On the 0.5-Round of Whirlpool

Yu Sasaki

NTT Corporation

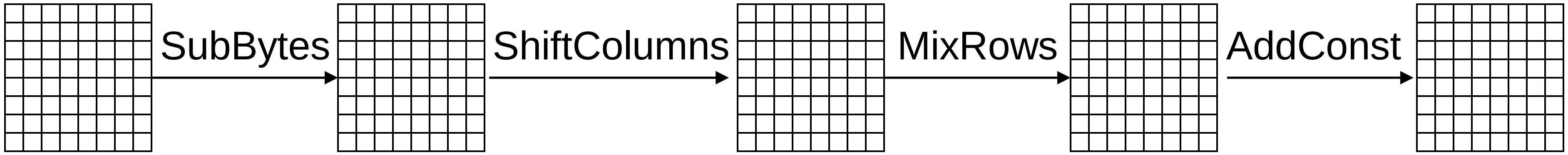
(Feb.14, 2011, Rump session of FSE2011)

Whirlpool

- 512-bit hash function standardized by NESSIE and ISO.

- Based on AES with 8*8-byte state.

Round function



- 10-rounds with MixRows in the last round.

Current Best Attacks

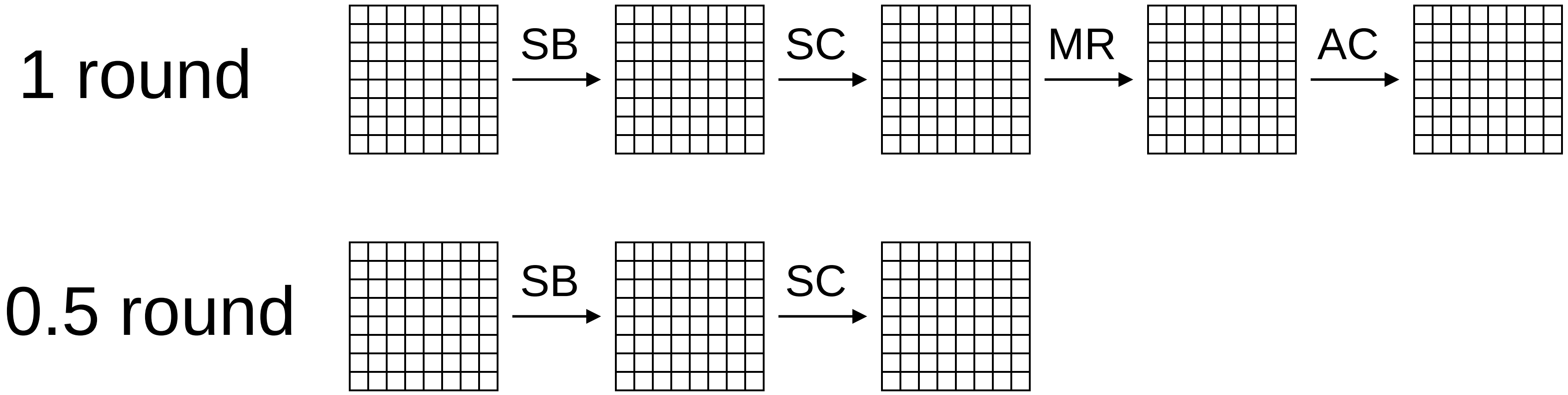
- Distinguisher on the compression function
  - 10 (full) rounds [LMRRS09]
- Preimage attack on the hash function
  - Nothing
- Collision attack on the hash function
  - 5.5 rounds [LMRRS09]

Current Best Attacks

- Distinguisher on the compression function
  - 10 (full) rounds [LMRRS09]
- Preimage attack on the hash function
  - Nothing
- Collision attack on the hash function
  - 5.5 rounds [LMRRS09]

0.5 round ??

0.5 round of Whirlpool [MRST09]



1 round: SB → SC → MR → AC

0.5 round: SB → SC

- Reasonable if AES structure is taken into account. (Omission of MixColumns in the last round)

However,

- 1 round is asymmetric. 0.5 round is not the half.

Attack Results on Whirlpool

(Details will be presented on the last day.)

