Analysis of Kupyna

Christoph Dobraunig **Maria Eichlseder** **Florian Mendel**

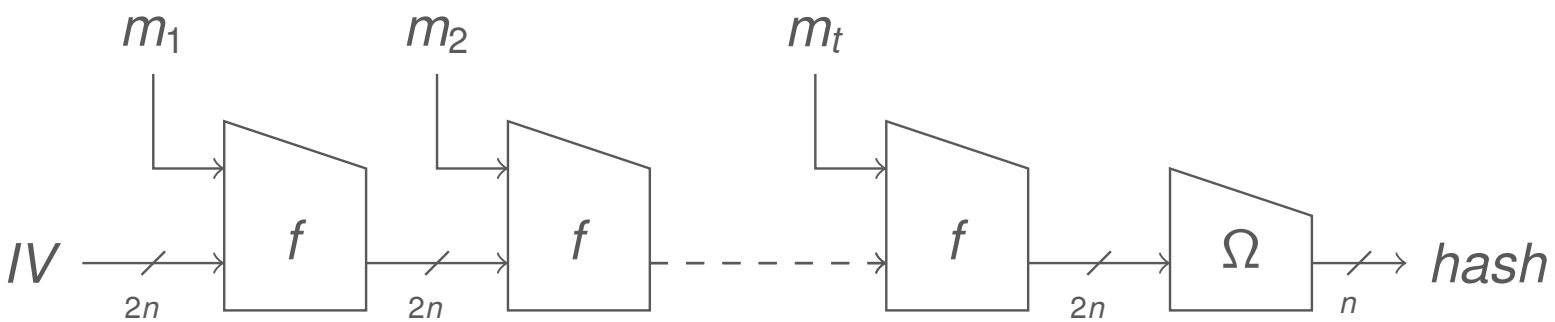
ASK 2015

The Kupyna Hash Function

The Kupyna Hash Function

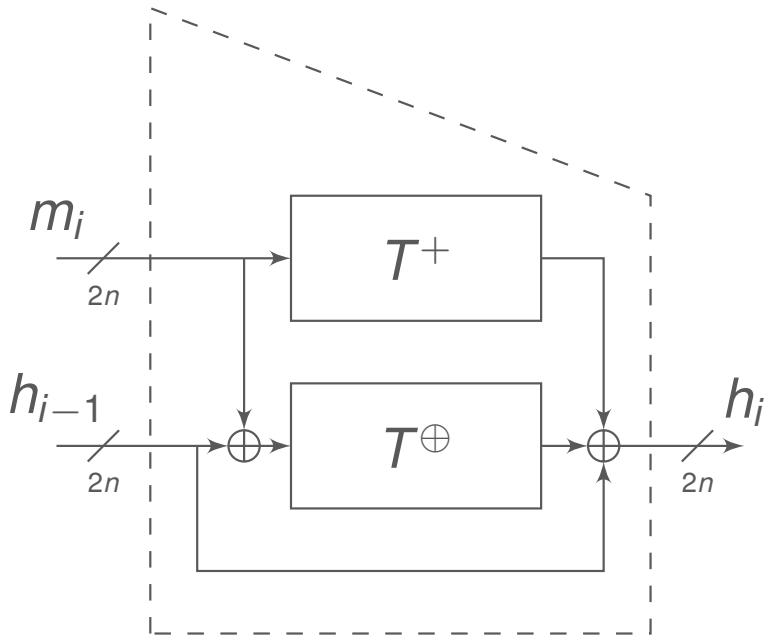
- Defined in the Ukrainian standard DSTU 7564:2014
- Replacement for GOST R 34.11-94
- Design is similar to Grøstl

