MITSUBISHI ELECTRIC
Changes for the Better

# Collision Attacks on Spongent with Grouping Method

Keita Toyama[1] Kosei Sakamoto[2,3] Takanori Isobe[3]

[1]University of Hyogo
[2]Mitsubishi Electric Corporation
[3]The University of Osaka

SAC 2025

# Contents

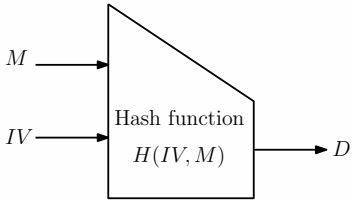
# Hash Functions

## Functionality

- Hash functions map an arbitrary-length input to a fixed-length digest

## Security requirements

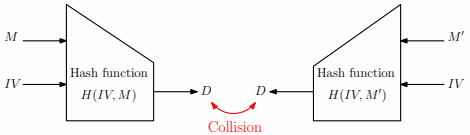
- Collision resistance
- Preimage resistance
- Second-preimage resistance



# Collision Attack and its Variants

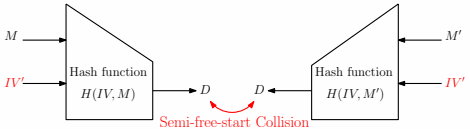
## Collision Attacks

- Find $M$ and $M'$ such that $H(IV, M) = H(IV, M')$ for a pre-fixed $IV$




## Semi-free-start Collision Attacks

- Find $M$, $M'$, and $IV'$ such that $H(IV', M) = H(IV', M')$



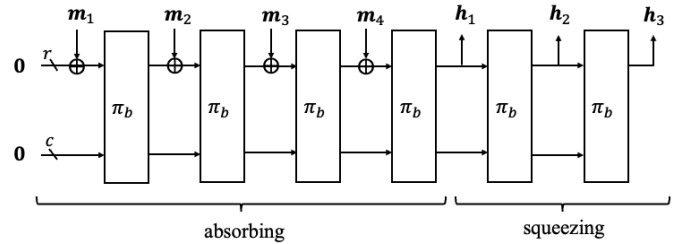

## Free-start Collision Attacks

- Find $M$, $M'$, $IV'_0$, and $IV'_1$ such that $H(IV'_0, M) = H(IV'_1, M')$

# SPONGENT: Sponge-based Hash Function

## SPONGENT

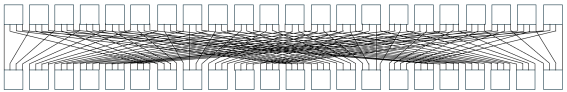
- Proposed by Bogdanov et al. at CHES 2011
- Based on sponge construction with PRESENT-like permutations [BKL+07]
- Comprises 13 variants, denoted as SPONGENT-$n/c/r$,
  - ✓ $n$: hash size, $c$: capacity, $r$: rate, $r + c$: block size



# SPONGENT: Underlying Permutations

## PRESENT-like permutations [BKL+07]

- Based on Substitution-Permutation Network
- Consist of a 4-bit S-box and a bit-wise permutation



The round function of SPONGENT-88/80/8

- sBoxLayer
  - ✓ Apply the 4-bit S-box in parallel

$$S[\cdot] = \{\texttt{0xE}, \texttt{0xD}, \texttt{0xB}, \texttt{0x0}, \texttt{0x2}, \texttt{0x1}, \texttt{0x4}, \texttt{0xF}, \texttt{0x7}, \texttt{0xA}, \texttt{0x8}, \texttt{0x5}, \texttt{0x9}, \texttt{0xC}, \texttt{0x3}, \texttt{0x6}\}$$

- pLayer
  - ✓ Apply a $b$-bit permutation

$$P_b(j) = \begin{cases} j \cdot b/4 \mod (b-1), & \text{if } j \in \{0, \ldots, b-2\} \\ b-1, & \text{if } j = b-1. \end{cases}$$

