Cryptanalysis of Reduced Gimli-Hash

Fukang Liu[1,3], Takanori Isobe[2,3],Willi Meier[4]

[1]East China Normal University, China
[2]NICT, Japan
[3]University of Hyogo, Japan
[4]FHNW, Windisch, Switzerland

Dec. 13, 2019

Background

◊ NIST Lightweight Cryptography Standardization process

- Start: 2013
- Call For Submissions: 2018
- Public (the first round): April 18, 2019
- Number (the first round): 56 candidates
- Public (the second round): Aug. 31, 2019
- Number (the second round): 32 candidates

◊Third-party cryptanalysis is essential

Target

- ►Gimli-Hash (the hash scheme based on Gimli)

- ♦ Designers
  - Daniel J. Bernstein
  - Stefan Kölbl
  - Stefan Lucks
  - Pedro Maat Costa Massolino
  - Florian Mendel
  - Kashif Nawaz
  - Tobias Schneider
  - Peter Schwabe
  - François-Xavier Standaert
  - Yosuke Todo
  - Benoît Viguier

Description of Gimli

The Gimli state (3×4 two-dimensional array):

$s_{0,0}$	$s_{0,1}$	$s_{0,2}$	$s_{0,3}$
$s_{1,0}$	$s_{1,1}$	$s_{1,2}$	$s_{1,3}$
$s_{2,0}$	$s_{2,1}$	$s_{2,2}$	$s_{2,3}$

Figure: The Gimli state, where $S_{i,j} \in F_2^{32}$

The sequence of operations for 24-round permutation:

$$
\begin{aligned}
& (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}).
\end{aligned}
$$

The Nonlinear Operation: SP

SP-Box: $F_2^{32\times 3} \rightarrow F_2^{32\times 3}$:

$$\text{Input: } (IX, IY, IZ) \in F_2^{32\times 3}$$
$$\text{Output: } (OX, OY, OZ) \in F_2^{32\times 3}$$

Specification of *SP*:

$$\begin{aligned}
IX &\leftarrow IX \lll 24 \\
IY &\leftarrow IY \lll 9 \\
OZ &\leftarrow IX \oplus (IZ \ll 1) \oplus (IY \wedge IZ) \ll 2 \\
OY &\leftarrow IY \oplus IX \oplus (IX \vee IZ) \ll 1 \\
OX &\leftarrow IZ \oplus IY \oplus (IX \wedge IY) \ll 3
\end{aligned}$$

The Linear Operation: S_SW and B_SW

Small-Swap (S_SW) & Big-Swap (B_SW)

