round construction of I-PRESENT

表 2 I-PRESENT 的 S 盒映射关系

Table 2 The S-box used in I-PRESENT

State	Correspondence
x	0 1 2 3 4 5 6 7 8 9 A B C D E F
$S(x)$	D 6 1 F 4 8 B 5 0 3 A C 9 E 7 2
x	0 1 2 3 4 5 6 7 8 9 A B C D E F
$S^{-1}(x)$	8 2 F 9 4 7 1 E 5 C A 6 B 0 D 3

函数包括轮子密钥变换、非线性 S 盒变换、线性 P 盒变换和对合变换. I-PRESENT 的轮结构如图 7 所示.

设 64 bit 明文为 X_0 约定从左至右为高比特到低比特的排列, 加密得到密文 X_{30} 过程如下. 对 $1 \leqslant i \leqslant 30$, $X_i = F(X_{i-1}, k^i)$ 定义如下:

(1) 密钥加变换. $X = X_{i-1} \oplus k^i$.

(2) 非线性 S 盒变换. 规则见表 2.

(3) 线性 P 盒变换. 规则见图 7.

(4) 对合 S 盒变换. 规则见表 3.

本文工作只针对 I-PRESENT-128, 这里只介绍 I-PRESENT-128 的密钥扩展算法. 设 $K = K[127, 126, \ldots, 0]$ 为长度为 128 bit 的主密钥, $\text{state}^{-1} \leftarrow K$, 则由主密钥生成 30 个 64 bit 的轮密钥 k^i ($0 \leqslant i \leqslant 29$) 的过程如下:

(1) $\text{state}^i \leftarrow \text{state}^{i-1} <<< 53$;

(2) $\text{state}^i \leftarrow S(\text{state}^i_{[127\sim124]})||S(\text{state}^i_{[123\sim120]})||\text{state}^i_{[119\sim0]}$;

(3) $\text{state}^i \leftarrow \text{state}^i_{[127\sim68]}||\text{state}^i_{[67\sim63]} \oplus \text{RC}||\text{state}^i_{[62\sim0]}$;

(4) $k^i \leftarrow \text{state}^i_{[127\sim64]}$.

表 3 对合层的 S 盒映射关系

Table 3 The S-box used in the function Invo

State	Correspondence
x	0 1 2 3 4 5 6 7 8 9 A B C D E F
$\hat{S}(x)$	E A 2 C 4 8 F D 5 9 1 B 3 7 0 6