# Claimed Security and Previous Results

## Claimed security for collision attacks

| | $n$ | $b$ | $c$ | $r$ | Rounds | Security (bit) | $n$ | $b$ | $c$ | $r$ | Rounds | Security (bit) | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| SPONGENT-88/80/8 | 88 | 88 | 80 | 8 | 45 | 40 | SPONGENT-224/224/16 | 224 | 240 | 224 | 16 | 120 | 112 |
| SPONGENT-88/176/88 | 88 | 264 | 176 | 88 | 135 | 44 | SPONGENT-224/224/112 | 224 | 336 | 224 | 112 | 170 | 112 |
| SPONGENT-128/128/8 | 128 | 136 | 128 | 8 | 70 | 64 | SPONGENT-224/448/224 | 224 | 672 | 448 | 224 | 340 | 112 |
| SPONGENT-128/256/128 | 128 | 384 | 256 | 128 | 195 | 64 | SPONGENT-256/256/16 | 256 | 272 | 256 | 16 | 140 | 128 |
| SPONGENT-160/160/16 | 160 | 176 | 160 | 16 | 90 | 80 | SPONGENT-256/256/128 | 256 | 384 | 256 | 128 | 195 | 128 |
| SPONGENT-160/160/80 | 160 | 240 | 160 | 80 | 120 | 80 | SPONGENT-256/512/256 | 256 | 768 | 512 | 256 | 385 | 128 |
| SPONGENT-160/320/160 | 160 | 480 | 320 | 160 | 240 | 80 | | | | | | | |

## Previous results

- The designers demonstrated a rebound attack on 6-round SPONGENT-88/80/8
  - ✓ Time complexity is $2^{55.2} (> 2^{40})$
- Abdelraheem demonstrated the distinguishing attacks based on differential and linear characteristics [Abd12]
- Zhang and Liu demonstrated the distinguishing attacks based on truncated differentials with a MITM technique [ZL17]
- No third-party security analysis on collision resistance has been reported

# Obstacles for Efficient Collision Attacks

■ Difficulty in obtaining sufficient degrees of freedom (DoF)

- ➢ For block-cipher-based hash functions, this can be done by counting the available DoF in each S-box independently, such as in the super-S-box technique used in rebound attacks [GP10].
- ➢ For public-permutation-based hash functions, we need to consider the dependency across all S-boxes in all rounds
  - ✓ Making it much more complex to obtain sufficient DoF

■ Automatic search method proposed by Liu et al. [LIM20].

- ➢ Finding a valid differential characteristic for Gimli
  - ✓ They showed that many differential characteristics in previous studies on sponge-based hash functions are invalid

We extend Liu et al.'s method to obtain sufficient DoF
for public-permutation-based hash functions

# Our Results

- First third-party security analysis for collision resistance of SPONGENT
  - ∗ indicates that the real colliding pair was found