The Kupyna Hash Function



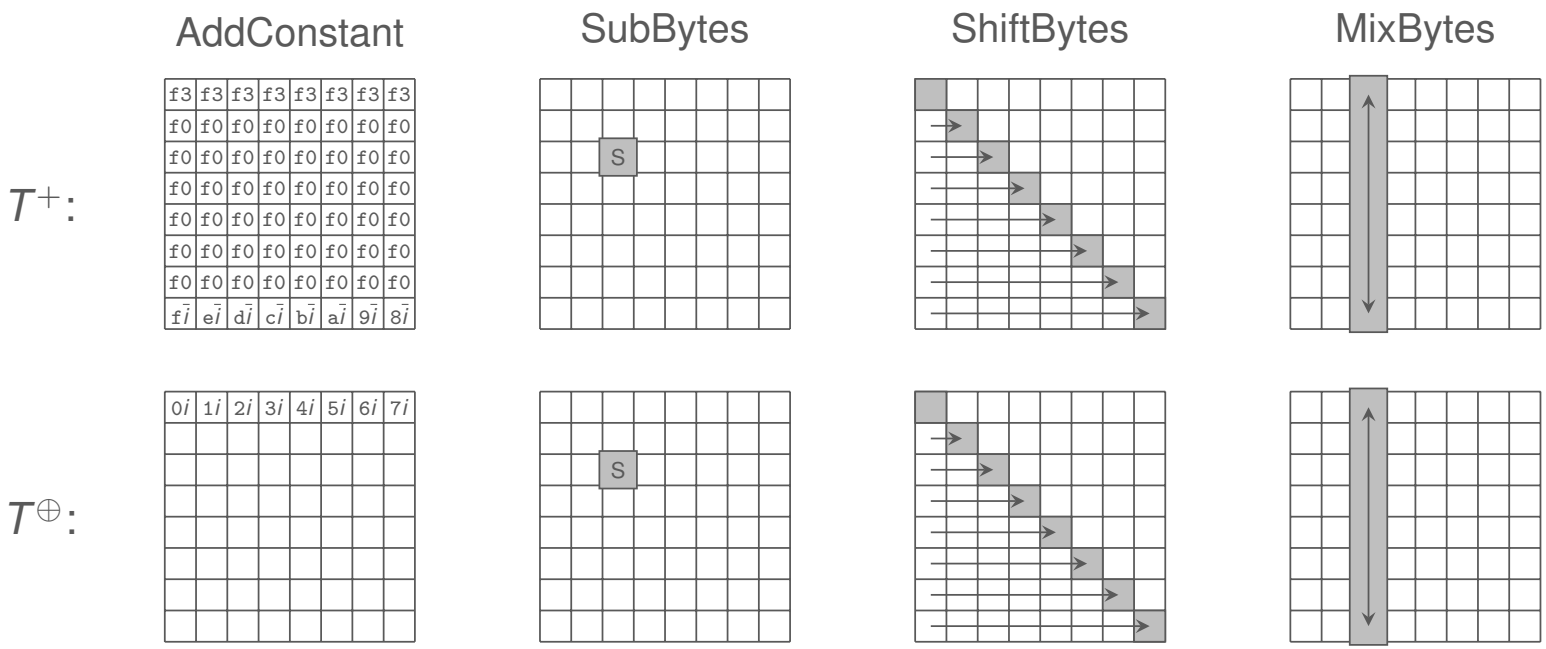
- Iterated hash function
  - Wide-pipe design
  - Merkle-Damgård design principle
  - Strong output transformation

The Kupyna Compression Function



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

The Kupyna-256 Round Transformations



- AES-like round transformation

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

Analysis of Kupyna

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

F. Mendel, T. Peyrin, C. Rechberger, and M. Schläffer
Improved Cryptanalysis of the Reduced Grøstl Compression Function, ECHO Permutation and AES Block Cipher
Selected Areas in Cryptography 2009

F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen
The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl
FSE 2009

H. Gilbert and T. Peyrin
Super-Sbox Cryptanalysis: Improved Attacks for AES-Like Permutations
FSE 2010

K. Ideguchi, E. Tischhauser, and B. Preneel
Improved Collision Attacks on the Reduced-Round Grøstl Hash Function
ISC 2010

F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen
Rebound Attacks on the Reduced Grøstl Hash Function
CT-RSA 2010

Existing Analysis of Grøstl

T. Peyrin
Improved Differential Attacks for ECHO and Grøstl
CRYPTO 2010

Y. Sasaki, Y. Li, L. Wang, K. Sakiyama, and K. Ohta
Non-full-active Super-Sbox Analysis: Applications to ECHO and Grøstl
ASIACRYPT 2010

C. Boura, A. Canteaut, and C. De Cannière
Higher-Order Differential Properties of Keccak and Luffa
FSE 2011

M. Schläffer
Updated Differential Analysis of Grøstl
2011

J. Jean, M. Naya-Plasencia, and T. Peyrin
Improved Rebound Attack on the Finalist Grøstl
FSE 2012

Existing Analysis of Grøstl

S. Wu, D. Feng, W. Wu, J. Guo, L. Dong, and J. Zou
(Pseudo) Preimage Attack on Round-Reduced Grøstl Hash Function and Others
FSE 2012

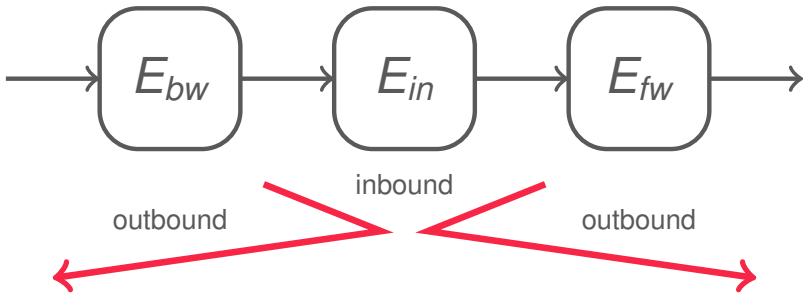
J. Jean, M. Naya-Plasencia, and T. Peyrin
Multiple Limited-Birthday Distinguishers and Applications
Selected Areas in Cryptography 2013

M. Minier and G. Thomas
An Integral Distinguisher on Grøstl-512
INDOCRYPT 2013

F. Mendel, V. Rijmen, and M. Schläffer
Collision Attack on 5 Rounds of Grøstl
FSE 2014

Y. Sasaki, Y. Tokushige, L. Wang, M. Iwamoto, and K. Ohta
An Automated Evaluation Tool for Improved Rebound Attack: New Distinguishers and Proposals of ShiftBytes Parameters for Grøstl
CT-RSA 2014

