Cryptanalysis of Simpira v1

Christoph Dobraunig **Maria Eichlseder** **Florian Mendel**

SAC 2016

The Simpira Family of Permutations

Gueron and Mouha [GM16a]

Simpira

Motivation

- Scalable permutation family for 128-bit security
- Using Intel's AES-NI instructions
- For hash-based signatures, wide-block encryption, . . .

Design

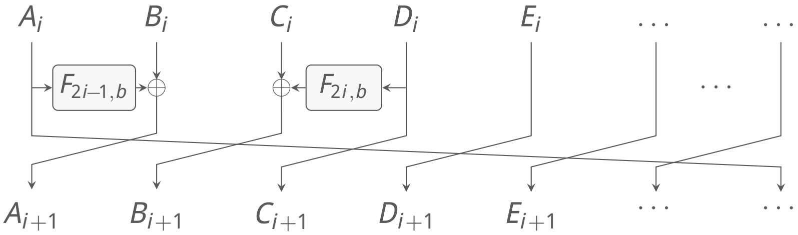
- Simpira-b for $b \times$ 128-bit inputs
- Feistel (GFS) with b branches & AES-based F-function

This paper

Distinguisher & collision attack for full-round Simpira-4

Simpira's Feistel Structure

Type-1.x GFS by Yanagihara and Iwata [YI14]

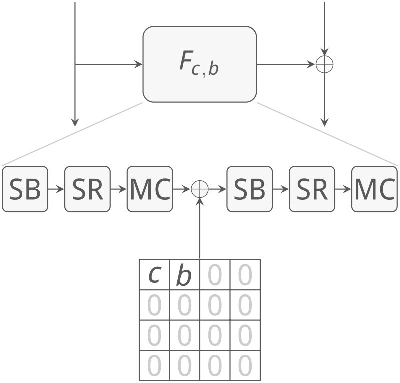


Feistel round i of Simpira-b ($b \geq 4$, $b \neq 6, 8$)

We'll focus on Simpira-4.

Simpira's *F*-Function

2 rounds of AES



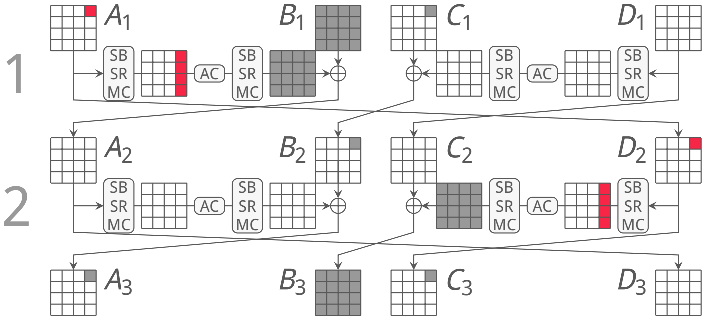
c	*b*	0	0
0	0	0	0
0	0	0	0
0	0	0	0

- Round constant 1: Counter *c*, Simpira-*b*
- Round constant 2: Used for Feistel

Designers’ Security Analysis for Simpira-4

MILP-based bounds like Mouha et al. [Mou+11]

- $\geq$ 75 active S-boxes for the 15 rounds (tight bound):



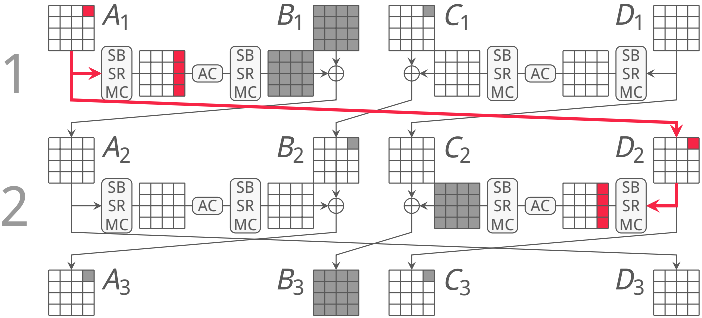
Iterative trail ▨ for Simpira-4 with 5 active S-boxes 🟥 per round

- Is it safe to assume these S-boxes are independent?

