Higher Order Differential Cryptanalysis

Marcel Nageler — Graz, 2019-11-23

2019-11-23

Table of Contents

Differential Cryptanalysis

Definition

For $f : S \to T$ we define the (first order) derivate at point a as

$$\Delta_a f(x) = f(x+a) - f(x)\,.$$

Idea: maximise $Pr(\Delta_a f(x) = b)$

Table 1: Differential Distribution Table of a 4-bit S-box

	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
0	16	.	.	.	.	.	.	.	.	.	.	.	.	.	.	.
1	.	.	.	2	6	.	.	4	.	2	.	.	.	.	2	.
2	.	.	.	.	6	2	.	.	6	2	.	.	.	.	.	.
3	.	2	.	4	.	.	.	2	.	.	2	.	6	.	.	.
4	.	.	.	.	.	2	4	2	.	2	2	.	2	2	.	.
5	.	2	4	.	2	.	.	.	2	.	.	.	.	2	4	.
6	.	2	4	2	2	2	.	.	.	.	.	.	.	2	2	.
7	.	2	.	.	.	2	4	.	.	2	4	.	.	2	.	.
8	.	4	.	.	.	.	.	.	.	.	2	2	.	4	2	2
9	.	.	.	.	.	2	2	.	2	4	2	.	.	.	2	2
a	.	.	2	2	.	4	.	.	.	4	2	2	.	.	.	.
b	.	2	2	.	.	.	2	2	.	.	.	.	2	4	2	.
c	.	2	.	.	.	.	.	6	4	.	2	.	2	.	.	.
d	.	.	.	6	.	.	2	.	.	.	.	2	.	.	2	4
e	.	.	2	.	.	2	.	.	2	.	.	.	4	.	.	6
f	.	.	2	.	.	.	2	.	.	.	.	10	.	.	.	2

Second Order Differentials

What if we differentiate again?

$$
\begin{aligned}
\Delta^{(2)}_{a_1,a_2} f(x) &= \Delta_{a_2}\Delta_{a_1} f(x) \\
&= \Delta_{a_2}\big(f(x+a_1) - f(x)\big) \\
&= f(x+a_1+a_2) - f(x+a_1) - f(x+a_2) + f(x)
\end{aligned}
$$

Higher Order Differentials [Lai94]

Definition

For $f : S \to T$ we define the *derivate of order i* at points $a_1, \ldots, a_i$ as

$$\Delta^{(i)}_{a_1,\ldots,a_i} f(x) = \Delta_{a_i} \Delta^{(i-1)}_{a_1,\ldots,a_{i-1}} f(x).$$

Properties

Theorem

Let $\deg(f)$ *denote the degree of a polynomial. Then*

$$\deg\left(\Delta_a f(x)\right) \leq \deg\left(f(x)\right) - 1$$

Theorem

Let f *be a function of degree* d *and* $a_1, \dots, a_d$ *linearly independent points. Then*

$$\Delta^{(d)}_{a_1,\dots,a_d} f(x) = c$$

Derivative of a binary function

Let f be a binary function and $\mathcal{L}$ denote the set of linear combinations.

$$\Delta^{(i)}_{a_1,\dots,a_i} f(x) = \sum_{c \in \mathcal{L}[a_1,\dots,a_n]} f(x \oplus c)$$

Zero-Sum Distinguishers

Definition

A *zero sum* for a function f is a set of inputs $x_1, \ldots, x_s$ such that

$$\sum_{i=1}^{s} x_i = \sum_{i=1}^{s} f(x_i) = 0 \,.$$

- Allows us to distinguish f from a random permutation.
- Should be hard to find

Zero sum from higher order differential

If

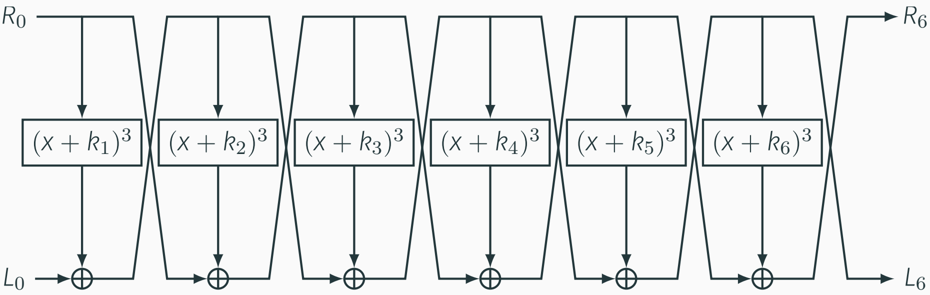
$$\deg(f) = d$$

then

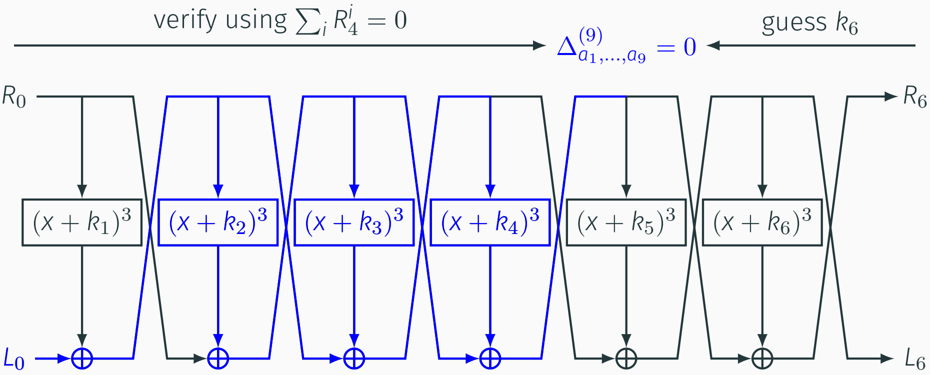
$$\Delta^{(d+1)}_{a_1,\dots,a_{d+1}} f(x) = \sum_{c \in \mathcal{L}[a_1,\dots,a_{d+1}]} f(x \oplus c) = 0$$

The $\mathcal{PURE}$ cipher

- Feistel structure
- $F(x, k) = (x + k)^3$ in $GF(2^{32})$



A Key Recovery Attack on a $\mathcal{PURE}$ [JK97]



Questions?

Higher Order Differential Cryptanalysis

Marcel Nageler — Graz, 2019-11-23

2019-11-23

References

Thomas Jakobsen and Lars R Knudsen.
The interpolation attack on block ciphers.
In *International Workshop on Fast Software Encryption*, pages 28–40. Springer, 1997.

Lars R Knudsen.
Truncated and higher order differentials.
In *International Workshop on Fast Software Encryption*, pages 196–211. Springer, 1994.

Xuejia Lai.
Higher order derivatives and differential cryptanalysis.
In *Communications and Cryptography*, pages 227–233. Springer, 1994.