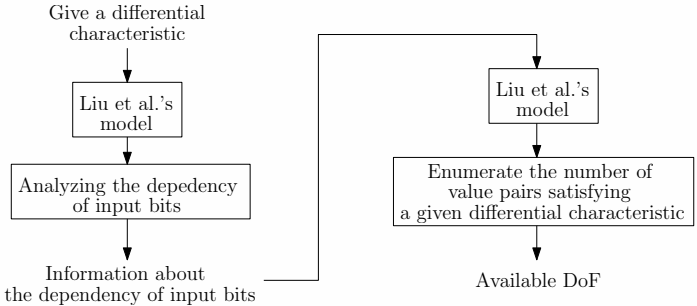
| | Collision | | Semi-free-start | | Ref | Full round | Claimed security |
|---|---|---|---|---|---|---|---|
| | Rounds | Time | Rounds | Time | | | |
| SPONGENT-88/80/8 | - | - | 8* | $2^{17}$ | Ours | 45 | $2^{40}$ |
| | 6† | $2^{55.2}$ | - | - | [BKL+11] | | |
| SPONGENT-88/176/88 | 9 | $2^{42}$ | 9* | $2^{33}$ | Ours | 135 | $2^{44}$ |
| | 8* | $2^{28}$ | | | | | |
| SPONGENT-128/128/8 | - | - | 8* | $2^{22}$ | Ours | 70 | $2^{64}$ |
| SPONGENT-128/256/128 | 12 | $2^{58}$ | 14 | $2^{63}$ | Ours | 195 | $2^{64}$ |
| | 8* | $2^{28}$ | | | | | |
| SPONGENT-160/160/16 | - | - | 7 | $2^{47}$ | Ours | 90 | $2^{80}$ |
| SPONGENT-160/160/80 | 11 | $2^{61}$ | 14 | $2^{78}$ | Ours | 120 | $2^{80}$ |
| SPONGENT-160/320/160 | 11 | $2^{56}$ | 13 | $2^{79}$ | Ours | 240 | $2^{80}$ |
| | 8* | $2^{28}$ | | | | | |
| SPONGENT-224/224/16 | - | - | 8 | $2^{91}$ | Ours | 120 | $2^{112}$ |
| SPONGENT-224/224/112 | 10 | $2^{60}$ | 11 | $2^{62}$ | Ours | 170 | $2^{112}$ |
| SPONGENT-224/448/224 | 10 | $2^{47}$ | 11 | $2^{57}$ | Ours | 340 | $2^{112}$ |
| | 8* | $2^{21}$ | | | | | |
| SPONGENT-256/256/16 | - | - | 11 | $2^{110}$ | Ours | 140 | $2^{128}$ |
| SPONGENT-256/256/128 | 15 | $2^{79}$ | 15 | $2^{75}$ | Ours | 195 | $2^{128}$ |
| SPONGENT-256/512/256 | 15 | $2^{73}$ | 15 | $2^{73}$ | Ours | 385 | $2^{128}$ |
| | 9* | $2^{28}$ | | | | | |

# Contents

# The Core Idea of the Grouping Method

## Analyzing the dependency of input bits

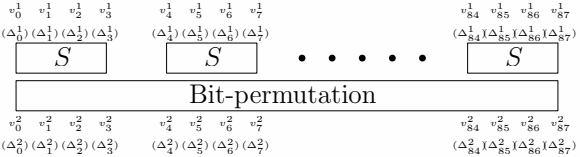
- Employing Liu et al.'s model that describes the dependency between the internal difference and the value pair [LIM20]
  - ✓ Using it twice: to reveal the dependency of input bits, and to enumerate the value pairs satisfying a differential characteristics




Our Method

# How to Enumerate the DoF

- Procedure to enumerate the DoF (Consisting of 6 steps)




**Step 1.** Express this dependency as CNF by Espresso

$$(v_0^0 \vee v_0^1 \vee \Delta_0^0 \vee \neg\Delta_0^1) \wedge (v_2^0 \vee v_5^1 \neg\Delta_2^0 \vee \Delta_5^1) \wedge \cdots \wedge (v_{77}^{r-1} \vee v_{79}^r \vee \Delta_{77}^{r-1} \vee \Delta_{79}^{r-1}) = 1$$

**Step 2.** Assign a given differential characteristics to CNF generated in Step 1

$$(v_0^0 \vee v_0^1 \vee 1 \vee \neg 0) \wedge (v_2^0 \vee \neg v_5^1 \vee 0 \vee 0) \wedge \cdots \wedge (v_{77}^{r-1} \vee v_{79}^r \vee 0 \vee 1) = 1$$

**Step 3.** Express all Variables by the variable of input bits

$$(v_0^0 \vee v_3^0 \vee v_{18}^0) \wedge (v_2^0 \vee \neg v_5^0) \wedge \cdots \wedge (v_2^0 \vee v_{16}^0 \vee v_{35}^0 \vee \neg v_{55}^0 \vee v_{79}^0) = 1$$

**Step 4.** Convert the CNF into a product of terms, minimizing the number of terms, using simplify-logic tools (We use simplify-logic() in SymPy library for Python)

$$((v_0^0 \vee v_3^0) \oplus v_{18}^0) \wedge (v_2^0 \vee \neg v_5^0) \wedge \cdots \wedge ((v_2^0 \vee v_{16}^0) \oplus (v_{35}^0 \vee v_{79}^0)) = 1$$

