Grøstl$_{512}$ Distinguishing Attack: A New Rebound Attack of an AES-like Permutation

Victor Cauchois [1,2] Clément Gomez [1] Reynald Lercier [1,2]

[1]DGA-MI
[2]IRMAR

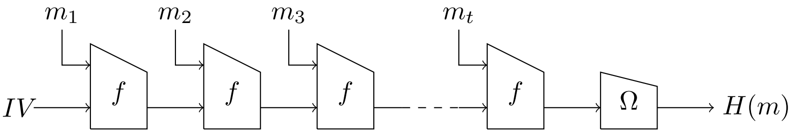
FSE 2018

Outline

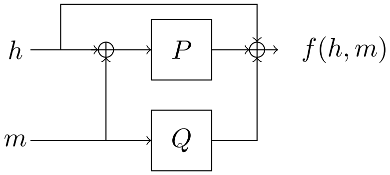
1. Grøstl$_{512}$ hash function
2. 10-round Rebound Attack on Grøstl$_{512}$ Permutations
3. 11-round Rebound Attack on Grøstl$_{512}$ Permutations

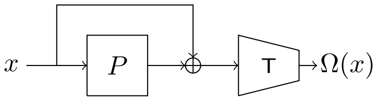
Outline

Grøstl$_{512}$ Mode of Operation



Grøstl$_{512}$ internal functions

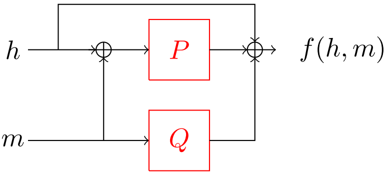




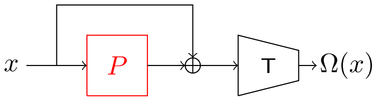
The compression function f

The output transformation Ω

Grøstl$_{512}$ internal functions



The compression function f



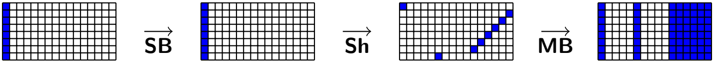
The output transformation Ω

Grøstl$_{512}$ security assertion

- P and Q ideal $\Rightarrow f$ collision and preimage resistant [FSZ09].
- P and Q ideal, independant $\Rightarrow$ Grøstl$_{512}$ indifferentiable from a random oracle [AMP10].

Grøstl$_{512}$ inner permutation P

14 iterations of the following round function:



Outline

Limited-birthday distinguishers

Problem

Limited-birthday(P, E_{in}, E_{out}): *Given a permutation* P *and two* $\mathbb{F}_2$*-linear subspaces* E_{in} *and* E_{out}*, find a pair of input values* (X, X') *such that* $X \oplus X' \in E_{in}$ *and* $P(X) \oplus P(X') \in E_{out}$.

Theorem (Gilbert,Peyrin in [GP10])

For a n*-bit permutation* P*, a* $\mathbb{F}_2$*-subspace* E_{in} *of dimension* d_i*, a* $\mathbb{F}_2$*-subspace* E_{out} *of dimension* d_o *and* $d_i \leq d_o$*, the computational complexity* $\mathcal{C}_{gen}$ *of the generic limited-birthday algorithm solving* **Limited-birthday**(P, E_{in}, E_{out}) *satisfies:*

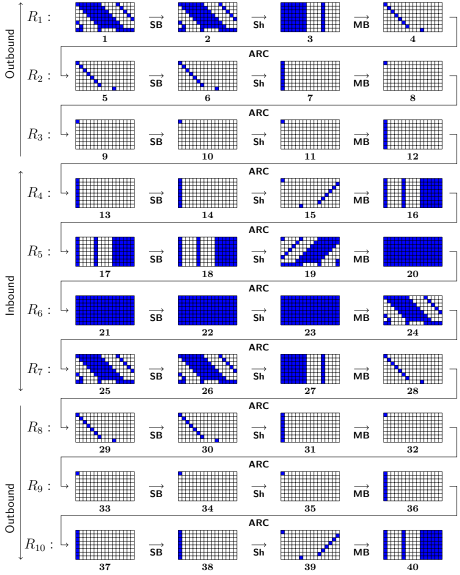
$$\log_2(\mathcal{C}_{gen}) = \begin{cases} (n - d_o)/2 & if\ n < 2d_i + d_o\,, \\ n - d_i - d_o & otherwise. \end{cases}$$

Optimality has been proven by Iwamoto, Peyrin and Sasaki in [IPS13].

Goals of a Rebound Attack

- Find E_{in} and E_{out} such that their exist an algorithm which solves **Limited-birthday**(P, E_{in}, E_{out}) faster than the generic algorithm.
- The assumption on which the security proof of the hash function relies on is not valid anymore.
- Some rebound attack may be used to mount collision attacks [MRST09].