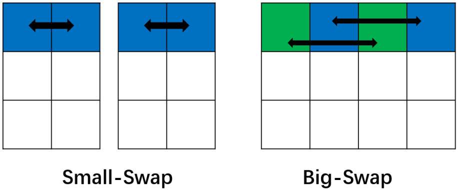


Figure: Illustration of Small-Swap and Big-Swap

Illustration of 1-Round Permutation

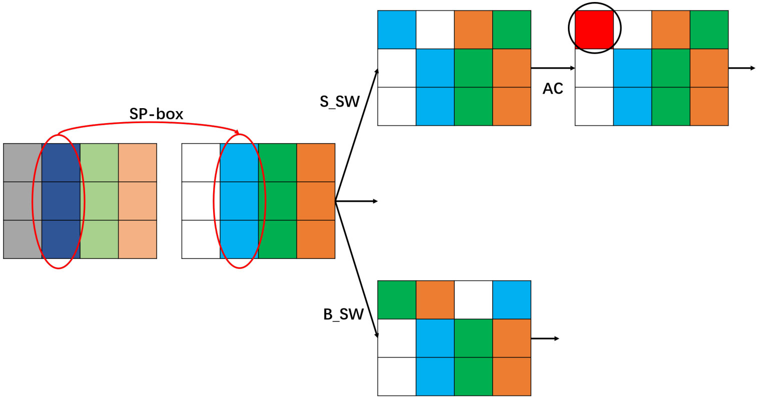


Figure: Illustration of 1-round permutation

Gimli-Hash

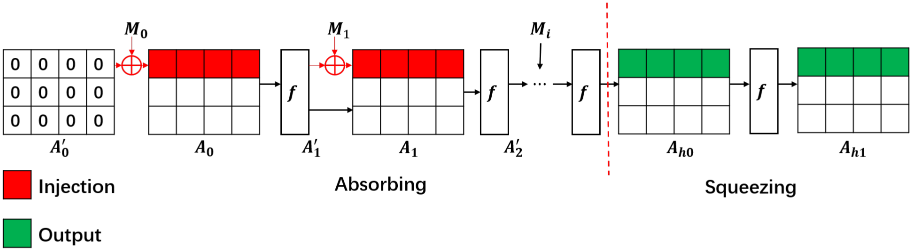


Figure: The process to compress the message

Generic Preimage Attack Framework

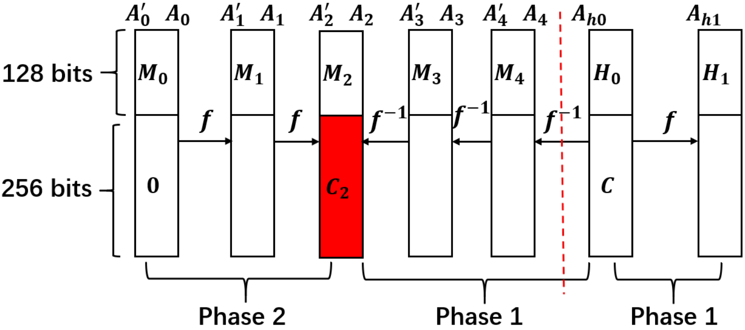


Figure: The generic preimage attack framework

Time: 2^{128} Memory: 2^{128}

Ideas for Preimage Attacks on Reduced Gimli-Hash

Step 1: **Finding a valid capacity part.** Find a valid value of C to match H_1 in less than 2^{128} time.

Step 2: **Choose random values.** Choose a random value for M_3 and M_4 and compute backward to obtain C_2.

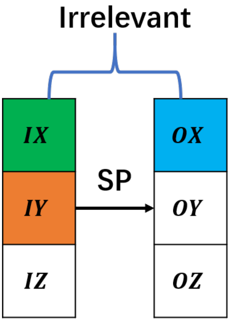
Step 3: **Matching the capacity part.** Exhaust all the 2^{256} possible values of $M_0||M_1$ to match the 256-bit C_2 in less than 2^{128} time.

It is expected that Step 2 is carried out only once.

Properties of the SP-box: Property 1

Property

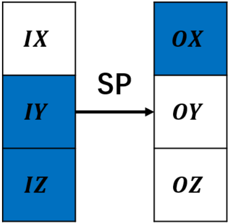
If $(IY \lll 9) \wedge \texttt{0x1fffffff} = 0$, *OX is irrelevant to IX*.



Properties of the SP-box: Property 2

Property

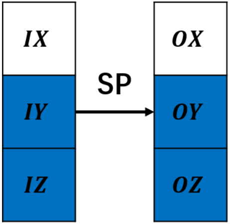
Given (IY, IZ, OX), the probability Pr that (IY, IZ, OX) is a potentially valid tuple without knowing IX is $2^{-3} \times (1 - 0.25)^{29} \approx 2^{-15.5}$.



Properties of the SP-box: Property 3

Property

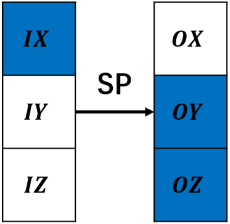
Given (OZ, IY, IZ)*,* (IX, OX, OY) *is fully determined. Moreover, a random tuple* (IY, IZ, OY, OZ) *is valid with probability* 2^{-32}*.*



Properties of the SP-box: Property 4

Property

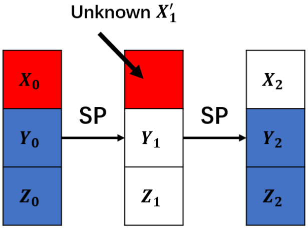
Given (OZ, OY, IX)*, it is a valid tuple with probability* 2^{-1}*. Once it is a valid tuple,* $(OX[30 \sim 0], IY, IZ[30 \sim 0])$ *can be fully determined.*



