Radboud University

Algebraic and Higher-Order Differential Cryptanalysis of Pyjamask-96

C. Dobraunig, Y. Rotella, J. Schoone

FSE, 12 November 2020

ESCADA

Pyjamask

Pyjamask is a 2^{nd}-round candidate for the NIST lightweight competition

by Goudarzi, Jean, Kölbl, Peyrin, Rivain, Sasaki and Sim.

- Pyjamask-128-AEAD
  - based on Pyjamask-128
  - uses OCB as mode
- Pyjamask-96-AEAD
  - based on Pyjamask-96
  - uses OCB as mode

Key recovery attack on full-round Pyjamask-96

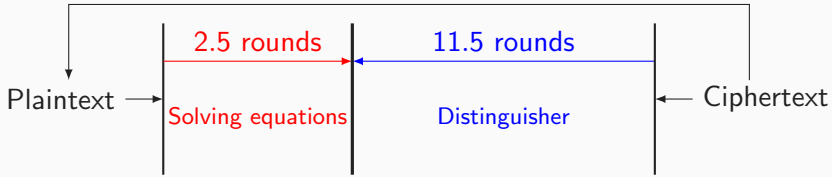
Higher order derivatives

Bounds by Boura, Canteaut, De Cannière [2011]

Theory of higher order derivatives by Lai [1994]

Certain affine spaces V of dimension 94 give distinguisher

$$\sum_{v \in V} \mathrm{Pyj}_K^{11}(x + v) = C^{\mathrm{st}}$$



Solving equations

- Taking key-bits as variables gives system of equations
- Linearise to solve linear system of monomials
- Reducing number of monomials:
  - S-box properties

$$(L \circ S)(P) + (L \circ S)(K_0) + K_1 + \sum_{\substack{i,j \in I \\ |I|=11,13}} p_i k_j + p_j k_i$$

    - Equivalent key: $\kappa = (L \circ S)(K_0) + K_1$,
    - Equivalent plaintext: $P' = (L \circ S)(P)$
  - Guess 100 round-key bits

Conclusions and future research

- Key-recovery attack with a complexity of 2^{115} on full-round Pyjamask-96
- Future: attack Pyjamask-96-AEAD or Pyjamask-128-AEAD