10-round truncated differential path [Jea13]



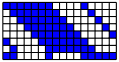
Ways of a Rebound Attack

- **Inbound phase:** Collect many samples designed to satisfy 4 middle rounds of the truncated differential path. Find couples of state values compatible with 2 differentials δ_{in} and δ_{out} propagated respectively forward and backward.

- **Outbound phase:** Find among those couples of state values one satisfying both probabilistic transitions towards the first and last rounds.

Generic limited-birthday algorithm complexity

- Initial state:



$$\dim(E_{in}) = 64 \cdot 8$$

- Final state:

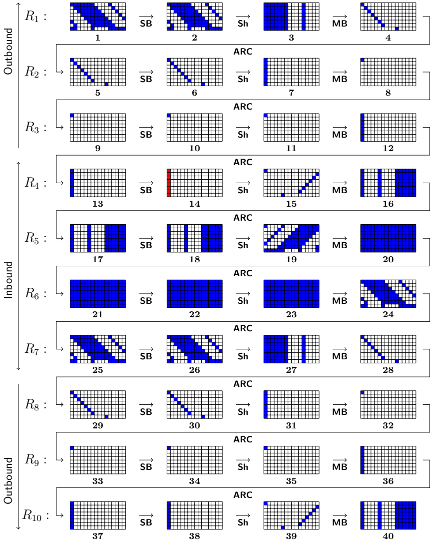
$$\dim(E_{out}) = 8 \cdot 8$$

- Computational complexity:

$$\log_2(\mathcal{C}_{gen}) = (128 - 64 - 8) \cdot 8 = 56 \cdot 8 = 448$$

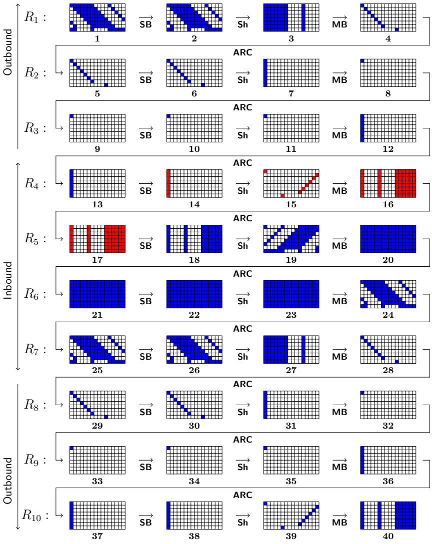
Selection of a differential δ_{in}

- Choose $\delta_{in} \in P_{14}$.
($2^{8 \cdot 8}$ elements)



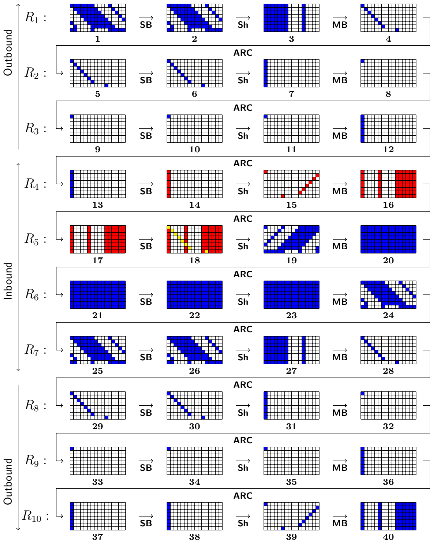
Deterministic propagation of δ_{in}

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\ \delta_{in})$.



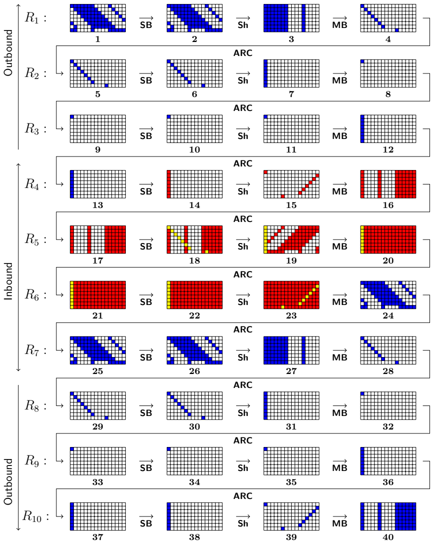
Computation of the 16 lists L_i

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.



Deterministic propagation of lists L_i

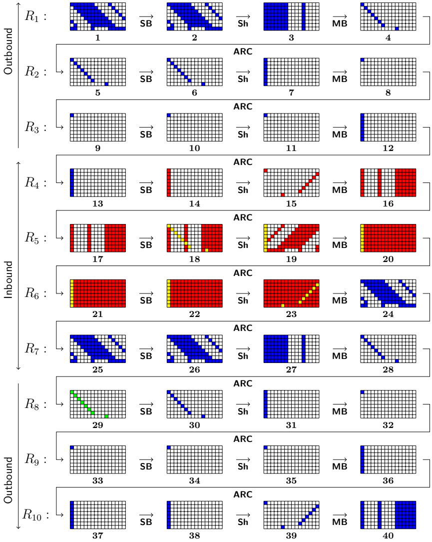
- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.



