Algebraic and Higher-Order Differential Cryptanalysis of Pyjamask-96

C. Dobraunig, Y. Rotella, J. Schoone

ESCADA

28 February 2020

Pyjamask

Pyjamask is a second-round candidate for the NIST lightweight competition, by Goudarzi, Jean, Kölbl, Peyrin, Rivain, Sasaki, Sim

1. Pyjamask-128-AEAD
   1. based on Pyjamask-128
   2. uses OCB as mode
2. Pyjamask-96-AEAD
   1. based on Pyjamask-96
   2. uses OCB as mode

Focus on the block cipher Pyjamask-96.

Key recovery attack on full-round Pyjamask-96

Round Function

Pyjamask-96 state:

x_0	x_1	x_2	x_3	x_4	x_5	x_6	x_7	x_8	x_9	x_{10}	x_{11}	x_{12}	x_{13}	x_{14}	x_{15}	x_{16}	x_{17}	x_{18}	x_{19}	x_{20}	x_{21}	x_{22}	x_{23}	x_{24}	x_{25}	x_{26}	x_{27}	x_{28}	x_{29}	x_{30}	x_{31}
x_{32}	x_{33}	x_{34}	x_{35}	x_{36}	x_{37}	x_{38}	x_{39}	x_{40}	x_{41}	x_{42}	x_{43}	x_{44}	x_{45}	x_{46}	x_{47}	x_{48}	x_{49}	x_{50}	x_{51}	x_{52}	x_{53}	x_{54}	x_{55}	x_{56}	x_{57}	x_{58}	x_{59}	x_{60}	x_{61}	x_{62}	x_{63}
x_{64}	x_{65}	x_{66}	x_{67}	x_{68}	x_{69}	x_{70}	x_{71}	x_{72}	x_{73}	x_{74}	x_{75}	x_{76}	x_{77}	x_{78}	x_{79}	x_{80}	x_{81}	x_{82}	x_{83}	x_{84}	x_{85}	x_{86}	x_{87}	x_{88}	x_{89}	x_{90}	x_{91}	x_{92}	x_{93}	x_{94}	x_{95}

1. AddRoundKey: linear key schedule applied to key of 128 bits
2. SubBytes: [1,3,6,5,2,4,7,0] on columns (degree 2)
3. MixRows: circulant binary matrix to rows

Pyjamask-96 consists of 14 rounds

Higher order derivatives

Definition 1 (Derivative (Lai 1994))

Let $F\colon \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$ be given. Then the derivative of F to a is $\Delta_a F(x) = F(x+a) + F(x)$

Properties:

- $\Delta_{a_k}\Delta_{a_{k-1}}\cdots\Delta_{a_1}F(x) = \sum_{v\in[\![a_1,\ldots,a_k]\!]} F(x+v)$
- $\deg \Delta_V F(x) \leq \deg F - \dim V$
- If $\dim V > \deg F$, then we have $\Delta_V F(x) = 0$

Cube attack

The degrees of the n-round versions of Pyjamask-96 are upper bounded by

n	1	2	3	4	5	6	7	8	9	10	11+
degree	2	4	8	16	32	64	80	88	92	94	95

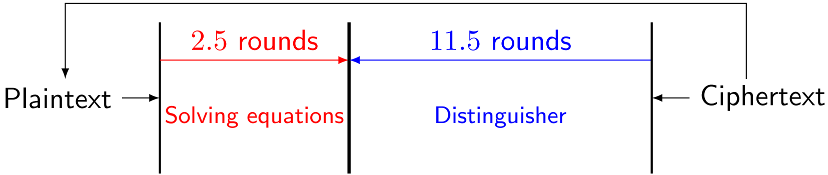
Bounds by Boura, Canteaut, De Cannière [FSE2011]

Affine spaces V of dimension 94 give distinguisher

$$\sum_{v \in V} \mathrm{Pyj}_K^{10}(x+v) = C^{\mathrm{st}}$$

Same for Pyj^{-1}!

Meet-in-the-Middle



1. Smartly choosing affine ciphertext space gives 11 rounds instead
2. Taking key-bits as variables gives system of equations
   - Full codebook gives 448 equations
   - Too many monomials
3. Smart guesses to reduce number of monomials
   - Guessing 100 bits reduces to 411 monomials

Solving the system of equations

Solving a system of polynomials equations is hard.

Solving a system of linear equations is easy.

$\implies$ Linearization: Assign a new variable to every monomial of degree > 1.

Example 2

$$\begin{cases} x_0x_1 + x_2 = 1 \\ x_0 + x_1 + x_2 = 0 \\ x_0x_1 + x_1 = 0 \\ x_1x_2 + x_0 = 1 \\ x_0 + x_1 = 0 \end{cases} \implies \begin{cases} {\color{red}y_0} + x_2 = 1 \\ x_0 + x_1 + x_2 = 0 \\ {\color{red}y_0} + x_1 = 0 \\ {\color{red}y_1} + x_0 = 1 \\ x_0 + x_1 = 0 \end{cases}$$

Complexities

Rounds	Time (in Pyjamask-96 calls)	Data (in blocks)
14/14	2^{115}	2^{96}
13/14	2^{99}	2^{96}
12/14	2^{96}	2^{96}
11/14	2^{91}	2^{95}
10/14	2^{83}	2^{87}
9/14	2^{67}	2^{71}
8/14	2^{35}	2^{39}
7/14	2^{27}	2^{23}

Further Research

1. Attacking Pyjamask-96 with better complexities
2. Attacking Pyjamask-128
3. Attacking Pyjamask-96-AEAD
   - We got to 7 rounds with 2^{86} time complexity, 2^{41} data
4. Attacking Pyjamask-128-AEAD