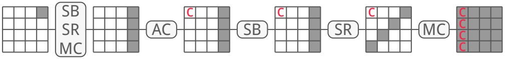
8-Round Differential Trail

Dependencies 1 – Fewer S-boxes

- Simpira’s GFS feeds the same input to two F-functions:



- Recall the sparse round constants for AC:



- If trail in round 1 holds, round 2 will hold with probability 1
- 8 rounds have only $4 \cdot 5 = 20$, not 40 “active” S-boxes

Dependencies 2 – Higher Probability

- Trail for F with probability 2^{-30} (assuming independence):

$$\begin{tikzcd}
\begin{bmatrix} 00 & 00 & 00 & 40 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} \arrow[r, mapsto, "\text{SB}"] \arrow[r, bend right, "2^{-6}"'] & \begin{bmatrix} 00 & 00 & 00 & 6a \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} \arrow[r, mapsto, "\substack{\text{SR}\\ \text{MC}\\ \text{AC}}"] & \begin{bmatrix} 00 & 00 & 00 & d4 \\ 00 & 00 & 00 & 6a \\ 00 & 00 & 00 & 6a \\ 00 & 00 & 00 & be \end{bmatrix} \arrow[r, mapsto, "\text{SB}"] \arrow[r, bend right, "2^{-6\times 4}"'] & \begin{bmatrix} 00 & 00 & 00 & 2b \\ 00 & 00 & 00 & 61 \\ 00 & 00 & 00 & 61 \\ 00 & 00 & 00 & cd \end{bmatrix} \arrow[r, mapsto, "\substack{\text{SR}\\ \text{MC}}"] & \begin{bmatrix} cd & 61 & a3 & 56 \\ cd & a3 & c2 & 2b \\ 4c & c2 & 61 & 2b \\ 81 & 61 & 61 & 7d \end{bmatrix}
\end{tikzcd}$$

- Differential for F with probability $2^{-27.54}$:

$$\begin{tikzcd}
\begin{bmatrix} 00 & 00 & 00 & 40 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} \arrow[r, mapsto, "\text{SB}"] \arrow[rrr, bend right, "22 \times 2^{-32} \approx 2^{-27.54}"'] & \begin{bmatrix} 00 & 00 & 00 & ?? \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 \end{bmatrix} \arrow[r, mapsto, "\substack{\text{SR}\\ \text{MC}\\ \text{AC}}"] & \begin{bmatrix} 00 & 00 & 00 & ?? \\ 00 & 00 & 00 & ?? \\ 00 & 00 & 00 & ?? \\ 00 & 00 & 00 & ?? \end{bmatrix} \arrow[r, mapsto, "\text{SB}"] & \begin{bmatrix} 00 & 00 & 00 & 2b \\ 00 & 00 & 00 & 61 \\ 00 & 00 & 00 & 61 \\ 00 & 00 & 00 & cd \end{bmatrix} \arrow[r, mapsto, "\substack{\text{SR}\\ \text{MC}}"] & \begin{bmatrix} cd & 61 & a3 & 56 \\ cd & a3 & c2 & 2b \\ 4c & c2 & 61 & 2b \\ 81 & 61 & 61 & 7d \end{bmatrix}
\end{tikzcd}$$

- Probability for 8 rounds: $2^{-4\times 27.54} = 2^{-110.16}$

16-Round Differential Trail

Initial Structures

- Permutation is keyless
- Use message modification to satisfy first rounds

  8-round initial structure (many solutions)

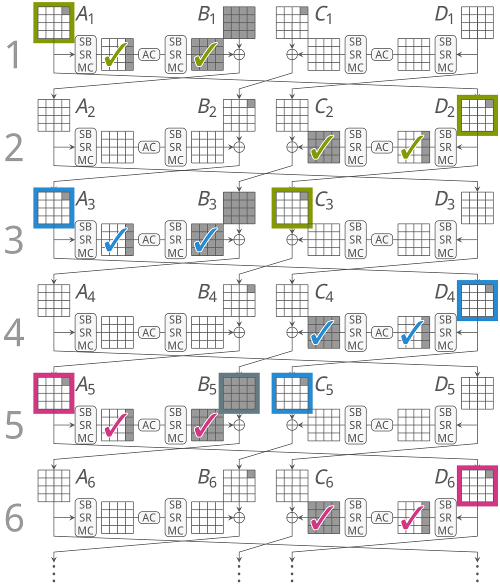
$+$ 8-round trail (probabilistic, $2^{-110.16}$)

