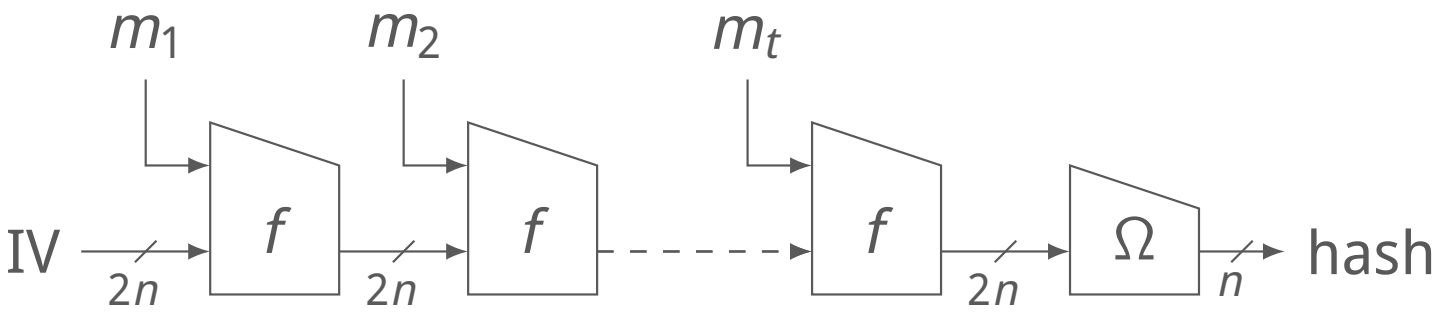
Analysis of the Kupyna-256 Hash Function

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

FSE 2016

The Kupyna Hash Function

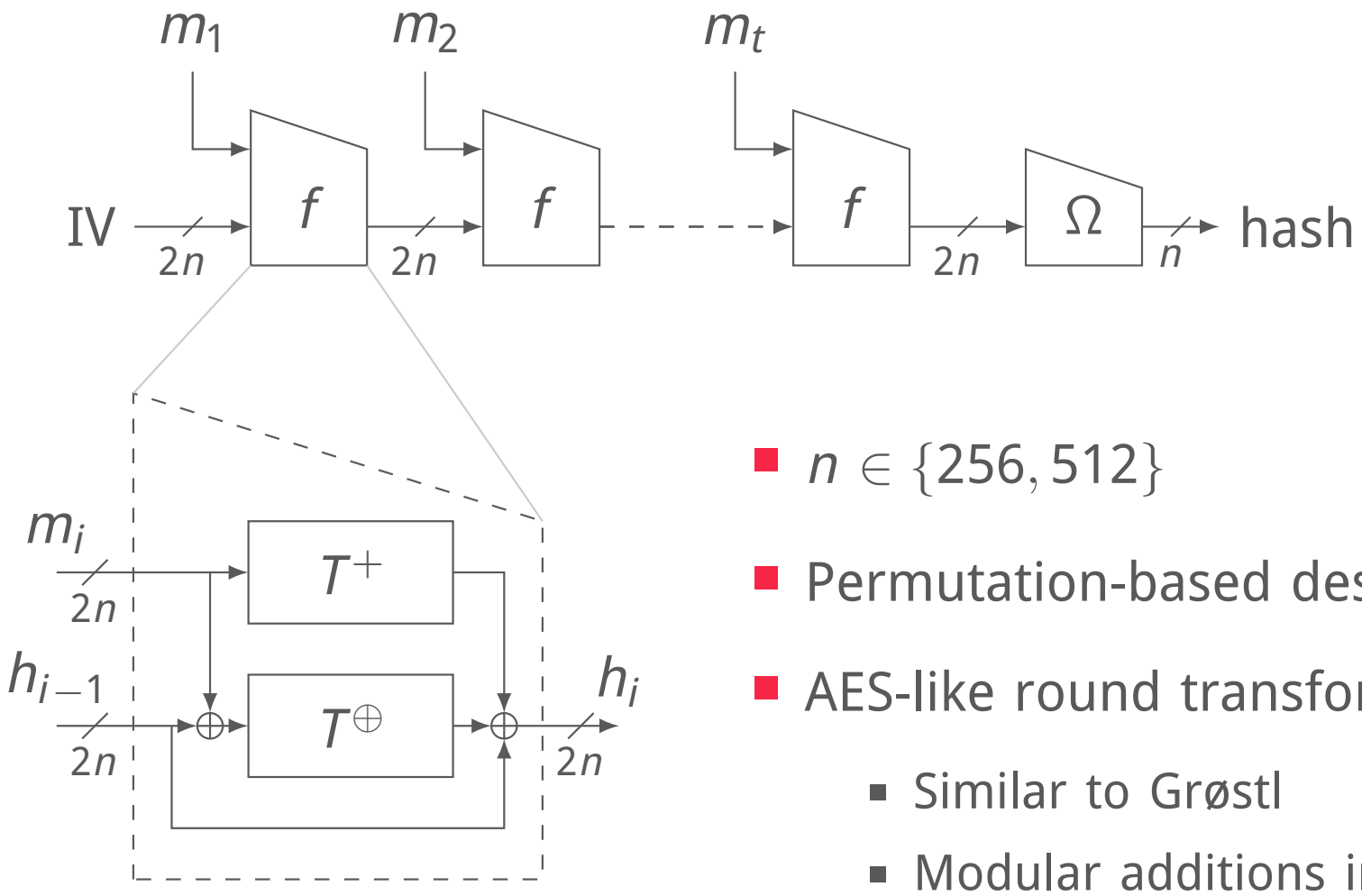
Ukrainian standard DSTU 7564:2014 [Oli+15; Олі+15a]



- $n \in \{256, 512\}$

The Kupyna Hash Function

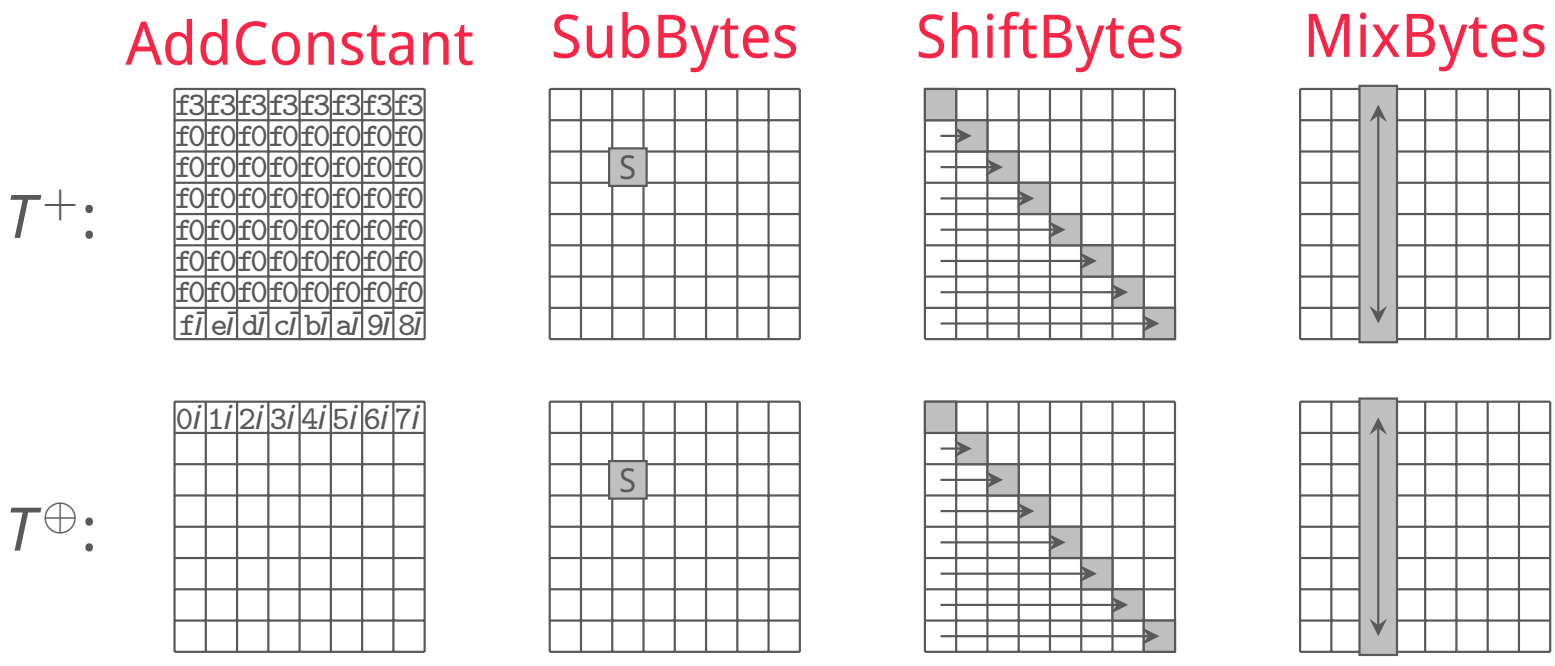
Ukrainian standard DSTU 7564:2014 [Oli+15; Oлi+15a]



- $n \in \{256, 512\}$
- Permutation-based design
- AES-like round transformations
  - Similar to Grøstl
  - Modular additions inside

The Kupyna-256 Round Transformations

- Kupyna-512: 8×16 state, 14 rounds
- Kupyna-256: 8×8 state, 10 rounds:



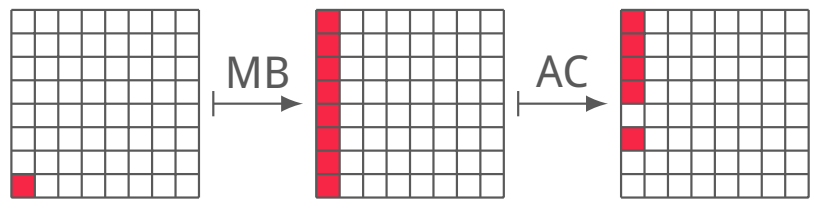
$$r_i = \mathrm{MB} \circ \mathrm{RB} \circ \mathrm{SB} \circ \mathrm{AC}$$

Modular Constant Addition

- Prevent same trails for T^{+}, $T^{\oplus}$
- Grøstl instead has different rotation constants

Modular Constant Addition

- Prevent same trails for T^{+}, $T^{\oplus}$
- Grøstl instead has different rotation constants
- Destroys byte-alignment & MDS property
- Branch number of T^{+} reduced from 9 to ≤ 6:



