Collision Attack on 5 Rounds of Grøstl

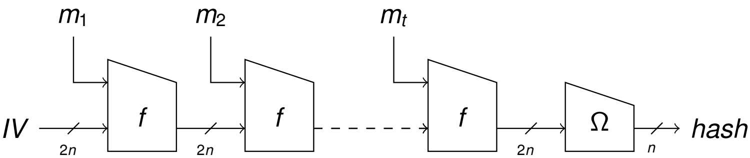
Florian Mendel Vincent Rijmen Martin Schläffer

TU Graz

KU LEUVEN

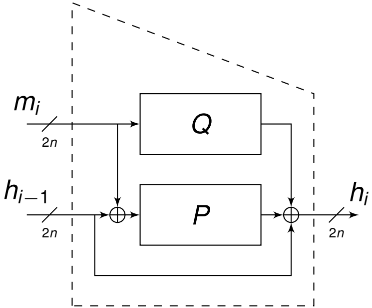
The Grøstl Hash Function

The Grøstl Hash Function



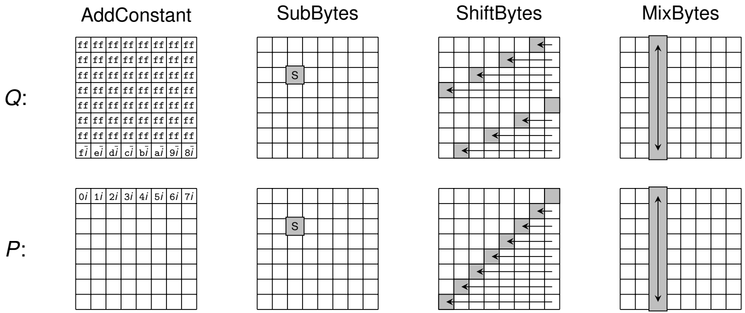
- SHA-3 finalist designed by Knudsen et al.
  - iterative, Merkle-Damgård design principle
  - wide-pipe construction, $2n$-bit chaining value

The Grøstl Compression Function



- Permutation based design
  - 8×8 state and 10 rounds for Grøstl-256
  - 8×16 state and 14 rounds for Grøstl-512

The Grøstl-256 Round Transformations



- AES like round transformation

$$r_i = MB \circ SH \circ SB \circ AC$$

Existing Analysis of Grøstl

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis
- Initiated by the design team itself $\rightarrow$ rebound attack

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis
- Initiated by the design team itself $\rightarrow$ rebound attack
- Several improvements have been made

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis
- Initiated by the design team itself $\rightarrow$ rebound attack
- Several improvements have been made
  - Internal differential attack

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis
- Initiated by the design team itself $\rightarrow$ rebound attack
- Several improvements have been made
  - Internal differential attack
  - Zero-sum distinguisher

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis
- Initiated by the design team itself $\rightarrow$ rebound attack
- Several improvements have been made
  - Internal differential attack
  - Zero-sum distinguisher
  - Meet-in-the-middle attacks

Existing Analysis of Grøstl

- Grøstl received a large amount of cryptanalysis
- Initiated by the design team itself $\rightarrow$ rebound attack
- Several improvements have been made
  - Internal differential attack
  - Zero-sum distinguisher
  - Meet-in-the-middle attacks
  - ...

Existing Analysis of Grøstl I

Elena Andreeva, Bart Mennink, and Bart Preneel.
On the Indifferentiability of the Grøstl Hash Function.
In Juan A. Garay and Roberto De Prisco, editors, *SCN*, volume 6280 of *LNCS*, pages 88–105. Springer, 2010.

Elena Andreeva, Bart Mennink, Bart Preneel, and Marjan Skrobot.
Security Analysis and Comparison of the SHA-3 Finalists BLAKE, Grøstl, JH, Keccak, and Skein.
In Aikaterini Mitrokotsa and Serge Vaudenay, editors, *AFRICACRYPT*, volume 7374 of *LNCS*, pages 287–305. Springer, 2012.

Paulo S. L. M. Barreto.
An observation on Grøstl.
NIST hash function mailing list, 2008.

Christina Boura, Anne Canteaut, and Christophe De Cannière.
Higher-Order Differential Properties of Keccak and Luffa.
In Antoine Joux, editor, *FSE*, volume 6733 of *LNCS*, pages 252–269. Springer, 2011.

Sareh Emami, Praveen Gauravaram, Josef Pieprzyk, and Ron Steinfeld.
(Chosen-multi-target) preimage attacks on reduced Grøstl.
`http://web.science.mq.edu.au/~rons/preimageattack-final.pdf`.