Our Method

# Step 5

## Details of Step 5 (2 rounds of SPONGENT-160/160/80)

- Analyze all terms in the product of terms and categorize variables
- **Free bits**: A variable that does not appear in the Boolean function, such as $v_1$, $v_2$, and $v_5$
- **Fixed bits**:A variable that appears in a term consisting only of itself
- **Dependent bits**: A Variable that depends on other variables in a term
  - ✓ Grouping dependent bits by how they depend on each other
    $\neg(\mathbf{v_{70}} \oplus \mathbf{v_{71}} \oplus (\mathbf{v_{69}} \wedge \mathbf{v_{72}}) \oplus (\mathbf{v_{70}} \wedge \mathbf{v_{71}} \wedge \mathbf{v_{72}})) \rightarrow$ Categorized into the same group

$$v_{49} \bigwedge \neg v_{52} \bigwedge v_{57} \bigwedge \neg v_{60} \bigwedge v_{67} \bigwedge v_{75} \bigwedge (v_{65} \vee v_{68}) \bigwedge (v_{73} \vee v_{76}) \bigwedge (v_{50} \vee \neg v_{51}) \bigwedge (v_{51} \vee \neg v_{50}) \bigwedge (v_{58} \vee \neg v_{59})$$
$$\bigwedge (v_{59} \vee \neg v_{58}) \bigwedge (v_{66} \vee \neg v_{65}) \bigwedge (v_{74} \vee \neg v_{73}) \bigwedge (\neg v_{66} \vee \neg v_{68}) \bigwedge (\neg v_{74} \vee \neg v_{76}) \bigwedge (v_{78} \oplus v_{79} \oplus (v_{77} \wedge v_{80}) \oplus (v_{78} \wedge v_{79} \wedge v_{80}))$$
$$\bigwedge (v_{61} \oplus (v_{61} \wedge v_{64}) \oplus (v_{62} \wedge v_{63}) \oplus (v_{62} \wedge v_{64}) \oplus (v_{63} \wedge v_{64}) \oplus (v_{62} \wedge v_{63} \wedge v_{64})) \bigwedge (v_{77} \oplus (v_{77} \wedge v_{80}) \oplus (v_{78} \wedge v_{79}) \oplus (v_{78} \wedge v_{80})$$
$$\oplus (v_{79} \wedge v_{80}) \oplus (v_{78} \wedge v_{79} \wedge v_{80})) \bigwedge \neg(v_{53} \oplus (v_{53} \wedge v_{56}) \oplus (v_{54} \wedge v_{55}) \oplus (v_{54} \wedge v_{56}) \oplus (v_{55} \wedge v_{56}) \oplus (v_{54} \wedge v_{55} \wedge v_{56}))$$
$$\bigwedge \neg(v_{69} \oplus (v_{69} \wedge v_{72}) \oplus (v_{70} \wedge v_{71}) \oplus (v_{70} \wedge v_{72}) \oplus (v_{71} \wedge v_{72}) \oplus (v_{70} \wedge v_{71} \wedge v_{72})) \bigwedge ((v_{58} \wedge v_{59}) \vee \neg(v_{50} \wedge v_{51}) \vee (v_{61} \oplus (v_{61} \wedge v_{64})$$
$$\oplus (v_{62} \wedge v_{63}) \oplus (v_{62} \wedge v_{64}) \oplus (v_{63} \wedge v_{64}) \oplus (v_{62} \wedge v_{63} \wedge v_{64}))) \bigwedge ((v_{74} \oplus (v_{73} \wedge v_{76}) \oplus (v_{74} \wedge v_{76})) \vee \neg(v_{66} \oplus (v_{65} \wedge v_{68}) \oplus (v_{66} \wedge v_{68}))$$
$$\vee (v_{78} \oplus v_{79} \oplus (v_{77} \wedge v_{80}) \oplus (v_{78} \wedge v_{79} \wedge v_{80}))) \bigwedge ((v_{65} \oplus v_{66} \oplus v_{68} \oplus (v_{65} \wedge v_{68})) \vee \neg(v_{73} \oplus v_{74} \oplus v_{76} \oplus (v_{73} \wedge v_{76}))$$
$$\vee (v_{77} \oplus (v_{77} \wedge v_{80}) \oplus (v_{78} \wedge v_{79}) \oplus (v_{78} \wedge v_{80}) \oplus (v_{79} \wedge v_{80}) \oplus (v_{78} \wedge v_{79} \wedge v_{80}))) \bigwedge \neg(\mathbf{v_{70}} \oplus \mathbf{v_{71}} \oplus (\mathbf{v_{69}} \wedge \mathbf{v_{72}}) \oplus (\mathbf{v_{70}} \wedge \mathbf{v_{71}} \wedge \mathbf{v_{72}})) = 1$$