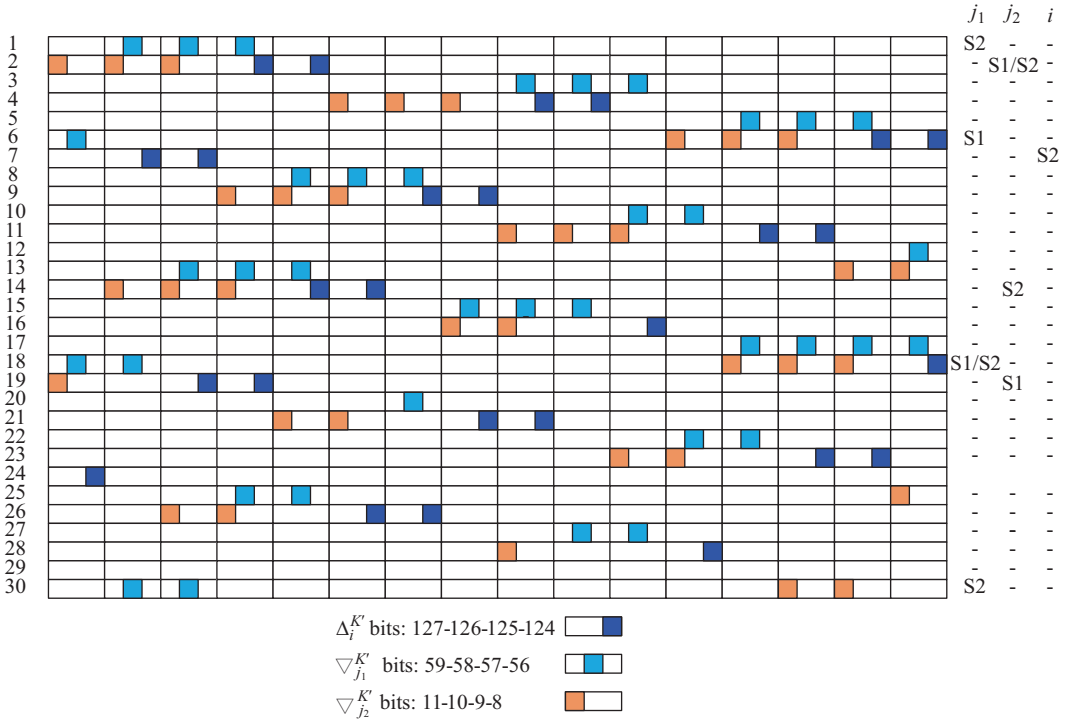


图 8 (网络版彩图) I-PRESENT-128 的密钥扩展方案

Figure 8 (Color online) Key schedule of I-PRESENT-128

6 I-PRESENT-128 的非对称 Biclique 攻击

6.1 攻击方案

我们利用密钥扩展中后向混淆中的弱密钥性来提高 Biclique 的攻击效果, 以此降低攻击的计算复杂度. 假设 K' 是 24 轮中主密钥状态, 定义 $K'^f = K'[127-124]$, $K'^{b_1} = K'[59-56]$ 和 $K'^{b2} = K'[11-8]$ (如图 8).

图 8 中可以看出, 在密钥扩展阶段, 任意的 $\Delta_i^{K'}, \nabla_{j1}^{K'}$ 和 $\nabla_{j2}^{K'}$ 差分没用共享活动的 S 盒. 因此, 可以忽略密钥分发阶段的计算复杂度. 在 I-PRESENT-128 的 25~30 轮可以构造 6 轮的 $(d, 2d)$ 维的 Biclique 结构 (如图 9). 另外 13 轮的中间状态中第 16 和第 12 个 4 位值分别作为匹配变量 $V_{i,j_1,j_2}^{(1)}$ 和 $V_{i,j_1,j_2}^{(2)}$ (如图 10 和 11).

