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:

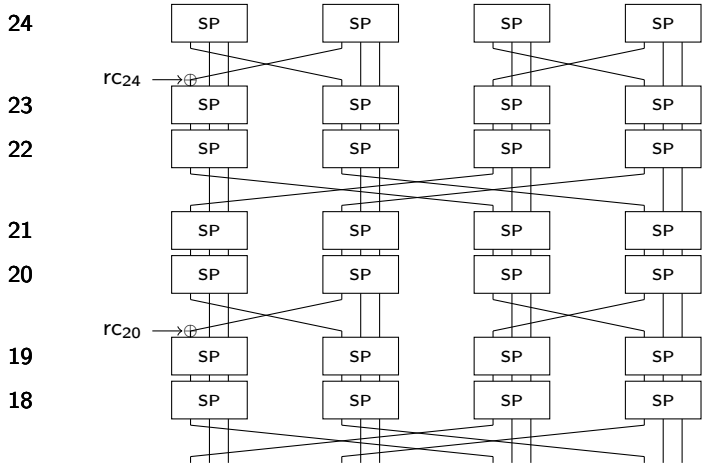
- 4 "columns" of $96 = 3 \times 32$ bits
- each column has three 32-bit "words" x, y, z

It applies 24 rounds (24 to 1) of:

- SP-Box on each column
- (Every 2 rounds) "big" or "small" swap: swaps the x words between pairs of 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.

We can distinguish:

- full Gimli (rounds 24 to 1) in time 2^{64} and constant memory
- **28**/24 rounds (27 to 0) with the same attack
- **23**/24 rounds (23 to 1) in practical time

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).

	7f9fcf70	6aedf7e6	7f9fcf70	cb2f0e6a
Input:	0ba2f1f9	f339b619	0ba2f1f9	f70cf15c
	b2ee8259	df0b4801	b2ee8259	3856106d
	a8ef848d	8c17b743	9615b3bc	8c17b743
Output:	541122c5	30530879	8d9d5d30	30530879
	74b6dbe6	18885a6e	744b55c1	18885a6e

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!