

PRINCE 密码算法的差分-线性分析

刘正斌

(保密通信重点实验室, 四川 成都 610041)

摘 要: PRINCE 是一个低时延轻量级分组密码算法, 广泛应用于各种资源受限设备。PRINCE 使用 FX 结构, 其核心部件是 $\text{PRINCE}_{\text{core}}$ 。差分-线性分析是一种经典分析方法, 它将差分分析和线性分析结合起来, 使用短的高概率差分特征和线性特征来攻击密码算法。研究了 $\text{PRINCE}_{\text{core}}$ 的差分-线性分析, 使用 2 轮差分-线性区分器攻击 4 轮 $\text{PRINCE}_{\text{core}}$, 需要 2^6 个选择明文, 时间复杂度为 $2^{14.58}$ 次 4 轮加密。对于 6 轮和 7 轮 $\text{PRINCE}_{\text{core}}$ 的差分-线性分析, 数据复杂度分别为 $2^{12.84}$ 和 $2^{29.02}$ 个选择明文, 时间复杂度分别为 $2^{25.58}$ 和 $2^{41.53}$ 。

关键词: 轻量级分组密码; PRINCE; 差分-线性分析

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021072

Differential-linear cryptanalysis of PRINCE cipher

LIU Zhengbin

Science and Technology on Communication Security Laboratory, Chengdu 610041, China

Abstract: PRINCE is a low-latency lightweight block cipher, which is widely used in a lot of resource constrained devices. It is based on the FX construction and the core component is $\text{PRINCE}_{\text{core}}$. Differential-linear cryptanalysis is a classical cryptographic technique, which combines differential cryptanalysis and linear cryptanalysis together. Short differential characteristics and linear characteristics with high-probability were concatenated to break the cipher. Differential-linear cryptanalysis were applied to attack $\text{PRINCE}_{\text{core}}$. Using 2-round differential-linear distinguisher, 4-round $\text{PRINCE}_{\text{core}}$ can be broken with 2^6 chosen plaintext and $2^{14.58}$ encryption. For 6-round and 7-round $\text{PRINCE}_{\text{core}}$, the data complexity is $2^{12.84}$ and $2^{29.02}$ respectively, and the time complexity is $2^{25.58}$ and $2^{41.53}$.

Keywords: lightweight block cipher, PRINCE, differential-linear cryptanalysis

收稿日期: 2020-12-16; 修回日期: 2021-05-18

通信作者: 刘正斌, zhengbinliu@126.com

基金项目: 国家重点研发计划 (2017YFB0802000)

Foundation Item: The National Key R&D Program of China (2017YFB0802000)

论文引用格式: 刘正斌. PRINCE 密码算法的差分-线性分析[J]. 网络与信息安全学报, 2021, 7(4): 131-140.

LIU Z B. Differential-linear cryptanalysis of PRINCE cipher[J]. Chinese Journal of Network and Information Security, 2021, 7(4): 131-140.

1 引言

PRINCE 算法^[1]是 Borgho 等在 ASIACRYPT2012 年会上提出的轻量级分组密码,它具有非常低的硬件实现代价,可以广泛应用于各种资源受限环境。PRINCE 算法的重要特性是时延非常低,它能够在 1 个时钟周期内完成一次加密或解密运算,是专门为低时延应用而设计的分组密码。

PRINCE 算法采用 FX 结构^[2],由一个核心算法 PRINCE_{core}和两个白化密钥组成,其安全性主要依赖于 PRINCE_{core}的安全性。PRINCE_{core}是一个 SPN 型分组密码,它采用对称结构,具有加解密相似性,将加密密钥异或常数 α ,使用该密钥进行加密即可实现解密过程 (α 反射性质)。

自 PRINCE 算法被提出以后,其就受到了密码学界和工业界的广泛关注,目前学术界发表了许多分析 PRINCE 算法安全性的文章。在 FSE 2013 年会上, Jean 等^[3]首次给出了对 PRINCE 算法的第三方分析结果,他们提出了对约减轮数的 PRINCE 版本的积分攻击以及对 PRINCE 全轮的相关密钥攻击和时间-存储-数据折中攻击。2013 年, Soleimany 等^[4]研究了 PRINCE 的 α 反射性质,以及 α 的取值对 PRINCE 安全性的影响,对于某些特定的 α 值,他们提出了对 PRINCE 全轮的密钥恢复攻击。在 CRYPTO 2013 年会上, Canteaut 等^[5]使用 Sieve-in-the-Middle 技术攻击了 8 轮 PRINCE。在 FSE 2014 年会上, Canteaut 等^[6]利用多差分分析方法攻击了 10 轮 PRINCE,他们同时研究了 PRINCE 算法族中 S 盒的选择对于安全性的影响。在 FSE 2015 年会上, Derbez 等^[7]使用中间相遇攻击分析 10 轮 PRINCE。

虽然理论分析能够加深人们对于 PRINCE 算法的安全性和设计原理的理解,但来自工业界的研究人员和工程师更关注 PRINCE 的实际攻击。为了鼓励密码学者对 PRINCE 算法开展实际攻击,算法设计者在 2014 年发起了 PRINCE 挑战^[8] (PRINCE challenge),该挑战共包含 3 轮,第三轮评估在 2016 年结束。PRINCE 挑战提供了两种场景:选择明文和已知明文。选择明文场景提供 2^{20} 个选择明/密文,已知明文场景提供 2^{30} 个已知

明文,要求分析者使用尽可能少的选择或已知明文对算法进行攻击。对于每一种场景,根据攻击的轮数,设计者分别设置了 5 项挑战,最终的分析结果公布在其网站上^[8]。

本文研究 PRINCE 算法在差分-线性攻击模型下的安全性,给出了对 4 轮、6 轮和 7 轮 PRINCE_{core} 的实际攻击,攻击的数据复杂度分别为 2^6 、 $2^{12.84}$ 和 $2^{29.02}$,时间复杂度分别为 $2^{14.58}$ 、 $2^{25.58}$ 和 $2^{41.53}$ 。本文的分析结果与公开文献的对比如表 1 所示^[9-14]。

2 差分-线性分析

差分分析和线性分析是两种最有效的密码分析技术,它们给出了许多分组密码目前已知的最优分析结果。因此,抵抗差分分析和线性分析已经成为分组密码的一个基本设计准则。

差分分析是 Biham 和 Shamir^[15]在 1990 年提出的一种分析方法,它研究一个特定的明文差分在整个加密过程中的传播特性。差分分析使用一条高概率的差分(或差分特征)将分组密码和随机置换区分开,并在此基础上进行密钥恢复。差分概率的定义如下。

定义 1 (差分概率)。设 $P \in \mathbb{F}_2^n$ 为分组密码 E 的输入明文, $\alpha, \beta \in \mathbb{F}_2^n$ 分别表示输入差分和输出差分,则差分 $\alpha \rightarrow \beta$ 的概率定义为

$$P_r(\alpha \rightarrow \beta) = P_r\{E(P) \oplus E(P \oplus \alpha) = \beta\} \quad (1)$$