Selection of a differential δ_{out}

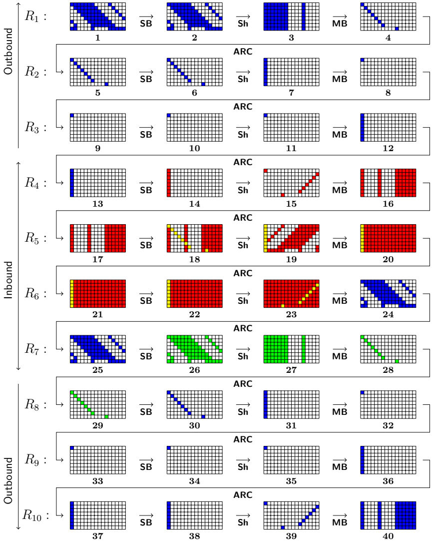
- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8\cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.

($2^{8\cdot 8}$ elements)



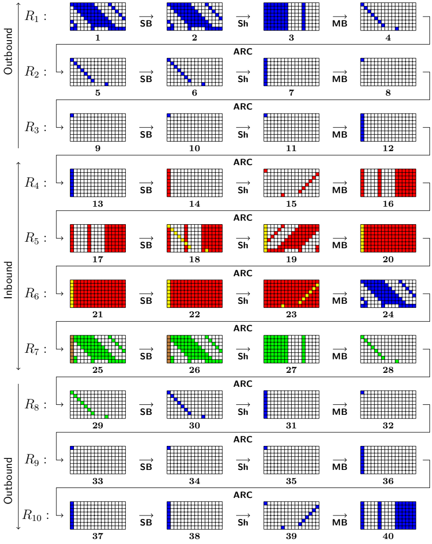
Deterministic propagation of δ_{out}

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8\cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.



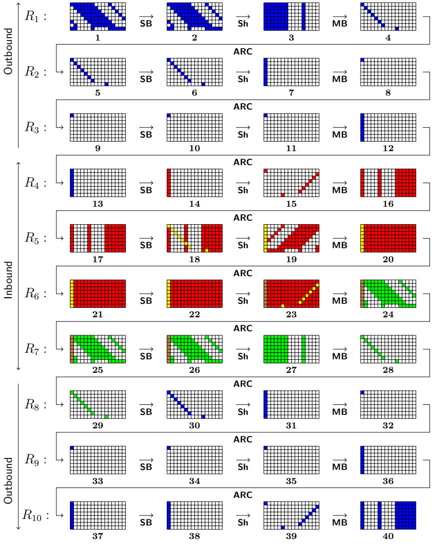
Computation of the 16 lists R_i

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.



Deterministic propagation of lists R_i

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\ \delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(\ L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\ \delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(\ R_i)$.

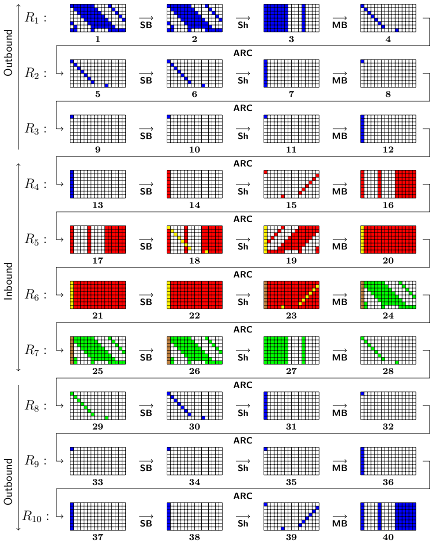


Merging lists

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(R_i)$.
- Merging lists L'_i and R'_i.

(Guess and Determine)

We find a match with $\mathcal{C} \simeq 2^{280}$ and $\mathcal{M} \simeq 2^{64}$.

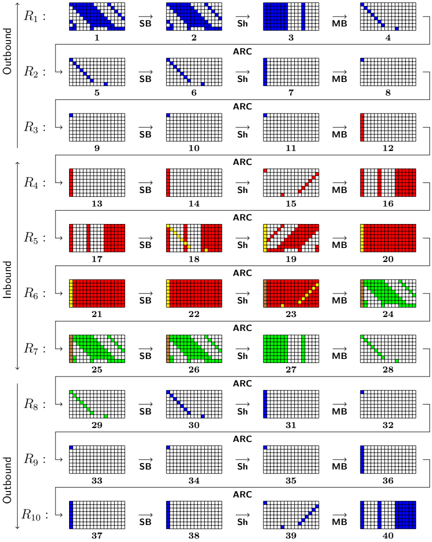


Probabilisitic transition through MB^{-1}

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(R_i)$.
- Merging lists L'_i and R'_i.

