# Cryptanalysis Results on the NIST Candidate Gimli (WIP)

Antonio Flórez Gutiérrez, Gaëtan Leurent, María Naya-Plasencia, Léo Perrin, André Schrottenloher, Ferdinand Sibleyras

Inria, France


# Context

- Gimli is a permutation proposed by Bernstein *et al.* (CHES 2017) *and* a candidate in the second round of the NIST lightweight crypto competition
- We study the permutation and Gimli-Hash

The permutation operates on a 384-bit state:

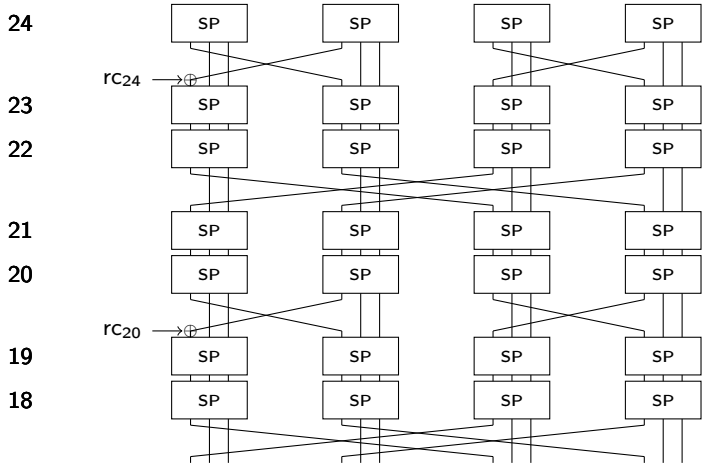
- 4 "columns" of $96 = 3 \times 32$ bits
- each column has three 32-bit "words" $x$, $y$, $z$

It applies 24 rounds of:

- SP-Box on each column
- (Every 2 rounds) "big" or "small" swap: swaps the $x$ words between some columns
- (Every 4 rounds) Constant addition

# Illustration

# Illustration (ctd.)



# Distinguishers on the full permutation

## Limited-birthday distinguishers

We create a state $s$ such that $s$ and Gimli($s$) both have 2 identical columns (up to swap / constant addition).

- in time $2^{64}$ (instead of $2^{96}$) for full Gimli (24 rounds)
- in practical time for 20-round Gimli (round 23 to 4 included)

Idea: start from the middle and complete the middle state column by column (each swap brings a new condition to satisfy in order to retain the symmetry).

| | | | | |
|---|---|---|---|---|
| | f40cdb12 | 4746a811 | 443446fe | 4746a811 |
| Input: | 1b4fe79a | ac3eccd5 | 9872eabf | ac3eccd5 |
| | aff58474 | 65bbdee1 | 9afd2e36 | 65bbdee1 |
| | fecdc4cf | c75aa57f | 60fabdcb | 6c045e77 |
| Output: | 38ae0737 | 2e9327ff | d8a3651b | 2e9327ff |
| | 6252d3bf | 0ca56547 | 4c6f878a | 0ca56547 |

# Collisions on reduced-round Gimli-Hash

Gimli-hash is a sponge where the 128-bit rate contains the $x$ word of each column.
Using the slow diffusion and the SP-Box, we found full-state collisions:

- up to 12 rounds
- up to 14 rounds quantumly
- practically up to 8 rounds (21 to 14):

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| First message block | | | | | | | |
| dc84bf38 | 00000000 | 00000000 | 00000000 | dc84bf38 | 00000000 | 00000000 | 00000000 |
| Second message block | | | | | | | |
| bbdb41f3 | 4333192c | bc17e444 | 8a9d06c7 | 1b1da6e4 | 4333192c | bc17e444 | 8a9d06c7 |
| Third message block | | | | | | | |
| 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | 00000000 | afad801e | 00000000 |

# Ongoing work

- investigate linear trails in the permutation
- performing differential-linear cryptanalysis (Even-Mansour Gimli cipher):
  - 16 rounds with complexity $2^{137.4}$
  - 17 rounds with complexity $2^{156.8}$
- dominate the NIST lightweight competition

Thanks you for your attention!