线性分析是 Matsui^[16]在 1993 年的欧洲密码学年会上提出的,它研究一组明文比特和密文比特之间的线性近似关系。线性分析使用一条高偏差的线性近似来区分分组密码和随机置换,并在此基础上恢复密钥。线性近似的偏差定义如下。

定义 2 (线性近似的偏差)。设 $P \in \mathbb{F}_2^n$ 为分组密码 E 的输入明文, $\mu, \nu \in \mathbb{F}_2^n$ 分别表示输入掩码和输出掩码,则线性近似 $\mu P \oplus \nu E(P)$ 的偏差定义为

$$\varepsilon_{\mu, \nu} = P_r\{\mu P \oplus \nu E(P) = 0\} - \frac{1}{2} \quad (2)$$

差分分析和线性分析成功的关键是寻找一条长的高概率的差分(差分特征)和高偏差的线性近似(线性特征),因此,只要保证分

表 1 PRINCE_{core} 的分析结果比较
Table 1 Comparison of the cryptanalysis of PRINCE_{core}

攻击轮数	攻击类型	数据复杂度	时间复杂度	存储复杂度	参考文献
4	积分分析	2^4	2^8	2^4	文献[3]
4	差分-线性分析	2^6	$2^{14.58}$	2^{12}	本文
5	混合差分分析	2^{14}	$2^{23.68}$	2^8	文献[9]
6	积分分析	2^{16}	2^{30}	2^{16}	文献[3]
6	差分分析	2^{48}	$2^{56.26}$	2^{48}	文献[10]
6	差分-线性分析	$2^{12.84}$	$2^{25.58}$	2^{16}	本文
7	截断差分分析	2^{50}	$2^{48.2}$	$2^{22.6}$	文献[11]
7	差分-线性分析	$2^{29.02}$	$2^{41.53}$	2^{16}	本文
8	中间相遇攻击	2^{53}	2^{53}	2^{28}	文献[12]
9	不可能差分分析	$2^{61.2}$	$2^{54.3}$	$2^{17.7}$	文献[13]
12	Biclique 攻击	2^{32}	$2^{62.69}$	2^8	文献[14]

组密码中不存在这种长的差分和线性近似, 就能保证其抵抗差分分析和线性分析。在很多情况下, 短的差分 and 线性近似仍然可以用于攻击分组密码。

1994 年, Langford 和 Hellman^[17]提出了差分-线性分析方法, 第一次将差分分析和线性分析结合起来。差分-线性分析的基本思想是: 将分组密码 E 分成两个子密码 E_0 和 E_1 , 即 $E = E_1 \circ E_0$, 其中 E_0 存在一条概率为 1 的截断差分, E_1 存在一条高偏差的线性近似。通过将 E_0 的差分 and E_1 的线性近似结合起来, 分析者可以攻击整个分组密码 E 。

2002 年, Biham 等^[18]提出了一个增强版本的差分-线性分析, 通过对 E_0 使用高概率的截断差分, 并且对输出对的奇偶性增加一些额外假设, 提高了差分-线性分析攻击的轮数。随后, Liu 等^[19]对 E_1 使用多重线性近似提高了近似的偏差, 降低了差分-线性分析的数据复杂度。Lu^[20]提出了差分-线性分析的一种改进方法, 该方法只需使用 Langford 和 Hellman 的两个默认假设, 减少了 Biham 等方法的假设数量, 进一步扩大了差分-线性分析的应用范围。2014 年, Blondeau 等^[21]使用差分分析和线性分析之间的理论关系^[22-23], 给出了计算差分-线性近似的偏差的一个精确公式, 该公式只需要一个假设, 即两个子密码 E_0 和 E_1 相互独立。

Bar-on 等^[24]研究了差分-线性分析中两个子密码之间的依赖性对于分析结果的影响, 并提出

了一个新的分析工具: 差分-线性连接表 (DLCT, differential-linear connectivity table)。DLCT 考虑了两个子密码之间的依赖性, 这使差分-线性分析的效率更高、应用范围更广。

定义 3 (差分-线性连接表)。设 $S: \mathbb{F}_2^n \rightarrow \mathbb{F}_2^m$ 是一个向量布尔函数, S 的 DLCT 是一个 $2^n \times 2^m$ 的表, 它的行对应 S 的输入差分, 列对应 S 的输出掩码。对于 $\alpha \in \mathbb{F}_2^n$, $\lambda \in \mathbb{F}_2^m$, DLCT 中的项 (α, λ) 定义为

$$\text{DLCT}_S = P_r \{ \lambda S(x) = \lambda S(x \oplus \alpha) \} - \frac{1}{2} \quad (3)$$

使用 DLCT, 分组密码 E 分成 3 个子密码 E'_0 、 E_m 和 E'_1 , 即 $E = E'_1 \circ E_m \circ E'_0$, 其中 E' 存在差分 $\alpha \rightarrow \beta$, E_m 包含 DLCT, E'_1 包含剩余的线性近似 $\mu \rightarrow \nu$ 。假设 E'_0 的差分概率为 $P_r(\alpha \rightarrow \beta)$, E'_1 的线性近似的相关性系数为 $c_{\mu, \nu} = 2\varepsilon_{\mu, \nu}$, 那么差分-线性近似的偏差为

$$\varepsilon_{\alpha, \nu} = \sum_{\beta, \mu} P_r(\alpha \rightarrow \beta) \text{DLCT}_S(\beta, \mu) c_{\mu, \nu}^2 \quad (4)$$

3 PRINCE 密码算法简介

PRINCE 算法^[1]是一个 64 bit 的分组密码, 支持 128 bit 的密钥长度, 迭代轮数为 12 轮。PRINCE 算法采用 FX 构造: 在核心算法 PRINCE_{core} 的两端分别加上一个白化密钥。PRINCE 的内部状态可以表示为一个 4×4 的矩阵, 矩阵中的每一个元

素为 4 bit 值。128 bit 的密钥 k 被分成两个 64 bit 的子密钥 k_0 和 k_1 , 即 $k = k_0 \parallel k_1$, 其中 k_0 生成另一个子密钥 $k'_0 = (k_0 \ggg 1) \oplus (k_0 \ggg 63)$, k_0 和 k'_0 用作白化密钥, k_1 用作核心算法 $\text{PRINCE}_{\text{core}}$ 的加密密钥。 PRINCE 的结构如图 1 所示。

$\text{PRINCE}_{\text{core}}$ 是 PRINCE 算法的核心, 它本身也是一个 SPN 型分组密码, 共迭代 12 轮。 $\text{PRINCE}_{\text{core}}$ 具有对称结构, 它的中间两轮是对合的, 剩余 10 轮除了使用不同的轮常数, 前、后 5 轮互为逆变换。 $\text{PRINCE}_{\text{core}}$ 的轮函数可以表示为 $R = \text{ARK} \circ \text{ARC} \circ \text{SR} \circ M' \circ S$, 包括以下 5 个变换: S 盒层、变换矩阵 M' 、行移位 SR 、轮常数加 ARC 、轮密钥加 ARK 。