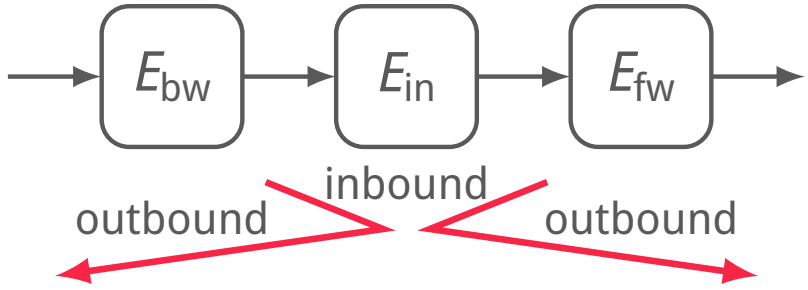
$$x_1\colon \left(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\right)^{\top} \xmapsto{\text{MB}} \left(00\ 00\ 00\ 00\ 00\ 00\ 00\ 00\right)^{\top} \xmapsto{\text{AC}} \left(\texttt{F3}\ \texttt{F0}\ \texttt{F0}\ \texttt{F0}\ \texttt{F0}\ \texttt{F0}\ \texttt{F0}\ 70\right)^{\top},$$

$$x_2\colon \left(00\ 00\ 00\ 00\ 00\ 00\ 00\ \texttt{FF}\right)^{\top} \xmapsto{\text{MB}} \left(\texttt{DB}\ \texttt{C7}\ 38\ \texttt{AB}\ \texttt{FF}\ 24\ \texttt{FF}\ \texttt{FF}\right)^{\top} \xmapsto{\text{AC}} \left(\texttt{CE}\ \texttt{B8}\ 29\ \texttt{9C}\ \texttt{F0}\ 15\ \texttt{F0}\ 70\right)^{\top},$$

$$\Delta\colon \left(00\ 00\ 00\ 00\ 00\ 00\ 00\ \texttt{FF}\right)^{\top} \xmapsto{\text{MB}} \left(\texttt{DB}\ \texttt{C7}\ 38\ \texttt{AB}\ \texttt{FF}\ 24\ \texttt{FF}\ \texttt{FF}\right)^{\top} \xmapsto{\text{AC}} \left(\texttt{3D}\ 48\ \texttt{D9}\ \texttt{6C}\ 00\ \texttt{E5}\ 00\ 00\right)^{\top}.$$

The Rebound Attack

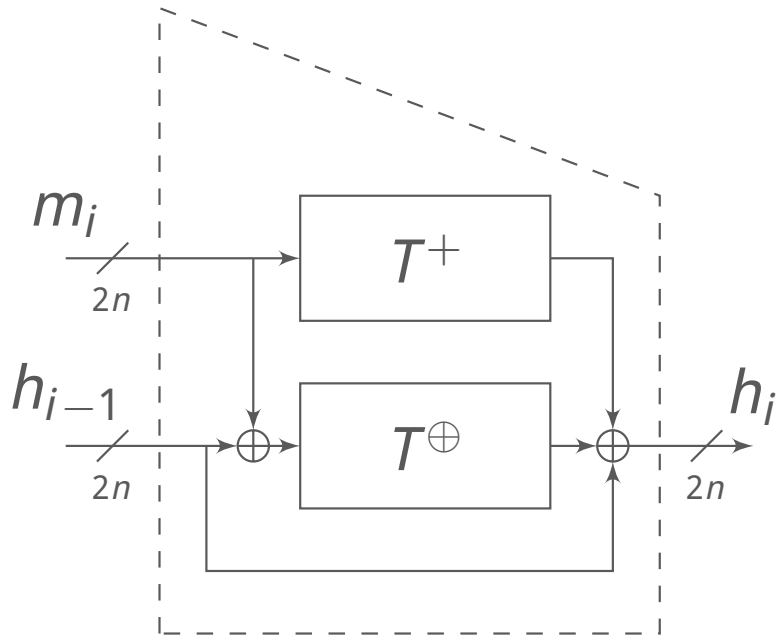
[Men+09]



- Inbound phase
  - Efficient match-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

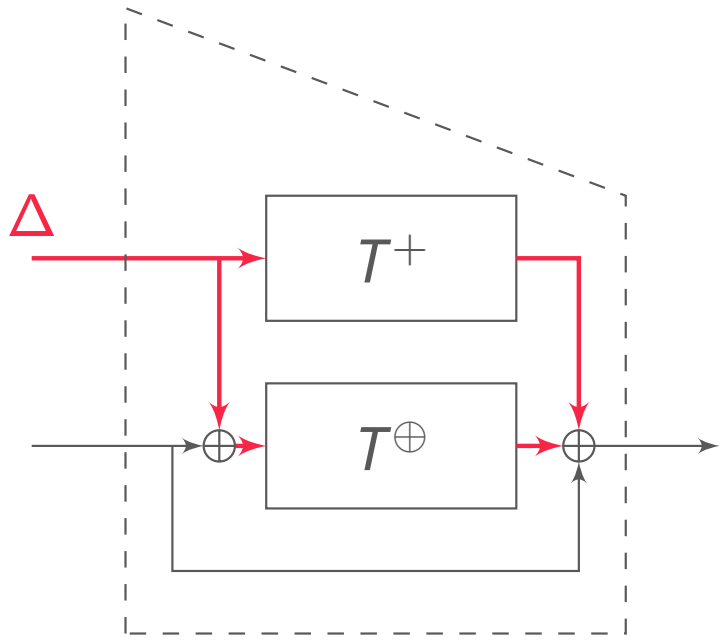
Basic Attack Strategy



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}

Basic Attack Strategy



Semi-free-start collision:

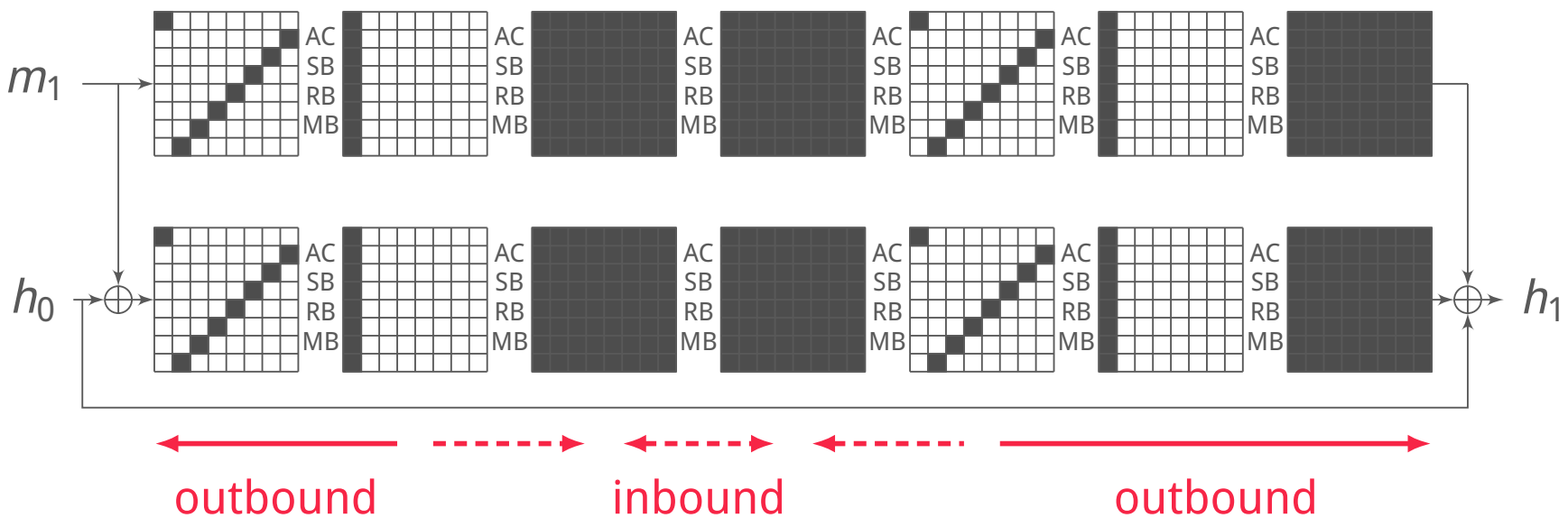
- $f(h_{i-1}, m_i) = f(h_{i-1}, m_i^*),\ m_i \neq m_i^*$
- Arbitrary h_{i-1}

Rebound attack on 6 Rounds

Similar to [Men+10]

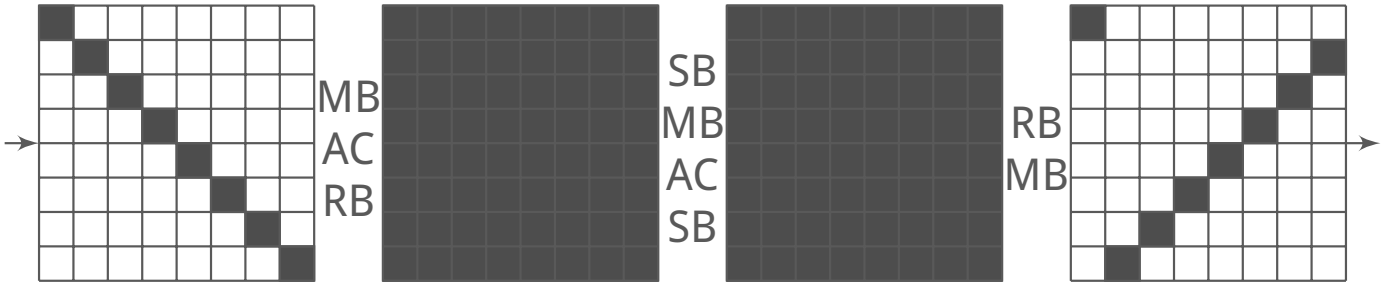
Same truncated differential trail in both permutations $T^{\oplus}$ and T^{+}:

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



Inbound phase for $T^{\oplus}$

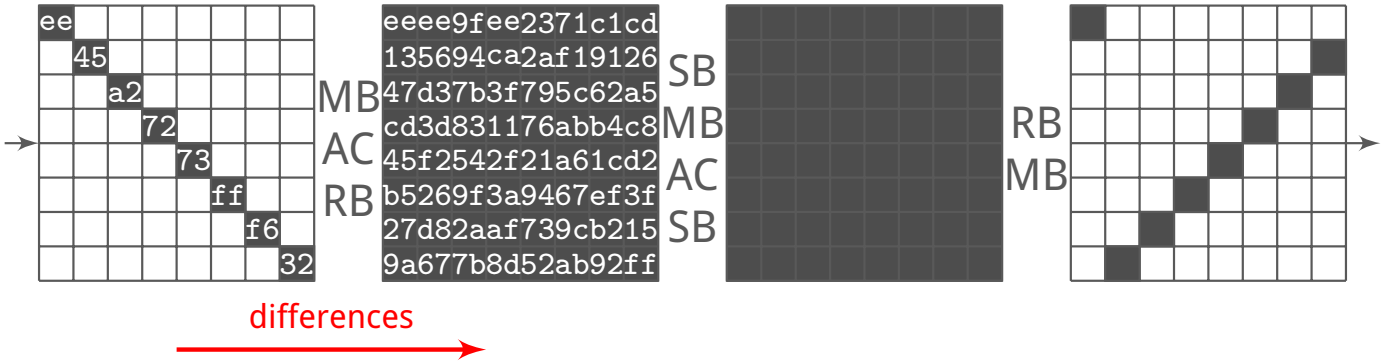
Similar to [Men+10]



1. Start with arbitrary differences in round 2 and 4

Inbound phase for $T^{\oplus}$

Similar to [Men+10]