	Collision [LMRS09]	Preimage [Ours]
5 rounds	✓	✓
5.5 rounds	✓	✓
6 rounds	✗	✗
6.5 rounds	✗	

Attack Results on Whirlpool

(Details will be presented on the last day.)

	Collision [LMRS09]	Preimage [Ours]
5 rounds	✓	✓
5.5 rounds	✓	✓
6 rounds	✗	✗
6.5 rounds	✗	✓

Attack Results on Whirlpool

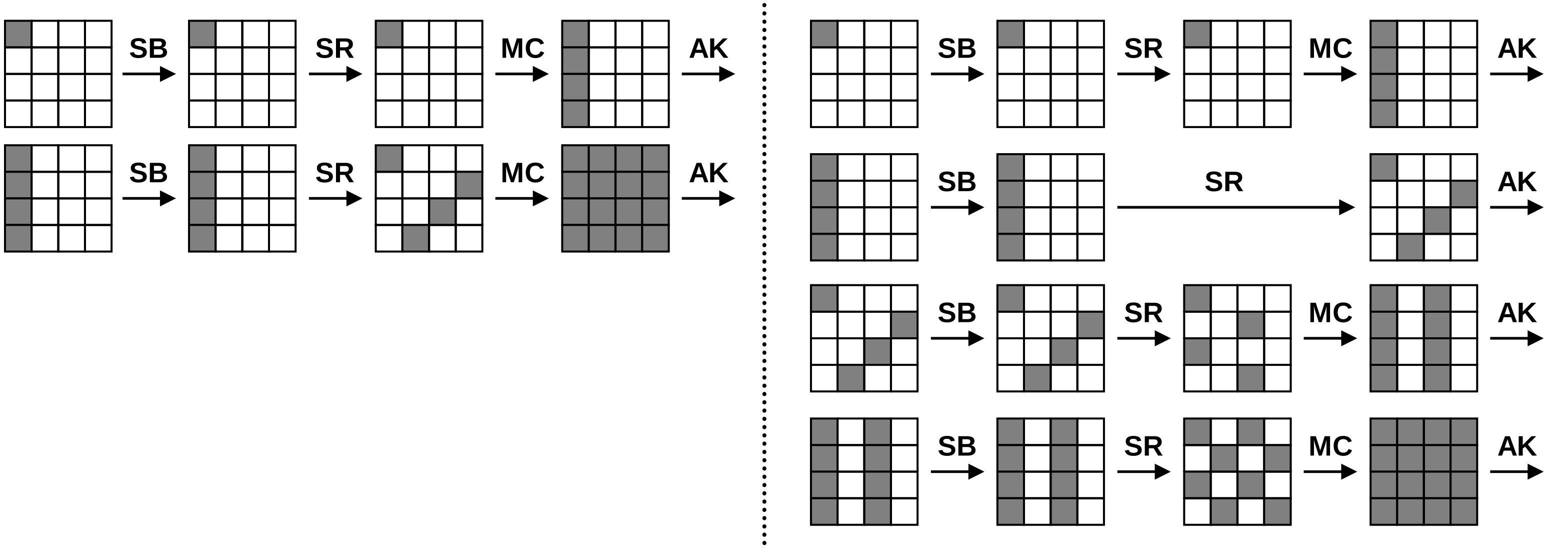
(Details will be presented on the last day.)

	Collision [LMRS09]	Preimage [Ours]
5 rounds	✓	✓
5.5 rounds	✓	✓
6 rounds	✗	✗
6.5 rounds	✗	✓

6.5R is weaker than 6R !!

Omission of last MixColumns

- Omission of the last MixColumns does not impact to the security of block-ciphers.
- In hash functions, we can access to internal states, and start the analysis from the second last round.



Full diffusion after 2R.   4R is needed for full diffusion.

Summary

- 6.5-round Whirlpool is weaker than 6-round Whirlpool in our analysis.
- This seems to be caused by the asymmetric counting method of 0.5 round.
- We suggest to stop the 0.5-round count, which seems unsuitable for hash functions.

Thank you for your attention!!

Details will be presented on the last day.