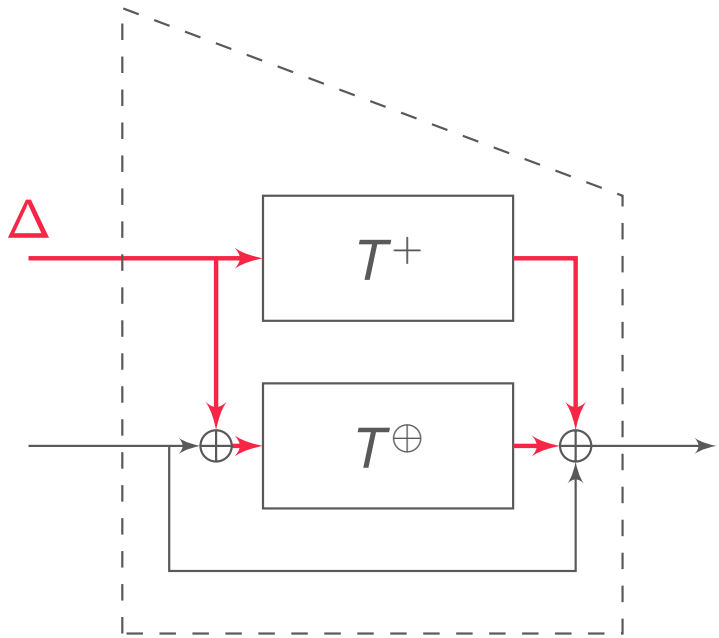
The Rebound Attack



- Inbound phase
  - efficient meet-in-the-middle phase in E_{in}
  - using available degrees of freedom
- Outbound phase
  - probabilistic part in E_{bw} and E_{fw}
  - repeat inbound phase if needed

Attack on the Compression Function

Basic Attack Strategy



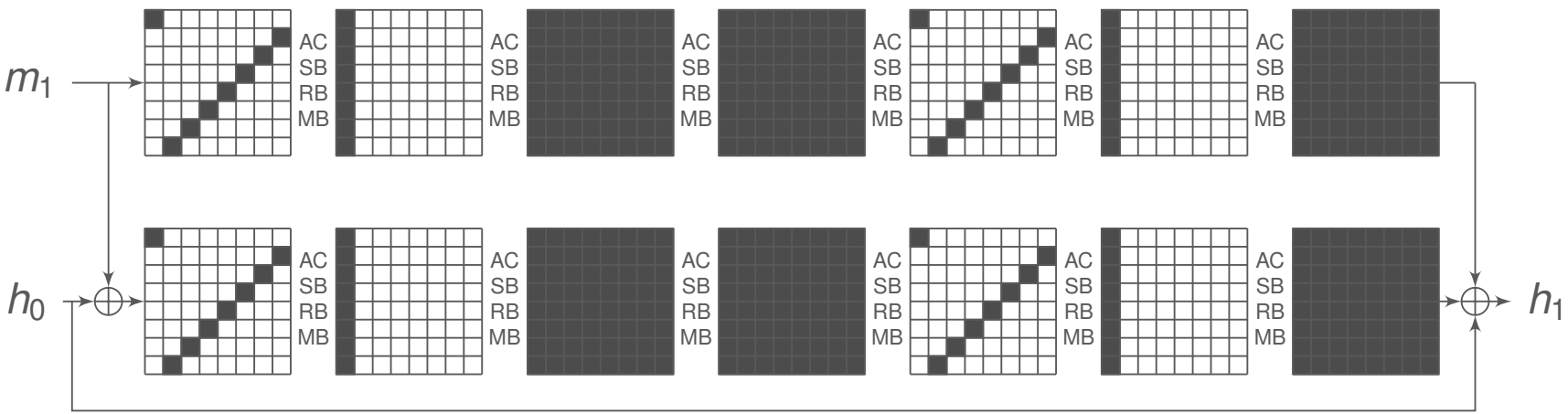
semi-free-start collision:

- $f(h_{i-1}, m_i) = f(h_{i-1}, m_i^*),\ m_i \neq m_i^*$
- arbitrary h_{i-1}

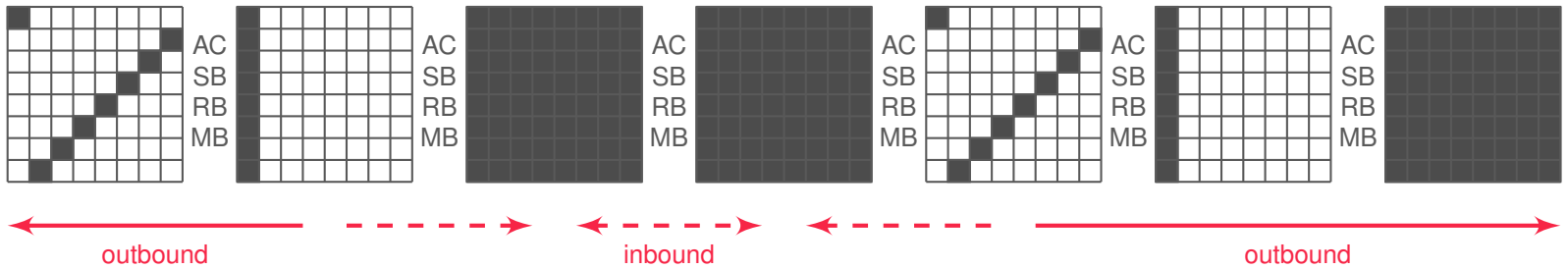
Attack on 6 Rounds

- In the attack we use the same truncated differential trail in both permutations $T^{\oplus}$ and T^{+}:

$$8 \xrightarrow{r_1} 8 \xrightarrow{r_2} 64 \xrightarrow{r_3} 64 \xrightarrow{r_4} 8 \xrightarrow{r_5} 8 \xrightarrow{r_6} 64$$

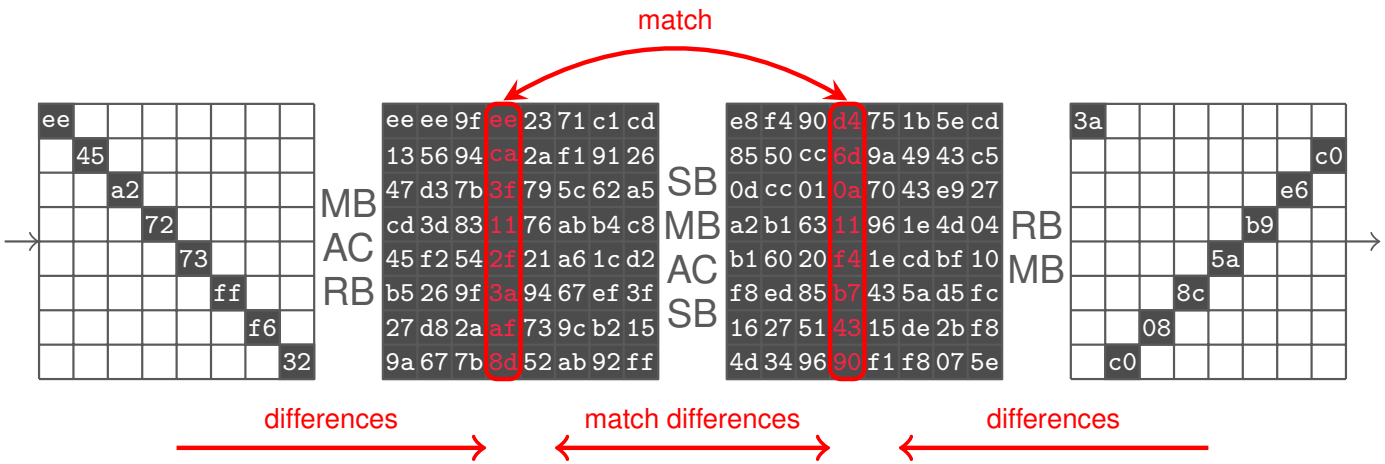


Rebound attack for $T^{\oplus}$



- Inbound phase
  - start with differences in round 2 and 4
  - match-in-the-middle using values of the state
- Outbound phase
  - uses truncated differentials
  - probabilistic propagation in MixBytes

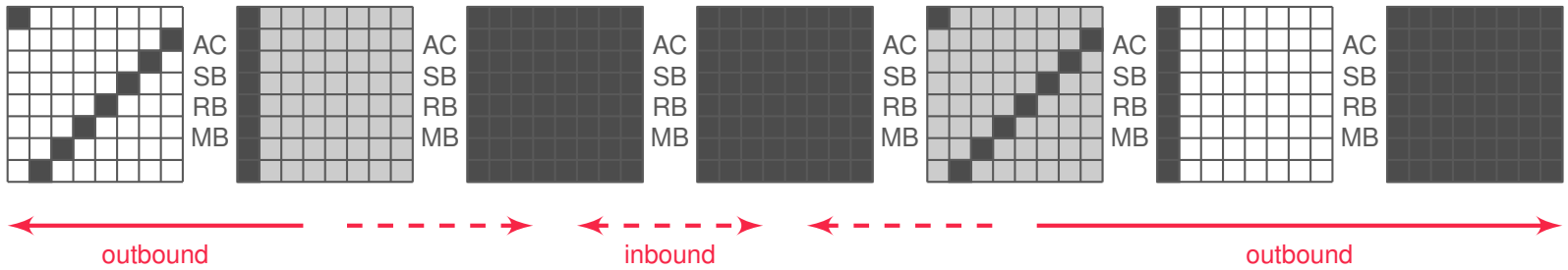
Inbound phase for $T^{\oplus}$



- Start with arbitrary differences in round 2 and 4
- Match-in-the-middle at SuperBox (SB – MB – AC – SB)
  - with complexity 2^{64} we get ~ 1 right pairs
  - time-memory trade-off with $T \cdot M = 2^{128}$ with $T \geq 2^{64}$

$\Rightarrow$ 2^{64} solutions with complexity of 2^{64} (amortized cost 1)

