Algebraic Cryptanalysis of STARK-Friendly JARVIS and FRIDAY

Martin R. Albrecht, Carlos Cid, Lorenzo Grassi, Dmitry Khovratovich, Reinhard Lüftenegger, Christian Rechberger, Markus Schofnegger

27 March 2019
Design

- JARVIS: block cipher, FRIDAY: hash function
- Primitives proposed by T. Ashur and S. Dhooge [AD18]
- Goal: efficiency in STARK setting
- Some security arguments borrowed from the AES
Design cont.

- Very similar in structure to MiMC [Alb+16]:

\[ s_i \xrightarrow{k \oplus c_i} x^3 \xrightarrow{\oplus} s_{i+1} \Rightarrow s_i \xrightarrow{S} B^{-1} \xrightarrow{C} s_{i+1} \]

- \( S(x) = x^{2^n-2} \)
- Affine polynomials \( B, C \) of degree 4
- 10-14 rounds (depending on block size)
Attack Idea

- Exploit two facts:
  - Low degree of affine polynomials $B$ and $C$
  - $\forall x \neq 0 : x^{2^n-2} = x^{-1}, \quad y = x^{-1} \implies xy = 1$

- Procedure:
  1. Describe round from both sides and connect S-box parts with degree-2 equation
  2. Compute a Gröbner basis and solve for the unknown variables (round keys...)
Equation System

- Intermediate variable for every second round (after optimization)
- Every round key a linear function of the master key
- System for e.g. FRIDAY (assume $r$ even):
  - $n_e = \frac{r}{2}$ equations of degree 32
  - $n_v = \frac{r}{2}$ variables
## Results on FRIDAY

Generic formula for complexity estimation and setting linear algebra constant to $\omega = 2$:

<table>
<thead>
<tr>
<th>$r$</th>
<th>$n_v$</th>
<th>$D_{reg}$</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 (JARVIS-128)</td>
<td>5</td>
<td>156</td>
<td>59 bits</td>
</tr>
<tr>
<td>12 (JARVIS-192)</td>
<td>6</td>
<td>187</td>
<td>72 bits</td>
</tr>
<tr>
<td>14 (JARVIS-256)</td>
<td>7</td>
<td>218</td>
<td>85 bits</td>
</tr>
<tr>
<td>40</td>
<td>20</td>
<td>621</td>
<td>250 bits</td>
</tr>
</tbody>
</table>

Full results + practical verification to be published soon™!