$=$ 16-round solution (full rounds $=$ 15)

- To satisfy F-trail, pick 1 (of the 22) valid superbox solutions:

$$\begin{bmatrix} \texttt{00} & \texttt{00} & \texttt{00} & \texttt{40} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \end{bmatrix} \xrightarrow{\text{SB}} \begin{bmatrix} \texttt{00} & \texttt{00} & \texttt{00} & \texttt{??} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{00} \end{bmatrix} \xrightarrow{\substack{\text{SR}\\ \text{MC}\\ \text{AC}}} \begin{bmatrix} \texttt{00} & \texttt{00} & \texttt{00} & \texttt{??} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{??} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{??} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{??} \end{bmatrix} \xrightarrow{\text{SB}} \begin{bmatrix} \texttt{00} & \texttt{00} & \texttt{00} & \texttt{2b} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{61} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{61} \\ \texttt{00} & \texttt{00} & \texttt{00} & \texttt{cd} \end{bmatrix} \xrightarrow{\substack{\text{SR}\\ \text{MC}}} \begin{bmatrix} \texttt{cd} & \texttt{61} & \texttt{a3} & \texttt{56} \\ \texttt{cd} & \texttt{a3} & \texttt{c2} & \texttt{2b} \\ \texttt{4c} & \texttt{c2} & \texttt{61} & \texttt{2b} \\ \texttt{81} & \texttt{61} & \texttt{61} & \texttt{7d} \end{bmatrix}$$

6-Round Initial Structure



1 Satisfy 1 and 2

- fixed
- free

2 Satisfy 3 and 4

- fixed
- free

3 Satisfy 5 and 6

- fixed
- free

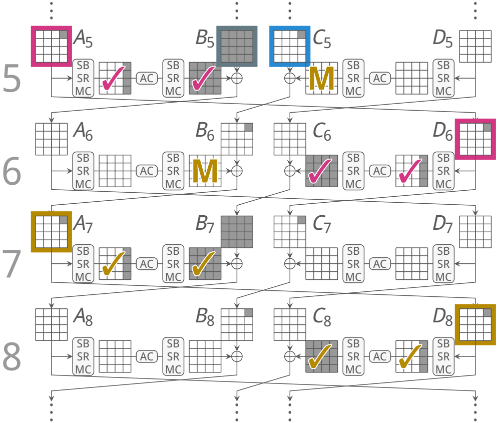
4 Complete

- free

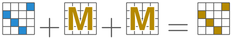
Freedom: 416 bits

Matching to Satisfy 7 and 8

To satisfy 7 and 8, we need a match for the superboxes:



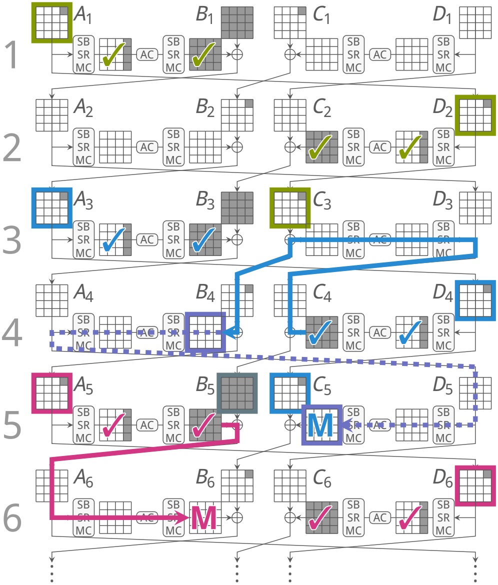
5 Hope that



Birthday effect:

Need to randomize M, M independently!