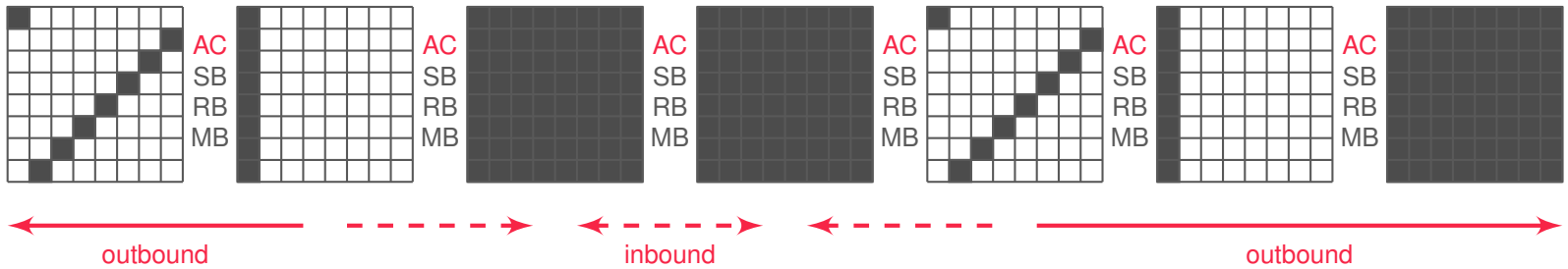
Outbound phase for $T^{\oplus}$



- Propagate through MixBytes of round 1, 5 and 6
  - using truncated differences (active bytes: $8 \rightarrow 8$ resp. $1 \rightarrow 8$)
  - probability: 1 in each direction

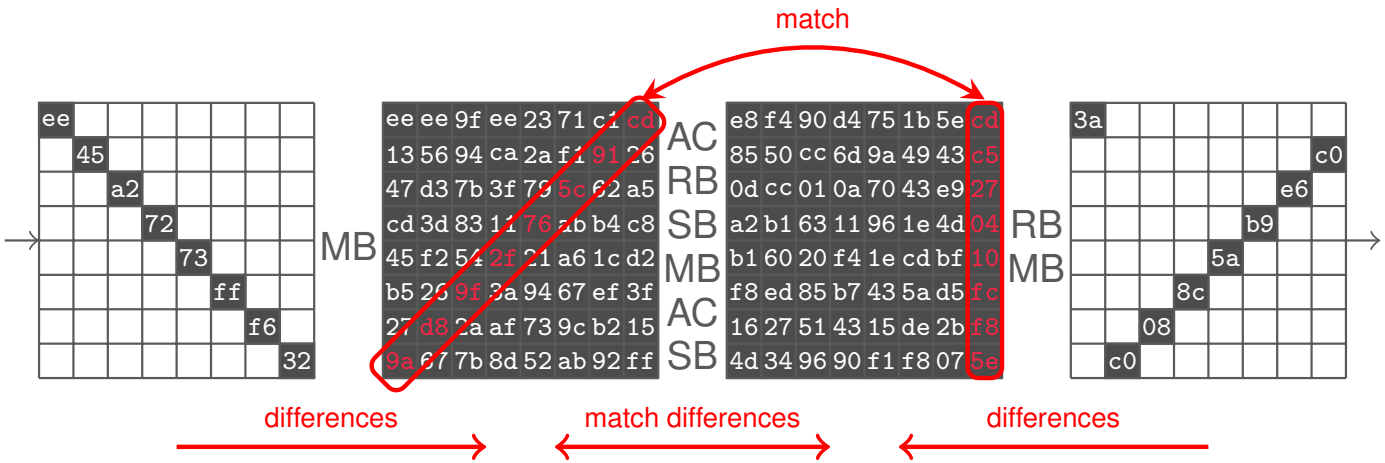
$\Rightarrow$ 2^{64} solutions following the differential trail with compexity 2^{64}

Rebound attack for T^+



- AddConstant (AC)
  - modular addition destroys the byte-alignment
  - complicates the application of the attack

Inbound phase for T^+



- Start with arbitrary differences in round 2 and 4
- Match-in-the-middle (AC – RB – SB – MB – AC – SB)
  - first AC creates dependences between SuperBoxes
  - only consider inputs that never (resp. always) result in a carry

