Analysis of reduced-SHAvite-3-256 v2

Marine Minier[1], María Naya-Plasencia[2], Thomas Peyrin[3]

[1]Université de Lyon, INRIA, INSA Lyon, France

[2]FHNW, Switzerland

[3]Nanyang Technological University, Singapore

FSE 2011

- **Introduction**
- **The `SHAvite-3`-256 Hash Function**
- **Rebound and Super-Sbox Analysis of** `SHAvite-3-256`
- **Chosen-Related-Salt Distinguishers**
  - 7-round Distinguisher with 2^7 computations
  - 8-round Distinguisher with 2^{25} computations
- **Conclusion**

Hash functions and the SHA3 competition

- Due to attacks against MD5 and the SHA family, NIST launched the SHA-3 competition. Among the phase 2 finalists: SHAvite-3
- Previous analysis on SHAvite-3-512 [Gauravaram et al. 10]: chosen-counter chosen-salt preimage attack on the full compression function
- In this talk, we give a first analysis SHAvite-3-256 which is an AES-based proposal
- Our analysis is based on
  - rebound attack
  - Super-Sbox cryptanalysis
  - chosen related salt

General Overview of SHAvite-3-256

- `SHAvite-3-256` = 256-bit version of `SHAvite-3`
  - based on the HAIFA framework [Biham - Dunkelman 06]
  - The message M is padded and split into 512-bit message blocks $M_0 \| M_1 \| \ldots \| M_{\ell-1}$
  - compression function C_{256} = 256-bit internal state

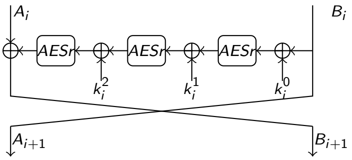
$$\begin{aligned} h_0 &= IV \\ h_i &= C_{256}(h_{i-1}, M_{i-1}, salt, cnt) \\ hash &= trunc_n(h_i) \end{aligned}$$

- C_{256} consists of a 256-bit block cipher E^{256} used in classical Davies-Meyer mode

$$h_i = C_{256}(h_{i-1}, M_{i-1}, salt, cnt) = h_{i-1} \oplus E^{256}_{M_{i-1}\|salt\|cnt}(h_{i-1})$$

The block cipher E^{256}

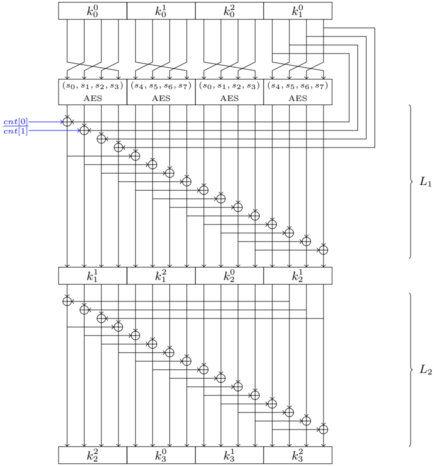
- **12 rounds** of a Feistel scheme
- $h_{i-1} = (A_0, B_0)$, the ith round $(i = 0, \ldots, 11)$ is:



- $AESr$ is unkeyed AES round: SubBytes SB, ShiftRows ShR and MixColumns MC
- k_i^0, k_i^1 and k_i^2 are 128-bit local keys generated by the message expansion

The message expansion of C_{256}: key schedule of E^{256}

- Inputs:
  - M_i: 16 32-bit words $(m_0, m_1, \ldots, m_{15})$
  - *salt*: 8 32-bit words $(s_0, s_1, \ldots, s_7)$
  - *cnt*: 2 32-bit words (cnt_0, cnt_1)
- Outputs:
  - 36 128-bit subkeys k_i^j used at round i
  - k_0^0, k_0^1, k_0^2 and k_1^0 initialized with the m_i
- Process (4 times):
  - 4 parallel AES rounds (key first)
  - 2 linear layers L_1 and L_2



Super-Sbox Analysis of SHAvite-3-256 (1/2)

The cryptanalyst tool 1: the truncated differential path: the trail $\mathtt{D} \mapsto \mathtt{1} \mapsto \mathtt{C} \mapsto \mathtt{F}$ happens with probability 2^{-24}