1. Start with arbitrary differences in round 2 and 4

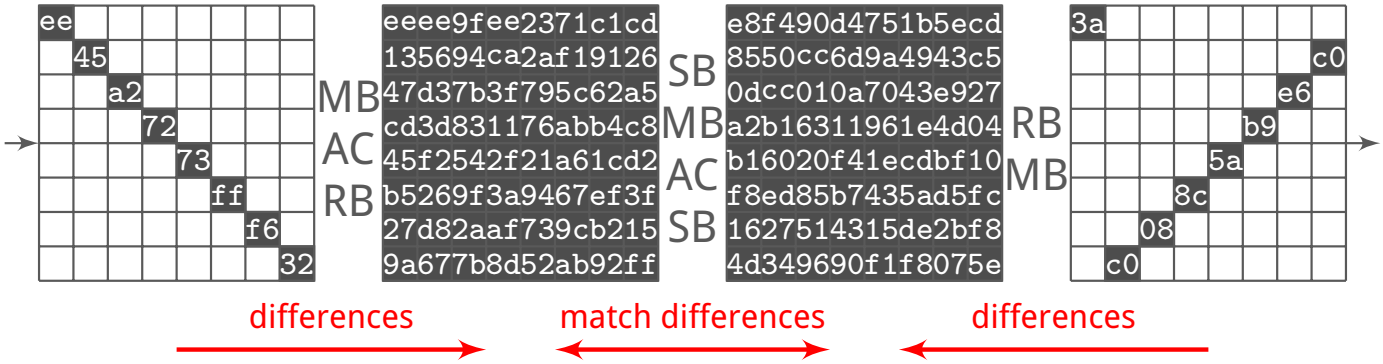
Inbound phase for $T^{\oplus}$

Similar to [Men+10]

1. Start with arbitrary differences in round 2 and 4

Inbound phase for $T^{\oplus}$

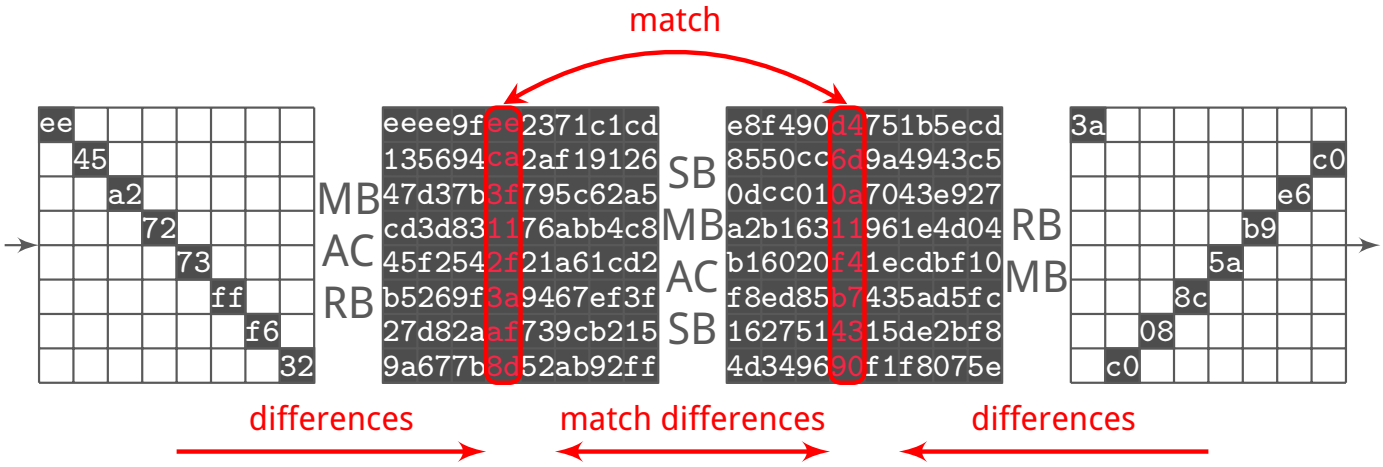
Similar to [Men+10]



1. Start with arbitrary differences in round 2 and 4

Inbound phase for $T^{\oplus}$

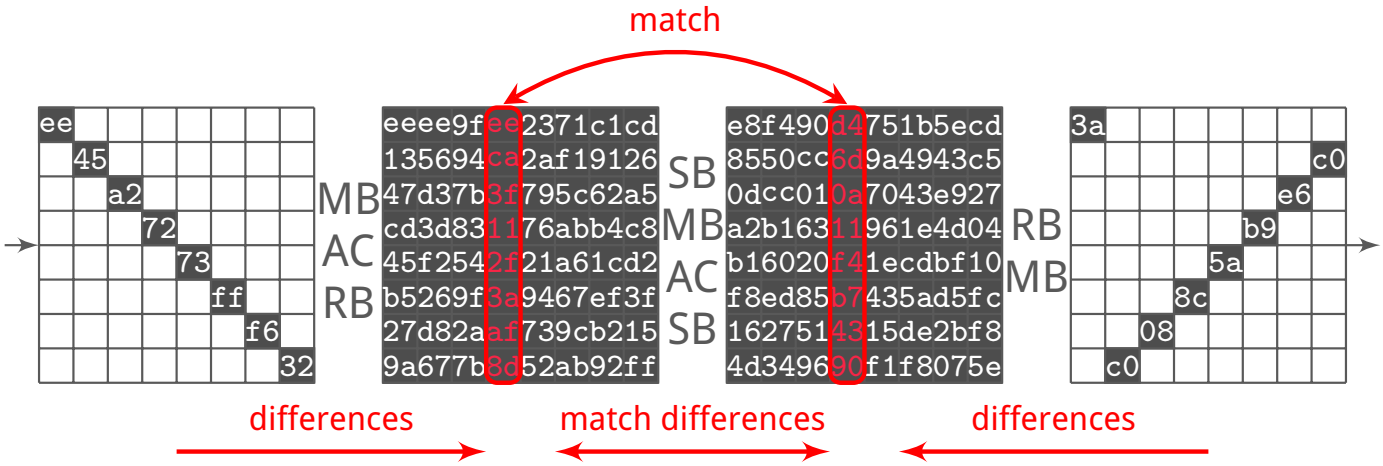
Similar to [Men+10]



1. Start with arbitrary differences in round 2 and 4
2. Match-in-the-middle at SuperBox (SB – MB – AC – SB)

Inbound phase for $T^{\oplus}$

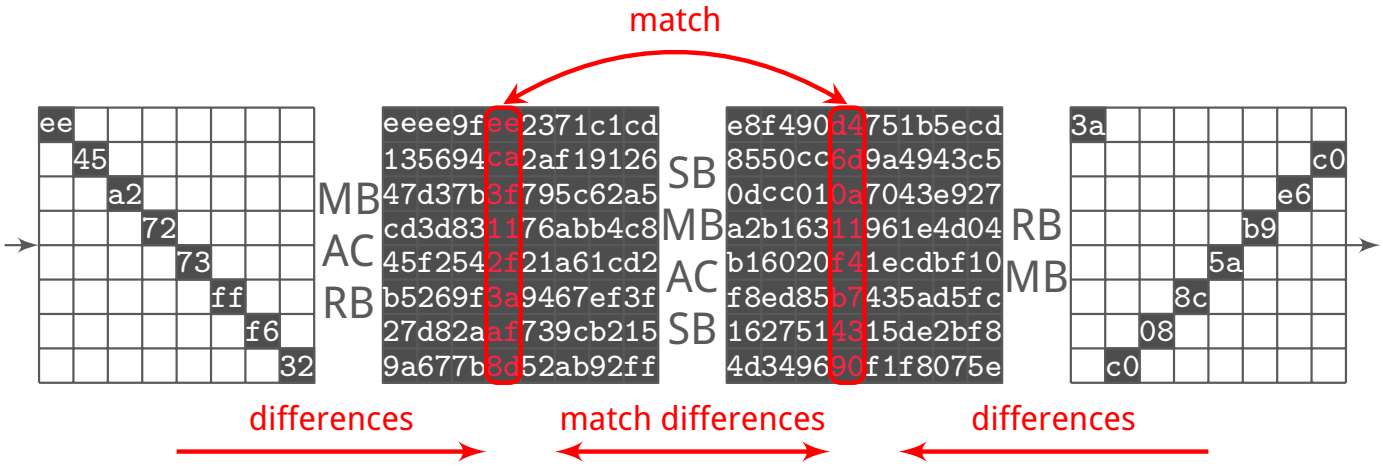
Similar to [Men+10]



1. Start with arbitrary differences in round 2 and 4
2. Match-in-the-middle at SuperBox (SB – MB – AC – SB)
   - $\approx$ 1 right pair with complexity 2^{64}

Inbound phase for $T^{\oplus}$

Similar to [Men+10]

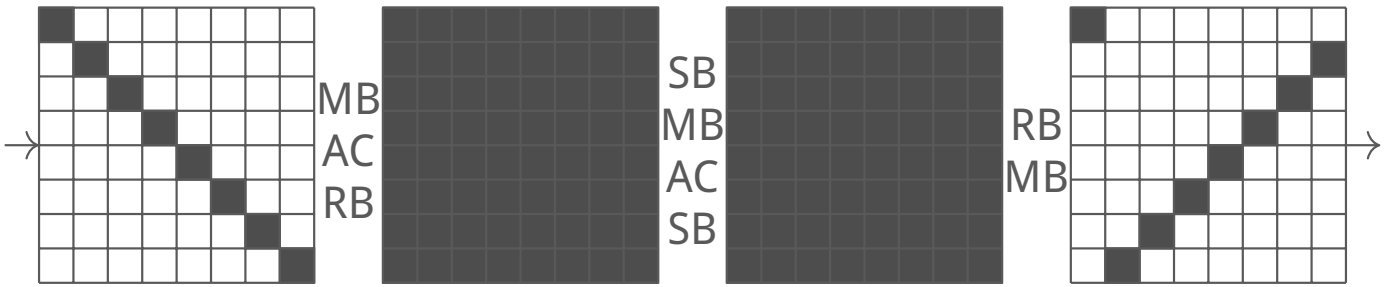


1. Start with arbitrary differences in round 2 and 4
2. Match-in-the-middle at SuperBox (SB − MB − AC − SB)
   - $\approx$ 1 right pair with complexity 2^{64}
   - time-memory trade-off with $T \cdot M = 2^{128}$ with $T \geq 2^{64}$

