PRINT Cipher

Aayush Deshmukh[1,2], Aman Khan[1] and Manohar Das[1]

[1] Institute A, City, Country, jane@institute
[2] Institute B, City, Country, john@institute

Abstract. In this paper we prove that the One-Time-Pad has perfect security.

Keywords: Something · Something else

1 Introduction

Widely used primitives like the AES [**?**] do not have perfect security, and can be analysed with linear cryptanalysis [**?**], differential cryptanalysis [**?**], or differential power analysis [**?**]. We show that the One-Time-Pad is unconditionally secure in Section 2.

2 Main Result

2.1 Sbox Analysis

The sbox for the PRINT cipher is a 3-bit to 3-bit. Since input is 3-bit so for a b-bit block, the sbox is applied $\frac{b}{3}$ parallely. The current state for the sbox is a $\frac{b}{3}$ words, for each word same sbox is used and the next state is the concatenation of outputs.It is a balanced sbox and has a linear structure.The sbox is given in the following table :-

x	0	1	2	3	4	5	6	7
s[x]	0	1	3	6	7	4	5	2

2.1.1 Difference Distribution Table

The sbox has a differential branch number defined as $\min_{v,\, w \neq v} \{wt(v \oplus w) + wt(S(v) \oplus S(w))\}$ of **2**. The difference distribution table (ddt) which is generated using Sage is as follows :-

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	2
3	0	2	2	0	0	2	2	0
4	0	0	0	0	2	2	2	2
5	0	2	0	2	2	0	2	0
6	0	0	2	2	2	2	0	0
7	0	2	2	0	2	0	0	2

2.1.2 Linear Approximation Table

The linear branch number which is defined as $\min_{\alpha \neq, \beta, \mathrm{LAM}(\alpha,\beta)\neq 0}\{\mathrm{wt}(\alpha) + \mathrm{wt}(\beta)\}$ for this sbox is **2**. The linearity of this sbox is **4**. The linear approximation table generated from Sage is as follows:-

	0	1	2	3	4	5	6	7
0	4	0	0	0	0	0	0	0
1	0	-2	0	2	0	2	0	2
2	0	0	2	2	0	0	2	-2
3	0	2	-2	0	0	2	2	0
4	0	0	0	0	2	-2	2	2
5	0	2	0	2	2	0	-2	0
6	0	0	2	-2	2	2	0	0
7	0	2	2	0	-2	0	0	2

2.1.3 Additional Properties of Sbox

1. The component funcion in 3 variables in algebraic normal form of the sbox is

x0*x2 + x0 + x1*x2

2. The interpolation polynomial for the sbox is

$$\mathbf{(a + 1)x^6 + (a^2 + a + 1)x^5 + (a^2 + 1)x^3}$$

3. The polynomials which satisfy the sbox is

- x0*x2 + x0 + x1 + y1
- x0*x1 + x0 + x1 + x2 + y2
- x0*y1 + x0 + x2+ y1 + y2
- x0*y2 + x1 + y1

- x1*x2 + x0 + y0
- x1*y0 + x1 + x2 + y0 + y2
- x0*y0 + x1*y1 + x2 + y2
- x1*y2 + x0 + x1 + y0
- x2*y0 + x1 + y0 + y1
- x2*y1 + x0 + y0
- x0*y0 + x2*y2 + x0 + x1 + x2 + y0 + y1
- y0*y1 + x2 + y0 + y1 + y2
- y0*y2 + x1 + y1
- y1*y2 + x0+ y0 + y1

x - input variables y - output variables

4. Maximum degree of component function - 2

5. Minimum degree of component function - 2

6. Maximal differential probability - 0.25

7. Absolute maximal linear bias - 2

8. Relative maximal linear bias - 0.25

References