Super-Sbox Analysis of SHAvite-3-256 (1/2)

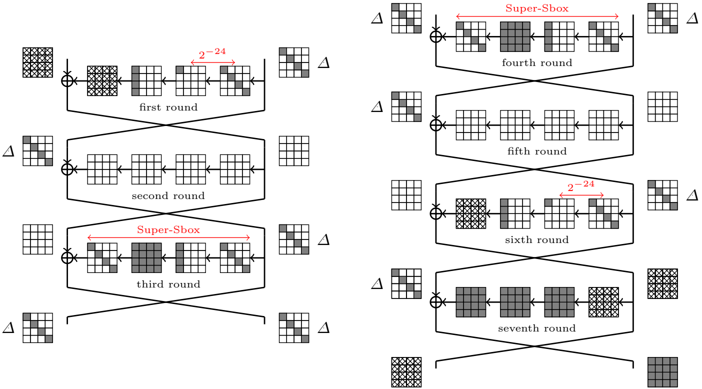
The cryptanalyst tool 1: the truncated differential path: the trail $\mathtt{D} \mapsto \mathtt{1} \mapsto \mathtt{C} \mapsto \mathtt{F}$ happens with probability 2^{-24}

The cryptanalyst tool 2: the freedom degrees and the Super-Sbox

- **Rebound attack** on 2 AES rounds: local meet-in-the-middle-like technique: the freedom degrees are consumed in the middle part of the differential
- **Super-Sbox** on 3 AES rounds:
  - Complexity: $\max\{2^{32}, k\}$ computations; 2^{32} memory
  - For k solutions
- Both methods find **in average one solution for one operation**

Super-Sbox Analysis of SHAvite-3-256 (2/2)

- **7-round distinguisher in 2^{48} computations and 2^{32} memory** (v.s. 2^{64} computations for the ideal case)

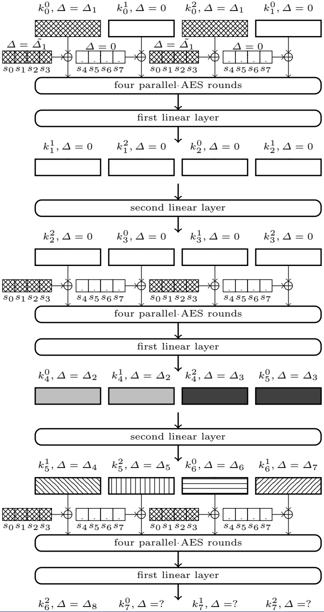


- **1st and 6th rounds:** 2^{-48} to find a valid pair when Δ is fixed
- **Middle part (3d and 4th rounds):** Fix Δ then using Super-Sbox, find 2^{32} valid 128-bit pair for the 4th round, do the same for the 3d round

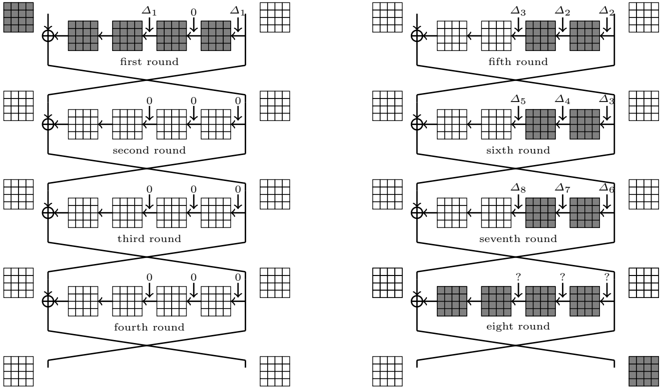
Chosen-Related-Salt Distinguishers

7-round Distinguisher with 2^7 computations (1/2)

- Principle: up to initial transform $\Delta_1 = \Delta(s_0, s_1, s_2, s_3) = \Delta(m_0, m_1, m_2, m_3) = \Delta(m_8, m_9, m_{10}, m_{11})$
- Cancel the subkeys in round 2,3 and 4
- Distinguisher: find a valid pair that verifies the path for the rounds 5, 6 and 7
- begin at round 5 by fixing the differences Δ_2 and Δ_3