(Guess and Determine)

- $\mathbb{P}(P_{12} \to P_{11}) = 2^{-7 \cdot 8}$.

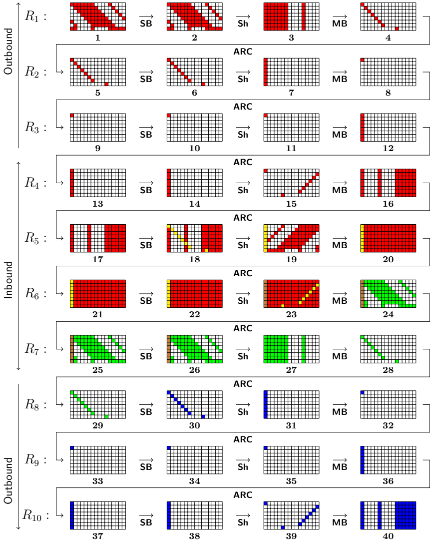


Deterministic transition

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8\cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8\cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(R_i)$.
- Merging lists L'_i and R'_i.

(Guess and Determine)

- $\mathbb{P}(P_{12} \rightarrow P_{11}) = 2^{-7\cdot 8}$.

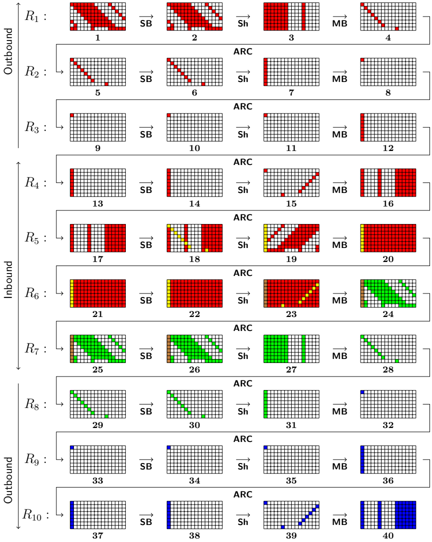


Probablistic transition through MB

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(R_i)$.
- Merging lists L'_i and R'_i.

(Guess and Determine)

- $\mathbb{P}(P_{12} \to P_{11}) = 2^{-7 \cdot 8}$.
- $\mathbb{P}(P_{31} \to P_{32}) = 2^{-7 \cdot 8}$.

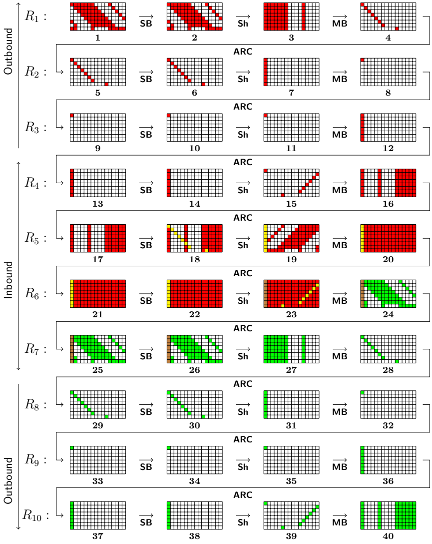


Deterministic transition

- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(R_i)$.
- Merging lists L'_i and R'_i.

(Guess and Determine)

- $\mathbb{P}(P_{12} \rightarrow P_{11}) = 2^{-7 \cdot 8}$.
- $\mathbb{P}(P_{31} \rightarrow P_{32}) = 2^{-7 \cdot 8}$.



10-round distinguisher

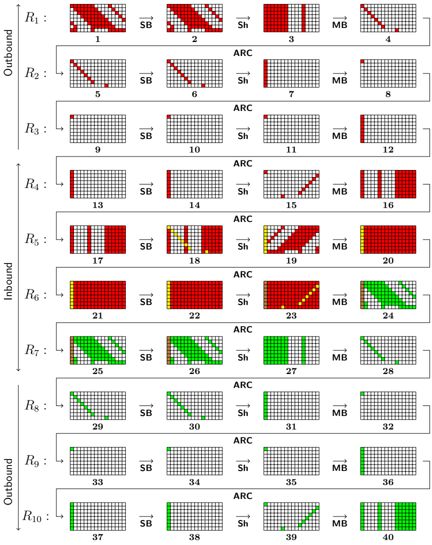
- Choose $\delta_{in} \in P_{14}$.
- $\delta'_{in} = \mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh}(\delta_{in})$.
- $L_i = \{(X, X \oplus \delta'_{in}), X \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $L'_i = \mathbf{Sh} \circ \mathbf{SB} \circ \mathbf{R}_5(L_i)$.
- Choose $\delta_{out} \in P_{29}$.
- $\delta'_{out} = (\mathbf{ARC} \circ \mathbf{MB} \circ \mathbf{Sh})^{-1}(\delta_{out})$.
- $R_i = \{(Y, Y \oplus \delta'_{out}), Y \in \mathbb{F}_2^{8 \cdot 8}\}$.
- $R'_i = (\mathbf{SB} \circ \mathbf{ARC} \circ \mathbf{MB})^{-1}(R_i)$.
- Merging lists L'_i and R'_i.