6.2 复杂度分析

图 9 中可以看出, 对于每个 Biclique 来说, 都有 16 个活动的 4 位比特值, 所以攻击的数据复杂度

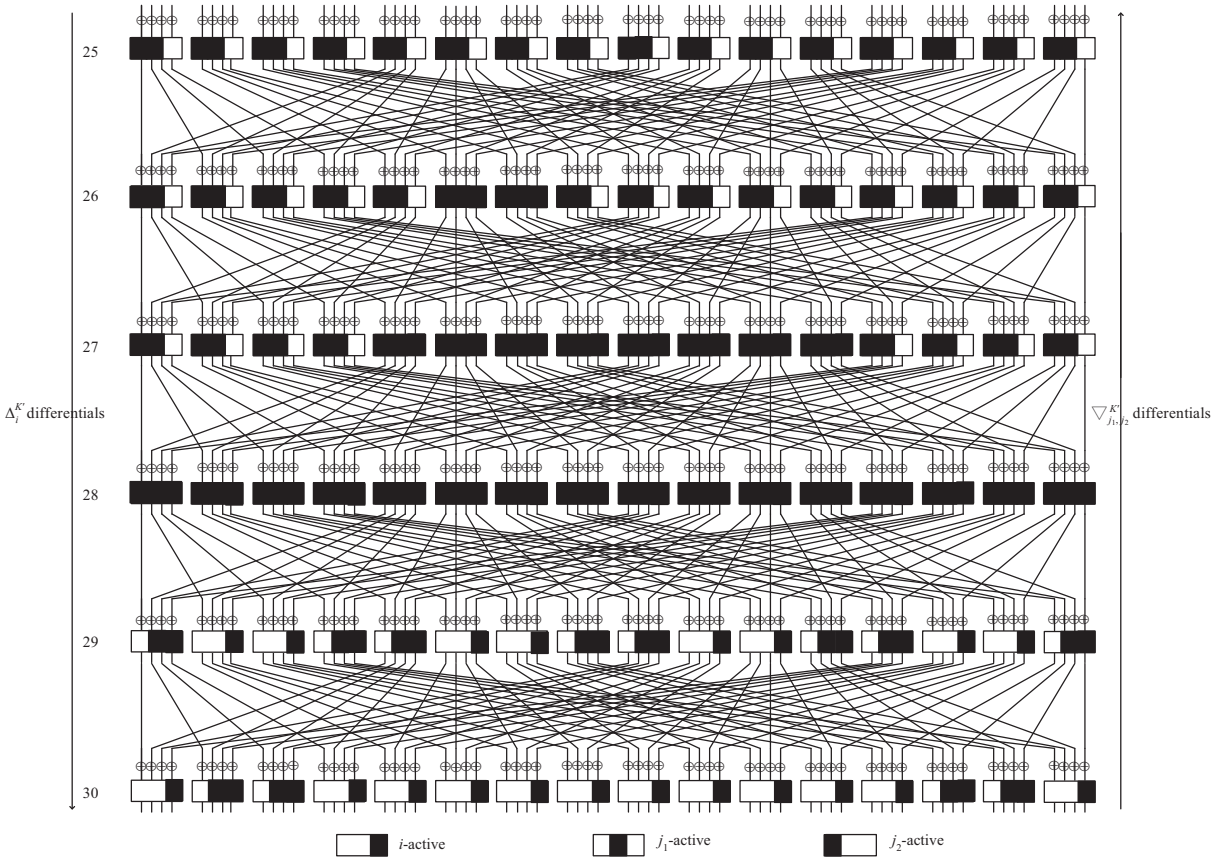


图 9　I-PRESENT-128 的 6 轮 Bicilque 结构

Figure 9　6 rounds Biclique of I-PRESENT-128

为 2^{64}.

考虑到攻击的计算复杂度相对于其他线性单元来说, 主要是受 S 盒的影响, 所以我们要算出攻击涉及到的 S 盒的总数. I-PRESENT-128 在加密阶段有 30×16=480 个 S 盒, 以及密钥扩展阶段的 29×2=58 个 S 盒. 因此, 30 轮的 I-PRESENT-128 共有 538 个 S 盒要计算.

在 Biclique 构造部分, 有 20 个 S 盒需要计算一次, 50 个 S 盒需要计算 2^4 次以及 26 个 S 盒需要计算 2^8 次. 因此, Biclique 构造所需的计算复杂度为

$$C_{\text{Biclique}} = \frac{20 + 50 \times 2^4 + 26 \times 2^8}{538} = 2^{3.80}.$$

部分匹配的前向计算 (1~12 轮) 中, 对每个明文 P_i 来说, 为了获得第一个匹配变量 $\overrightarrow{V_{i,j_1,j_2}^{(1)}}$, 23 个 S 盒需要计算一次, 18 个 S 盒需要计算 2^4 次以及 139 个 S 盒需要计算 2^8 次. 同样地, 对于后向计算 (13~24 轮) 中每个中间变量 S_j 来说, 为了获得第一个匹配变量 $\overleftarrow{V_{i,j_1,j_2}^{(1)}}$, 有 27 个 S 盒需要计算一次, 137 个 S 盒需要计算 2^4 次. 如果 $\overrightarrow{V_{i,j_1,j_2}^{(1)}} = \overleftarrow{V_{i,j_1,j_2}^{(1)}}$, 我们就还要获得 $\overrightarrow{V_{i,j_1,j_2}^{(2)}}$ 和 $\overleftarrow{V_{i,j_1,j_2}^{(2)}}$, 计算过程中, 在前向计算有 0 个 S 盒需要计算 2^4 次; 后向计算中 5 个 S 盒需要计算 2^8 次. 对于每一个错误的猜测密钥来说, 每组密钥中都有 2^{-4} 的概率出现 $\overrightarrow{V_{i,j_1,j_2}^{(1)}} = \overleftarrow{V_{i,j_1,j_2}^{(1)}}$ 的情况, 所以, 需要额外的计算 S 盒 $2^{12} \times 2^{-4} =$