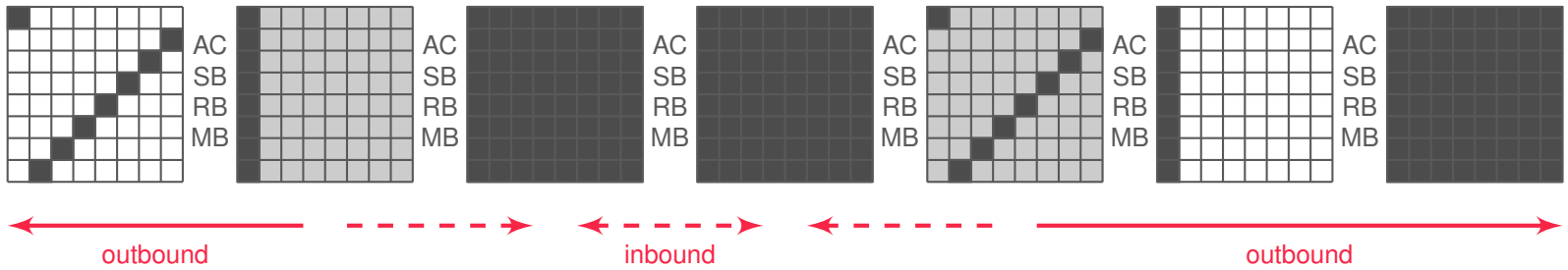
Number of solutions

- Byte 0: $x + \texttt{F3} > \texttt{FF} \rightarrow 243$ solutions
- Byte 1: $x + 1 + \texttt{F0} > \texttt{FF} \rightarrow 241$ solutions
- ...

Byte position	Valid values	Valid pairs (average)
Byte 0	243	230.6
Byte 1–6	241	226.8
Byte 7	256	256

$\Rightarrow$ $2^{54.4}$ solutions in total (cost $2^{63.4}$)

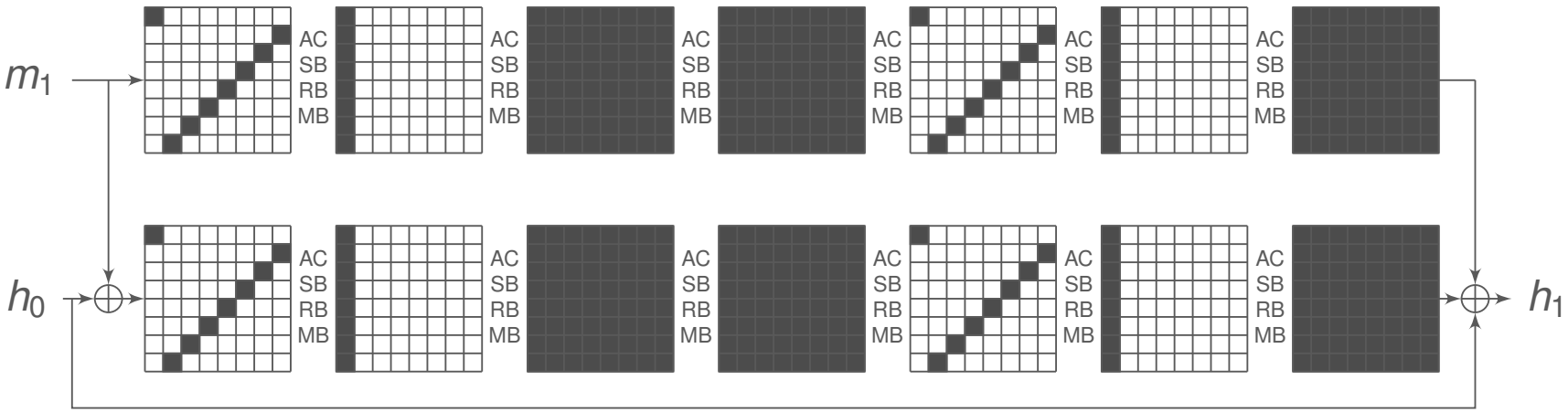
Outbound phase for $T^{\oplus}$



- Propagate through MixBytes in round 1, 5 and 6
  - probability: 1 (same as for $T^{\oplus}$)
- Propagate through AddConstant in round 1, 2, 5 and 6
  - probability: $2^{-2.45}$

$\Rightarrow$ $2^{51.95}$ solutions following the differential trail with complexity $2^{63.4}$

Attack on 6 Rounds



- Construct 2^a pairs following the differential trail in $T^{\oplus}$
  - one solution with amortized cost 1
- Construct 2^{128-a} pairs following the differential trail in T^{+}
  - one solution with amortized cost $2^{11.55}$

$\Rightarrow$ semi-free-start collision with complexity $2^{69.8}$ (for $a = 69.8$)

Extending the Attack to 7 Rounds

- Sequence of active SBoxes:

$$8 \xrightarrow{r_1} 8 \xrightarrow{r_2} 64 \xrightarrow{r_3} 64 \xrightarrow{r_4} 8 \xrightarrow{r_5} 1 \xrightarrow{r_6} 8 \xrightarrow{r_7} 64$$

- Inbound phase is the same as before
- Outbound phase is extended by one round (probability: 2^{-56})

$\Rightarrow$ semi-free-start collision with complexity $2^{125.8}$

Attacks on Kupyna-256

- Compression Function

rounds	complexity	memory
6	$2^{69.8}$	2^{64}
7	$2^{125.8}$	2^{64}

Attack on the Hash Function

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 (e.g. $T^{\oplus}$)