(1) S 盒层

S 盒层使用 16 个完全相同的 4 bit S 盒, S 盒的变换过程如表 2 所示。

(2) 变换矩阵 M'

$\text{PRINCE}_{\text{core}}$ 的变换矩阵是一个 64×64 的二元对角型对合矩阵 $M' = \text{diag}(\hat{M}^0, \hat{M}^1, \hat{M}^1, \hat{M}^0)$, 其中 $\hat{M}^0$ 和 $\hat{M}^1$ 分别是 16×16 的二元对合矩阵。 $\hat{M}^0$ 和 $\hat{M}^1$ 定义为

$$\hat{M}^0 = \begin{bmatrix} M_0 & M_1 & M_2 & M_3 \\ M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \end{bmatrix}$$

$$\hat{M}^1 = \begin{bmatrix} M_1 & M_2 & M_3 & M_0 \\ M_2 & M_3 & M_0 & M_1 \\ M_3 & M_0 & M_1 & M_2 \\ M_0 & M_1 & M_2 & M_3 \end{bmatrix}$$

其中

$$M_0 = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad M_1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

$$M_2 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix} \quad M_3 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

(3) 行移位 SR

PRINCE 使用和 AES 相同的行移位, 即将状

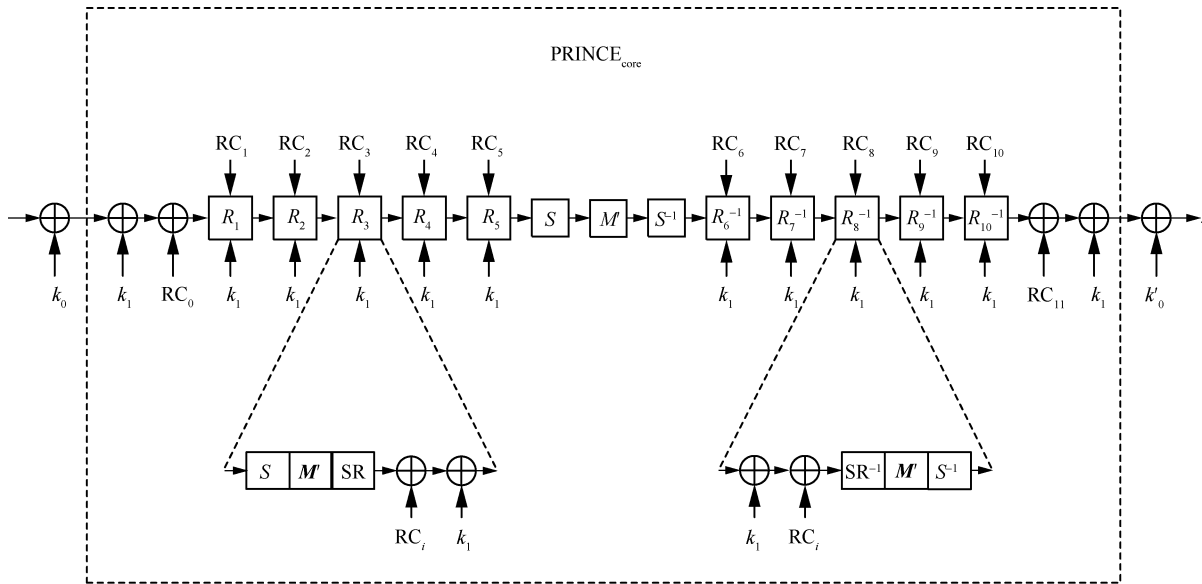


图 1 PRINCE 的结构

Figure 1 The structure of PRINCE

表 2 PRINCE 的 S 盒
Table 2 The S-box of PRINCE

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

态的第 i 行循环左移 i 个位置, $0 \leq i \leq 3$ 。

(4) 轮常数加 ARC

64 bit 的状态与 64 bit 的轮常数 RC_i 进行按位异或, 轮常数 RC_i 满足 $RC_i \oplus RC_{11-i} = \alpha$, $0 \leq i \leq 11$ 。

(5) 轮密钥加 ARK

64 bit 的状态与 64 bit 的轮密钥 k_i 进行按位异或。

因为 PRINCE_{core} 具有对称结构, M' 是对合矩阵, 并且轮常数满足 $RC_i \oplus RC_{11-i} = \alpha$, 所以 PRINCE 在密钥 k 下的解密过程等于在密钥 $k \oplus \alpha$ 下的加密, 即 $D_{(k_0 \| k_0 \| k_1)}(\cdot) = E_{(k_0 \| k_0 \| k_1 \oplus \alpha)}(\cdot)$, 这种性质被称为 α 反射性质。由于具有 α 反射性质, PRINCE 可以使用相同的电路完成加、解密。

4 PRINCE 算法的差分-线性分析

设 PRINCE_{core} 的明文为 $P = P_0 \| P_1 \cdots \| P_{15}$, 密钥为 $k_1 = k_1^0 \| k_1^1 \cdots \| k_1^{15}$, 密文为 $C = C_0 \| C_1 \cdots \| C_{15}$, 内部状态为 $X = X_0 \| X_1 \cdots \| X_{15}$, P_i 、 k_i^1 、 C_i 、 X_i ($0 \leq i \leq 15$) 均表示 4 bit 值。内部状态可以表示为 4×4 的矩阵。

$$X = \begin{bmatrix} X_0 & X_4 & X_8 & X_{12} \\ X_1 & X_5 & X_9 & X_{13} \\ X_2 & X_6 & X_{10} & X_{14} \\ X_3 & X_7 & X_{11} & X_{15} \end{bmatrix}$$

对 PRINCE 进行差分-线性分析, 首先需要构造 S 盒的差分分布表和线性近似表, 然后寻找高概率的差分特征和高偏差的线性特征, 通过 DLCT 将差分特征和线性特征连接起来, 得到差分-线性区分器。S 盒的差分分布表和线性近似表分别如表 3 和表 4 所示。

从差分分布表中, 可以得到输入差分 $\alpha = 0x1$ 经过 S 盒传播到输出差分 $\beta = 0x1$ 的概率为 $P_r(0x1 \rightarrow 0x1) = 2^{-2}$ 。通过查线性近似表可知, 输入掩码 $\mu = 0x2$ 经过 S 盒传播到输出掩码 $\nu = 0x2$ 的偏差为 $\varepsilon_{0x2,0x2} = -2^{-2}$ 。

PRINCE_{core} 的中间两轮 R_{mid} 由 S 盒层、矩阵变换层和 S 盒层的逆变换 $R_{mid} = S^{-1} \circ M' \circ S$ 构成, 由于矩阵变换使用了对角分块矩阵 $M' = \text{diag}(\hat{M}^0, \hat{M}^1, \hat{M}^1, \hat{M}^0)$, 因此任意两列内部