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

Inbound phase for T^+

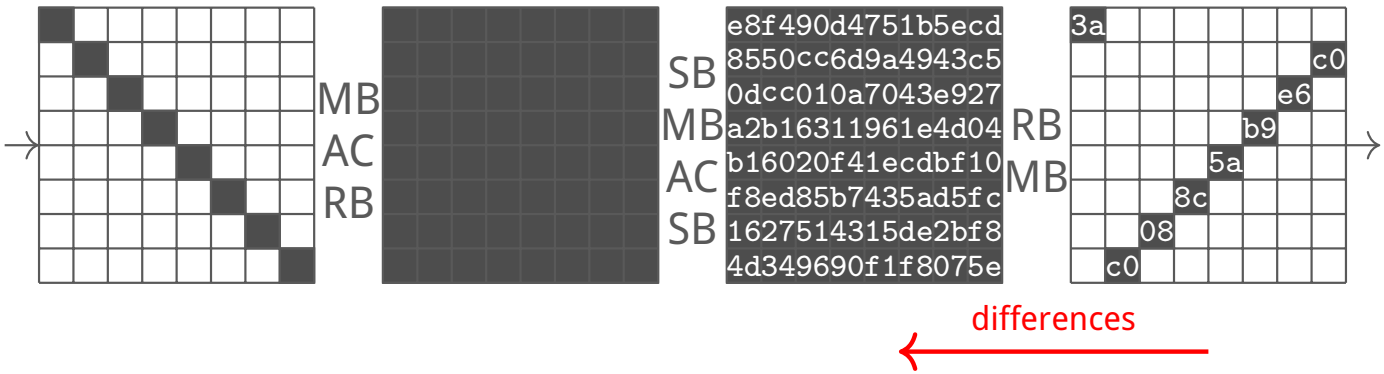
AddConstant complicates analysis



1′ Start with arbitrary differences in round 2 and 4

Inbound phase for T^+

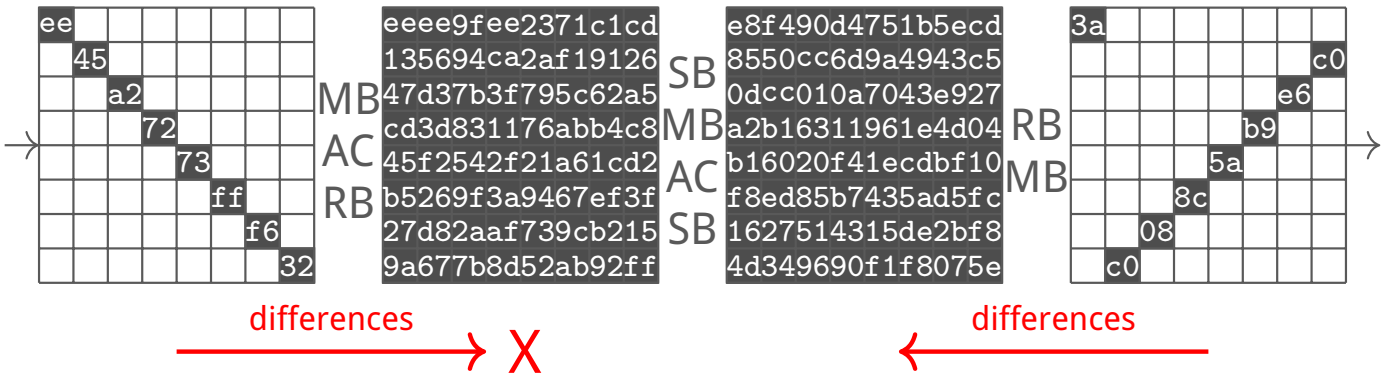
AddConstant complicates analysis



1′ Start with arbitrary differences in round 2 and 4

Inbound phase for T^+

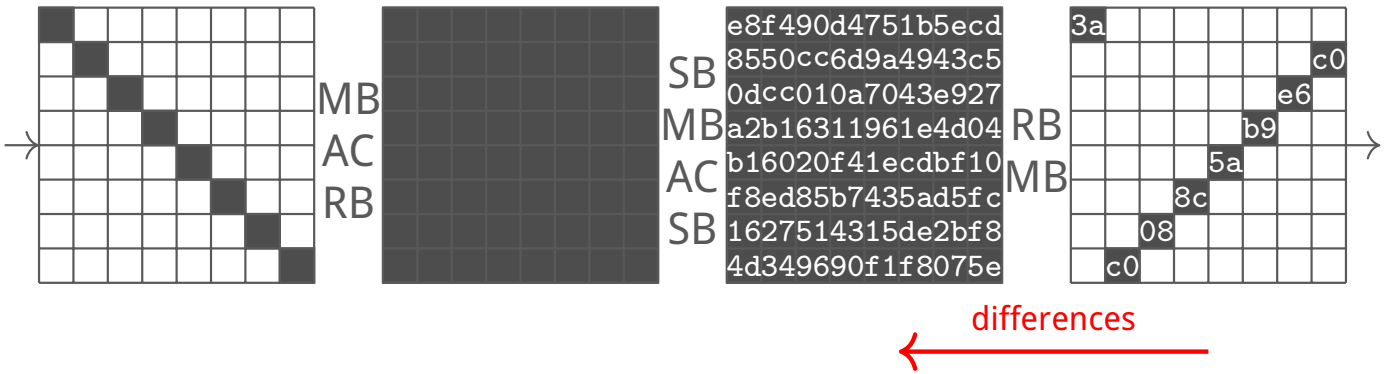
AddConstant complicates analysis



1′ Start with arbitrary differences in round 2 and 4

Inbound phase for T^+

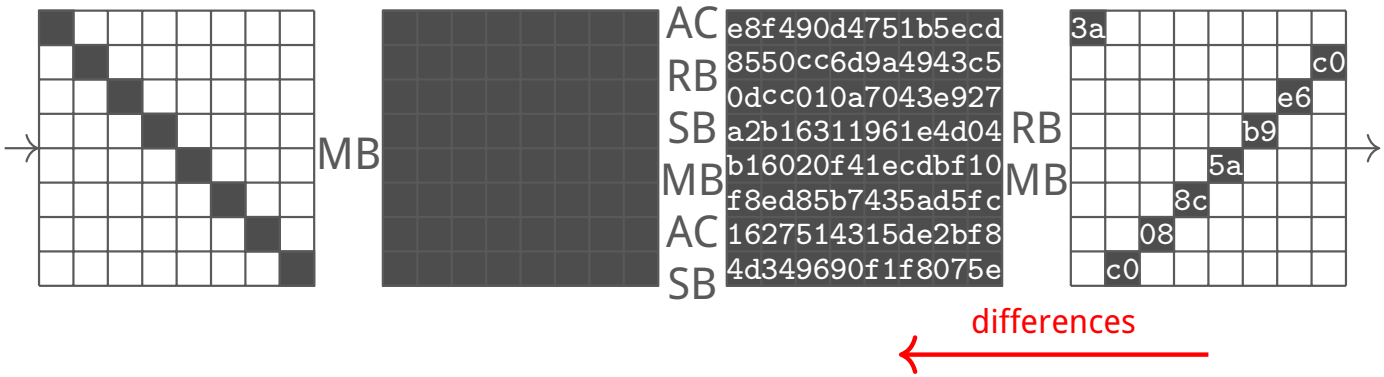
AddConstant complicates analysis



1′ Start with arbitrary differences in round 2 and 4

Inbound phase for T^+

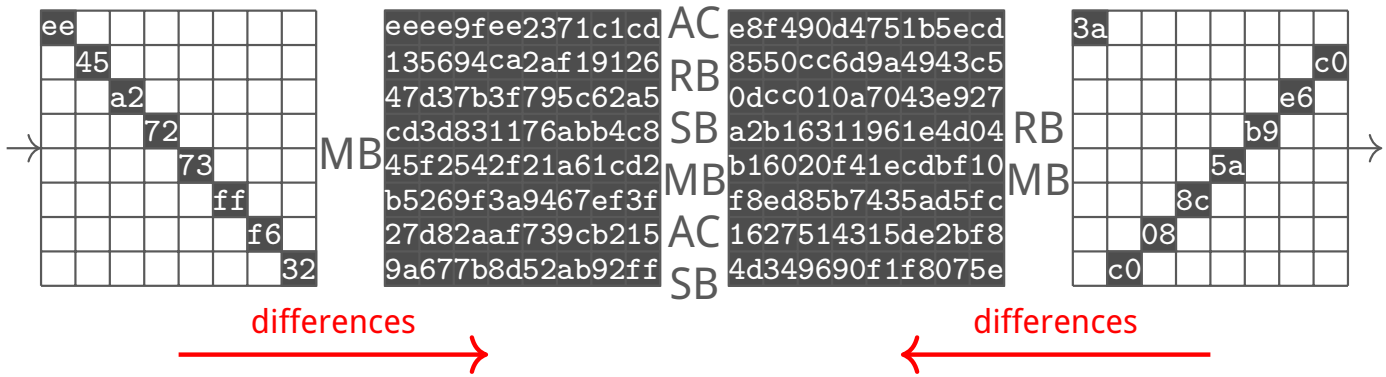
AddConstant complicates analysis



1′ Start with arbitrary differences in round 2 and 4

Inbound phase for T^+

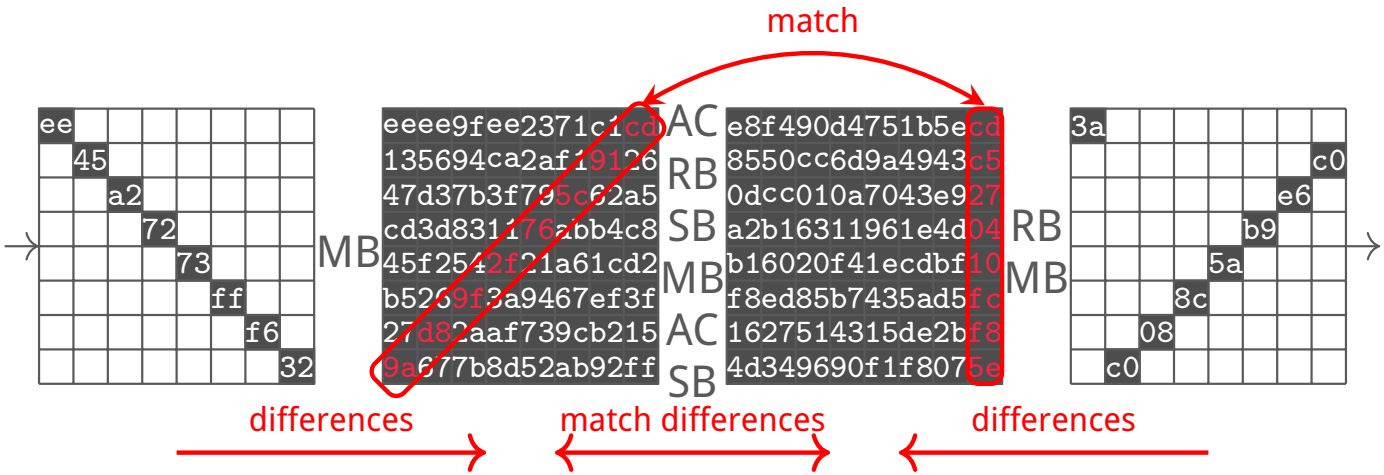
AddConstant complicates analysis



1′ Start with arbitrary differences in round 2 and 4

Inbound phase for T^+

AddConstant complicates analysis

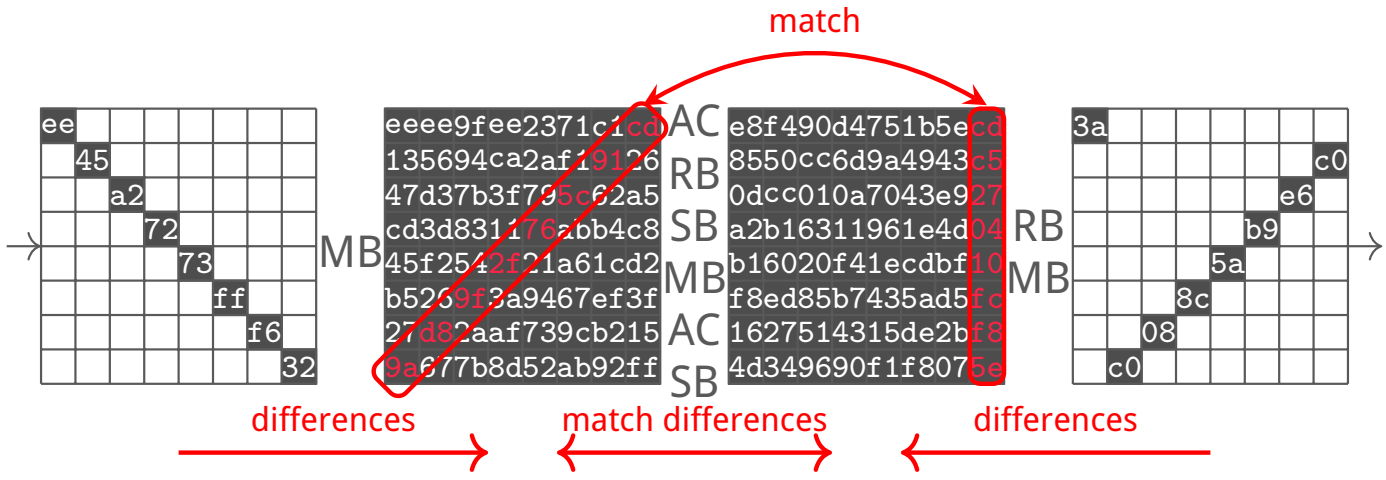


1′ Start with arbitrary differences in round 2 and 4

2′ Match-in-the-middle (AC – RB – SB – MB – AC – SB)