Equivalent Description of Kupyna

- To simplify the description of the attack we use an equivalent description of the hash function

$$\begin{aligned} \hat{h}_0 &= MB^{-1}(\mathrm{IV}) \\ \hat{h}_i &= \hat{T}^{\oplus}(MB(\hat{h}_{i-1}) \oplus m_i) \oplus \hat{T}^{+}(m_i) \oplus \hat{h}_{i-1} \quad \text{for } 1 \leq i \leq t \\ hash &= \Omega(MB(\hat{h}_t)) \end{aligned}$$

  with $h_i = MB(\hat{h}_i)$

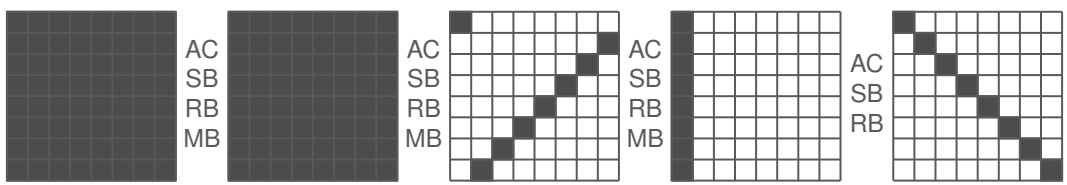
- The last MixBytes transformation of the permutations $T^{\oplus}$ and T^{+} are swapped with the XOR operation of the feed-forward

Attack on 4 Rounds

- The core of the attack on 4 rounds are truncated differential trails for $\hat{T}^{\oplus}$ with only 8 active bytes at the output of round r_4

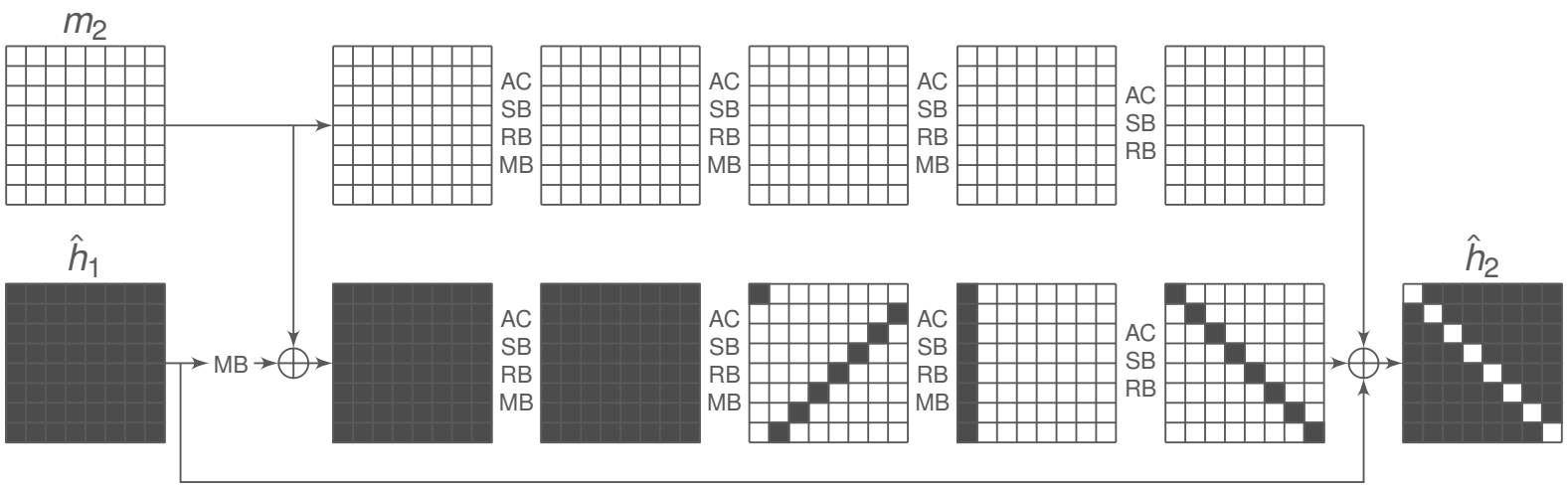
$$64 \xrightarrow{r_1} 64 \xrightarrow{r_2} 8 \xrightarrow{r_3} 8 \xrightarrow{r_4} 8$$