状态的矩阵乘法是相互独立的, 可以将中间两轮看作 4 个 16 bit 的大 S 盒变换。将 PRINCE_{core} 每一列中 4 个 4 bit S 盒的并置记为 S , 其逆变换为 S^{-1} , 因为 M' 中使用了两个子矩阵 $\hat{M}^0$ 和 $\hat{M}^1$, 所以可以构造两个大 S 盒 BS : ① $BS_0 = S^{-1} \circ \hat{M}^0 \circ S$; ② $BS_1 = S^{-1} \circ \hat{M}^1 \circ S$ 。对于给定的输入差分 α 和输出掩码 ν , 可以根据式②计算 BS_0 和 BS_1 的差分-线性偏差 $DLCT_{BS}(\alpha, \nu)$ 。

4.1 4 轮 PRINCE_{core} 的差分-线性分析

使用 2 轮差分-线性区分器可以攻击 4 轮 PRINCE_{core}, 假设要攻击 PRINCE_{core} 的中间 4 轮, 使用偏差为 0.5 的差分-线性区分器。设中间两轮 R_{mid} 的输入差分为 $\alpha = 0x0100, 0000, 0000, 0000$, 输出掩码为 $\nu = 0x0000, 2000, 0000, 0000$, 对于任意输入 x , $P_r(\alpha \rightarrow \nu) = P_r\{\nu R_{mid}(x) = \nu R_{mid}(x \oplus \alpha)\} = 1$, 因此差分-线性偏差为 $\varepsilon_{\alpha, \nu} = P_r(\alpha \rightarrow \nu) - 0.5 = 0.5$ 。差分-线性分析过程如图 2 所示。

攻击过程如下。

(1) 随机选择 2^5 个明文 $P_i = P_{i,0} \| P_{i,1} \cdots \| P_{i,15}$ ($i = 0, \dots, 2^5 - 1$), 加密得到相应的密文 $C_i = C_{i,0} \| C_{i,1} \cdots \| C_{i,15}$ 。

(2) 设置 2^{12} 个计数器 CT_i ($i = 0, \dots, 2^{12} - 1$), 并将其初始化为 0。

(3) 对于每一个明文 P_i , 猜测密钥 k_1^4 、 k_1^6 和 k_1^7 。

① 对于它们的每一个可能取值, 使用密钥 (k_1^4, k_1^6, k_1^7) 异或明文单元 $(P_{i,4}, P_{i,6}, P_{i,7})$, 得到中间状态值 $(X_{i,4}, X_{i,6}, X_{i,7})$, 分别对其进行 $S(X) \oplus 0x1$ 运算, 对计算结果求 S^{-1} 并异或相应轮密钥, 得到相应的明文单元 $(P_{i,4}^*, P_{i,6}^*, P_{i,7}^*)$ 。令 $P_i^* = P_{i,0} \| \cdots \| P_{i,3} \| P_{i,4}^* \| P_{i,5} \| P_{i,6}^* \| P_{i,7}^* \| P_{i,8} \cdots \| P_{i,15}$, 加密 P_i^* 得到相应密文 $C_i^* = C_{i,0}^* \| C_{i,1}^* \cdots \| C_{i,15}^*$ 。

② 对于每一个密文对 (C_i, C_i^*) , 使用密钥 (k_1^4, k_1^6, k_1^7) 分别对 $(C_{i,4}, C_{i,6}, C_{i,7})$ 和 $(C_{i,4}^*, C_{i,6}^*, C_{i,7}^*)$ 进行异或和 S 运算, 得到中间状态值 $(Y_{i,4}, Y_{i,6}, Y_{i,7})$ 和 $(Y_{i,4}^*, Y_{i,6}^*, Y_{i,7}^*)$ 。

③ 判断 $0x2(Y_{i,4} \oplus Y_{i,6} \oplus Y_{i,7})$ 与 $0x2(Y_{i,4}^* \oplus Y_{i,6}^* \oplus Y_{i,7}^*)$ 是否相等, 如果相等, 将相应的密钥计数器加 1。

表3 PRINCE 算法 S 盒的差分分布
Table 3 The difference distribution of S box of PRINCE

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2^{-2}	0	0	2^{-3}	0	2^{-3}	0	2^{-2}	2^{-3}	0	2^{-3}	0	0	0	0
2	0	2^{-3}	0	2^{-2}	0	0	0	2^{-3}	2^{-3}	0	0	0	0	2^{-2}	2^{-3}	0
3	0	0	0	0	0	2^{-3}	2^{-3}	0	2^{-3}	2^{-3}	2^{-3}	2^{-3}	2^{-3}	0	0	2^{-3}
4	0	2^{-3}	2^{-3}	2^{-2}	2^{-3}	2^{-3}	0	0	2^{-3}	0	2^{-3}	0	0	0	0	0
5	0	0	2^{-3}	2^{-3}	0	2^{-3}	0	2^{-3}	0	2^{-3}	0	2^{-3}	2^{-3}	2^{-3}	0	0
6	0	0	2^{-3}	2^{-3}	0	2^{-3}	2^{-3}	0	0	2^{-3}	0	2^{-3}	0	0	2^{-2}	0
7	0	0	2^{-3}	0	0	0	2^{-3}	0	2^{-3}	0	2^{-2}	0	0	2^{-3}	2^{-3}	2^{-3}
8	0	0	2^{-3}	0	2^{-2}	2^{-3}	0	0	2^{-3}	2^{-3}	0	2^{-3}	0	2^{-3}	0	0
9	0	0	2^{-3}	2^{-3}	0	0	0	0	0	2^{-3}	2^{-3}	0	2^{-2}	2^{-3}	0	2^{-3}
10	0	0	0	2^{-3}	2^{-3}	2^{-2}	0	2^{-2}	2^{-3}	0	0	0	0	0	0	2^{-3}
11	0	2^{-3}	0	0	2^{-2}	0	0	2^{-3}	0	0	0	2^{-3}	2^{-3}	0	2^{-3}	2^{-3}
12	0	2^{-2}	0	0	0	2^{-3}	2^{-3}	0	0	0	2^{-3}	2^{-3}	2^{-3}	0	2^{-3}	0
13	0	2^{-3}	0	0	0	0	0	2^{-3}	0	2^{-2}	2^{-3}	0	0	2^{-3}	2^{-3}	2^{-3}
14	0	0	2^{-3}	0	0	0	2^{-2}	2^{-3}	0	0	0	2^{-3}	2^{-3}	2^{-3}	0	2^{-3}
15	0	0	2^{-3}	0	2^{-3}	0	2^{-3}	2^{-3}	0	0	2^{-3}	0	2^{-3}	0	2^{-3}	2^{-3}

