Algebraic and Higher-Order Differential Cryptanalysis of Pyjamask-96

C. Dobruiig, Y. Rotella, J. Schoone
FSE 2020
Pyjamask is a 2\textsuperscript{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

We focused on the block cipher Pyjamask-96.

Key recovery attack on full-round Pyjamask-96
Pyjamask-96 state \( x_i \in \{0,1\} \):

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

- **AddRoundKey**: linear key schedule applied to key of 128 bits
- **SubBytes**: a 3-bit S-box of degree 2
- **MixRows**: circulant binary matrix to rows

Pyjamask-96 consists of **14 rounds**.
Definition (Derivative [Lai, 1994])

Let $F : \mathbb{F}_2^n \to \mathbb{F}_2^n$ and $a \in \mathbb{F}_2^n$ be given.

Then the derivative of $F$ to $a$, $\Delta_a F$ is: $\Delta_a F(x) = F(x + a) + F(x)$.

Properties:

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

Degrees of the $n$-round versions of Pyjamask-96 are upper bounded by

<table>
<thead>
<tr>
<th>$n$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11+</th>
</tr>
</thead>
<tbody>
<tr>
<td>degree</td>
<td>2</td>
<td>4</td>
<td>8</td>
<td>16</td>
<td>32</td>
<td>64</td>
<td>80</td>
<td>88</td>
<td>92</td>
<td>94</td>
<td>95</td>
</tr>
</tbody>
</table>

Bounds by Boura, Canteaut, De Cannière [2011]

Affine spaces $V$ of dimension 94 give distinguisher

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

Same for the inverse of Pyjamask-96!
Meet-in-the-middle

- Smartly choosing affine ciphertext space gives 11 rounds instead
- $\mathcal{U} = \{ u \in \mathbb{F}_2^{96} \mid u_0 = u_{32} = u_{64} = 0 \}$ has codimension 3
- $\mathcal{V}_0 = \{0, v\}$ where $v_i = 0$ for all $i \in \{1, \ldots, 31, 33, \ldots, 63, \ldots, 95\}$
- $\mathcal{V} = \mathcal{U} \oplus \mathcal{V}_0$ has dimension 94 and
- $\sum_{v \in \mathcal{V}} \text{Proj}_{K}^{11}(x + v)$ constant
Solving equations

- Taking key-bits as variables gives system of equations
- Linearise to solve linear system of monomials
  - Full codebook gives 448 equations
  - Too many monomials
Reducing monomials

- Reducing in S-box:

\[
S(P + K)_0 = (p_0 + k_0)(p_2 + k_2) + p_1 + k_1 \\
= S(P)_0 + S(K)_0 + p_0 k_2 + p_2 k_0
\]

- Applying further MixRows and AddRoundKey:

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

- Equivalent key: \( \kappa = (L \circ S)(K_0) + K_1 \),
- Equivalent plaintext: \( P' = (L \circ S)(P) \)
- Still too many monomials
• Guess-and-determine on roundkey bits
  • Guess all bits in first roundkey:
    • 96 guesses $\rightarrow$ 569 monomials
  • Guess four more bits in the second roundkey:
    • 100 guesses $\rightarrow$ 411 monomials
• Introduces a $2^{100}$ factor in computation
<table>
<thead>
<tr>
<th>Rounds</th>
<th>Time (in Pyjamask-96 calls)</th>
<th>Data (in blocks)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7/14</td>
<td>$2^{27}$</td>
<td>$2^{23}$</td>
</tr>
<tr>
<td>8/14</td>
<td>$2^{35}$</td>
<td>$2^{39}$</td>
</tr>
<tr>
<td>9/14</td>
<td>$2^{67}$</td>
<td>$2^{71}$</td>
</tr>
<tr>
<td>10/14</td>
<td>$2^{83}$</td>
<td>$2^{87}$</td>
</tr>
<tr>
<td>11/14</td>
<td>$2^{91}$</td>
<td>$2^{95}$</td>
</tr>
<tr>
<td>12/14</td>
<td>$2^{96}$</td>
<td>$2^{96}$</td>
</tr>
<tr>
<td>13/14</td>
<td>$2^{99}$</td>
<td>$2^{96}$</td>
</tr>
<tr>
<td>14/14</td>
<td>$2^{115}$</td>
<td>$2^{96}$</td>
</tr>
</tbody>
</table>
Further research

• Attacking Pyjamask-96-AEAD
  • We got to 7 rounds with $2^{86}$ time complexity, $2^{41}$ data.
• Attacking Pyjamask-128-AEAD