Our Method

# Step 5

## Details of Step 5 (2 rounds of SPONGENT-160/160/80)

- Variables in each category can be determined independently
  - ✓ Enumerate the number of assignments for variables in each group independently in Step 6

| Category | Bits | Values |
|---|---|---|
| Free bits | 48 | $v_{25}, v_{13}, v_{28}, v_{46}, v_{23}, v_{22}, v_{19}, v_{37}, v_{17}, v_{11}, v_{30}, v_{8}, v_{41}, v_{6}, v_{32}, v_{43}, v_{45}, v_{16}, v_{21}, v_{47}, v_{31}, v_{14}, v_{34}, v_{36}, v_{18}, v_{33}, v_{4}, v_{38}, v_{48}, v_{29}, v_{5}, v_{26}, v_{3}, v_{20}, v_{27}, v_{1}, v_{39}, v_{15}, v_{40}, v_{12}, v_{24}, v_{44}, v_{42}, v_{9}, v_{35}, v_{7}, v_{2}, v_{10}$ |
| Fixed bits | 6 | $v_{49}, \neg v_{52}, v_{57}, \neg v_{60}, v_{67}, v_{75}$ |
| Group 1 | 4 | $v_{53}, v_{56}, v_{54}, v_{55}$ |
| Group 2 | 4 | $v_{69}, v_{72}, v_{70}, v_{71}$ |
| Group 3 | 8 | $v_{59}, v_{50}, v_{64}, v_{63}, v_{51}, v_{58}, v_{61}, v_{62}$ |
| Group 4 | 10 | $v_{80}, v_{78}, v_{77}, v_{73}, v_{68}, v_{66}, v_{65}, v_{76}, v_{79}, v_{74}$ |

# Step 6

## Details of Step 6

- Count the number of value pairs for each group independently
- Construct Liu et al.'s model using SAT and find one solution
  - ✓ If the solver returns "UNSAT", the given differential characteristic is invalid
- Enumerate the number of solutions for each group by solving the SAT model multiple times
  - ✓ Variables in other groups are fixed by the assignment found in the above procedure
  - ✓ **The number of solutions is equal to the available DoF**
- The total DoF is the product of the number of solutions in each group

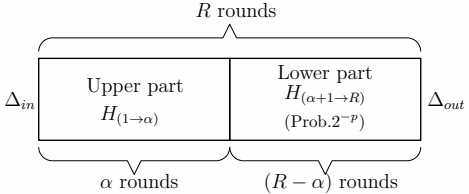
$$DoF = 2^{\#\text{ free bits}} \times \underbrace{N_1}_{\#\text{ solutions in group 1}} \times \underbrace{N_2}_{\#\text{ solutions in group 2}} \times \cdots \times \underbrace{N_a}_{\#\text{ solutions in group } a}$$