表4 PRINCE 算法 S 盒的线性近似表
Table 4 The linear approximation table of S box of PRINCE

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	2^{-1}	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	-2^{-3}	-2^{-3}	2^{-3}	-2^{-3}	0	2^{-2}	-2^{-2}	0	-2^{-3}	2^{-3}	-2^{-3}	-2^{-3}	0	0
2	0	0	-2^{-2}	0	-2^{-2}	0	0	0	-2^{-3}	-2^{-3}	2^{-3}	-2^{-3}	-2^{-3}	2^{-3}	2^{-3}	2^{-3}
3	0	2^{-2}	-2^{-3}	-2^{-3}	2^{-3}	-2^{-3}	0	0	2^{-3}	2^{-3}	2^{-2}	0	0	0	2^{-3}	-2^{-3}
4	0	0	-2^{-2}	2^{-2}	2^{-3}	2^{-3}	2^{-3}	2^{-3}	2^{-3}	2^{-3}	-2^{-3}	-2^{-3}	0	0	0	0
5	0	0	2^{-3}	2^{-3}	0	-2^{-2}	-2^{-3}	2^{-3}	2^{-3}	-2^{-3}	0	-2^{-2}	-2^{-3}	-2^{-3}	0	0
6	0	-2^{-2}	0	0	-2^{-3}	-2^{-3}	2^{-3}	-2^{-3}	0	2^{-2}	0	0	-2^{-3}	-2^{-3}	2^{-3}	-2^{-3}
7	0	0	2^{-3}	-2^{-3}	0	0	-2^{-3}	2^{-3}	0	2^{-2}	-2^{-3}	-2^{-3}	0	2^{-2}	2^{-3}	2^{-3}
8	0	-2^{-3}	-2^{-3}	0	2^{-2}	-2^{-3}	-2^{-3}	-2^{-2}	-2^{-3}	0	0	-2^{-3}	2^{-3}	0	0	2^{-3}
9	0	-2^{-3}	0	2^{-3}	2^{-3}	0	-2^{-3}	0	2^{-3}	0	2^{-3}	2^{-2}	-2^{-2}	2^{-3}	0	2^{-3}
10	0	2^{-3}	2^{-3}	2^{-2}	0	2^{-3}	-2^{-3}	0	-2^{-2}	2^{-3}	2^{-3}	0	0	-2^{-3}	2^{-3}	0
11	0	-2^{-3}	0	-2^{-3}	2^{-3}	2^{-2}	-2^{-3}	0	0	-2^{-3}	0	-2^{-3}	-2^{-3}	0	2^{-3}	-2^{-2}
12	0	-2^{-3}	-2^{-3}	0	-2^{-3}	0	-2^{-2}	2^{-3}	0	2^{-3}	2^{-3}	0	2^{-3}	0	-2^{-2}	-2^{-3}
13	0	-2^{-3}	0	2^{-3}	0	-2^{-3}	0	2^{-3}	0	-2^{-3}	0	2^{-3}	2^{-2}	2^{-3}	2^{-2}	-2^{-3}
14	0	-2^{-3}	2^{-3}	0	2^{-3}	0	2^{-2}	2^{-3}	-2^{-3}	0	2^{-2}	-2^{-3}	0	2^{-3}	-2^{-3}	0
15	0	2^{-3}	0	2^{-3}	0	-2^{-3}	0	-2^{-3}	-2^{-3}	0	-2^{-3}	0	-2^{-3}	2^{-2}	-2^{-3}	-2^{-2}

(4) 取值最大的计数器对应的部分密钥为正
确候选密钥。通过构造其他列对应的差分-线性区

分器, 可以恢复剩余密钥。

复杂度分析: ① 数据复杂度, 上述攻击共需

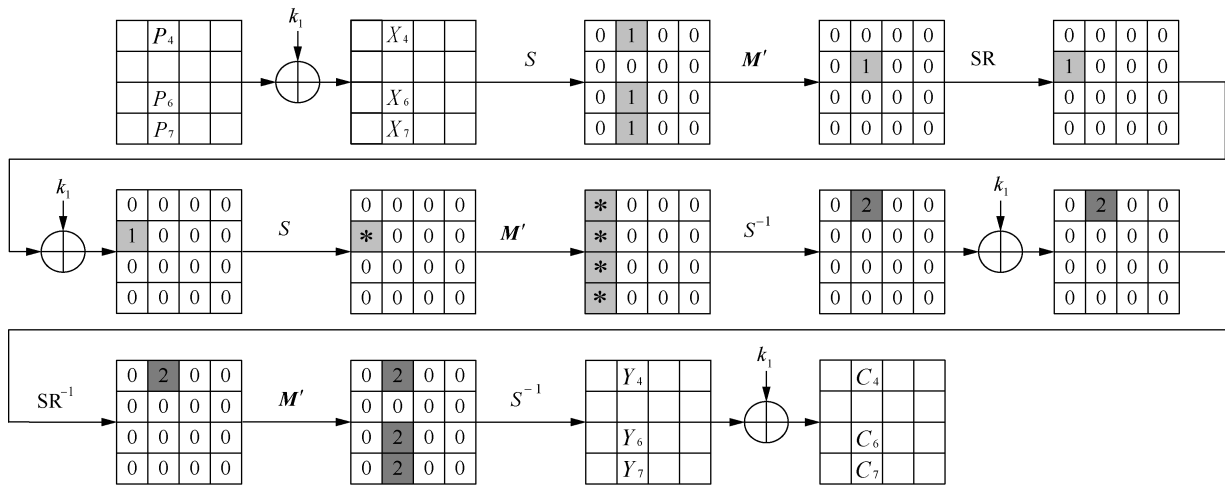


图2 4轮 PRINCE_{core} 的差分-线性分析
Figure 2 Differential-linear cryptanalysis of 4-round PRINCE_{core}

要 2^5 个选择明文对, 因此数据复杂度为 2^6 个选择明文; ② 时间复杂度, 对 2^5 个明文对进行加密共需要 2^6 次 4 轮 PRINCE_{core} 加密运算; 对于 2^{12} 个密钥猜测值, 分别对明、密文对进行 3 次 S 盒运算, 共需要 $2^{12} \times 2^5 \times 2^2 \times \frac{3}{16 \times 4} = 2^{14.58}$ 次 4 轮

PRINCE_{core} 加密运算 (假设每一轮加密需要 16 个 S 盒运算), 因此时间复杂度为 $2^6 + 2^{14.58} \approx 2^{14.58}$ 次加密运算; ③ 存储复杂度, 存储 2^{12} 个计数器需要 2^{12} 个存储单元, 存储复杂度为 2^{12} 。

4.2 6 轮 PRINCE_{core} 的差分-线性分析

6 轮 PRINCE_{core} 的差分-线性攻击仍然可以使用 2 轮差分-线性区分器, 假设要攻击 PRINCE_{core} 的中间 6 轮, 使用偏差为 0.047 的差分-线性区分器。设中间两轮 R_{mid} 的输入差分为 $\alpha = 0x1000, 0000, 0010, 0100$, 输出掩码为 $\nu = 0x2000, 0002, 0000, 0200$, 由于 R_{mid} 中任意两列的变换是相互独立的, 因此可以将 R_{mid} 中的每一列变换看作一个大 S 盒。计算每一个大 S 盒的差分-线性偏差 $DLCT_{BS}(0x1000, 0x2000) = 2^{-2.42}$, $DLCT_{BS}(0x0000, 0x0002) = 2^{-1}$, $DLCT_{BS}(0x0010, 0x0000) = 2^{-1}$, $DLCT_{BS}(0x0100, 0x0200) = 2^{-3}$, 使用堆积引理可以得到 R_{mid} 的差分-线性偏差为 $\varepsilon_{\alpha, \nu} = 2^{-4.42}$ 。差分-线性分析过程如图 3 所示。