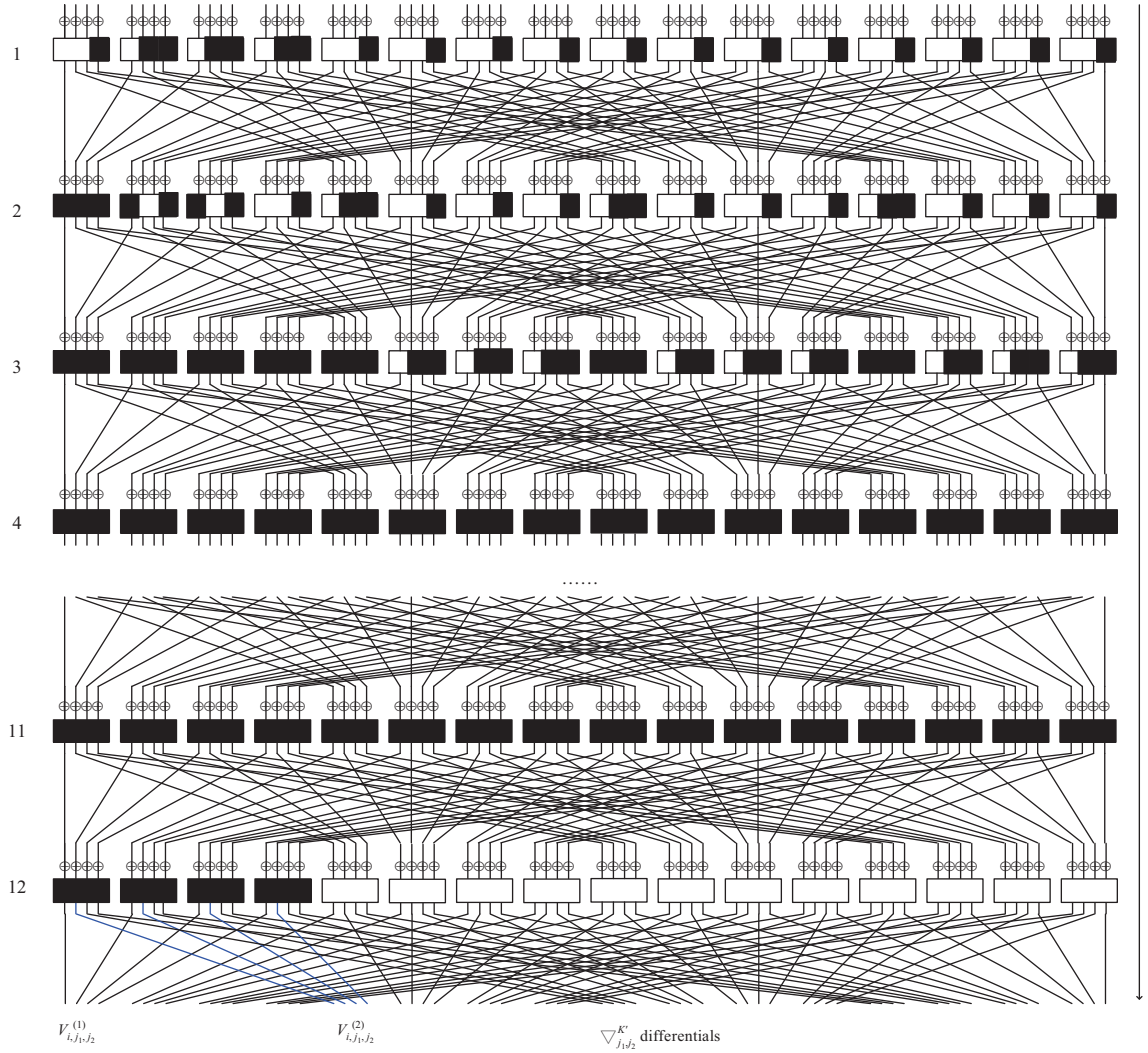


图 10 (网络版彩图) I-PRESENT-128 的前向部分匹配

Figure 10 (Color online) Forward partial matching of I-PRESENT-128

2^8 次. 因此, 检测 MIBS-80 匹配阶段所有密钥的计算复杂度为 $C_{\text{match}} = C_{\text{forward}} + C_{\text{backward}}$, 其中

$$C_{\text{forward}} = \frac{2^4 \times (23 + 18 \times 2^4 + 139 \times 2^8) + 2 \times 2^4}{538} = 2^{10.06},$$
$$C_{\text{backward}} = \frac{2^8 \times (27 + 137 \times 2^4) + 5 \times 2^8}{538} = 2^{10.05}.$$

因此, $C_{\text{match}} = 2^{11.05}$.