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



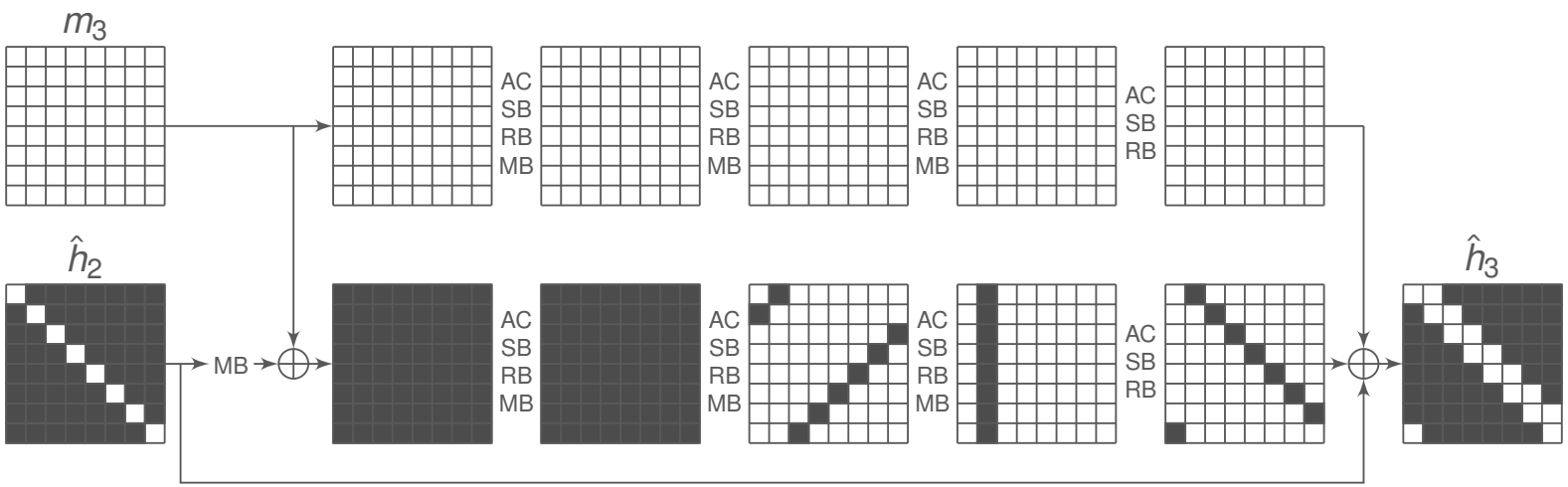
Attack on 4 Rounds

- 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



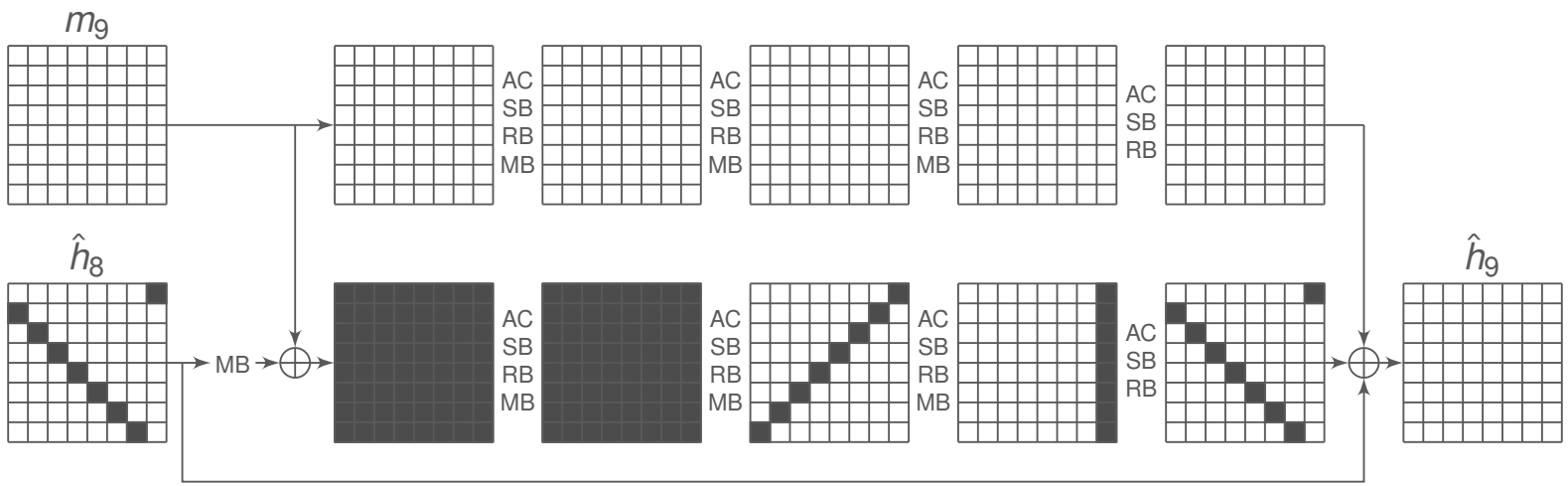
Attack on 4 Rounds

- 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

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



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

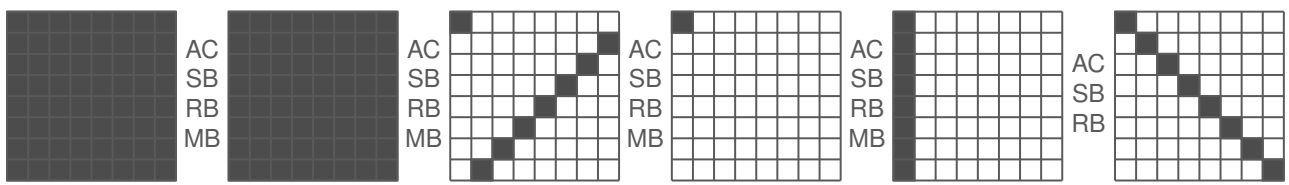
Extending the Attack to 5 Rounds

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

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

- 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

- 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 get 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

- Compression Function

rounds	complexity	memory
6	$2^{69.8}$	2^{64}
7	$2^{125.8}$	2^{64}

- Hash Function

rounds	complexity	memory
4	2^{67}	2^{64}
5	2^{120}	2^{64}

Thank you!

http://eprint.iacr.org/2015/956