攻击过程如下。

(1) 随机选择 $2^{11.84}$ 个明文 $P_i = P_{i,0} \parallel P_{i,1} \cdots \parallel P_{i,15} (i = 0, \dots, 2^{11.84} - 1)$, 加密得到相应的密文

$$C_i = C_{i,0} \parallel C_{i,1} \cdots \parallel C_{i,15}。$$

(2) 设置 2^{16} 个计数器 $CT_i (i = 0, \dots, 2^{16} - 1)$, 并将其初始化为 0。

(3) 对于每一个明文 P_i , 猜测密钥 k_1^0 、 k_1^1 、 k_1^2 和 k_1^3 。

① 对于它们的每一个可能取值, 使用密钥 $(k_1^0, k_1^1, k_1^2, k_1^3)$ 对明文单元 $(P_{i,0}, P_{i,1}, P_{i,2}, P_{i,3})$ 加密一轮, 得到中间状态 $(X_{i,0}, X_{i,1}, X_{i,2}, X_{i,3})$ 。使用 k_1^0 异或 $X_{i,0}$ 得到 $U = k_1^0 \oplus X_{i,0}$, 然后进行 $S(U) \oplus 0x1$ 运算, 对计算结果求 S^{-1} 并使用相同密钥解密一轮, 得到相应的明文单元 $(P_{i,0}^*, P_{i,1}^*, P_{i,2}^*, P_{i,3}^*)$ 。令 $P_i^* = P_{i,0}^* \parallel P_{i,1}^* \parallel P_{i,2}^* \parallel P_{i,3}^* \cdots \parallel P_{i,15}$, 加密 P_i^* 得到相应密文 $C_i^* = C_{i,0}^* \parallel C_{i,1}^* \cdots \parallel C_{i,15}^*$ 。

② 对于每一个密文对 (C_i^*, C_i^*) , 使用密钥 $(k_1^0, k_1^1, k_1^2, k_1^3)$ 分别对 $(C_{i,0}, C_{i,1}, C_{i,2}, C_{i,3})$ 和 $(C_{i,0}^*, C_{i,1}^*, C_{i,2}^*, C_{i,3}^*)$ 解密一轮, 得到中间状态值 $(Y_{i,0}, Y_{i,1}, Y_{i,2}, Y_{i,3})$ 和 $(Y_{i,0}^*, Y_{i,1}^*, Y_{i,2}^*, Y_{i,3}^*)$, 然后分别对 $Y_{i,0}$ 和 $Y_{i,0}^*$ 进行轮密钥加, 得到 V 和 V^* , 最后进行 S 运算, 相应结果记为 $Z = S(V)$ 和 $Z^* = S(V^*)$ 。

③ 判断 $0x2 \cdot Z$ 与 $0x2 \cdot Z^*$ 是否相等, 如果相等, 将相应的密钥计数器加 1。

(4) 取值最大的计数器对应的部分密钥为正确候选密钥。通过构造其他列对应的差分-线性区分器, 可以恢复剩余密钥。

复杂度分析: ① 数据复杂度, 上述攻击共需

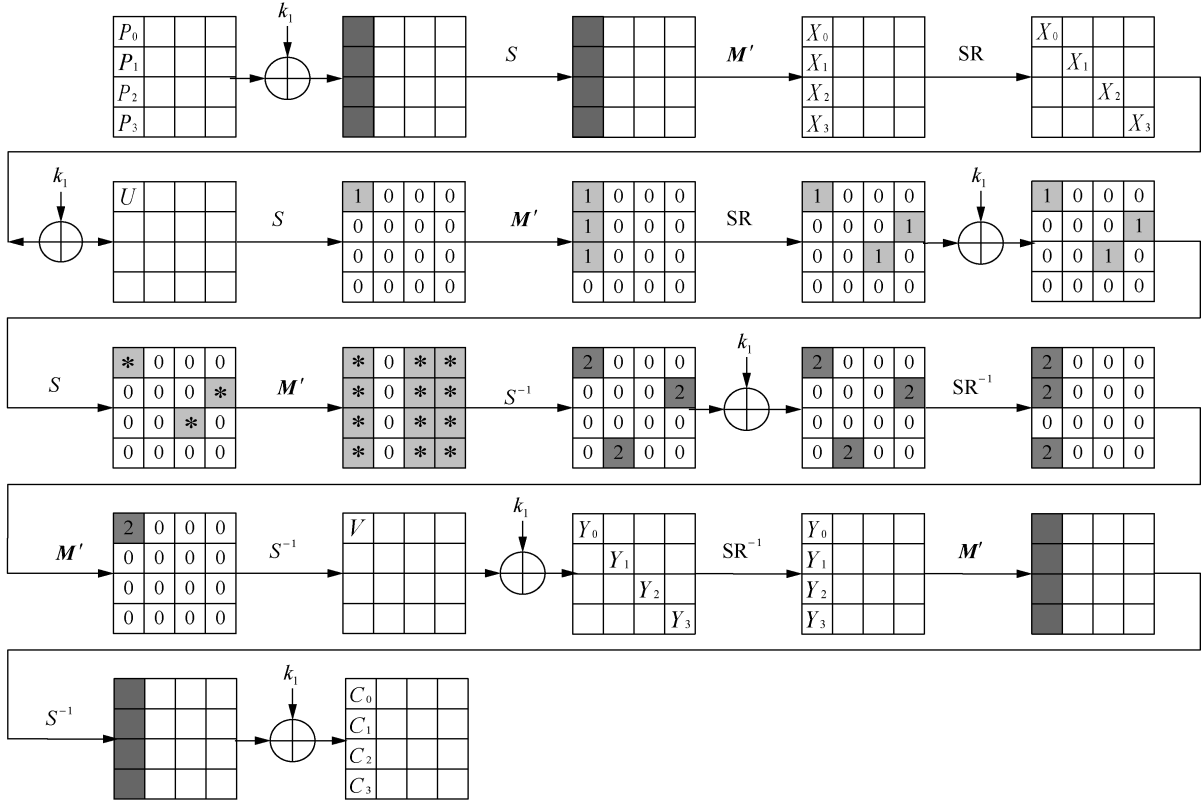


图 3 6 轮 PRINCE_{core} 的差分-线性分析
Figure 3 Differential-linear cryptanalysis of 6-round PRINCE_{core}

要 $2^{11.84}$ 个选择明文对，因此数据复杂度为 $2^{12.84}$ 个选择明文；② 时间复杂度，对 $2^{11.84}$ 个明文对进行加密共需要 $2^{12.84}$ 次 6 轮 PRINCE_{core} 加密运算；对于 2^{16} 个密钥猜测值，分别对明、密文对进行 5 次 S 盒运算，共需要 $2^{16} \cdot 2^{11.84} \cdot 2^2 \cdot \frac{5}{16 \times 6} = 2^{25.58}$

