Near Collisions for the Compression Function of Hamsi-256

Ivica Nikolić

University of Luxembourg

18 Aug 2009

Hamsi - SHA-3 candidate

Hamsi hash function

- Designed by Özgül Kücük, Katholieke Universiteit Leuven
- Second round NIST candidate
- Best (and only) attack: J.-Ph. Aumasson - On the pseudorandomness of Hamsi

The Compression Function of Hamsi-256

Input: 256-bit chaining value, 32-bit message

- Expand the message block to 256 bits
- Concatenate to the state, obtain 4×4 matrix of 32-bit words
- Apply 3-round permutation (constants addition, S-boxes and linear diffusions)
- Feedforward the chaining value

Output: Two rows of the matrix

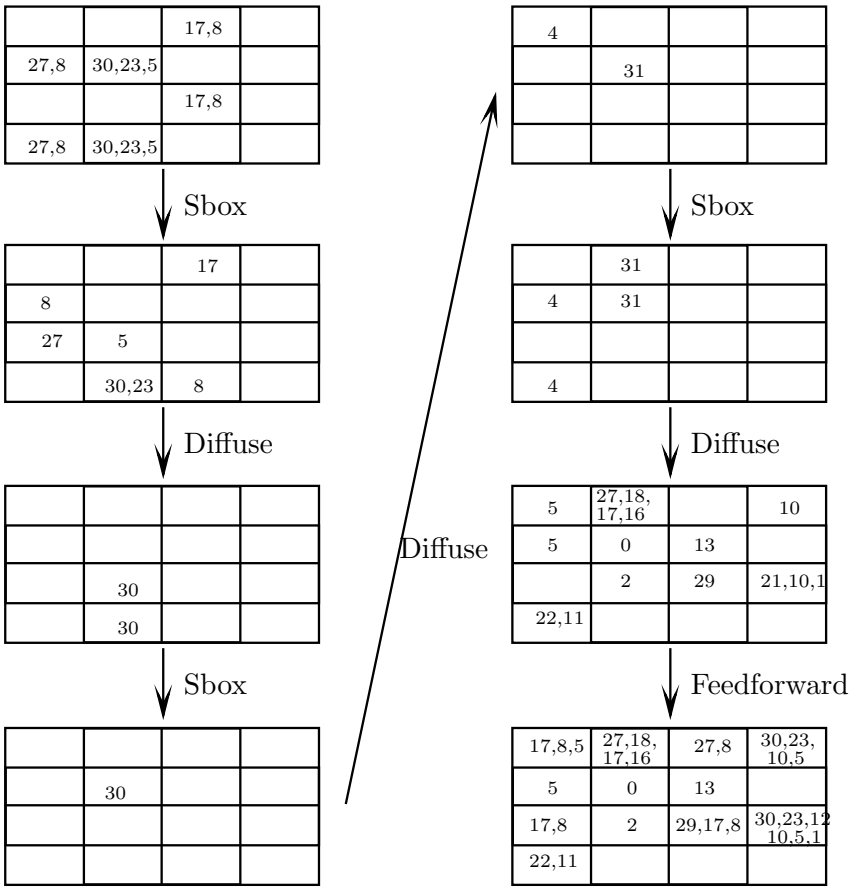
Initial Analysis

Pros and cons for the attacker:
−: Message expansion, relatively fast diffusion(S-boxes+linear diffusion)
+: Only 3 rounds

Ideas:

1. Introduce difference only in the chaining value
2. Start from a low Hamming weight state in the second round

Near collisions for Hamsi-256



- No difference in the message blocks
- Use message (chaining value) modification technique to get the first round for free
- Only three active S-boxes

Result: Near collisions with Hamming distance of 25 bits with 2^{21} CF evaluations