Properties of the SP-box: Property 5

Property

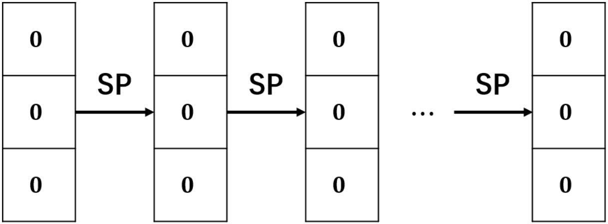
Suppose the input to an SP-box is (X_0, Y_0, Z_0) *and the corresponding output is* (X_1, Y_1, Z_1)*. Moreover, suppose the output of the SP-box is* (X_2, Y_2, Z_2) *when the input is* (X_1', Y_1, Z_1)*, where* X_1' *is a randomly chosen value. If given a random value of* (Y_0, Z_0, Y_2, Z_2)*, the pair* (X_0, X_1') *can be recovered with* $2^{10.4}$ *time complexity.*



Properties of the SP-box: Property 6

Property

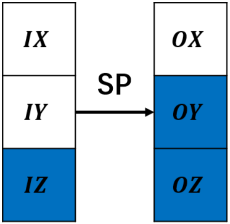
$$SP(0,0,0) = (0,0,0)$$



Properties of the SP-box: Property 7

Property

Given (OY, OZ, IZ), IY can be recovered by solving a linear equation system of size 32.



Attack Types

Collision attack: 3/4/5/6 rounds

Semi-free-start collision attack: 6 rounds

Preimage attack: 2/3/4/5 rounds

$$
\begin{aligned}
& (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}) \\
\rightarrow \quad & (\mathrm{SP} \rightarrow \mathrm{S\_SW} \rightarrow \mathrm{AC}) \rightarrow (\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}).
\end{aligned}
$$

Preimage Attack on 5-Round Gimli-Hash

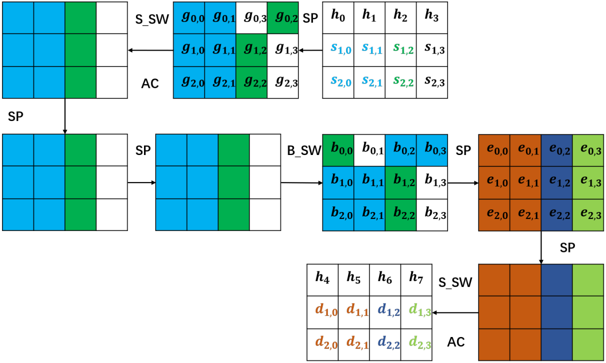


Figure: Finding a valid capacity part using Property 4

$$(s_{1,0}, s_{2,0}, s_{1,1}, s_{2,1}, d_{1,0}, d_{2,0}, d_{1,1}, d_{2,1}) \Rightarrow (b_{0,0}, b_{0,1}, b_{0,2}, b_{0,3})$$

$$(d_{1,2}, d_{2,2}) \Rightarrow (d_{1,2}, d_{2,2}, g_{0,2}, g_{0,3}[0, 1, \cdots, 30])(\mathrm{Total} : 2^{31})$$

$$(d_{1,3}, d_{2,3}) \Rightarrow (d_{1,3}, d_{2,3}, g_{0,2}[0, 1, \cdots, 30], g_{0,3})(\mathrm{Total} : 2^{31})$$

Preimage Attack on 5-Round Gimli-Hash

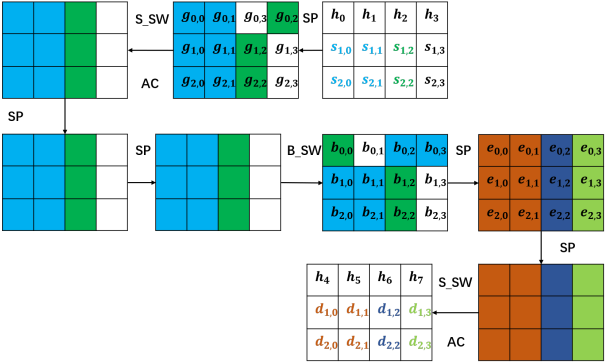


Figure: Finding a valid capacity part using Property 4

$$(s_{1,0}, s_{2,0}, s_{1,1}, s_{2,1}, d_{1,0}, d_{2,0}, d_{1,1}, d_{2,1}) \Rightarrow (b_{0,0}, b_{0,1}, b_{0,2}, b_{0,3})$$

$$(d_{1,2}, d_{2,2}) \Rightarrow (d_{1,2}, d_{2,2}, g_{0,2}, g_{0,3}[0, 1, \cdots, 30])(\mathrm{Total} : 2^{31})$$

$$(d_{1,3}, d_{2,3}) \Rightarrow (d_{1,3}, d_{2,3}, g_{0,2}[0, 1, \cdots, 30], g_{0,3})(\mathrm{Total} : 2^{31})$$