使用两个 4 位的匹配变量中接受到错误密钥的概率为 2^{-8}, 另外, 每组中需要检测的密钥数为 2^{12} 个, 因此, 重新检测错误密钥的计算复杂度为 $C_{\text{recheck}} = 2^{12} \times 2^{-8} = 2^4$.

综上所述, 攻击所需的总的计算复杂度为

$$\begin{aligned} C_{\text{total}} &= 2^{116} \times (C_{\text{Biclique}} + C_{\text{match}} + C_{\text{recheck}}) \\ &= 2^{116} \times (2^{3.80} + 2^{11.05} + 2^4) = 2^{127.07}. \end{aligned}$$

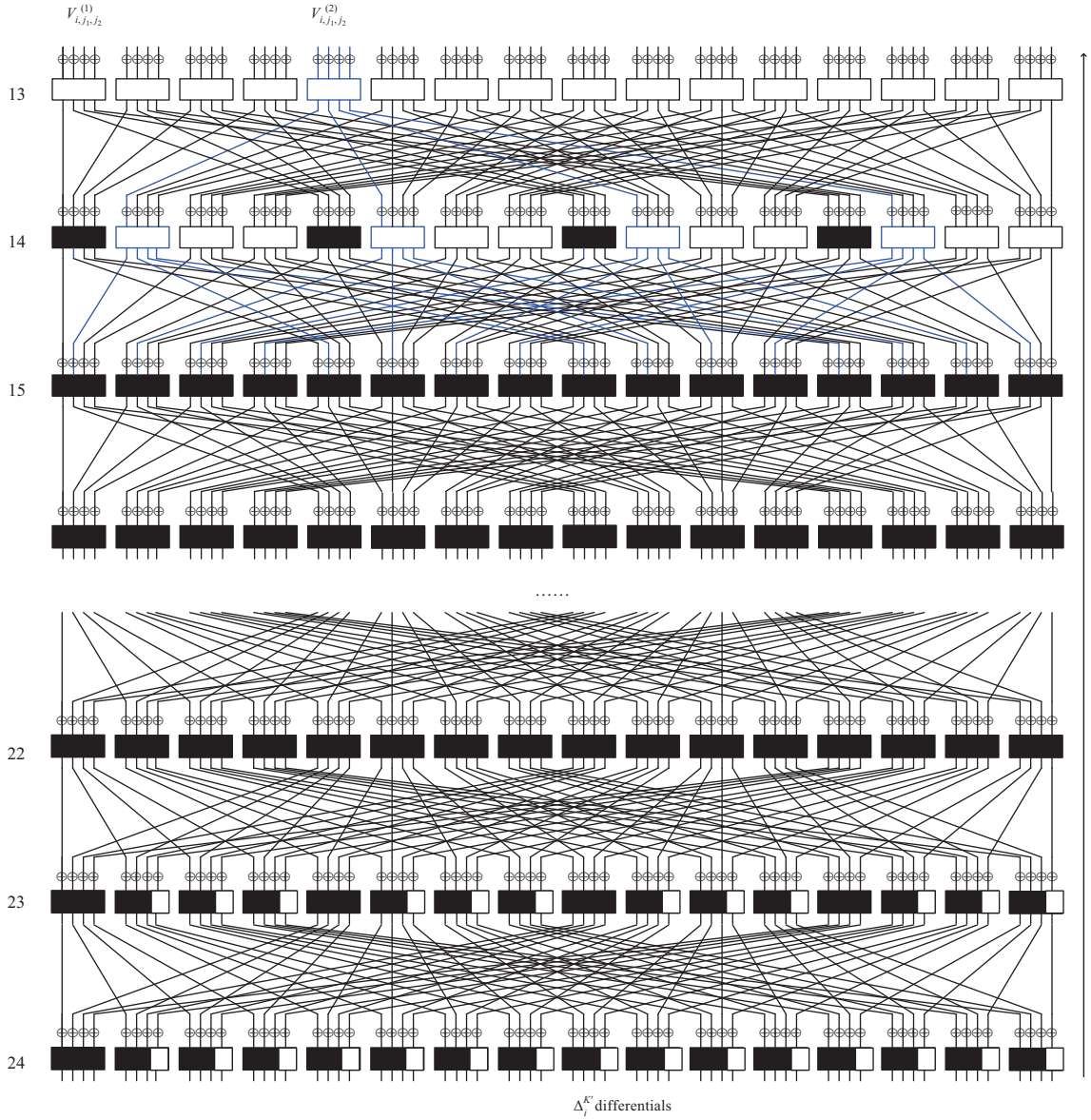


图 11　(网络版彩图) I-PRESENT-128 的后向部分匹配

Figure 11　(Color online) Backward partial matching of I-PRESENT-128

7　总结

通过使用非对称 Biclique 结构和 early abort 技术, 可以有效改善 Biclique 攻击中匹配阶段的计算复杂度. 文中对全轮 MIBS-80 和全轮 I-PRESENT-128 分别进行了攻击, 结果表明, 对这两种分组密码的攻击计算复杂度都有所改善. 与已有攻击方案对比表明, 本文两种方案的计算复杂度均是最优的. 此外, 本文也是首次运用非对称 Biclique 方案对全轮 I-PRESENT-128 进行攻击.

参考文献

1　Bogdanov A, Knudsen L R, Leander G, et al. PRESENT: an ultra-lightweight block cipher. In: Proceedings of

International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2007. 450–466
2 Cannière C, Dunkelman O, Knežević M, et al. KATAN and KTANTAN — a family of small and efficient hardware-oriented block ciphers. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2009. 272–288
3 Wu W L, Zhang L. LBLOCK: a lightweight block cipher. In: Proceedings of the 9th International Conference on the Applied Cryptography and Network Security, Malaga, 2011. 327–344
4 Guo J, Peyrin T, Poschmann A, et al. The LED block cipher. Cryptographic Hardware Embedded Syst, 2011, 6917: 326–341
5 Borghoff J, Canteaut A, Güneysu T, et al. PRINCE–a low-latency block cipher for pervasive computing applications. In: Proceedings of the 18th International Conference on International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer, 2012. 208–225
6 Beaulieu R, Shors D, Smith J, et al. The simon and speck families of lightweight block ciphers. In: Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference, San Francisco, 2015. 1–6
7 Izadi M, Sadeghiyan B, Sadeghian S S, et al. MIBS: a new lightweight block cipher. In: Proceedings of International Conference on Cryptology and Network Security, Kanazawa, 2009. 334–348
8 Bay A, Jr J N, Vaudenay S. Cryptanalysis of reduced-round MIBS block cipher. In: Proceedings of Cryptology and Network Security. Berlin: Springer, 2010. 1–19
9 Yu X L, Wu W L, Li Y J. Integral attack of reduced-round MIBS block cipher. J Comput Res Dev, 2013, 50: 2117–2125 [于晓丽, 吴文玲, 李艳俊. 低轮 MIBS 分组密码的积分分析. 计算机研究与发展, 2013, 50: 2117–2125]
10 Pan Z S, Guo J S, Cao J K, et al. Integral attack on MIBS block cipher. J Commun, 2014, 35: 157–163 [潘志舒, 郭建胜, 曹进克, 等. MIBS 算法的积分攻击. 通信学报, 2014, 35: 157–163]