Inbound phase for T^+

AddConstant complicates analysis



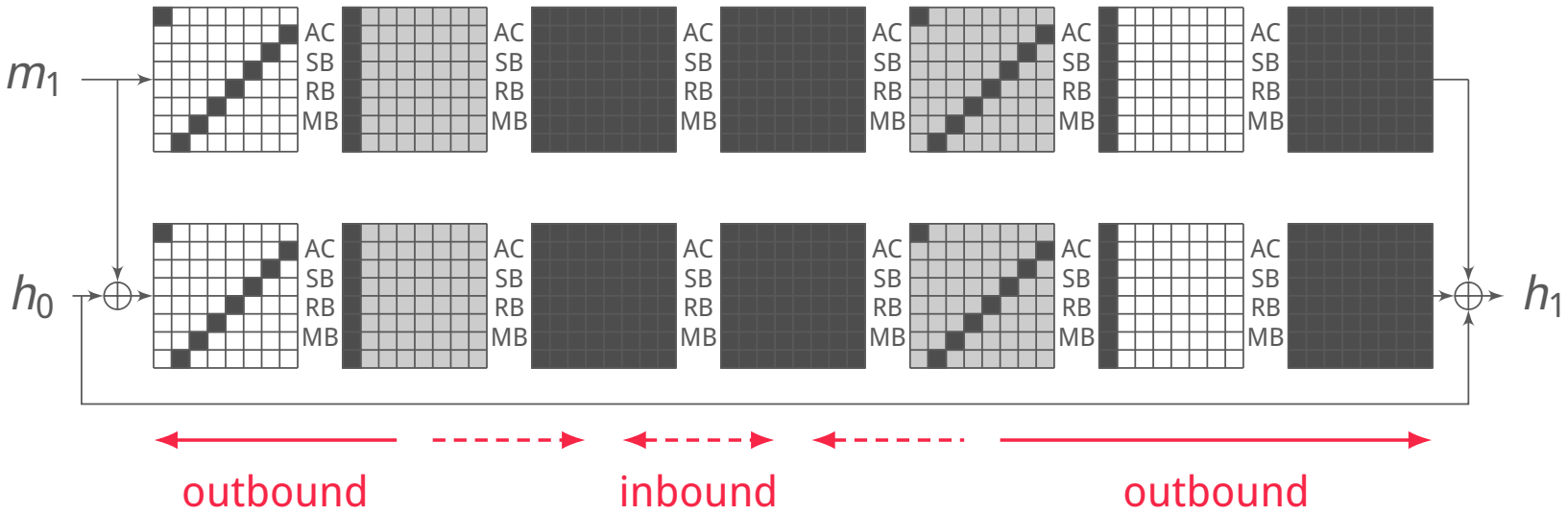
1′ Start with arbitrary differences in round 2 and 4

2′ Match-in-the-middle (AC – RB – SB – MB – AC – SB)

- AC creates dependences between SuperBoxes → fix carry!
- Byte 0: $x + \texttt{F3} > \texttt{FF} \rightarrow$ 243 solutions → 230.6 valid pairs avg,...

$\Rightarrow$ $2^{54.4}$ solutions with complexity of $2^{63.4}$

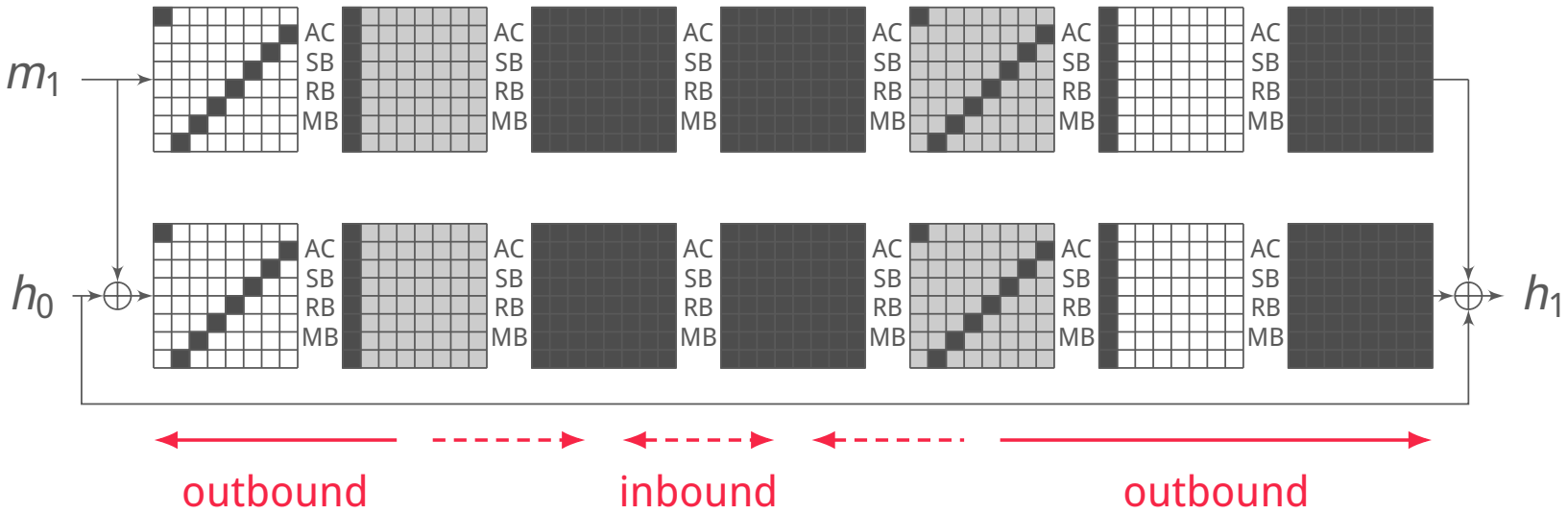
Outbound phase for $T^{\oplus}$, T^{+} and Match



3 Propagate $T^{\oplus}$ outbound (truncated MixBytes: prob 1)

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

Outbound phase for $T^{\oplus}$, T^{+} and Match



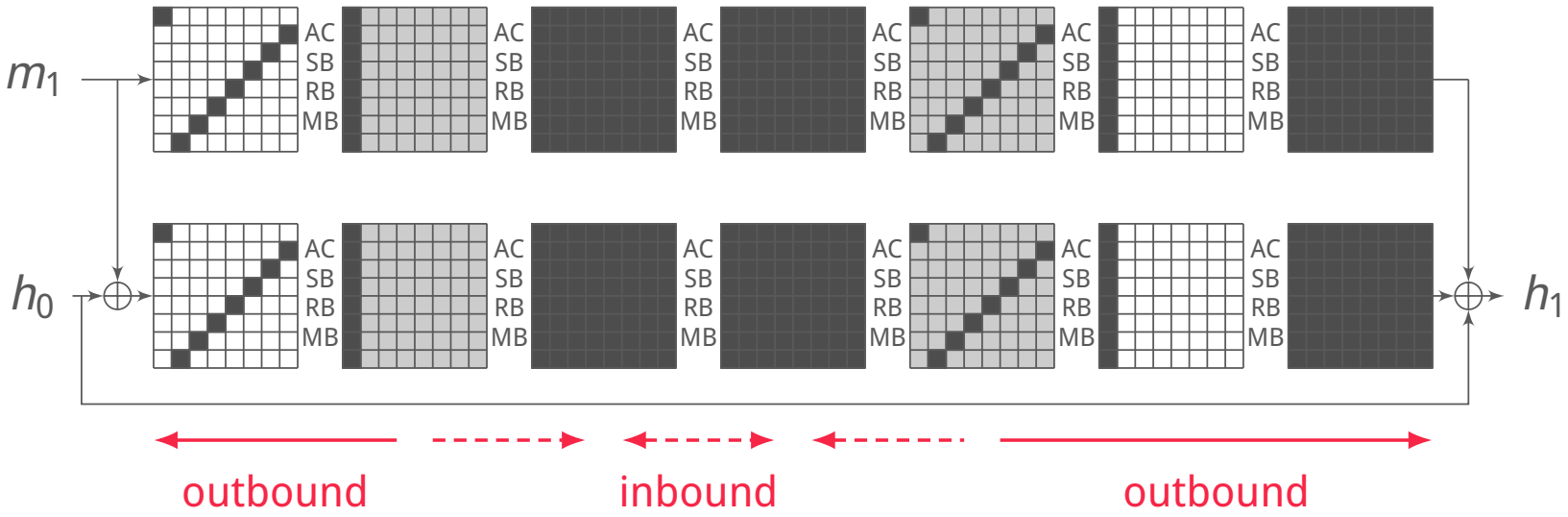
3 Propagate $T^{\oplus}$ outbound (truncated MixBytes: prob 1)

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

3′ Propagate T^{+} outbound (AddConstant: prob $2^{-2.45}$)

$\Rightarrow$ $2^{51.95+}$ solutions with complexity $2^{63.4+}$ ($2^{11.55}$ amortized)