8-Round Initial Structure



1 Satisfy 1 and 2

▦ ▦ fixed

▦ ▦ , ▦ free

2 Satisfy 5 and 6

▦ ▦ fixed

▦ ▦ match input

3 Satisfy 3 and 4

▦ fixed

▦ match input

- - -> works because:

▦ fixed → ▦ known

▦ fixed → ▦ known

Matching Complexity

0 Fix ▦, ▦, ▦

1 For $2^{110.16-32} = 2^{78.16}$ values of ▦ , ▦ :

2 For 2^{32} values of ▦ :
Compute superbox of M and store in table

3 For 2^{32} values of ▦ :
Compute superbox of M and search for match in table

4 Expect about $2^{2\times 32-32} = 2^{32}$ matches
For each match, test the probabilistic 8-round trail

Expect 1 match, complexity $2^{110.16}$ calls, memory 2^{28} states

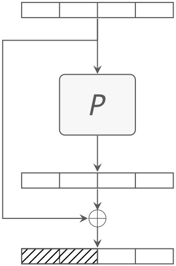
Application: Collision Attacks

Short-Input Hashing with Simpira

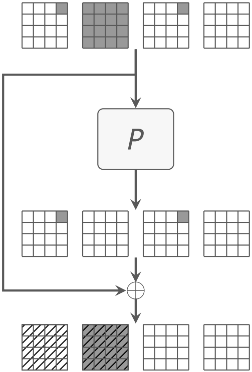
- Proposed application of Simpira [GM16a]

- Permutation with feed-forward
- Input size = permutation size
- Hash size $\leq$ permutation size (truncation)

- Let’s try Simpira-4 with 256-bit hash



15-Round Collisions



256-bit collision with complexity $2^{-110.16}$

Conclusions

Invariant Subspaces

Rønjom [Røn16]

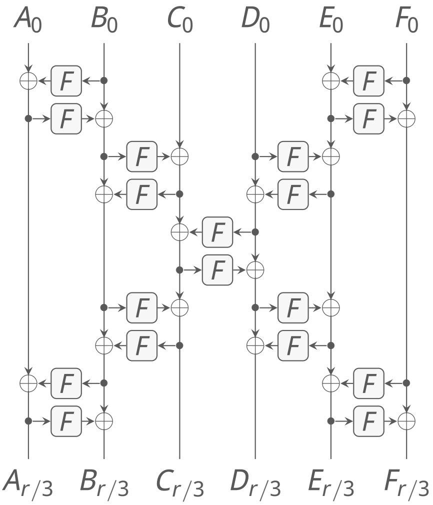
- Independent analysis
- Invariant subspaces for Simpira-4
- Any even number of rounds

- Partition input space in invariant cosets of dim 56 over $\mathbb{F}_{256}^{64}$
- Exploits similar properties of GFS and round constants

Simpira v2

Gueron and Mouha [GM16b]

- Fixes the attack
- Dense round constants
- New Feistel structure



Conclusion

- Distinguisher & collisions for full-round Simpira-4
- Exploited properties:
  - Feistel: Same input to different F-functions
  - F-function: Very similar, round constants too sparse
  - Unkeyed
  - In short: “Active” S-boxes not really independently active
- Observations also affect Simpira-b for $b \geq 4$, $b \neq 6, 8$
- Simpira v2 seems to fix the issues

Bibliography

[Mou+11] N. Mouha, Q. Wang, D. Gu, and B. Preneel
Differential and Linear Cryptanalysis Using Mixed-Integer Linear Programming
Inscrypt 2011

[YI14] S. Yanagihara and T. Iwata
Type 1.x Generalized Feistel Structures
IEICE Transactions 97-A:4,

[GM16a] S. Gueron and N. Mouha
Simpira: A Family of Efficient Permutations Using the AES Round Function
Cryptology ePrint Archive, Report 2016/122

[GM16b] S. Gueron and N. Mouha
Simpira v2: A Family of Efficient Permutations Using the AES Round Function
Cryptology ePrint Archive, Report 2016/122

[Røn16] S. Rønjom
Invariant subspaces in Simpira
Cryptology ePrint Archive, Report 2016/248