TU Graz

SCIENCE
PASSION
TECHNOLOGY

# Algebraic Cryptanalysis of STARK-Friendly JARVIS and FRIDAY

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

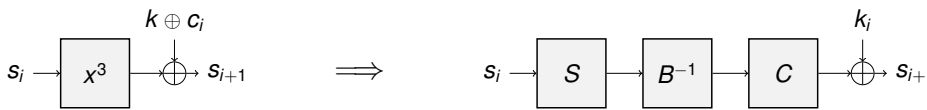
27 March 2019

# 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]:




- $S(x) = x^{2^n-2}$
- 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 $C$
  - $\forall x \neq 0 : x^{2^n-2} = x^{-1}, y = x^{-1} \implies xy = 1$
  - 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 $\omega = 2$:

| $r$ | $n_v$ | $D_{reg}$ | Security level |
|---|---|---|---|
| 10 (JARVIS-128) | 5 | 156 | 59 bits |
| 12 (JARVIS-192) | 6 | 187 | 72 bits |
| 14 (JARVIS-256) | 7 | 218 | 85 bits |
| 40 | 20 | 621 | 250 bits |

Full results + practical verification to be published soon$^{TM}$!