(Guess and Determine)

- $\mathbb{P}(P_{12} \to P_{11}) = 2^{-7 \cdot 8}$.
- $\mathbb{P}(P_{31} \to P_{32}) = 2^{-7 \cdot 8}$.
- Overall complexity:

$$\begin{cases} \mathcal{C} \simeq 2^{112} \cdot 2^{280} = 2^{392} < 2^{448} \\ \mathcal{M} \simeq 2^{7 \cdot 8} \end{cases}$$

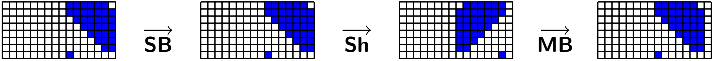
Distinguisher!



Outline

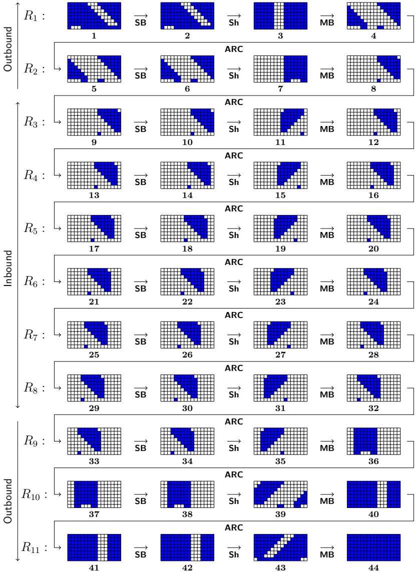
1. Grøstl$_{512}$ hash function
2. 10-round Rebound Attack on Grøstl$_{512}$ Permutations
3. 11-round Rebound Attack on Grøstl$_{512}$ Permutations

Mixed-Integer Linear Programming



Probabilistic step through MB of probability $2^{-22 \cdot 8}$.

11-round truncated differential path

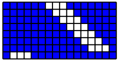


Re-Rebound Attack

- **Inbound phase:** Collect many samples designed to satisfy 6 middle rounds of the truncated differential path. Find couples of state values compatible with 3 differential values δ_1, δ_2 and δ_3 propagated forward and backward.
- **Outbound phase:** Find among those couples of state values one satisfying both probabilistic transitions towards the first and last rounds.

Generic limited-birthday algorithm complexity

- Initial state:



$$\dim(E_{in}) = 104 \cdot 8$$

- Final state:

$$\dim(E_{out}) = 104 \cdot 8$$

- Computational complexity:

$$\log_2(\mathcal{C}_{gen}) = \frac{128 - 104}{2} \cdot 8 = 12 \cdot 8 = 96$$

Plausibility

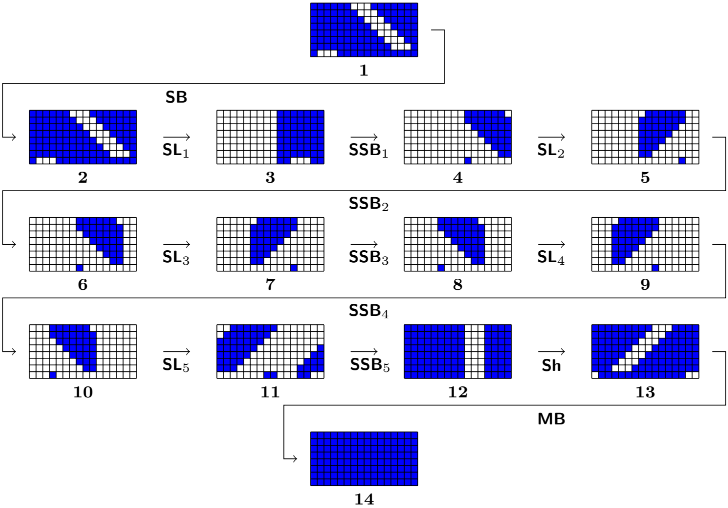
- Sequence of numbers of active bytes:

$$104 \xrightarrow{R_1} 53 \xrightarrow{R_2} 34 \xrightarrow{R_3} 34 \xrightarrow{R_4} 34 \xrightarrow{R_5} 34 \xrightarrow{R_6} 34 \xrightarrow{R_7} 34 \xrightarrow{R_8} 34 \xrightarrow{R_9} 53 \xrightarrow{R_{10}} 104 \xrightarrow{R_{11}} 128$$

