The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl

Florian Mendel[1], Christian Rechberger[1], *Martin Schläffer*[1], Søren S. Thomsen[2]

[1] Institute for Applied Information Processing and Communications (IAIK)
Graz University of Technology, Inffeldgasse 16a, A-8010 Graz, Austria

[2] Department of Mathematics, Technical University of Denmark
Matematiktorvet 303S, DK-2800 Kgs. Lyngby, Denmark

Overview

Overview

Motivation

- NIST SHA-3 Competition
  - diversity of designs
  - diversity of cryptanalytic tools needed
- Many AES based designs
  - how to analyze them?
  - we contribute with new attack to this toolbox
- Applications?
  - idea of attack is widely applicable
  - Whirlpool, Grøstl

Overview

Collision Attacks on Hash Functions

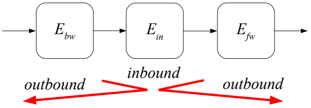
- iterated hash function $h(M, IV)$
  - compression function f: $H_t = f(M_t, H_{t-1}),\ H_0 = IV$
- different types of collision attacks:
  (1) collision:
  - fixed IV
  - $f(M_t, IV) = f(M'_t, IV),\ M_t \neq M'_t$

  (2) semi-free-start collision:
  - random chaining input
  - $f(M_t, H_{t-1}) = f(M'_t, H_{t-1}),\ M_t \neq M'_t$

  (3) free-start collision:
  - random differences and values of chaining input
  - $f(M_t, H_{t-1}) = f(M'_t, H'_{t-1}),\ M_t \neq M'_t, H_{t-1} \neq H'_{t-1}$

$\Rightarrow$ increasing degrees of freedom

The Rebound Attack



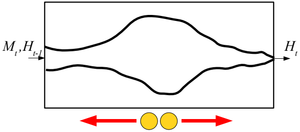
- Applies to block-cipher and permutation based designs:

$$E = E_{fw} \circ E_{in} \circ E_{bw} \qquad P = P_{fw} \circ P_{in} \circ P_{bw}$$

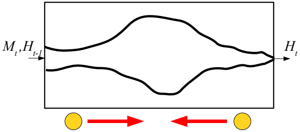
- **Inbound phase:**
  - efficient meet-in-the-middle phase in E_{in}
  - aided by available degrees of freedom
  - called *match-in-the-middle*
- **Outbound phase:**
  - probabilistic part in E_{bw} and E_{fw}
  - repeat inbound phase if needed

Comparison with other Strategies

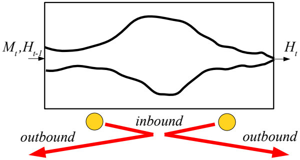
- inside-out approach:



- meet-in-the-middle attack:

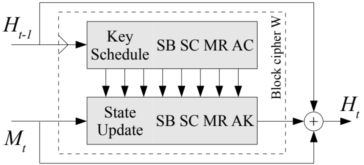


- rebound attack:



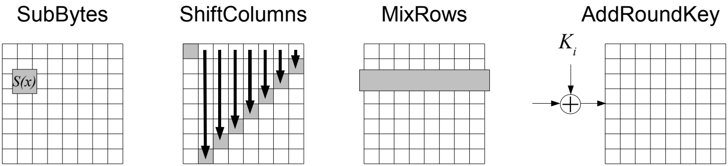
Overview

The Whirlpool Hash Function



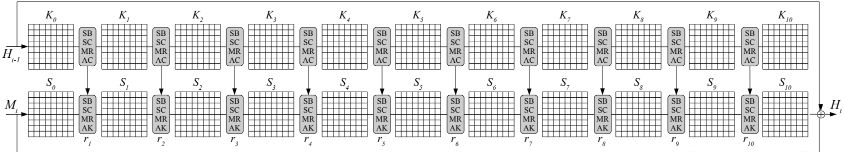
- Designed by Barretto and Rijmen
  - submitted to NESSIE in 2000
  - standardized by ISO/IEC 10118-3:2003
- 512-bit hash value and using 512-bit message blocks
- Block-cipher based (AES)
  - Miyaguchi-Preneel mode with conservative key-schedule
- No attacks in 8 years of existence

The Whirlpool Round Transformations

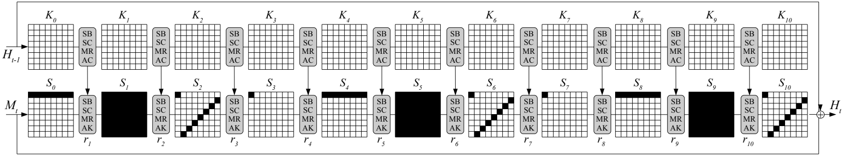


- 10 rounds
- AES like round transformations on two 8 × 8 states

$$k_i = AC \circ MR \circ SC \circ SB \qquad r_i = AK \circ MR \circ SC \circ SB$$



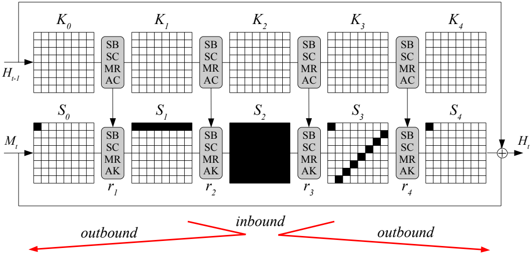
Wide-Trails in Whirlpool



- Minimum number of active S-boxes
  - 81 for any 4-round trail: $(8 - 64 - 8 - 1)$
  - maximum differential probability: $(2^{-5})^{81} = 2^{-405}$
- Collision attack on Whirlpool: $< 2^{256}$
  - use “message modification” techniques (first rounds)
  - a full active state remains: probability $(2^{-5})^{64} = 2^{-320}$