# Contents

# Overview of Our Collision Attacks

## Rebound-like attack

- Divide the underlying permutation into upper and lower parts

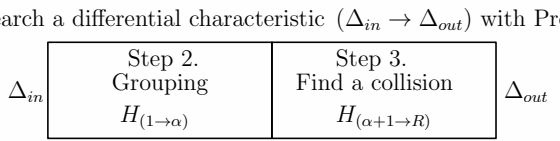



- For the upper part
  - ✓ Apply the Grouping method to obtain sufficient DoF
- For the lower part
  - ✓ Find a colliding pair using the DoF obtained in the upper part
- Complexity analysis

$$T = \underbrace{\frac{\alpha}{R}\left(2^{\#\textit{free bits}} \times N_1 \times N_2 \times \cdots \times N_a\right)}_{\text{The upper part}} + \underbrace{\frac{R-\alpha}{R} \cdot 2^p}_{\text{The lower part}}$$

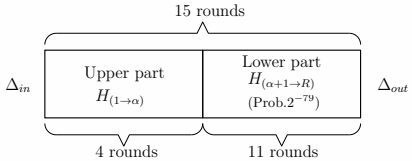
# Attack Procedure

- Step 1: Search for a differential characteristic by SAT-based automatic search method
  - Restrect $2^p$ to be lower than the claimed security
- Step 2: Apply the Grouping method into the upper part
  - If the DoF obtained is smaller than $2^p$, we repeat Step 1
- Step 3: Find a colliding pair
  - Explore a value pair satisfying a given differential characteristic in the lower part



# Application to the 15-round SPONGENT-256/256/128

## Collision attacks on the 15-round SPONGENT-256/256/128




| Rounds | Differences at the input of each round | Prob. | Phase |
|---|---|---|---|
| 1(Input) | 0000000000000000ee8000002950000000000000000000000000000000000000000000000000000000000000000000000000000000 | | |
| 2 | 0000e020000000000000000000000000000000000000000000000e0e0000000000000000000000000000000000000000000000000 | | |
| 3 | 0500000000005000000000000000000000000000000000005000000000005000000000000000000000000000000000000000000 | | $H_{(1\to4)}$ |
| 4 | 0000000000000000000000000000000000000000000020020000000020020000000000000000000000000000000000000000000 | | |
| 5 | 0000000000000000000000000000000000009090900000000000000000000000000000000000000000000000000000000000000 | | |
| 6 | 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 | | |
| 7 | 0000000000000000000000000000000000000020020000000000000000000000000000000000000000000000000000000000000 | | |
| 8 | 0000000000210000000000000000000000000000000000000000000021000000000000000000000000000000000000000000000 | | |
| 9 | 00c000000000000c0000000000000000000000000000000000c000000000000c0000000000000000000000000000000000000000 | | |
| 10 | 4004000000004004000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 | $2^{-79}$ | $H_{(5\to15)}$ |
| 11 | 0000000000000000000000000000000000000000000000009090900000000000000000009090900000000000000000000000000 | | |
| 12 | 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 | | |
| 13 | 0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000140 | | |
| 14 | 0000000000000000000000006000000000000000000006000000000000000000000000000000000000000000000000000000000 | | |
| 15 | 0000080000800000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000 | | |
| Output | 0280000000000000000000002800000000000000000000000000000000000000000000000000000000000000000000000000000 | | |