- $2^{(104+128)\cdot 8}$ possible initial states.
- Probabilistic transitions :
  - 1 transition with probability $2^{-51\cdot 8}$
  - 7 transitions with probability $2^{-22\cdot 8}$
  - 1 transitions with probability $2^{-3\cdot 8}$

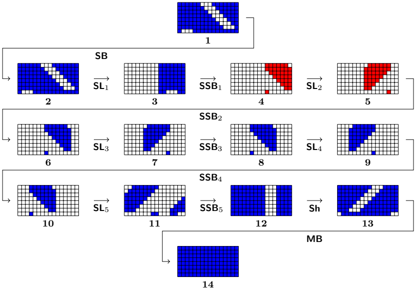
$\Rightarrow 2^{24\cdot 8}$ such differences are expected.

Super SBOX description



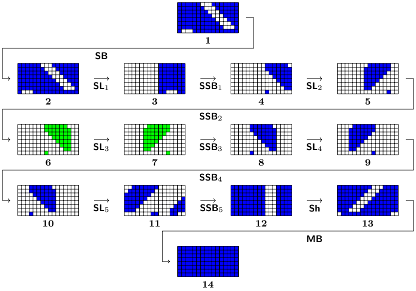
Computation of differential set Δ_1

$$\Delta_1 = \{\delta_1 \in P_4 \mid \delta_1' = \mathbf{SL}_2(\delta_1) \in P_5\}.$$



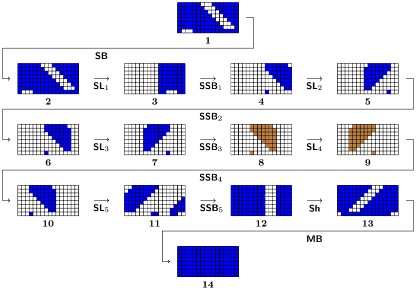
Computation of differential set Δ_2

$$\Delta_2 = \{\delta_2 \in P_6 \mid \delta_2' = \mathbf{SL}_3(\delta_2) \in P_7\}.$$



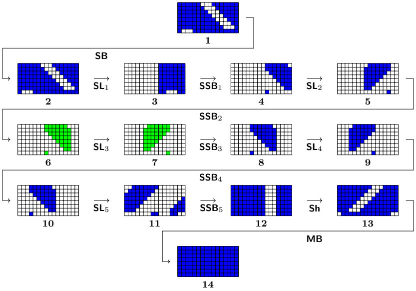
Computation of differential set Δ_3

$$\Delta_3 = \{\delta_3 \in P_8 \mid \delta_3' = \mathbf{SL}_4(\delta_3) \in P_9\}.$$



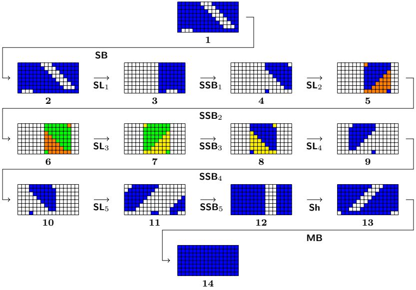
Selection of a differential δ_2

- Choose $\delta_2 \in \Delta_2$.



Computation of 7 lists C_i and 7 lists C'_i

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i:



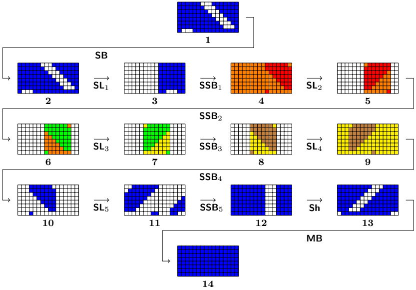
Column by column, complexity: $\mathcal{C} \simeq 2^{7\cdot 8}$, $\mathcal{M} \simeq 2^{7\cdot 8}$

$$C_i = \{ (X, Y = X \oplus (\delta_2)_{|i}) | \, \mathbf{SSB}_2^{-1}(X) \oplus \mathbf{SSB}_2^{-1}(Y) \in (P_5)_{|i} \},$$

$$C'_j = \{ (X, Y = X \oplus (\delta'_2)_{|j}) | \, \mathbf{SSB}_3(X) \oplus \mathbf{SSB}_3(Y) \in (P_8)_{|j} \}.$$

Computation of lists E and F

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i.
- Compute E and F:

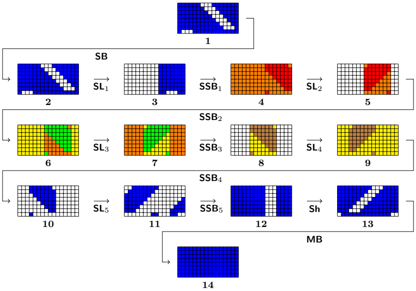


To construct $|E| = 2^{6 \cdot 8}$ and $|F| = 2^{6 \cdot 8}$, we need $\mathcal{C}_3 \simeq 2^{6 \cdot 8}$ and $\mathcal{M}_3 \simeq 2^{6 \cdot 8}$.

