Improved Rebound Attack on the Finalist Grøstl

Jérémy Jean\textsuperscript{1}  María Naya-Plasencia\textsuperscript{2}  Thomas Peyrin\textsuperscript{3}

\textsuperscript{1}École Normale Supérieure, France  
\textsuperscript{2}University of Versailles, France  
\textsuperscript{3}Nanyang Technological University, Singapore

FSE’2012 – March 19, 2012
Grøstl: Compression Function (CF)

Grøstl-v0 [Knudsen et al. 08] has been tweaked for the final:

- **Grøstl-256**: $|h| = |m| = 512$ bits.
- **Grøstl-512**: $|h| = |m| = 1024$ bits.
**Grøstl Internal Permutations**

Permutations P and Q apply the wide-trail strategy from the AES.

- **Grøstl-256**: 10 rounds on state a $8 \times 8$.
- **Grøstl-512**: 14 rounds on state a $8 \times 16$.

Tweak: constants in ARK and Sh changed to introduce asymmetry between P and Q.
Grøstl: Finalization Round

Once all blocks of message have been treated: truncation.

\[ h_{i-1} \rightarrow P \rightarrow h \]
Grøstl: Best Analysis After the Tweak

- **Grøstl-256**:
  - [Sasaki et al A10]: 8-round permutation distinguisher.
  - [Gilbert et al. FSE10]: 8-round CF distinguisher.
  - [Boura et al. FSE11]: 10-round zero-sum.

- **Grøstl-512**
  - [Schläffer 2011]: 6-round collision on the CF.
Our New Results 1/2

► Based on the rebound technique [Mendel et al. FSE09].

► Based on a way of finding solutions for three consecutive full active rounds: new.

► They apply both to 256 and 512 versions.
Our New Results 2/2

▶ On Grøstl-256, we provide distinguishers for 9 rounds of the permutation (total: 10).

▶ On Grøstl-512, we provide distinguishers for 8, 9 and 10 rounds of the permutation (total: 14).
Rebound Attack
Rebound Attack

Inbound

Outbound

Outbound

FSE'2012 – J. Jean, M. Naya-Plasencia, T. Peyrin – Improved Rebound Attack on the Finalist Grøstl
**SuperSBox**

\[
\text{SuperSBox} = \text{SB} \circ \text{MC} \circ \text{SB}
\]
Grøstl-256 Permutation
Differential Characteristic for 9 rounds
Inbound for 3 Full-Active Rounds
Inbound for 3 Full-Active Rounds
Inbound for 3 Full-Active Rounds
Inbound for 3 Full-Active Rounds

\[ \begin{array}{cccc}
S0 & S1 & S2 & S3 \\
SB & Sh & Mb & \\
S3 & S4 & S5 & S6 \\
SB & Sh & Mb & \\
S6 & S7 & S8 & S9 \\
SB & Sh & Mb & \\
S9 & S10 & S11 & S12 \\
SB & Sh & Mb & \\
\end{array} \]
Inbound for 3 Full-Active Rounds: Analysis

Counting
- 8 forward SuperSBox sets of $2^{64}$ values and differences
- 8 backward SuperSBox sets of $2^{64}$ values and differences
- Overlapping on 512 bits of values + 512 bits of differences

Number of Solutions Expected

\[
2^{8 \times 64} \times 2^{8 \times 64} \times 2^{-512-512} = 2^{512+512-512-512} = 1
\]

Limited Birthday
- $2^{384}$ operations

Our Algorithm
- $2^{256}$ operations, memory $2^{64}$
Solving the 3 Active Rounds: Context

The 8 forward $L_i$ overlaps the 8 backwards $L'_i$ like this:
Solving the 3 Active Rounds: Step 1

We start by choosing one element in each of the four first $L_i'$. 

\[
\begin{array}{cccc}
\uparrow & \uparrow & \uparrow & \uparrow \\
L_1' & L_2' & L_3' & L_4'
\end{array}
\]
Solving the 3 Active Rounds: Step 2

This determines a single element in each $L_i$. 