Henri Gilbert and Thomas Peyrin.
Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations.
In Seokhie Hong and Tetsu Iwata, editors, *FSE*, volume 6147 of *LNCS*, pages 365–383. Springer, 2010.

Existing Analysis of Grøstl II

Kota Ideguchi, Elmar Tischhauser, and Bart Preneel.
Improved Collision Attacks on the Reduced-Round Grøstl Hash Function.
In Mike Burmester, Gene Tsudik, Spyros S. Magliveras, and Ivana Ilic, editors, *ISC*, volume 6531 of *LNCS*, pages 1–16. Springer, 2010.

Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin.
Improved Rebound Attack on the Finalist Grøstl.
In Anne Canteaut, editor, *FSE*, volume 7549 of *LNCS*, pages 110–126. Springer, 2012.

Jérémy Jean, María Naya-Plasencia, and Thomas Peyrin.
Multiple Limited-Birthday Distinguishers and Applications.
In Tanja Lange, Kristin Lauter, and Petr Lisonek, editors, *Selected Areas in Cryptography*, LNCS. Springer, 2013.

John Kelsey.
Some notes on Grøstl.
NIST hash function mailing list, 2009.

Florian Mendel, Thomas Peyrin, Christian Rechberger, and Martin Schläffer.
Improved Cryptanalysis of the Reduced Grøstl Compression Function, ECHO Permutation and AES Block Cipher.
In Michael J. Jacobson Jr., Vincent Rijmen, and Reihaneh Safavi-Naini, editors, *Selected Areas in Cryptography*, volume 5867 of *LNCS*, pages 16–35. Springer, 2009.

Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen.
The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl.
In Orr Dunkelman, editor, *FSE*, volume 5665 of *LNCS*, pages 260–276. Springer, 2009.

Existing Analysis of Grøstl III

Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen.
Rebound Attacks on the Reduced Grøstl Hash Function.
In Josef Pieprzyk, editor, *CT-RSA*, volume 5985 of *LNCS*, pages 350–365. Springer, 2010.

Marine Minier and Gaël Thomas.
An Integral Distinguisher on Grøstl-512.
In Goutam Paul and Serge Vaudenay, editors, *INDOCRYPT*, volume 8250 of *LNCS*, pages 50–59. Springer, 2013.

Thomas Peyrin.
Improved Differential Attacks for ECHO and Grøstl.
In Tal Rabin, editor, *CRYPTO*, volume 6223 of *LNCS*, pages 370–392. Springer, 2010.

Yu Sasaki, Yang Li, Lei Wang, Kazuo Sakiyama, and Kazuo Ohta.
Non-full-active Super-Sbox Analysis: Applications to ECHO and Grøstl.
In Masayuki Abe, editor, *ASIACRYPT*, volume 6477 of *LNCS*, pages 38–55. Springer, 2010.

Yu Sasaki, Yuuki Tokushige, Lei Wang, Mitsugu Iwamoto, and Kazuo Ohta.
An Automated Evaluation Tool for Improved Rebound Attack: New Distinguishers and Proposals of ShiftBytes Parameters for Grøstl.
In Josh Benaloh, editor, *CT-RSA*, volume 8366 of *LNCS*, pages 424–443. Springer, 2014.

Martin Schläffer.
Updated Differential Analysis of Grøstl.
`http://groestl.info`, 2011.

Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, and Jian Zou.
(Pseudo) Preimage Attack on Round-Reduced Grøstl Hash Function and Others.
In Anne Canteaut, editor, *FSE*, volume 7549 of *LNCS*, pages 127–145. Springer, 2012.

Attacks on the Hash Function

- Most of the analysis focus on the building blocks of Grøstl

Attacks on the Hash Function

- Most of the analysis focus on the building blocks of Grøstl
- Only a few results have been published for the hash function

	rounds	complexity	memory
Grøstl-256	3	2^{64}	-
Grøstl-512	3	2^{192}	-

Attacks on the Hash Function

- Most of the analysis focus on the building blocks of Grøstl
- Only a few results have been published for the hash function

	rounds	complexity	memory
Grøstl-256	3	2^{64}	-
Grøstl-512	3	2^{192}	-

$\Rightarrow$ We will show collision attacks for up to 5 rounds of Grøstl

Basic Attack Strategy

Basic Attack Strategy

- Combines ideas of the attack on SMASH with the rebound attack

Basic Attack Strategy

- Combines ideas of the attack on SMASH with the rebound attack
- Similar to the attack on Grindahl