Merging lists

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i.
- Compute E and F.
- Merging E and F.

(1^{st} Guess and Determine)



$\mathbb{P}(e \in E$ and $f \in F$ admits a matching completion$) = 2^{-12\cdot 8}$
Any fitting choice admits $2^{28\cdot 8}$ matching completions
We find such choice with $\mathcal{C}_4 \simeq 2^{7\cdot 8}$ and $\mathcal{M}_4 \simeq 2^{6\cdot 8}$

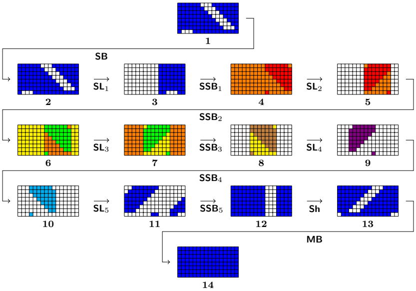
Tricky choice

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i.
- Compute E and F.
- Merging E and F.

(1^{st} Guess and Determine)

- Choose $(s, s \oplus \delta_3)$.

(2^{nd} Guess and Determine)



$\mathbb{P}(\ (s, s \oplus \delta_3)$ admits a completion$) = 2^{-12\cdot 8}$
Any fitting choice admits $2^{72\cdot 8}$ matching completions
We find such a choice with $\mathcal{C}_5 \simeq 2^{3\cdot 8}$ and $\mathcal{M}_5 \simeq 2^{3\cdot 8}$

Merging completions

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i.
- Compute E and F.
- Merging E and F.

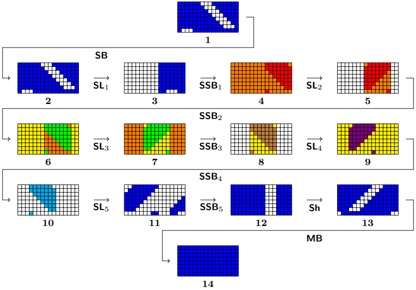
(1^{st} Guess and Determine)

- Choose $(s, s \oplus \delta_3)$.

(2^{nd} Guess and Determine)

- Merging completions.

(3^{rd} Guess and Determine)



$2^{6\cdot 8}$ complete state values are in the intersection of both completions
We compute and store them with $\mathcal{C}_6 \simeq 2^{9\cdot 8}$ and $\mathcal{M}_6 \simeq 2^{7\cdot 8}$

Probabilistic transition through SSB_1^{-1}

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i.
- Compute E and F.
- Merging E and F.

(1^{st} Guess and Determine)

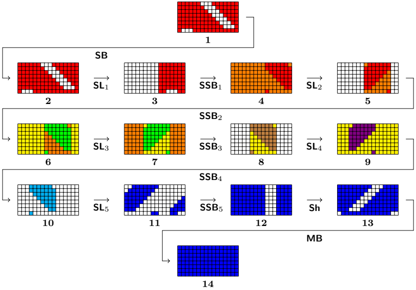
- Choose $(s, s \oplus \delta_3)$.

(2^{nd} Guess and Determine)

- Merging completions.

(3^{rd} Guess and Determine)

- $\mathbb{P}(P_4 \to P_3) = 2^{-3 \cdot 8}$.



Probabilistic transition through $\mathbf{SL}_5$

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C_i'.
- Compute E and F.
- Merging E and F.

(1^{st} Guess and Determine)

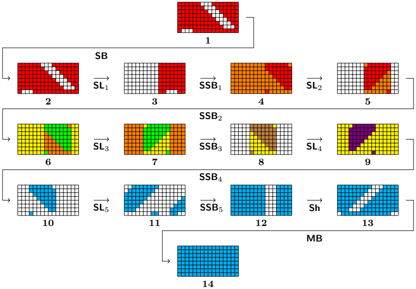
- Choose $(s, s \oplus \delta_3)$.

(2^{nd} Guess and Determine)

- Merging completions.

(3^{rd} Guess and Determine)

- $\mathbb{P}(P_4 \to P_3) = 2^{-3\cdot 8}$.
- $\mathbb{P}(P_{10} \to P_{11}) = 2^{-3\cdot 8}$.



11-round distinguisher

- Choose $\delta_2 \in \Delta_2$.
- Compute C_i and C'_i.
- Compute E and F.
- Merging E and F.