Outbound phase for $T^{\oplus}$, T^{+} and Match



3 Propagate $T^{\oplus}$ outbound (truncated MixBytes: prob 1)

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

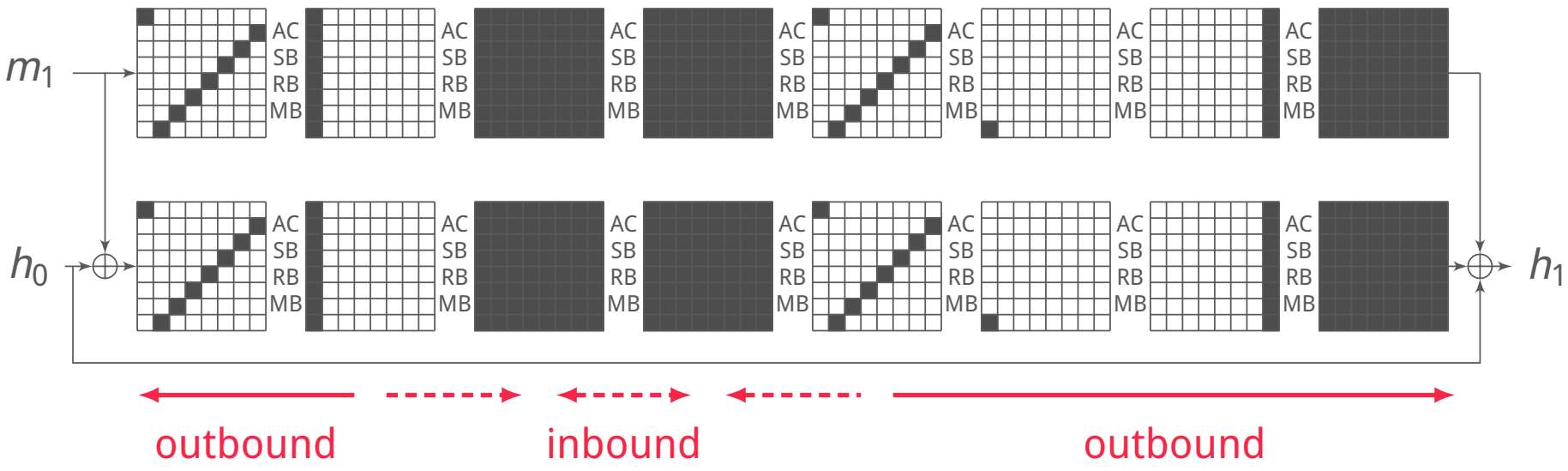
3′ Propagate T^{+} outbound (AddConstant: prob $2^{-2.45}$)

$\Rightarrow$ $2^{51.95+}$ solutions with complexity $2^{63.4+}$ ($2^{11.55}$ amortized)

4 Unbalanced Birthday: 2^{a} pairs for $T^{\oplus}$, 2^{128-a} pairs for T^{+}

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

Extending the Attack to 7 Rounds



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

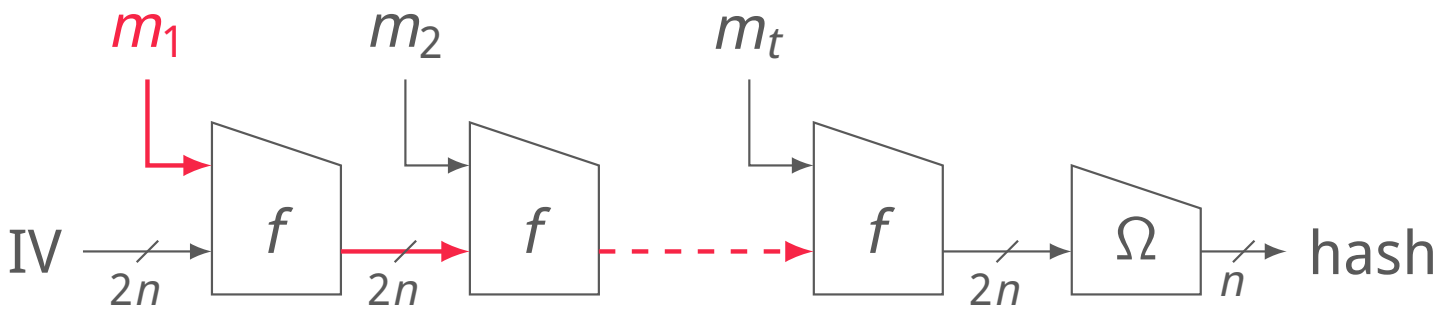
- Inbound phase: the same as before
- Outbound phase: extended by one round (probability: 2^{-56})

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

Attack on the Hash Function

Basic Attack Strategy

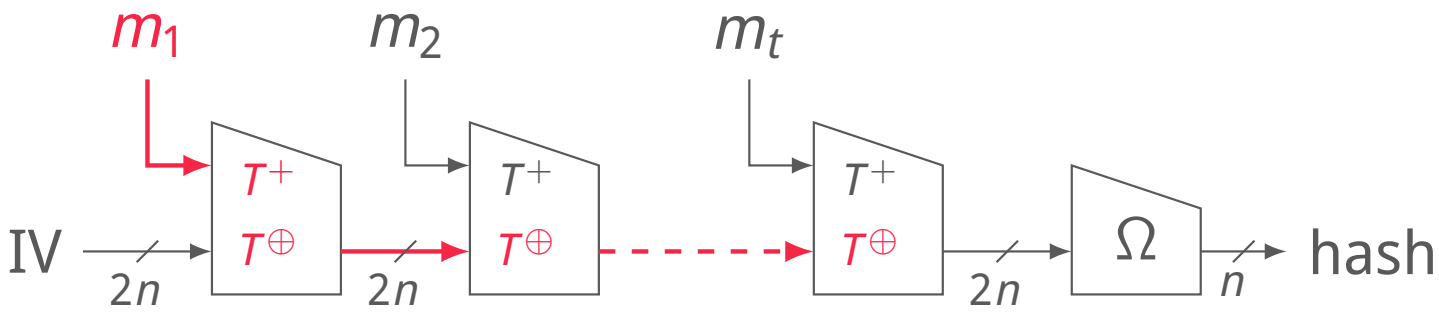
Similar to [MRS14]



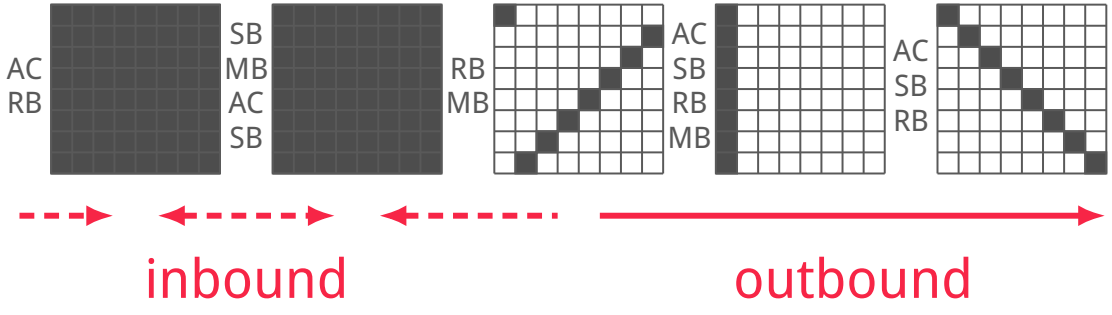
- Start with arbitrary difference in chaining variable
- Iteratively cancel differences in chaining variable

Basic Attack Strategy

Similar to [MRS14]



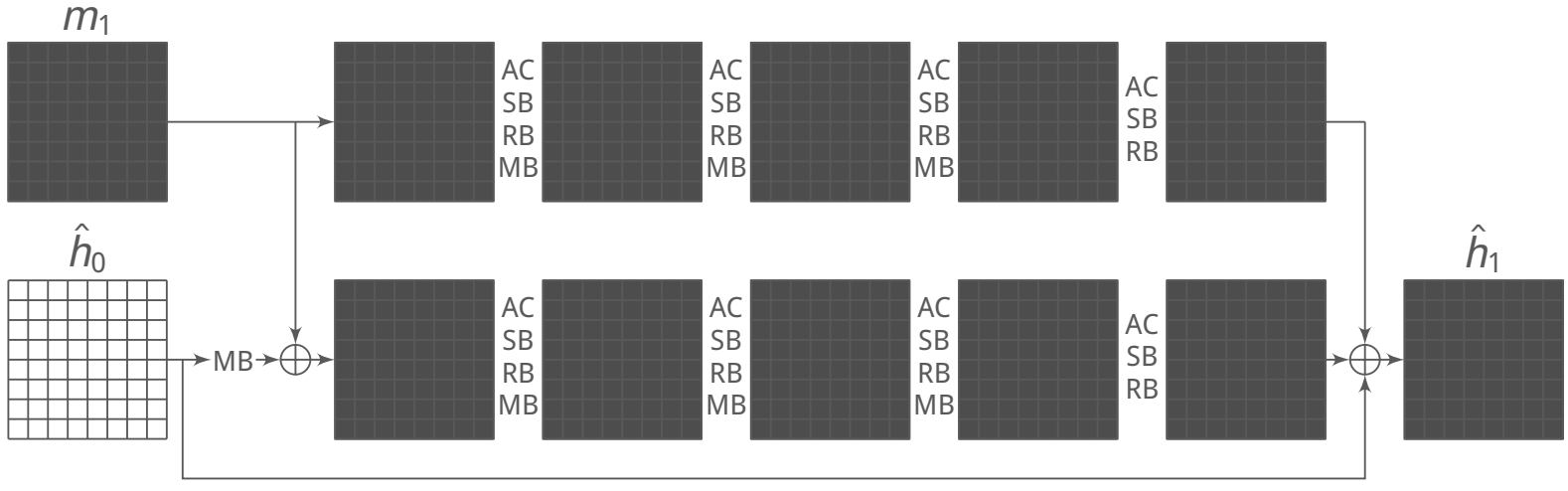
- Start with arbitrary difference in chaining variable
- Iteratively cancel differences in chaining variable
- Target trail for $T^\oplus$:



- No differences in T^+!