11 Chen P, Liao F C, Wei H R. Related-key impossible differential attack on a lightweight block cipher MIBS. J Commun, 2014, 35: 190–193 [陈平, 廖福成, 卫宏儒. 对轻量级 MIBS 算法的相关密钥不可能差分攻击. 通信学报, 2014, 35: 190–193]
12 Luo F, Ou Q Y, Zhou X G, et al. A Biclique cryptanalysis on lightweight block cipher MIBS-80. J Softw, 2015, 26: 8–16 [罗芳, 欧庆于, 周学广, 等. 轻量级分组密码 MIBS-80 算法的 Biclique 分析. 软件学报, 2015, 26: 8–16]
13 Hossein F S M, Mohammad D, Mohsen S. Biclique cryptanalysis of MIBS80 and PRESENT80 block ciphers. Secur Commun Netw, 2015, 9: 27–33
14 Z'aba M R, Jamil N, Rusli M E, et al. I-PRESENT: an involutive lightweight block cipher. J Inf Secur, 2014, 5: 114–122
15 Khovratovich D, Rechberger C, Savelieva A. Biclique for preimages: attacks on Skein-512 and the SHA-2 family. In: Proceedings of the 19th Annual Fast Software Encryption Workshop, Washington, 2012. 208–225
16 Bogdanov A, Khovratovich D, Rechberger C. Biclique cryptanalysis of the full AES. In: Proceedings of the 17th International Conference on the Theory and Application and Information Security, Seoul, 2011. 344–371
17 Chen S Z, Liu J. Biclique cryptanalysis on full 3D block cipher. Chinese J Comput, 2014, 37: 1063–1070 [陈少真, 刘佳. 对全轮 3D 分组密码算法的 Biclique 攻击. 计算机学报. 2014, 37: 1063–1070]
18 Mala H. Biclique-based cryptanalysis of the block cipher SQUARE. IET Inf Secur, 2014, 8: 207–212
19 Hong D, Koo B, Kwon D. Biclique attack on the full HIGHT. In: Proceedings of the International Conference on Information Security and Cryptology, Seoul, 2011. 365–374
20 Wang Y, Wu W, Yu X. Biclique cryptanalysis of reduced-bound Piccolo block cipher. In: Proceedings of the 8th International Conference on the Information Security Practice and Experience, Hangzhou, 2012. 337–352
21 Wang Y F, Wu W L, Yu X L, et al. Security on LBlock against biclique cryptanalysis. In: Proceedings of Information Security Applications. Berlin: Springer, 2012. 1–14
22 Çoban M, Karakoç F, Boztas Ö. Biclique Cryptanalysis of TWINE. Berlin: Springer, 2012. 43–55
23 Ahmadian Z, Salmasizadeh M, Aref M R. Biclique cryptanalysis of the full-round KLEIN block cipher. IET Inf Secur, 2015, 9: 294–301
24 Shakiba M, Dakhilalian M, Mala H. Non-isomorphic biclique cryptanalysis of full-round crypton. Comput Stand Inter, 2015, 41: 72–78
25 Lu J, Kim J, Keller N, et al. Improving the efficiency of impossible differential cryptanalysis of reduced Camellia and MISTY1. In: Proceedings of the Cryptopgraphers' Track at the RSA Conference on Topics in Cryptology. Berlin: Springer, 2008. 370–386