(1^{st} Guess and Determine)

- Choose $(s, s \oplus \delta_3)$.

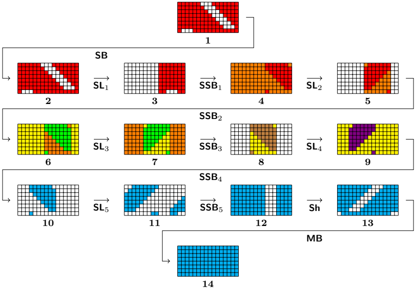
(2^{nd} Guess and Determine)

- Merging completions.

(3^{rd} Guess and Determine)

- $\mathbb{P}(P_4 \to P_3) = 2^{-3 \cdot 8}$.
- $\mathbb{P}(P_{10} \to P_{11}) = 2^{-3 \cdot 8}$.
- Overall complexity:

$$\begin{cases} \mathcal{C} & \simeq & 2^{9 \cdot 8} & < 2^{96} \\ \mathcal{M} & \simeq & 2^{7 \cdot 8} \end{cases}$$

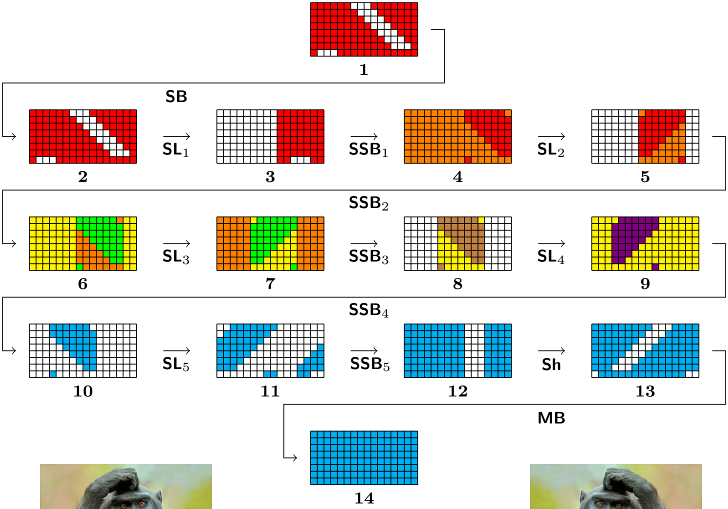


Distinguisher!

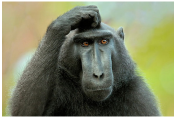
Conclusion

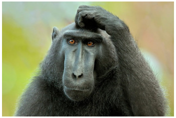
- First rebound attack on 11 round of Grøstl$_{512}$'s permutations.
- 12-round truncated differential path is statistically realized.
- It seems difficult to derive a distinguisher for 12 rounds.
- These methods shall generalize to all AES-like permutations.

Questions?



1
SB
2
$\overrightarrow{SL}_1$
3
$\overrightarrow{SSB}_1$
4
$\overrightarrow{SL}_2$
5
SSB_2
6
$\overrightarrow{SL}_3$
7
$\overrightarrow{SSB}_3$
8
$\overrightarrow{SL}_4$
9
SSB_4
10
$\overrightarrow{SL}_5$
11
$\overrightarrow{SSB}_5$
12
$\overrightarrow{Sh}$
13
MB
14





Elena Andreeva, Bart Mennink, and Bart Preneel.
On the indifferentiability of the grøstl hash function.
In Security and Cryptography for Networks, volume 6280 of Lecture Notes in Comput. Sci., pages 88–105. Springer, 2010.

Pierre-Alain Fouque, Jacques Stern, and Sébastien Zimmer.
Cryptanalysis of tweaked versions of SMASH and reparation.
In Selected Areas in Cryptography, volume 5381 of Lecture Notes in Comput. Sci., pages 136–150. Springer, 2009.

Henri Gilbert and Thomas Peyrin.
Super-sbox cryptanalysis: Improved attacks for aes-like permutations.
In Fast Software Encryption, volume 6147 of Lecture Notes in Comput. Sci., pages 365–383. Springer, 2010.

References

Mitsugu Iwamoto, Thomas Peyrin, and Yu Sasaki.
Limited-birthday distinguishers for hash functions - Collisions beyond the birthday bound can be meaningful.
In Advances in cryptology—ASIACRYPT 2013, volume 8870 of Lecture Notes in Comput. Sci., pages 504–523. Springer, 2013.

Jérémy Jean.
Cryptanalyse de primitives symétriques basées sur le chiffrement AES.
PhD thesis, Ecole Normale Supérieure, 2013.

Florian Mendel, Christian Rechberger, Martin Schläffer, and Søren S. Thomsen.
The rebound attack: Cryptanalysis of reduced whirlpool and grøstl.
In Fast Software Encryption, volume 5665 of Lecture Notes in Comput. Sci., pages 260–276. Springer, 2009.