- At least $2^{-79}$ DoF is required in $H_{(1\to4)}$

# Application to 15-round SPONGENT-256/256/128

## Collision attacks on the 15-round SPONGENT-256/256/128

| Category | Bits | Values |
|---|---|---|
| Free bits | 64 | $v_{13}, v_{23}, v_{12}, v_{43}, v_{53}, v_{60}, v_3, v_{34}, v_{37}, v_{14}, v_{11}, v_{30}, v_{19}, v_{49}, v_4, v_{25}, v_{59}, v_{64}, v_{18}, v_{22}, v_8, v_{24}, v_{51}, v_{58}, v_{21}, v_{16}, v_{56}, v_{17}, v_{39}, v_{33}, v_1, v_{15}, v_{32}, v_{28}, v_{55}, v_{62}, v_{52}, v_6, v_{50}, v_{42}, v_{54}, v_{10}, v_{38}, v_{48}, v_{45}, v_{46}, v_{26}, v_7, v_{47}, v_{40}, v_{44}, v_{31}, v_{35}, v_{27}, v_{29}, v_2, v_{63}, v_5, v_{57}, v_{36}, v_9, v_{20}, v_{41}, v_{61}$ |
| Fixed bits | 12 | $v_{69}, v_{73}, v_{77}, v_{78}, \neg v_{79}, \neg v_{101}, \neg v_{103}, \neg v_{104}, \neg v_{106}, \neg v_{107}, v_{110}, \neg v_{112}$ |
| Group 1 | 16 | $v_{87}, v_{93}, v_{85}, v_{81}, v_{96}, v_{82}, v_{89}, v_{90}, v_{91}, v_{94}, v_{95}, v_{84}, v_{92}, v_{86}, v_{88}, v_{83}$ |
| Group 2 | 36 | $v_{100}, v_{65}, v_{67}, v_{68}, v_{105}, v_{75}, v_{115}, v_{123}, v_{66}, v_{119}, v_{114}, v_{74}, v_{99}, v_{109}, v_{124}, v_{71}, v_{120}, v_{122}, v_{127}, v_{108}, v_{102}, v_{111}, v_{116}, v_{128}, v_{72}, v_{80}, v_{117}, v_{97}, v_{113}, v_{118}, v_{125}, v_{70}, v_{76}, v_{121}, v_{98}, v_{126}$ |
| Time of $H_{(1\to4)}$ | $2^{77.1}$ | |

- We obtain the DoF of $2^{64}$, $2^7$, and $2^8$ from free bits, Group 1, and Group 2, respectively.
- Time Complexity

$$T = \underbrace{\frac{4}{15}(2^{64} \times 2^7 \times 2^8)}_{H_{(1\to4)}} + \underbrace{\frac{11}{15} \cdot 2^{79}}_{H_{(5\to15)}} = 2^{79}$$

# Our Results

- First third-party security analysis for collision resistance of SPONGENT
  - $*$ indicates that we found the real colliding pair

| | Collision | | Semi-free-start | | Ref | Full round | Claimed security |
|---|---|---|---|---|---|---|---|
| | Rounds | Time | Rounds | Time | | | |
| SPONGENT-88/80/8 | - | - | 8* | $2^{17}$ | Ours | 45 | $2^{40}$ |
| | 6† | $2^{55.2}$ | - | - | [BKL+11] | | |
| SPONGENT-88/176/88 | 9 | $2^{42}$ | 9* | $2^{33}$ | Ours | 135 | $2^{44}$ |
| | 8* | $2^{28}$ | | | | | |
| SPONGENT-128/128/8 | - | - | 8* | $2^{22}$ | Ours | 70 | $2^{64}$ |
| SPONGENT-128/256/128 | 12 | $2^{58}$ | 14 | $2^{63}$ | Ours | 195 | $2^{64}$ |
| | 8* | $2^{28}$ | | | | | |
| SPONGENT-160/160/16 | - | - | 7 | $2^{47}$ | Ours | 90 | $2^{80}$ |
| SPONGENT-160/160/80 | 11 | $2^{61}$ | 14 | $2^{78}$ | Ours | 120 | $2^{80}$ |
| SPONGENT-160/320/160 | 11 | $2^{56}$ | 13 | $2^{79}$ | Ours | 240 | $2^{80}$ |
| | 8* | $2^{28}$ | | | | | |
| SPONGENT-224/224/16 | - | - | 8 | $2^{91}$ | Ours | 120 | $2^{112}$ |
| SPONGENT-224/224/112 | 10 | $2^{60}$ | 11 | $2^{62}$ | Ours | 170 | $2^{112}$ |
| SPONGENT-224/448/224 | 10 | $2^{47}$ | 11 | $2^{57}$ | Ours | 340 | $2^{112}$ |
| | 8* | $2^{21}$ | | | | | |
| SPONGENT-256/256/16 | - | - | 11 | $2^{110}$ | Ours | 140 | $2^{128}$ |
| SPONGENT-256/256/128 | 15 | $2^{79}$ | 15 | $2^{75}$ | Ours | 195 | $2^{128}$ |
| SPONGENT-256/512/256 | 15 | $2^{73}$ | 15 | $2^{73}$ | Ours | 385 | $2^{128}$ |
| | 9* | $2^{28}$ | | | | | |

# 4.1 Conclusion

## Summary

- We developed Liu et al.’s tool to obtain sufficient DoF
- We conducted the first collision attacks on the SPONGENT family
- We demonstrated real colliding pairs for several variants of SPONGENT

## Future work

- Extend the Grouping method to cover more rounds
- Consider dependencies between the upper and lower parts

Thank you for your attention!