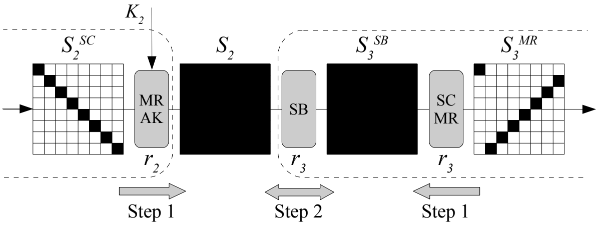
Overview

The Rebound Attack on Whirlpool



- Inbound phase:
  - (1) start with differences in round r_2 and r_3
  - (2) match-in-the-middle at S-box using values of the state
- Outbound phase:
  - (3) probabilistic propagation in MixRows of r_1 and r_4
  - (4) match one-byte difference of feed-forward

Inbound Phase

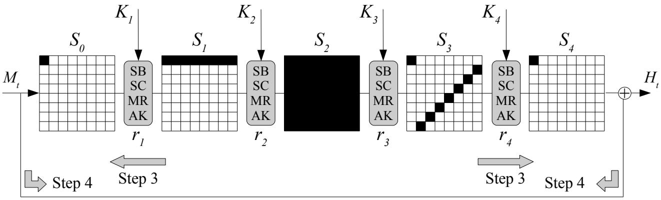


(1) Start with differences in state S_2^{SC} and S_3^{MR}
- linear propagation to full active state of S_2 and S_3^{SB}
- deterministic due to MDS property of MixRows

(2) Match-in-the-middle at S-box of round r_3
- differential match for single S-box: probability $\sim 2^{-1}$
- for each match we get 2-8 possible values for the S-box

$\Rightarrow$ with a complexity of 2^{64}, we get 2^{64} matches

Outbound Phase



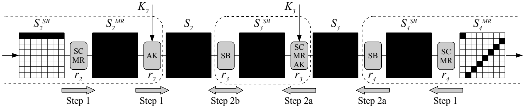
(3) Propagate through MixRows of r_1 and r_4

- using truncated differences (active bytes: $8 \rightarrow 1$)
- probability: 2^{-56} in each direction

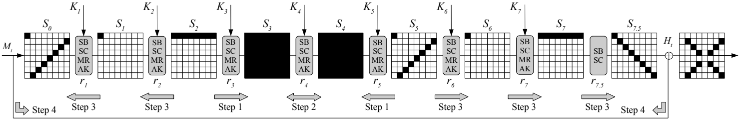
(4) Match difference in one active byte of feed-forward

$\Rightarrow$ complexity for 4 round collision of Whirlpool: 2^{120}

Extension to more Rounds



- Semi-free-start collision on 5 rounds
  - extend inbound phase using degrees of freedom in key
  - same complexity (2^{120}) as in 4 round attack



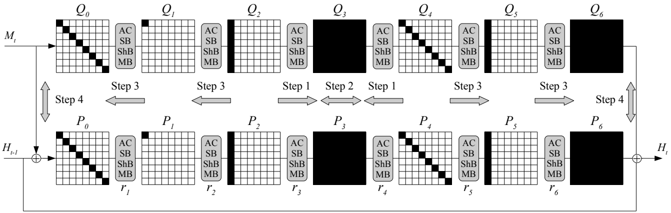
- Semi-free-start near-collision on 7.5 rounds
  - extend outbound phase with probability one (MixRows)
  - near-collision on 52 of 64 bytes (2^{128})

Overview

SHA-3 Candidate Grøstl

- Compression function of Grøstl
  - permutation based, no key-schedule inputs
  - AES based round transformations (AC, SB, ShB, MB)
- Grøstl-256: 8×8 state for P_{512} and Q_{512}
  - 8×8 state for P_{512} and Q_{512}
  - 10 rounds each

Rebound Attack on Grøstl-256



- Semi-free-start collision on 6 rounds of Grøstl-256
  - less degrees of freedom (no key schedule input)
  - maximize using differential trails in both permutations
  - birthday match on input and output differences
- Complexity of attack: $\sim 2^{120}$

Overview

Results

- Summary of attacks:

hash function	rounds	computational complexity	memory requirements	type
Whirlpool	4.5/10	2^{120}	2^{16}	collision
	5.5/10	2^{120}	2^{16}	semi-free-start collision
	7.5/10	2^{128}	2^{16}	semi-free-start near-collision
Grøstl-256	6/10	2^{120}	2^{70}	semi-free-start collision

- Improvements?
  - still degrees of freedom in key schedule left (Whirlpool)
  - 8.5/10 rounds attack on Maelstrom[1] (1024 bit key)
  - 8.5/12 rounds of SHA-3 candidate Cheetah-512

[1] Gazzoni Filho, Barreto, Rijmen (SBSeg 2006)

Conclusions

- The Rebound Attack
    - inbound phase for expensive parts
    - outbound phase for “cheaper” parts
- Contribute to hash function cryptanalysis toolbox
    - improved analysis of AES based designs
    - better attacks for more degrees of freedom
    - simple designs allow simple analysis
- Future work
    - apply to other design strategies
    - analyze SHA-3 candidates
    - give bounds for simple AES based designs