次 6 轮 PRINCE_{core} 加密运算（假设每一轮加密需要 16 个 S 盒运算），因此时间复杂度为 $2^{12.84} + 2^{25.58} \approx 2^{25.58}$ 次加密运算；③ 存储复杂度，存储 2^{16} 个计数器需要 2^{16} 个存储单元，存储复杂度为 2^{16} 。

4.3 7 轮 PRINCE_{core} 的差分-线性分析

使用 3 轮差分-线性区分器可以攻击 7 轮 PRINCE_{core}，设 7 轮 PRINCE_{core} 由 3 轮加密函数、中间两轮变换 R_{mid} 和 2 轮解密函数构成。3 轮差分-线性区分器由 1 轮差分特征和 R_{mid} 的 DLCT 构成，设 1 轮差分特征的输入差分为 $\alpha = 0x1000, 0000, 0010, 0100$ ，输出差分为 β ，差分概率为 $P_r(\alpha \rightarrow \beta)$ 。 R_{mid} 的输入差分为 β ，输出掩码为

$\nu = 0x0000, 2000, 0000, 0000$ ，其差分-线性偏差为 $\epsilon_{\alpha, \nu} = \sum_{\beta} P_r(\alpha \rightarrow \beta) DLCT_{BS}(\beta, \nu)$ 。通过遍历输入差分为 α 的所有可能的 1 轮差分特征，可以得到，3 轮差分-线性区分器的偏差为 $\epsilon_{\alpha, \nu} = 2^{-12.51}$ 。差分-线性分析过程如图 4 所示。

7 轮 PRINCE_{core} 的差分-线性攻击过程与 6 轮类似，这里不再详细描述，下面给出复杂度分析。

复杂度分析：① 数据复杂度，上述攻击共需要 $2^{28.02}$ 个选择明文对，因此数据复杂度为 $2^{29.02}$ 个选择明文；② 时间复杂度，对 $2^{28.02}$ 个明文对进行加密共需要 $2^{29.02}$ 次 7 轮 PRINCE_{core} 加密运算；对于 2^{16} 个密钥猜测值，分别对明、密文对进行 5 次 S 盒运算，共需要 $2^{16} \cdot 2^{28.02} \cdot 2^2 \cdot \frac{5}{16 \times 7} = 2^{41.53}$ 次

7 轮 PRINCE_{core} 加密运算，因此时间复杂度为 $2^{29.02} + 2^{41.53} \approx 2^{41.53}$ 次加密运算；③ 存储复杂度，存储 2^{16} 个计数器需要 2^{16} 个存储单元，存储复杂度为 2^{16} 。

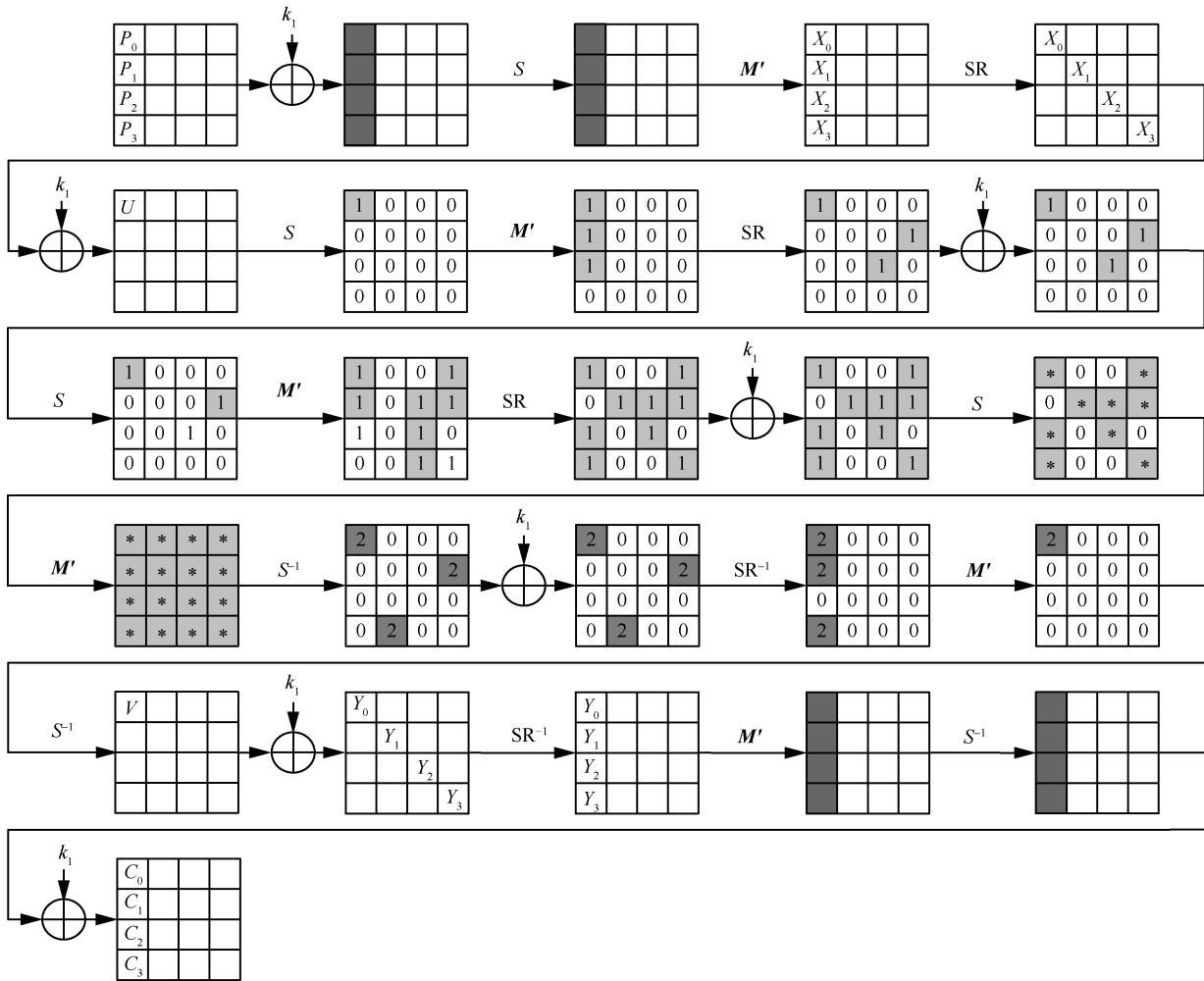


图4 7轮 PRINCE_{core} 的差分-线性分析
Figure 4 Differential-linear cryptanalysis of 7-round PRINCE_{core}

5 实验结果

本文通过实验验证了4轮、6轮和7轮 PRINCE_{core} 的差分-线性区分器的偏差,使用的实验平台为PC机(CPU为Intel Core i3-6100 3.7 GHz,内存为8 GB),程序使用C++编程语言实现,在VS2010软件中进行测试。对于4轮 PRINCE_{core},随机选择 2^{20} 个明文对,每一对明文经过第1轮S盒层的输出差分为0x0000,1011,0000,0000。使用100个随机密钥值进行加密,密文对沿解密方向经过S盒层,计算输出对在掩码0x0000,2022,0000,0000下奇偶性相等的概率及偏差。实验结果显示,在每一个随机密钥下,差分-线性区分器的偏差均为0.5,与理论结果相同。