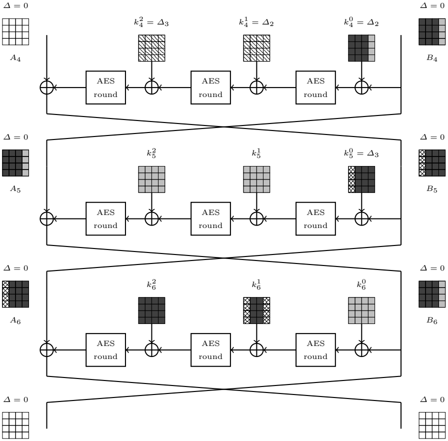
7-round Distinguisher with 2^7 computations (2/2)



- *5th round*: try 2^6 $B_4 \oplus k_4^0$ column by column to find a match. It will fix k_4^1
- *6th round*: Do the same with $B_5 \oplus k_5^0$ and k_5^1
- *Final step*: Fix Δ_1 and k_5^0 to fix all the other values
- **Total cost:** $2 \times 2^6 = 2^7$ operations

8-round Distinguisher with 2^{25} computations (1/2)

- Add a 8th round by canceling the differences in round 7
- Do Round 5 and 6 as previously: Δ_2, Δ_3, $B_4 \oplus k_4^0$, k_4^1, $B_5 \oplus k_5^0$ and k_5^1 are fixed
- Start by fixing the differences in the 7th round column by column:



Relations between the values:

$(B_6)^i \implies (A_5)^i = (B_4)^i \implies (k_4^0)^i$

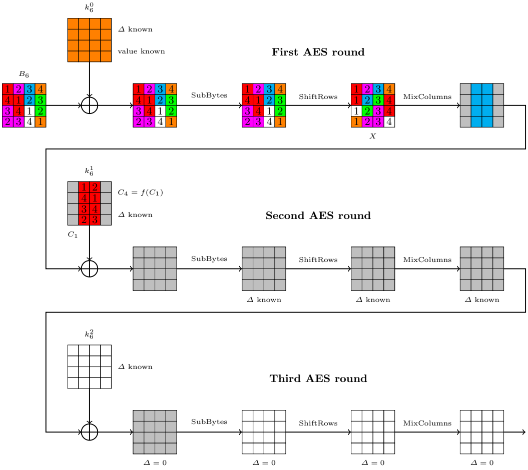
$(k_4^0)^i \implies (k_5^0)^{i+1} \implies (k_6^1)^{i+1}$

$(k_4^0)^2 \implies (k_5^0)^3 \implies (k_6^1)^3 = (k_5^0)^3 \oplus (k_6^1)^0$

8-round Distinguisher with 2^{25} computations (2/2)

Overall Complexity: 2^{25} computations

Requirements for verifying the path: $\Delta(k_6^0)^i$ compatible with $\Delta(X)^i$ and $MC(\Delta(X)^i) \oplus \Delta(k_6^1)^i$ compatible with Δk_6^2



- Test 2^{24} values for the 2nd diagonal $(B_6*)^1$, 2^{13} makes the path possible
- Do the same for the 3rd diagonal. 2^{12} values of $(B_6*)^1$ and $(B_6*)^2$ together are valid
- For each solution, find the 2^{20} values of $(B_6*)^3$ and $(B_6*)^0$ compatible
- Test the linear relation between $(k_6^1)^0$ and $(k_6^1)^3$

Conclusion

- First analysis of `SHAvite-3-256` v2: Super-Sbox cryptanalysis and the rebound attacks are efficient
- 7 and 8-round distinguishers have been implemented
- But `SHAvite-3-256` has 12 rounds, so a sufficient security margin. Maybe better paths in the key schedule

Table: Summary of results for the `SHAvite-3-256` compression function

rounds	computational complexity	memory requirements	type
6	2^{80}	2^{32}	free-start collision
7	2^{48}	2^{32}	distinguisher
7	2^{7}	2^{7}	chosen-related-salt distinguisher
7	2^{25}	2^{14}	chosen-related-salt free-start near-collision
7	2^{96}	2^{32}	chosen-related-salt semi-free-start collision
8	2^{25}	2^{14}	chosen-related-salt distinguisher

Thanks for your attention !