Basic Attack Strategy

- Combines ideas of the attack on SMASH with the rebound attack
- Similar to the attack on Grindahl

- Attack uses a new type of truncated differential trail spanning over more than one message block

Basic Attack Strategy

- Combines ideas of the attack on SMASH with the rebound attack
- Similar to the attack on Grindahl

- Attack uses a new type of truncated differential trail spanning over more than one message block
  - Starting with an (almost) arbitrary difference in the chaining variable

Basic Attack Strategy

- Combines ideas of the attack on SMASH with the rebound attack
- Similar to the attack on Grindahl

- Attack uses a new type of truncated differential trail spanning over more than one message block
  - Starting with an (almost) arbitrary difference in the chaining variable
  - Iteratively canceling the differences in the chaining variable

Basic Attack Strategy

- Combines ideas of the attack on SMASH with the rebound attack
- Similar to the attack on Grindahl

- Attack uses a new type of truncated differential trail spanning over more than one message block
  - Starting with an (almost) arbitrary difference in the chaining variable
  - Iteratively canceling the differences in the chaining variable
  - Having only differences in one of the two permutations

Equivalent Description of Grøstl

- To simplify the description of the attack we use an equivalent description of Grøstl

$$\begin{aligned} h'_0 &= MB^{-1}(\mathrm{IV}) \\ h'_i &= P'(MB(h'_{i-1}) \oplus m_i) \oplus Q'(m_i) \oplus h'_{i-1} \quad \text{for } 1 \leq i \leq t \\ hash &= \Omega(MB(h'_t)) \end{aligned}$$

  with $h_i = MB(h'_i)$

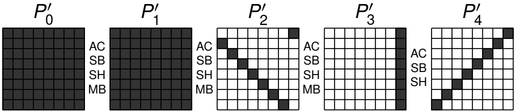
- The last MixBytes transformation of the permutations P and Q are swapped with the XOR operation of the feed-forward

Attack on 4 Rounds of Grøstl-256

- The core of the attack on 4 rounds are truncated differential trails for P' with only 8 active bytes at the output of round r_4

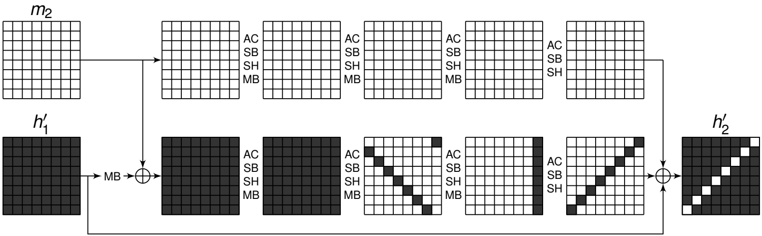
$$64 \xrightarrow{r_1} 64 \xrightarrow{r_2} 8 \xrightarrow{r_3} 8 \xrightarrow{r_4} 8$$

- Using the rebound attack all the 2^{64} solutions for this truncated differential trail with a given/fixed difference difference at the input of P' can be found with complexity 2^{64} in time and memory



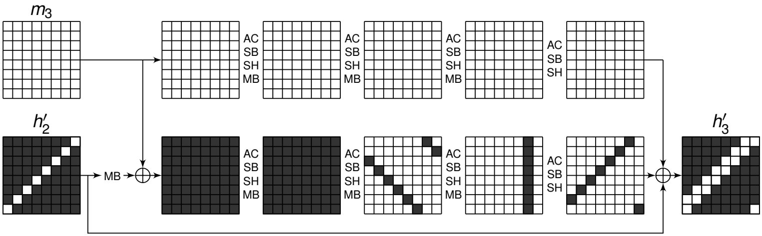
Attack on 4 Rounds of Grøstl-256

- Choose some arbitrary m_1, m_1^* to get a full active state in h_1'
- Construct 2^{64} solutions for the truncated differential trail in P' to find a m_2 such that 8 bytes of the difference in h_2' are canceled



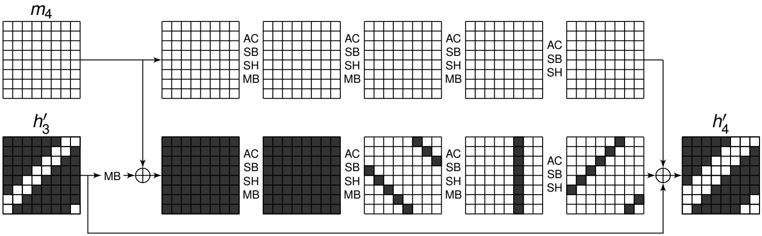
Attack on 4 Rounds of Grøstl-256

- Construct 2^{64} solutions for a rotated variant of the truncated differential trail to cancel another 8 bytes of the difference in h'_3