Preimage Attack on 5-Round Gimli-Hash

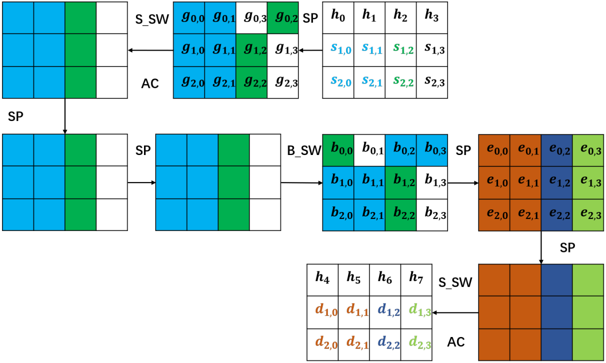


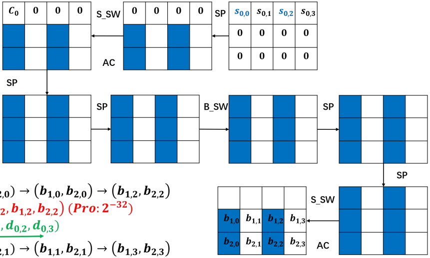
Figure: Finding a valid capacity part using Property 4

$$(s_{1,0}, s_{2,0}, s_{1,1}, s_{2,1}, d_{1,0}, d_{2,0}, d_{1,1}, d_{2,1}) \Rightarrow (b_{0,0}, b_{0,1}, b_{0,2}, b_{0,3})$$

$$(d_{1,2}, d_{2,2}) \Rightarrow (d_{1,2}, d_{2,2}, g_{0,2}, g_{0,3}[0, 1, \cdots, 30])(\mathrm{Total} : 2^{31})$$

$$(d_{1,3}, d_{2,3}) \Rightarrow (d_{1,3}, d_{2,3}, g_{0,2}[0, 1, \cdots, 30], g_{0,3})(\mathrm{Total} : 2^{31})$$

Preimage Attack on 5-Round Gimli-Hash



1. $(d_{0,0}, d_{1,0}, d_{2,0}) \rightarrow (b_{1,0}, b_{2,0}) \rightarrow (b_{1,2}, b_{2,2})$

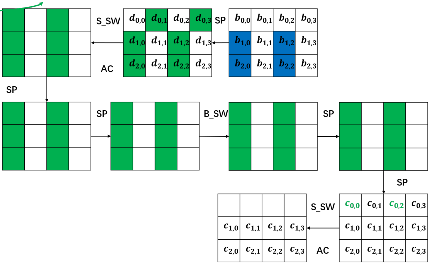
$check\ (d_{1,2}, d_{2,2}, b_{1,2}, b_{2,2})\ (Pro: 2^{-32})$

$\rightarrow 2^{64}(d_{0,0}, d_{0,1}, d_{0,2}, d_{0,3})$

2. $(d_{0,1}, d_{1,1}, d_{2,1}) \rightarrow (b_{1,1}, b_{2,1}) \rightarrow (b_{1,3}, b_{2,3})$