# References I

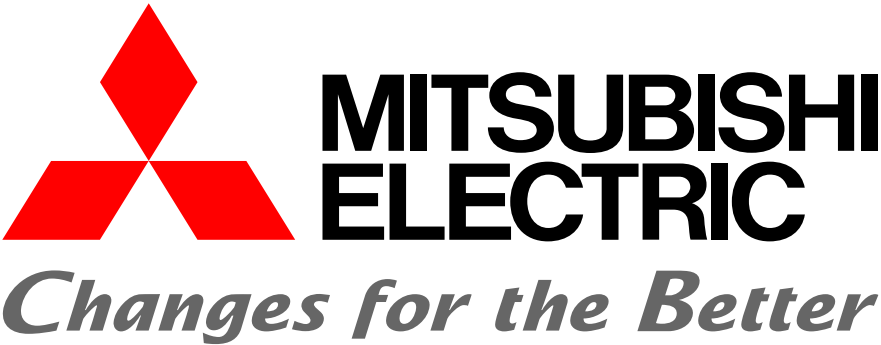

- Mohamed Ahmed Abdelraheem, *Estimating the probabilities of low-weight differential and linear approximations on present-like ciphers*, Information Security and Cryptology - ICISC 2012 - 15th International Conference, Seoul, Korea, November 28-30, 2012, Revised Selected Papers (Taekyoung Kwon, Mun-Kyu Lee, and Daesung Kwon, eds.), Lecture Notes in Computer Science, vol. 7839, Springer, 2012, pp. 368–382.
- Andrey Bogdanov, Lars R. Knudsen, Gregor Leander, Christof Paar, Axel Poschmann, Matthew J. B. Robshaw, Yannick Seurin, and C. Vikkelsoe, *PRESENT: an ultra-lightweight block cipher*, Cryptographic Hardware and Embedded Systems - CHES 2007, 9th International Workshop, Vienna, Austria, September 10-13, 2007, Proceedings (Pascal Paillier and Ingrid Verbauwhede, eds.), Lecture Notes in Computer Science, vol. 4727, Springer, 2007, pp. 450–466.

# References II


- Andrey Bogdanov, Miroslav Knezevic, Gregor Leander, Deniz Toz, Kerem Varici, and Ingrid Verbauwhede, *spongent: A lightweight hash function*, Cryptographic Hardware and Embedded Systems - CHES 2011 - 13th International Workshop, Nara, Japan, September 28 - October 1, 2011. Proceedings (Bart Preneel and Tsuyoshi Takagi, eds.), Lecture Notes in Computer Science, vol. 6917, Springer, 2011, pp. 312–325.
- Henri Gilbert and Thomas Peyrin, *Super-sbox cryptanalysis: Improved attacks for aes-like permutations*, FSE, Lecture Notes in Computer Science, vol. 6147, Springer, 2010, pp. 365–383.
- Fukang Liu, Takanori Isobe, and Willi Meier, *Automatic verification of differential characteristics: Application to reduced gimli*, Advances in Cryptology - CRYPTO 2020 - 40th Annual International Cryptology Conference, CRYPTO 2020, Santa Barbara, CA, USA, August 17-21, 2020, Proceedings, Part III (Daniele Micciancio and Thomas Ristenpart, eds.), Lecture Notes in Computer Science, vol. 12172, Springer, 2020, pp. 219–248.

# References III


Guoyan Zhang and Meicheng Liu, *A distinguisher on present-like permutations with application to SPONGENT*, Sci. China Inf. Sci. **60** (2017), no. 7, 72101.


MITSUBISHI
ELECTRIC
Changes for the Better