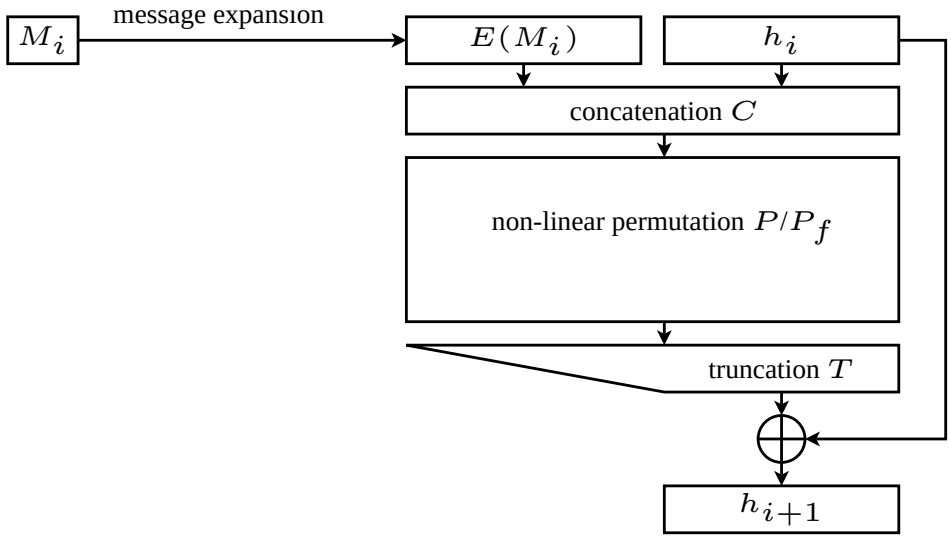
On Hamsi

Jean-Philippe Aumasson Emilia Käsper
Lars Ramkilde Knudsen Krystian Matusiewicz
Rune Ødegård Thomas Peyrin Martin Schläffer

Hamsi

- Second-round SHA-3 candidate by Kücük (KUL)
- Two main instances: **Hamsi-256** and Hamsi-512
- Serpent-like algorithm (4-bit Sbox + linear layer)

Davies-Meyer compression function



3 rounds (6 for the last compression)

Definitions

***k*-sum** problem for Hamsi's compression function f

Find $x_1, \ldots, x_k$ strings of n bits such that

$$\bigoplus_{i=1}^{k} f(x_k) = 0$$

Zero-sum problem: additional requirement that $\bigoplus_{i=1}^{k} x_i = 0$

Generic method: generalized birthday in $O(k2^{n/(1+\log k)})$

XHASH attack (linear algebra) for $k \approx n$

Finding k-sums and zero-sums

Observations:

- 3 rounds have degree 3 only, instead of ideally 27 (with respect to carefully chosen variables)
- Distribution of monomials and binomials is sparse

Finding k-sums and zero-sums

Observations:

- 3 rounds have degree 3 only, instead of ideally 27 (with respect to carefully chosen variables)
- Distribution of monomials and binomials is sparse

Consequences:

16-, 8-, 4-sums can be found efficiently

Example found for the default IV of Hamsi...

Zero-sums can be found efficiently for the permutation

Need only to know half the algorithm, deterministic
(see CHES'09 rump for details of the technique)

Near collisions (2/XXX)

Previous results:

- $(256 - 25)$-bit collision from 14 bit differences (Nikolic)
- $(256 - 23)$-bit collision from 16 bit differences (Wang et al.)

Near collisions (2/XXX)

Previous results:

- $(256 - 25)$-bit collision from 14 bit differences (Nikolic)
- $(256 - 23)$-bit collision from 16 bit differences (Wang et al.)

We found a differential characteristic of probability 2^{-26}

Consequence:

$(256 - 25)$-bit collision from 6 bit differences

Easier for the default IV than for a random one (prob. 2^{-23})

Search for differential characteristics

Analysis of Sbox and linear layer differential properties...

Found a 6-round characteristic with probability 2^{-148}

Ideally, each differential should have probability $\approx 2^{-256}$

Using "relaxable differential transitions" and truncated differentials, increase the probability to 2^{-121}

Search for differential characteristics

Analysis of Sbox and linear layer differential properties...

Found a 6-round characteristic with probability 2^{-148}

Ideally, each differential should have probability $\approx 2^{-256}$

Using "relaxable differential transitions" and truncated differentials, increase the probability to 2^{-121}

Multicollision-based approach

Differential multicollisions can be found in 2^{124} on 6 rounds

$\Rightarrow$ Distinguishers for the full 6-round compression of Hamsi-256

Conclusion

Higher-order and standard differential cryptanalysis applied to the compression function of Hamsi-256

- Suboptimal algebraic degree
- k-sums and zero-sums found efficiently
- Near collisions
- Differentials characteristic on 6 rounds
- Differential multicollisions on 6 rounds

Hash function safe, but building blocks unideal