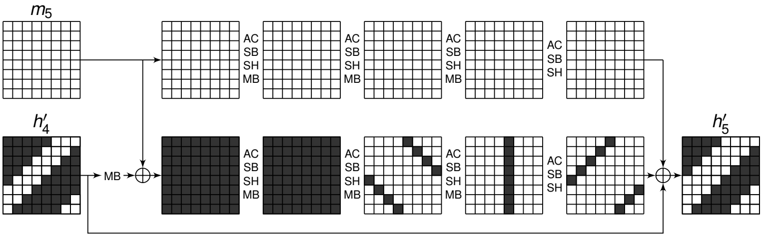
Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



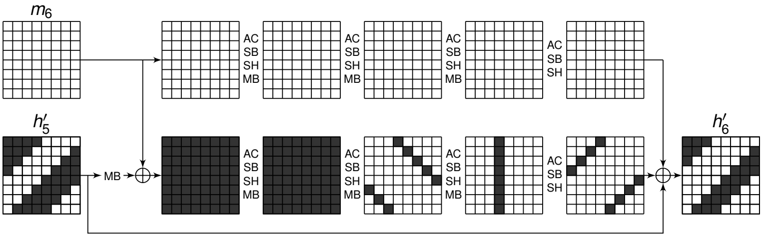
Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



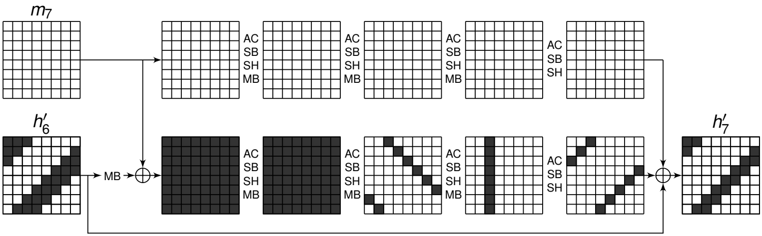
Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



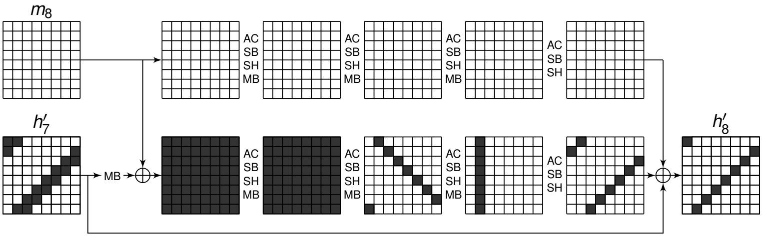
Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



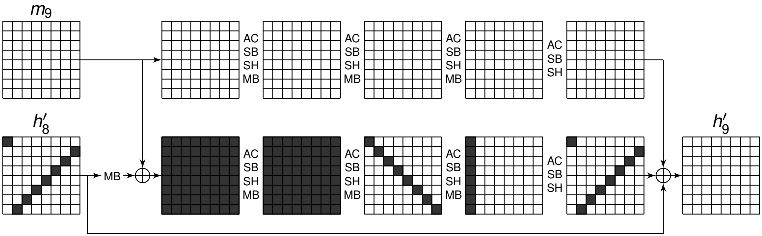
Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



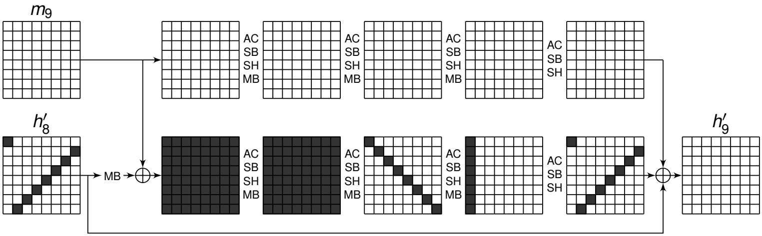
Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



Attack on 4 Rounds of Grøstl-256

- Repeat this in total 8 times until a collision has been found in h'_9



$\Rightarrow$ Collision attack for 4 rounds with complexity of $8 \cdot 2^{64} = 2^{67}$