$check\ (d_{1,3}, d_{2,3}, b_{1,3}, b_{2,3})\ (Pro: 2^{-32})$

$\rightarrow 2^{64}(d_{0,0}, d_{0,1}, d_{0,2}, d_{0,3})$



Practical Example for 3-Round Collision Attack

Table: Four-block message pair for full-state collision of 3-round Gimli-Hash

M_0	0xb28d37cb	0xf45c55d6	0xde66f7c3	0x311b4daf
M_1	0xff2ecb4b	0xad17efea	0x72cd23ee	0xd9b8184
M_2	0xe6c17a12	0x4e6b8149	0x6bcf4f78	0xb2bb53c3
M_3	0x41dc5ce8	0x556eee8c	0xe2a8eec	0xc6f2b830
M'_0	0xb28d37cb	0xf45c55d6	0x6385d8fc	0x2c337f96
M'_1	0xe2d9e2fb	0xd86356a7	0xb6e4ad39	0x23205c31
M'_2	0x1ded3fee	0xc29968a4	0x3a53f26	0x8e721abb
M'_3	0xa7604db7	0x271cc14a	0xe2a8eec	0xc6f2b830
Full-state Value	0xb058f51	0x7bdae866	0x9d91e603	0x2990292f
	0x3fc4504a	0x72dcd367	0xf28ddd2f	0x68af4c32
	0x28015655	0x7c507696	0x5f998b7f	0xb8638e53

Model the Collision Attack on 6-Round Gimli-Hash

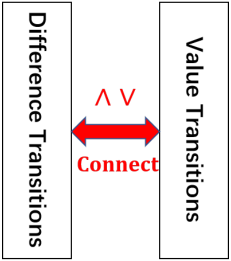
Main idea

Construct a model to describe the value transitions and difference transitions simultaneously.

Step 1: Construct the model to describe the difference transitions.

Step 2: Construct the model to describe the value transitions.

Step 3: Construct the model to connect the value transitions and difference transitions.



Difference-Value Connection via Nonlinear Operations

$$a[2] = a[0] \wedge a[1].$$

Table: The possible patterns for AND operation

$a[0]$	$a[1]$	$\Delta a[0]$	$\Delta a[1]$	$\Delta a[2]$
0	0	0	0	0
0	0	0	1	0
0	0	1	0	0
0	0	1	1	1
0	1	0	0	0
0	1	0	1	0
0	1	1	0	1
0	1	1	1	0
1	0	0	0	0
1	0	0	1	1
1	0	1	0	0
1	0	1	1	0
1	1	0	0	0
1	1	0	1	1
1	1	1	0	1
1	1	1	1	1

And-Model

$$\text{Target}: \quad a[2] = a[0] \wedge a[1].$$

$$\begin{cases} -a[0] - a[1] - \Delta a[1] + \Delta a[2] + 2 \geq 0 \\ a[0] - a[1] - \Delta a[1] - \Delta a[2] + 2 \geq 0 \\ -a[0] + a[1] - \Delta a[0] - \Delta a[2] + 2 \geq 0 \\ a[0] + \Delta a[0] - \Delta a[2] \geq 0 \\ a[0] + a[1] - \Delta a[0] - \Delta a[1] + \Delta a[2] + 1 \geq 0 \\ \Delta a[0] + \Delta a[1] - \Delta a[2] \geq 0 \\ a[1] + \Delta a[1] - \Delta a[2] \geq 0 \\ -a[1] - \Delta a[0] + \Delta a[1] + \Delta a[2] + 1 \geq 0 \\ -a[0] + \Delta a[0] - \Delta a[1] + \Delta a[2] + 1 \geq 0 \end{cases} \tag{1}$$

Difference-Value Connection via Nonlinear Operations

$$a[2] = a[0] \vee a[1].$$

Table: The possible patterns for OR operation

$a[0]$	$a[1]$	$\Delta a[0]$	$\Delta a[1]$	$\Delta a[2]$
0	0	0	0	0
0	0	0	1	1
0	0	1	0	1
0	0	1	1	1
0	1	0	0	0
0	1	0	1	1
0	1	1	0	0
0	1	1	1	0
1	0	0	0	0
1	0	0	1	0
1	0	1	0	1
1	0	1	1	0
1	1	0	0	0
1	1	0	1	0
1	1	1	0	0
1	1	1	1	1

OR-Model

$$\text{Target}: \quad a[2] = a[0] \vee a[1].$$

$$\begin{cases} -a[1] + \Delta a[1] - \Delta a[2] + 1 \geq 0 \\ -a[0] + \Delta a[0] - \Delta a[2] + 1 \geq 0 \\ a[1] - \Delta a[0] + \Delta a[1] + \Delta a[2] \geq 0 \\ a[0] + \Delta a[0] - \Delta a[1] + \Delta a[2] \geq 0 \\ a[0] + a[1] - \Delta a[1] + \Delta a[2] \geq 0 \\ \Delta a[0] + \Delta a[1] - \Delta a[2] \geq 0 \\ a[0] - a[1] - \Delta a[0] - \Delta a[2] + 2 \geq 0 \\ -a[0] - a[1] - \Delta a[0] - \Delta a[1] + \Delta a[2] + 3 \geq 0 \\ -a[0] + a[1] - \Delta a[1] - \Delta a[2] + 2 \geq 0 \end{cases} \tag{2}$$