6轮和7轮 PRINCE_{core} 的验证过程类似,随

机选择 2^{20} 个明文对,每一对明文经过第2轮S盒层的输出差分为0x1000,0000,0000,0000。使用100个随机密钥值进行加密,密文对沿解密方向经过第2轮S盒层,计算输出对在掩码0x2000,0000,0000,0000下奇偶性相等的概率及偏差。最后计算在100个随机密钥下,差分-线性区分器的平均偏差。实验结果显示,6轮差分-线性区分器的平均偏差为 $2^{-4.41}$,7轮差分-线性区分器的平均偏差为 $2^{-12.78}$,与理论分析结果一致。

6 结束语

本文研究了PRINCE算法在差分-线性分析下的安全性,给出了4轮、6轮和7轮 PRINCE_{core} 的差分-线性攻击。使用2轮差分-线性区分器,可以攻击4轮和6轮 PRINCE_{core},其数据复杂度

分别为 2^6 和 $2^{12.84}$ 个选择明文, 时间复杂度分别为 $2^{12.59}$ 和 $2^{25.58}$ 次 4 轮和 6 轮加密, 存储复杂度分别为 2^{12} 和 2^{16} 。7 轮 PRINCE_{core} 的差分-线性攻击需要使用 3 轮区分器, 攻击的数据复杂度为 $2^{29.2}$ 个选择明文, 数据复杂度为 $2^{41.53}$ 次 7 轮加密, 存储复杂度为 2^{16} 。通过本文分析可知, 差分-线性分析对于低轮数的 PRINCE_{core} 非常有效, 攻击的复杂度非常低, 是一种实际的安全威胁。如何扩展差分-线性分析的攻击轮数, 是下一步要研究的问题。

参考文献:

- [1] BORGHO J, CANTEAUT A, GÜNEYSU T, et al. PRINCE: a low-latency block cipher for pervasive computing applications[C]//ASIACRYPT 2012. 2012: 208-225.
- [2] KILIAN J, ROGAWAY P. How to protect DES against exhaustive key search (an analysis of DESX)[J]. Journal of Cryptology, 2021. 14(1): 17-35.
- [3] JEAN J, NIKOLIC I, PEYRIN T, et al. Security analysis of PRINCE[C]//International Workshop on Fast Software Encryption (FSE) 2013. 2013: 92-111.
- [4] SOLEIMANY H, BLONDEAU C, YU X L, et al. Reflection cryptanalysis of PRINCE-like ciphers[C]//International Workshop on Fast Software Encryption (FSE) 2013. 2013: 71-91.
- [5] CANTEAUT A, NAYA-PLASENCIA M, VAYSSIÈRE B. Sieve-in-the-middle improved MITM attacks[C]//Advances in Cryptology - CRYPTO. 2013: 222-240.
- [6] CANTEAUT A, FUHR T, GILBERT H, et al. Multiple differential cryptanalysis of round-reduced PRINCE[C]//International Workshop on Fast Software Encryption (FSE). 2014: 591-610.
- [7] DERBEZ P, PERRIN L. Meet-in-the-middle attacks and structural analysis of round-reduced PRINCE[C]//International Workshop on Fast Software Encryption(FSE). 2014: 190-216.
- [8] THE PRINCE TEAM. PRINCE challenge[R].
- [9] 段春晖, 谭林, 戚文峰. 减轮 PRINCE 的混合差分分析[J]. 信息工程大学学报, 2019, 20(6): 695-701.
DUAN C H, TAN L, QI W F. Mixture differential cryptanalysis on round-reduced PRINCE[J]. Journal of Information Engineering University, 2019, 20(6): 695-701.
- [10] ABED F, LIST E, LUCKS S. On the security of the core of prince against Biclique and differential cryptanalysis[R]. 2012.
- [11] ZHAO G Y, SUN B, LI C, et al. Truncated differential cryptanalysis of PRINCE[J]. Security and Communication Networks, 2015(8): 2875-2887.
- [12] LI L B, JIA K T, WANG X Y. Improved meet-in-the-middle attacks on AES-192 and PRINCE[R].
- [13] 魏悦川, 潘晓中, 戎宜生, 等. 对 PRINCE 分组密码的不可能差分攻击[J]. 西安电子科技大学学报, 2017, 44(1): 119-124.
WEI Y C, PAN X Z, RONG Y S, et al. Impossible differential cryptanalysis on the PRINCE[J]. Journal of Xidian University, 2017, 44(1): 119-124.
- [14] 袁征, 彭真. 轻量级分组密码 PRINCE 算法的 Biclique 分析[J]. 密码学报, 2017, 4(6): 517-527.
YUAN Z, PENG Z. Biclique cryptanalysis of lightweight block cipher PRINCE[J]. Journal of Cryptologic Research, 2017, 4(6): 517-527.
- [15] BIHAM E, SHAMIR A. Differential cryptanalysis of DES-like cryptosystems[J]. Journal of Cryptology, 1991, 4(1): 3-72.
- [16] MATSUI M. Linear cryptanalysis method for DES cipher[C]//Advances in Cryptology-Proceedings of EUROCRYPT '93. 1993: 386-397.
- [17] LANGFORD S K, HELLMAN M E. Differential-linear Cryptanalysis[C]//Advances in Cryptology-proceedings of CRYPTO '94. 1994: 17-25.
- [18] BIHAM E, DUNKELMAN O, KELLER N. Enhancing differential-linear cryptanalysis[C]//Advances in Cryptology-proceedings of ASIACRYPT 2002. 2002: 254-266.
- [19] LIU Z Q, GU D W, ZHANG J, et al. Differential-multiple linear cryptanalysis[C]//Proceedings of Information Security and Cryptology (In-scrypt 2009). 2009: 35-49.
- [20] LU J Q. A methodology for differential-linear cryptanalysis and its applications[J]. Des Codes Cryptography, 2015, 77(1): 11-48.
- [21] BLONDEAU C, LEANDER G, NYBERG K. Differential-linear cryptanalysis revisited[J]. Journal of Cryptology, 2017, 30(3): 859-888.
- [22] CHABAUD F, VAUDENAY S. Links between differential and linear cryptanalysis[C]//Advances in Cryptology-Proceedings of EUROCRYPT '94, 1994: 356-365.
- [23] BLONDEAU C, NYBERG K. New links between differential and linear cryptanalysis[C]//Advances in Cryptology-Proceedings of EUROCRYPT 2013. 2013: 388-404.
- [24] BAR-ON A, DUNKELMAN O, KELLER N, et al. DLCT: a new tool for differential-linear cryptanalysis[C]//EUROCRYPT 2019. 2019: 313-342.

[作者简介]



刘正斌 (1985-), 男, 山东青岛人, 保密通信重点实验室工程师, 主要研究方向为密码学理论、对称密码分析。