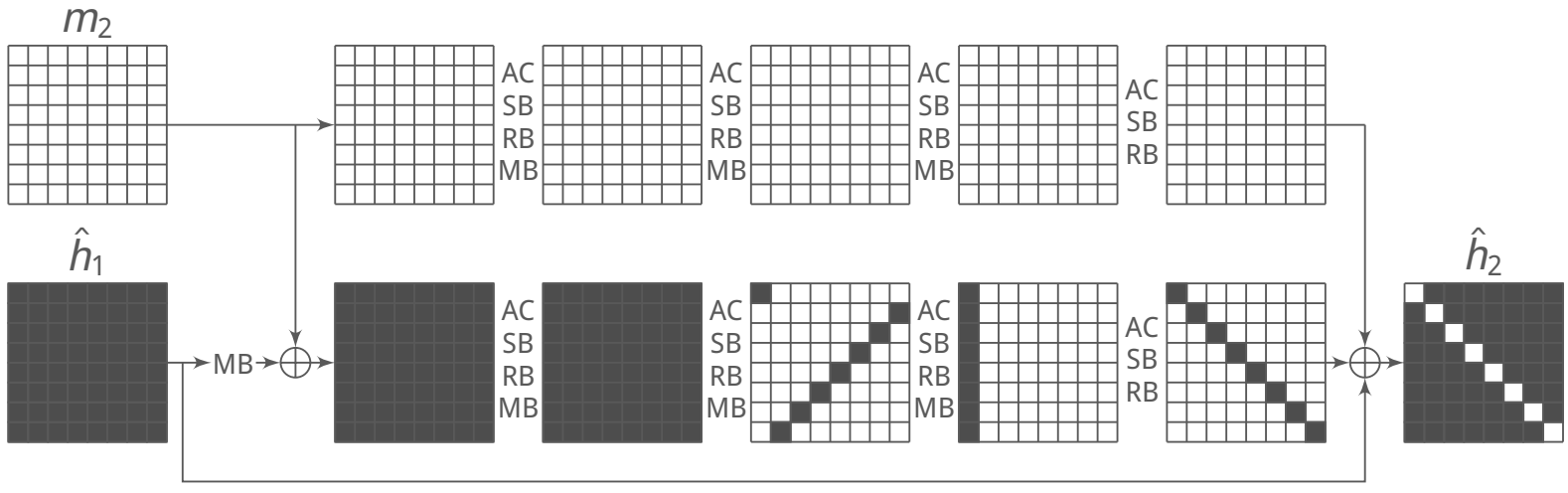
Attack on 4 Rounds

1. Start with random messages m_1, m_1^*



Attack on 4 Rounds

1. Start with random messages m_1, m_1^*
2. Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_2$

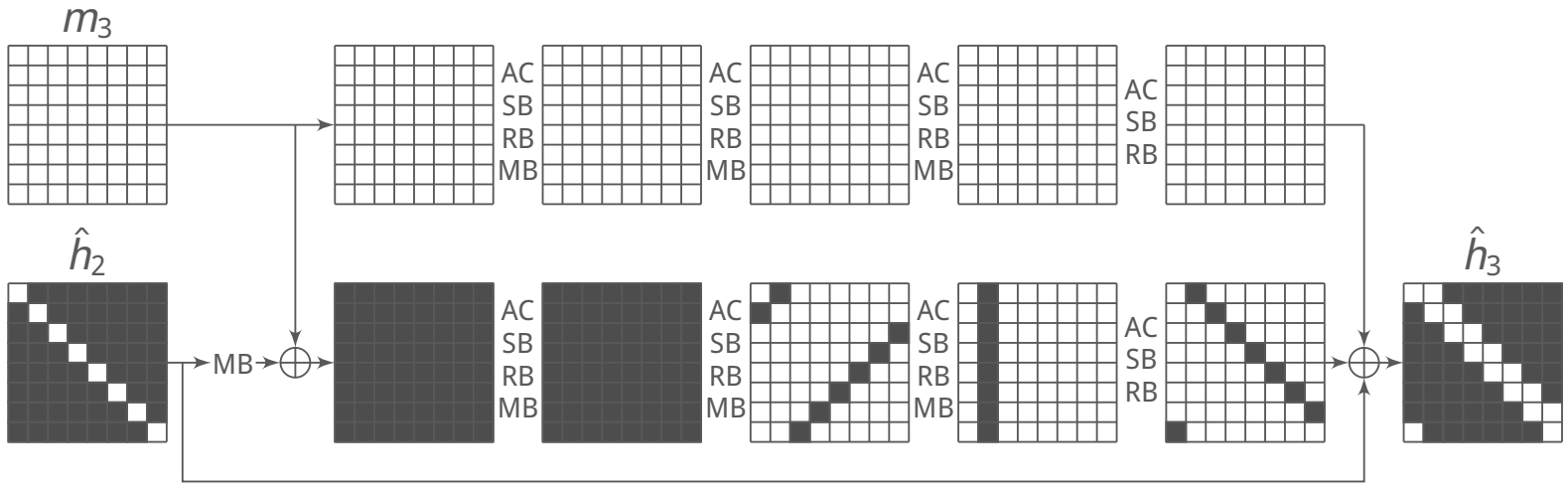


Attack on 4 Rounds

1. Start with random messages m_1, m_1^*

⋮

3. Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_3$

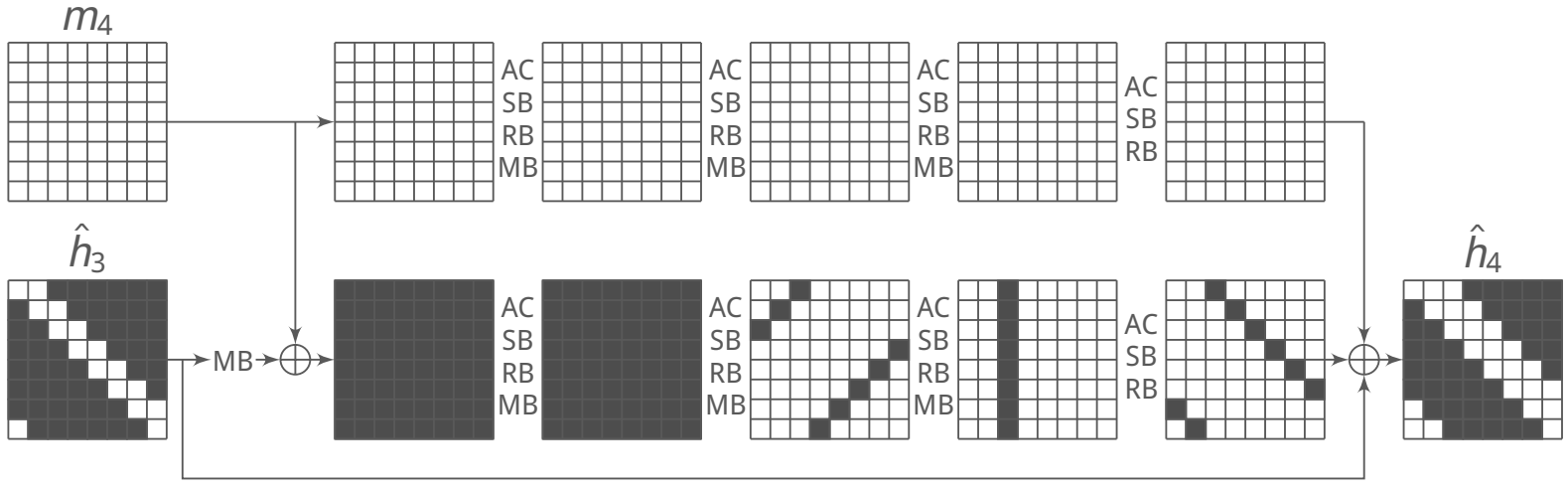


Attack on 4 Rounds

1. Start with random messages m_1, m_1^*

⋮

4. Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_4$

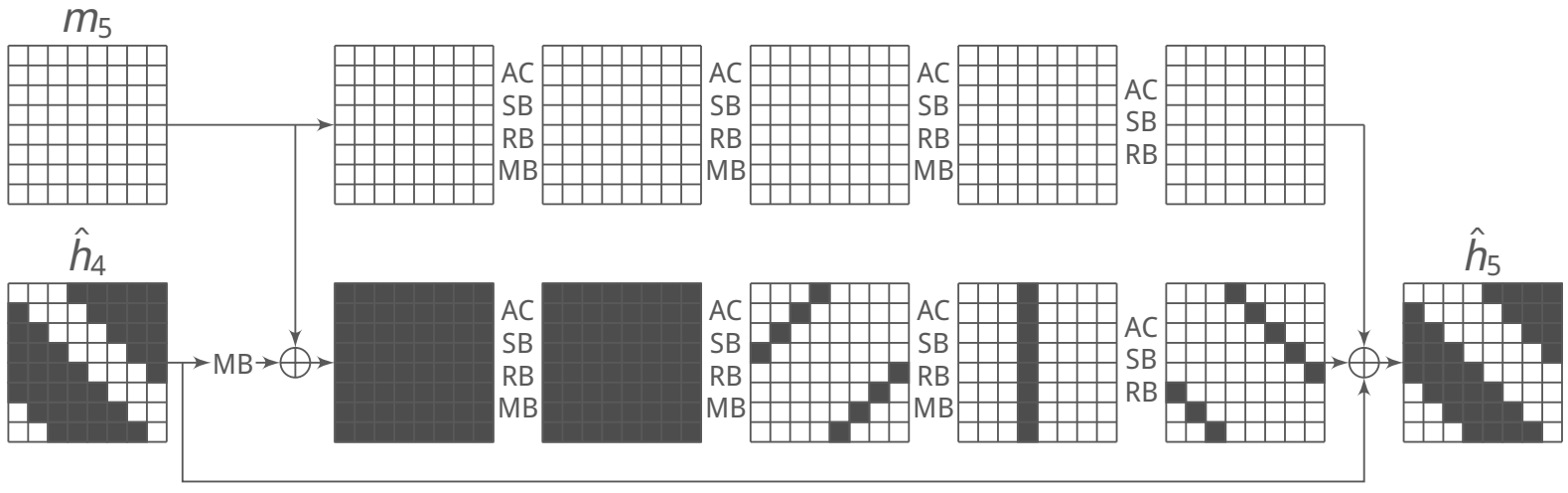


Attack on 4 Rounds

1. Start with random messages m_1, m_1^*

⋮

5. Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_5$

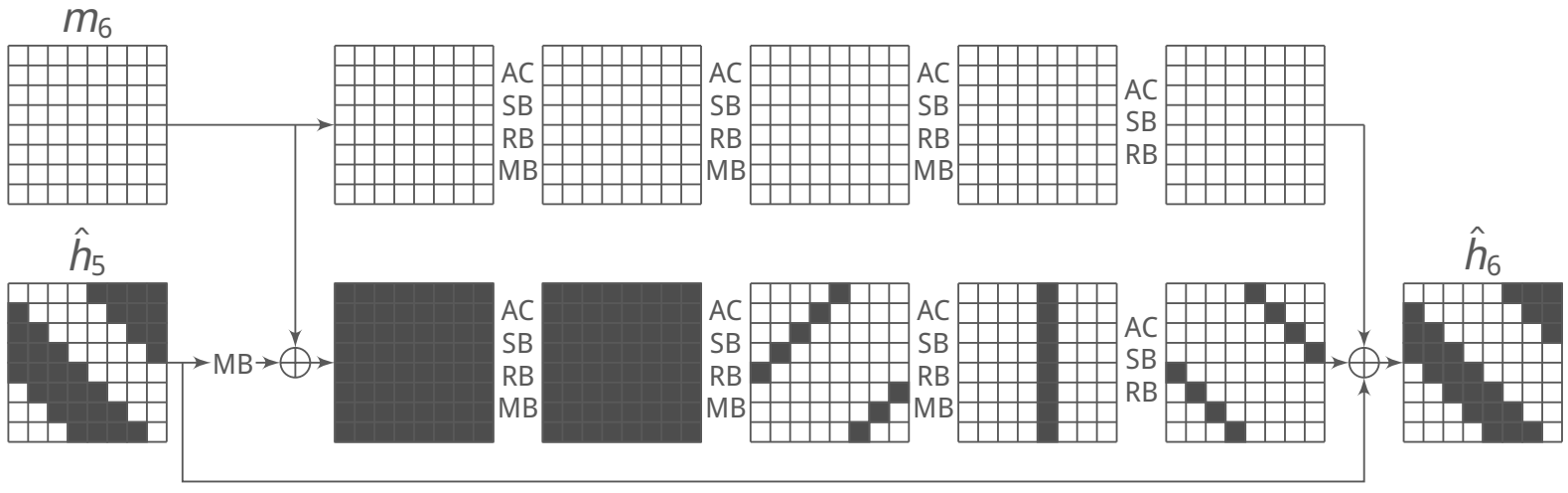


Attack on 4 Rounds

1. Start with random messages m_1, m_1^*

⋮

6. Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_6$

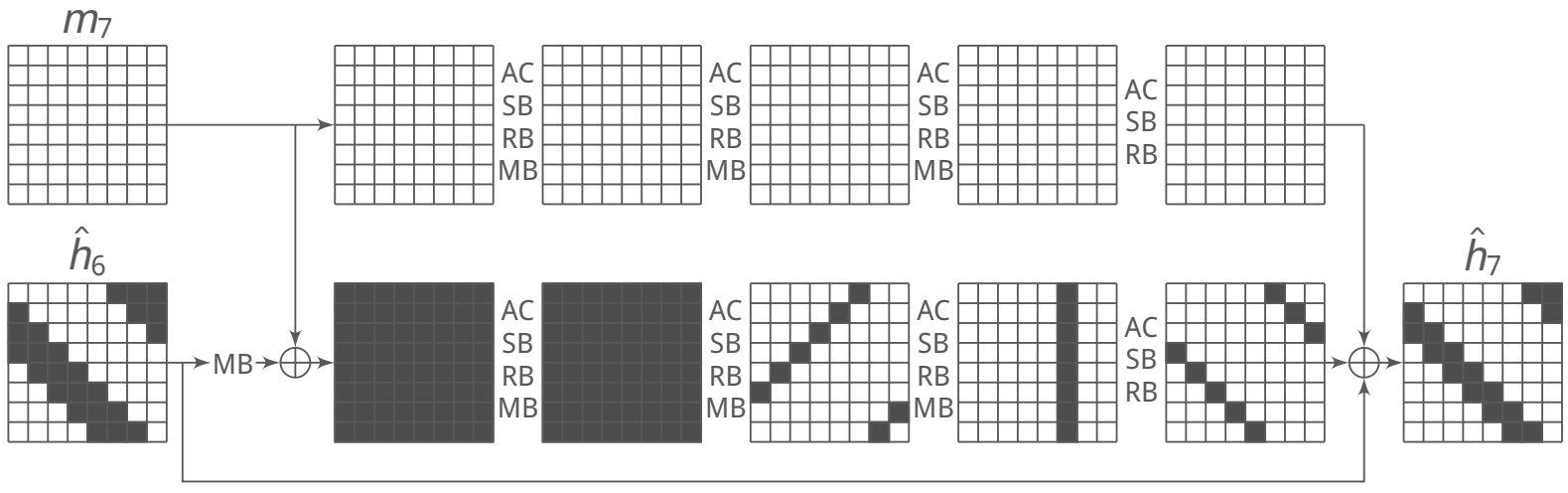


Attack on 4 Rounds

1. Start with random messages m_1, m_1^*

⋮

7. Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_7$

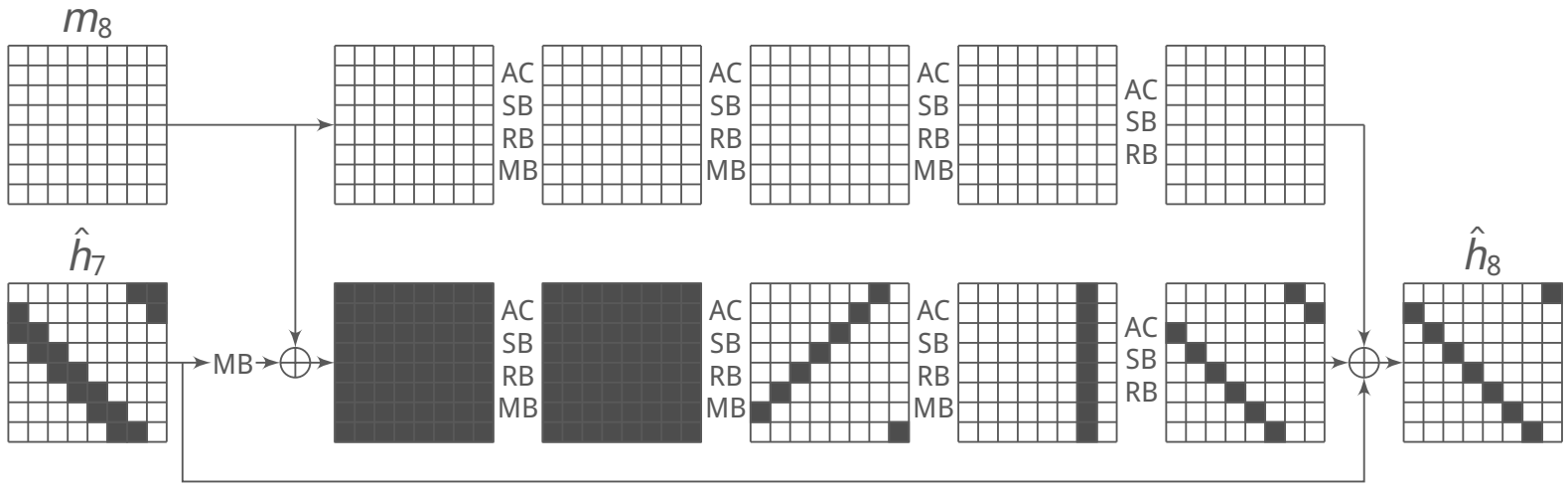


Attack on 4 Rounds

1 Start with random messages m_1, m_1^*

⋮

8 Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_8$

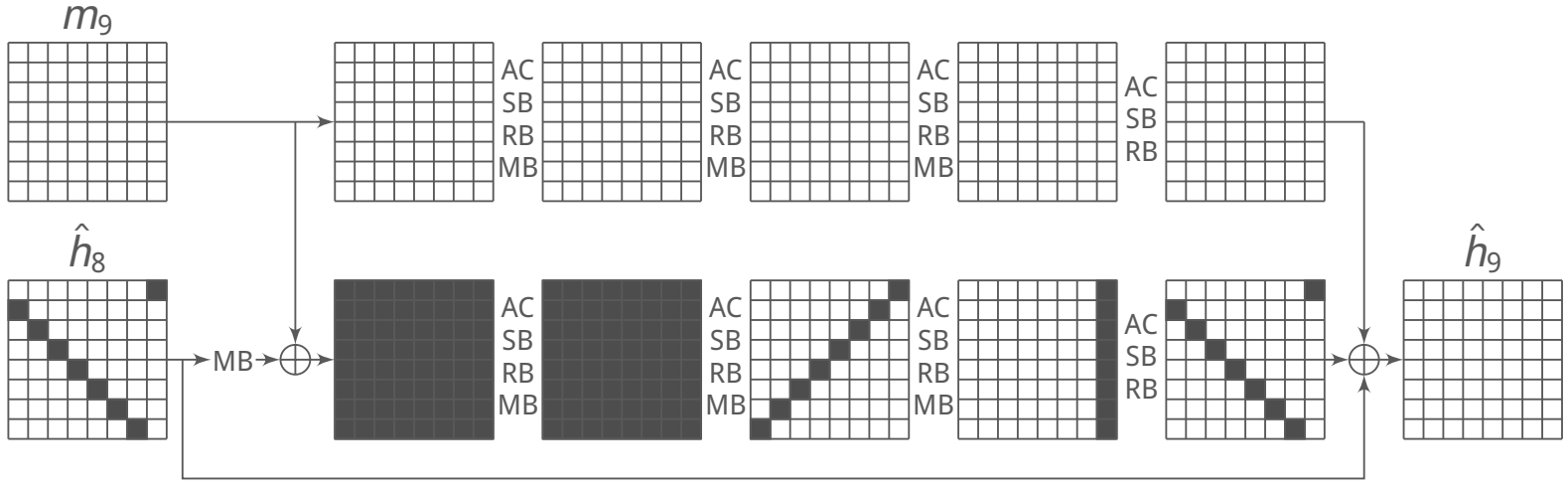


Attack on 4 Rounds

1 Start with random messages m_1, m_1^*

⋮

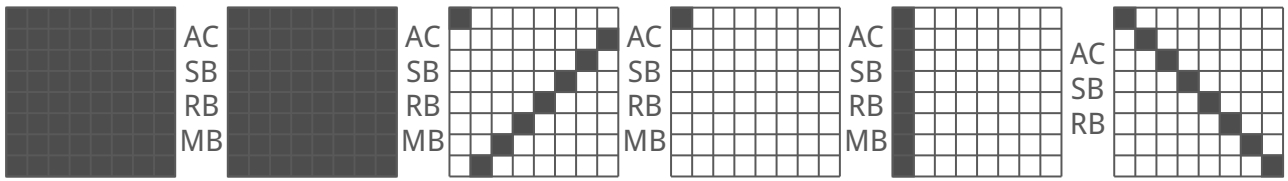
9 Find 2^{64} solutions for $T^{\oplus}$-trail $\rightarrow$ 1 will cancel 8 bytes of $\hat{h}_9$



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

Extending the Attack to 5 Rounds

- Target trail for $T^{\oplus}$:



- Rebound attack finds 2^8 solutions with 2^{64} time and memory
- Thus each step only succeeds with probability 2^{-56}

- Use tricks of [MRS14]

$\Rightarrow$ Collision attack with complexity 2^{120}