Usages of the Model

Usage 1: Check existing differential trails. (Validity Check)

Usage 2: Search colliding message pairs directly. (Search Valid Trails)

Results:

1. The official 12-round trail is invalid in the Gimli document.
2. The 6-round trail for collision attack is invalid in `https://eprint.iacr.org/2019/1115`.

Searching Semi-Free-Start(SFS) Colliding Message Pairs for 6-Round Gimli-Hash

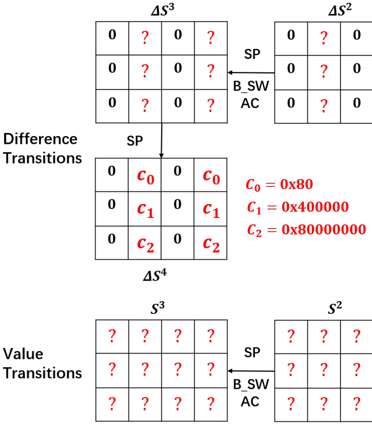


Figure: Search a colliding message pair for 6-round Gimli-Hash

The SFS Colliding Message Pair

Table: The conforming message pair for the 6-round differential characteristic

The input state S^0			
0xff792f16	0x9a757bef	0xff792f16	0x9a757bef
0x37feedd1	0x0d8080e8	0x37feedd1	0x0d8080e8
0xaca93960	0x88cda05b	0xaca93960	0x88cda05b
The input state $S'^0(S^0 \oplus \Delta S^0)$			
0xff792f16	0xe6591fc5	0xff792f16	0xe6591fc5
0x37feedd1	0x0d8080e8	0x37feedd1	0x0d8080e8
0xaca93960	0x88cda05b	0xaca93960	0x88cda05b
The output state S^6 after 6-round permutation for S^0			
0x0765a592	0xcda58e91	0xa5f12648	0xcf35aef1
0x2cecc20e	0xc11436eb	0xba243082	0xc0df1177
0xeda218de	0xeb3f7ab7	0xffb9fd21	0xebe4552b
The output state S'^6 after 6-round permutation for S'^0			
0x0765a592	0x4da58e91	0xa5f12648	0x4f35aef1
0x2cecc20e	0xc11436eb	0xba243082	0xc0df1177
0xeda218de	0xeb3f7ab7	0xffb9fd21	0xebe4552b
$\Delta S^6 = S'^6 \oplus S^6$			
0	0x80000000	0	0x80000000
0	0	0	0
0	0	0	0

The 6-Round Differential Characteristic

Table: The 6-round differential characteristic

State	XOR Difference			
ΔS^0	0	0x7c2c642a	0	0x7c2c642a
	0	0	0	0
	0	0	0	0
ΔS^1	0	0	0	0
	0	0x6e1c342c	0	0x6e1c342c
	0	0x2a7c2c64	0	0x2a7c2c64
ΔS^2	0	0x91143078	0	0x91143078
	0	0x28785014	0	0x28785014
	0	0x35288a58	0	0x35288a58
ΔS^3	0	0x80010008	0	0x80010008
	0	0x00002000	0	0x00002000
	0	0x44400080	0	0x44400080
ΔS^4	0	0x00000080	0	0x00000080
	0	0x00400000	0	0x00400000
	0	0x80000000	0	0x80000000
ΔS^5	0	0	0	0
	0	0	0	0
	0	0x80000000	0	0x80000000
ΔS^6	0	0x80000000	0	0x80000000
	0	0	0	0
	0	0	0	0

Converting SFS Collision Attack to Collision Attack

Step 1: Obtain all the solutions for the capacity part satisfying the differential characteristic.

Step 2: Reuse the preimage attack on 5-round Gimli-Hash to connect the capacity part.