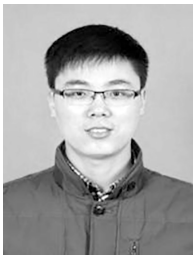
Asymmetric Biclique cryptanalysis of lightweight block ciphers MIBS and I-PRESENT

Jie CUI, Haifeng ZUO & Hong ZHONG*

School of Computer Science and Technology, Anhui University, Hefei 230039*, China*
* Corresponding author. E-mail: zhongh@ahu.edu.cn

Abstract The security evaluation of lightweight block ciphers plays a critical role in determining the security margins for these ciphers. One method for finding the security margin of a block cipher is Biclique cryptanalysis. In this paper, we present a new schematic for a Biclique attack, which combines asymmetric Biclique and early-abort techniques. We then apply the proposed schematic to MIBS-80 and I-PRESENT-128 to evaluate their security margins. The cryptanalysis for MIBS-80 has a computational complexity of $2^{78.62}$ and a data complexity of 2^{64}. The cryptanalysis for I-PRESENT-128 has a computational complexity of $2^{127.07}$ and a data complexity of 2^{64}. Compared to existing schemes, the computational complexity of the two schemes presented here is significantly reduced. Because the total complexity of cryptanalysis depends on the computational complexity, the proposed scheme provides significant advantages. Additionally, this study is the first to use an asymmetric Biclique to attack a full-round I-PRESENT-128.

Keywords lightweight block cipher, Biclique cryptanalysis, MIBS, I-PRESENT, partial matching



Jie CUI was born in 1980. He is currently an associate professor at the School of Computer Science and Technology, Anhui University. He received his Ph.D. degree from the University of Science and Technology of China in 2012. His research interests include network and information security.

Haifeng ZUO was born in 1992. He is currently studying at the School of Computer Science and Technology, Anhui University. His main research interests are the design and cryptanalysis of block ciphers.

Hong ZHONG was born in 1965. She is currently a professor (from 2009) and dean at the School of Computer Science and Technology, Anhui University, China. She received her Ph.D. from the University of Science and Technology of China in 2005. Her research interests include network and information security.