Conclusion

Attacks on Kupyna-256	Rounds	Complexity	Memory
Compression Function	6	$2^{69.8}$	2^{64}
	7	$2^{125.8}$	2^{64}
Hash Function	4	2^{67}	2^{64}
	5	2^{120}	2^{64}

- Modular additions
  - Destroy byte-alignment & MDS property
  - Not sufficient to diversify T^{+}, $T^{\oplus}$
- Designers' security claims violated [Олі+15b]
- Security of Kupyna is not threatened

Bibliography I

[Men+09] F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen
The Rebound Attack: Cryptanalysis of Reduced Whirlpool and Grøstl
FSE 2009

[Men+10] F. Mendel, C. Rechberger, M. Schläffer, and S. S. Thomsen
Rebound Attacks on the Reduced Grøstl Hash Function
CT-RSA 2010

[MRS14] F. Mendel, V. Rijmen, and M. Schläffer
Collision Attack on 5 Rounds of Grøstl
FSE 2014

[Oli+15] R. Oliynykov, I. Gorbenko, O. Kazymyrov, V. Ruzhentsev, O. Kuznetsov, Y. Gorbenko, A. Boiko, O. Dyrda, V. Dolgov, and A. Pushkaryov
A New Standard of Ukraine: The Kupyna Hash Function
Cryptology ePrint Archive, Report 2015/885 2015

[ZD15] J. Zou and L. Dong
Cryptanalysis of the Round-Reduced Kupyna Hash Function
`http://ia.cr/2015/959` 2015

Bibliography II

[Олі+15a] Р. В. Олійников, І. Д. Горбенко, О. В. Казимиров, В. І. Руженцев, А. О. Бойко, О. О. Кузнєцов, Ю. І. Горбенко, В. І. Долгов, О. В. Дирда, and А. І. Пушкарьов
ДСТУ 7564:2014. Національний стандарт України. Інформаційні технології. Криптографічний захист інформації. Функція ґешування “Купина”.
Ministry of Economical Development and Trade of Ukraine (in Ukrainian) 2015

[Олі+15b] Р. Олійников, І. Горбенко, О. Казимиров, В. Руженцев, А. Бойко, О. Кузнєцов, Ю. Горбенко, В. Долгов, О. Дирда, and А. Пушкарьов
Функція ґешування “Купина”: Основны Властивости.
http://de.slideshare.net/oliynykov/kupyna (in Ukrainian) 2015