Extending the Attack to 5 Rounds

Attack on 5 Rounds of Grøstl-256

- For the attack on 5 rounds we use truncated differential trails with only one active byte at the output of round r_3

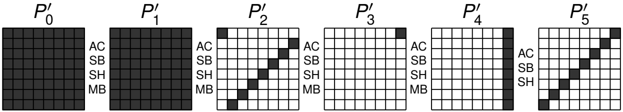
$$64 \xrightarrow{r_1} 64 \xrightarrow{r_2} 8 \xrightarrow{r_3} 1 \xrightarrow{r_4} 8 \xrightarrow{r_5} 8$$

Attack on 5 Rounds of Grøstl-256

- For the attack on 5 rounds we use truncated differential trails with only one active byte at the output of round r_3

$$64 \xrightarrow{r_1} 64 \xrightarrow{r_2} 8 \xrightarrow{r_3} 1 \xrightarrow{r_4} 8 \xrightarrow{r_5} 8$$

- Using the rebound attack all the 2^8 solutions for this truncated differential with a given/fixed difference at the input of P' can be found with complexity 2^{64} in time and memory



Attack on 5 Rounds of Grøstl-256

- Each step of the attack will succeed only with probability 2^{-56}

Attack on 5 Rounds of Grøstl-256

- Each step of the attack will succeed only with probability 2^{-56}
- We can compensate this by using more message blocks and repeating each step of the attack 2^{56} times

Attack on 5 Rounds of Grøstl-256

- Each step of the attack will succeed only with probability 2^{-56}
- We can compensate this by using more message blocks and repeating each step of the attack 2^{56} times
- Any of the 2^8 solutions can be used to generate a new starting point for the next iteration, while keeping the same bytes inactive in chaining variable

Attack on 5 Rounds of Grøstl-256

- Each step of the attack will succeed only with probability 2^{-56}
- We can compensate this by using more message blocks and repeating each step of the attack 2^{56} times
- Any of the 2^8 solutions can be used to generate a new starting point for the next iteration, while keeping the same bytes inactive in chaining variable

$\Rightarrow$ Collision attack for 5 rounds with complexity of $8 \cdot 2^{64+56} = 2^{123}$

Summary

	rounds	complexity	memory
Grøstl-256	3	2^{64}	-
	4	2^{67}	2^{64}
	5	2^{123}	2^{64}

Summary

	rounds	complexity	memory
Grøstl-256	3	2^{64}	-
	4	2^{67}	2^{64}
	5	2^{120}	2^{64}

Application to Grøstl-512

Application to Grøstl-512

- The attacks can be trivially extended to Grøstl-512

Application to Grøstl-512

- The attacks can be trivially extended to Grøstl-512
- We can use the following sequence of active bytes

$$128 \xrightarrow{r_1} 128 \xrightarrow{r_2} 16 \xrightarrow{r_3} 16 \xrightarrow{r_4} 16$$

  for the collision attack on 4 rounds

Application to Grøstl-512

- The attacks can be trivially extended to Grøstl-512
- We can use the following sequence of active bytes

$$128 \xrightarrow{r_1} 128 \xrightarrow{r_2} 16 \xrightarrow{r_3} 16 \xrightarrow{r_4} 16$$

for the collision attack on 4 rounds, and

$$128 \xrightarrow{r_1} 64 \xrightarrow{r_2} 8 \xrightarrow{r_3} 2 \xrightarrow{r_4} 16 \xrightarrow{r_5} 16$$

for the collision attack on 5 rounds

Application to Grøstl-512

- The attacks can be trivially extended to Grøstl-512
- We can use the following sequence of active bytes

$$128 \xrightarrow{r_1} 128 \xrightarrow{r_2} 16 \xrightarrow{r_3} 16 \xrightarrow{r_4} 16$$

for the collision attack on 4 rounds, and

$$128 \xrightarrow{r_1} 64 \xrightarrow{r_2} 8 \xrightarrow{r_3} 2 \xrightarrow{r_4} 16 \xrightarrow{r_5} 16$$

for the collision attack on 5 rounds

$\Rightarrow$ Collision attack on 4 and 5 rounds of Grøstl-512 with a complexity of 2^{131} and 2^{176}

Summary

	rounds	complexity	memory
Grøstl-256	3	2^{64}	-
	4	2^{67}	2^{64}
	5	2^{120}	2^{64}
Grøstl-512	3	2^{192}	-
	4	2^{131}	2^{64}
	5	2^{176}	2^{64}

Thank you for your attention!