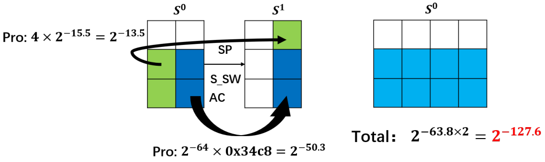


Figure: The Probability that the capacity part is valid

Connecting the Capacity Part

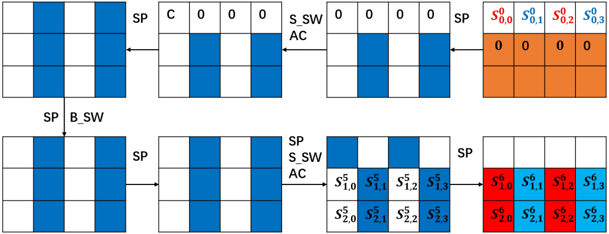


Figure: Connecting the capacity part using Property 1&3

$$\text{Total}: 2^{(64+27.4-64)=2^{27.4}} (S^0_{0,1}, S^0_{0,3}) \Rightarrow (S^6_{1,1}, S^6_{2,1}, S^6_{1,3}, S^6_{2,3})$$

$$\text{Total}: 2^{(64+27.4-64)=2^{27.4}} (S^6_{1,1}, S^6_{2,1}, S^6_{1,3}, S^6_{2,3}) \Rightarrow (S^0_{0,0}, S^0_{0,2})$$

$$\text{Total}: 2^{27.4-27} = 2^{0.4} (S^0_{0,0}, S^0_{0,2}) \Rightarrow (S^6_{1,0}, S^6_{2,0}, S^6_{1,2}, S^6_{2,2})$$

Summary

Table: The analytical results of reduced Gimli-Hash

Attack Type	Rounds	Memory	Time
Preimage	$5(S^0 \sim S^5)$	2^{64}	2^{96}
Collision	$6(S^0 \sim S^6)$	2^{64}	2^{64}

Conlusion

1. The difference transitions are not independent in different rounds.
2. The probability of a trail should not be simply computed by counting the number of conditions due to the weak diffusion of Gimli round function.
3. The interaction of the Swap (Big-Swap & Small-Swap) and SP-box should be taken into account when devising an attack on the structure.
4. The validity of the differential should be carefully checked (e.g. with our model) when mounting a differential-based attack.

Thank you

Practical Attacks on the Last 2/3 Rounds

The sequence of operations:

$$(\mathrm{SP}) \rightarrow (\mathrm{SP} \rightarrow \mathrm{B\_SW}) \rightarrow (\mathrm{SP}).$$

Conclusion

Based on Property 6, when the number of rounds is reduced to 2 or 3 rounds, given arbitrary message M, $M_0||M$ is the second the preimage of $H(M)$ where $M_0 = 0$ and M_0 is a 128-bit block.

Practical Attacks on the Last 2/3 Rounds

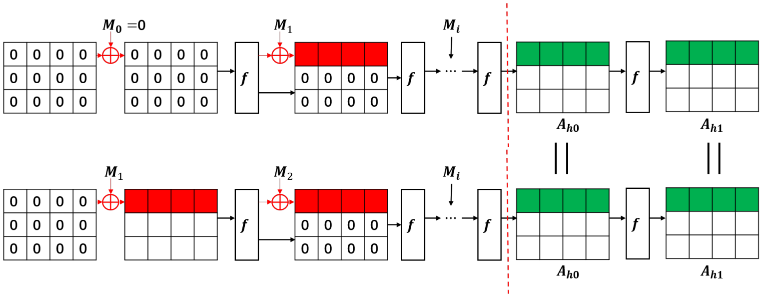


Figure: Practical second-preimage attack on the last 2/3 rounds of Gimli-Hash

Practical Preimage Attack on 2-Round Gimli-Hash Using Property 5

Table: A message leading to an all-zero state for 2-round Gimli-Hash

M_0	0x1c5c59da	0x41b61bb7	0	0
M_1	0x9cf49a4e	0x9a80d115	0	0
M_2	0xa31c3903	0x41e6e73c	0	0
M_3	0x456723c6	0xdc515cff	0	0
M_4	0x98694873	0x944a58ec	0	0
	0	0	0	0
Full-state Value	0	0	0	0
	0	0	0	0