$L_1 L_2 L_3 L_4 L_5 L_6 L_7 L_8$
Each determined element in the remaining $L'_i$ exists with $p = 2^{-8 \times 8}$. 
Summing Up

Inbound Phase

In total we try $2^{256}$ combinations of $(L'_1, L'_2, L'_3, L'_4)$ and each gives a solution with probability: $2^{-4 \times 8 \times 8} = 2^{-256}$.

Outbound Phase

Probability $2^{-2 \times 56}$ to pass two $8 \rightarrow 1$ transitions in the MixBytes.

Distinguisher

We distinguish the 9-round permutation in $2^{256+112} = 2^{367}$ operations and $2^{64}$ in memory.

Note: This compares to a generic complexity of $2^{384}$ operations.
Grøstl-512 Permutation
Differential Characteristic for 10 rounds
Inbound Phase
Inbound Phase
Inbound Phase

[Diagram showing the inbound phase with various grid patterns representing the steps of the Grøstl algorithm]

FSE'2012 – J. Jean, M. Naya-Plasencia, T. Peyrin – Improved Rebound Attack on the Finalist Grostl
Observations

Counting

- 16 forward SuperSBox sets of $2^{64}$ values and differences
- 16 backward SuperSBox sets of $2^{64}$ values and differences
- Overlapping on 1024 bits of values + 1024 bits of differences

Number of Solutions Expected

$$2^{16 \times 64} \times 2^{16 \times 64} \times 2^{-1024 - 1024} = 2^{1024 + 1024 - 1024 - 1024} = 1$$

Limited Birthday

$2^{896}$ operations

Our Algorithm

$2^{280}$ operations, memory $2^{64}$
Algorithm: Guess-and-Determine Approach

Constraints

The differences around the MixBytes layer are restricted since the right state is not fully active.

Notations

- Forward SuperSBoxes: $L_1, \ldots, L_{16}$.
- Backward SuperSBoxes: $L'_1, \ldots, L'_{16}$.
Algorithm: Guess-and-Determine Approach

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

\[ L_i \]

\[
\begin{array}{cccccccccccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 & 2 \\
3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 & 3 \\
5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 & 5 \\
6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 & 6 \\
7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 & 7 \\
8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 & 8 \\
9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 & 9 \\
10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 & 10 \\
12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 & 12 \\
13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 & 13 \\
16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 & 16 \\
\end{array}
\]

Number of different differences in each \( L_i \)

Current Complexity

\[ 2^{256} \]

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step
Guess-and-Determine Algorithm

Current Complexity

\[2^{256}\]

Current Probability

1

Next step: \(L'_5, L'_6, L'_7, L'_8\).

Legend

- ✓ Known value and difference
- • Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each \(L_i\)
Guess-and-Determine Algorithm

Current Complexity

\[2^{256}\]

Current Probability

1

Legend

- **Known value and difference**
- **Known difference**
- **Guessed value and difference**
- **Highlight current step**

Number of different differences in each \(L_i\)
## Guess-and-Determine Algorithm

<table>
<thead>
<tr>
<th>$L_i$</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
</tr>
<tr>
<td>2</td>
</tr>
<tr>
<td>3</td>
</tr>
<tr>
<td>4</td>
</tr>
<tr>
<td>5</td>
</tr>
<tr>
<td>6</td>
</tr>
<tr>
<td>7</td>
</tr>
<tr>
<td>8</td>
</tr>
<tr>
<td>9</td>
</tr>
<tr>
<td>10</td>
</tr>
<tr>
<td>11</td>
</tr>
<tr>
<td>12</td>
</tr>
<tr>
<td>13</td>
</tr>
<tr>
<td>14</td>
</tr>
<tr>
<td>15</td>
</tr>
<tr>
<td>16</td>
</tr>
</tbody>
</table>

Number of different differences in each $L_i$

### Current Complexity

$2^{256}$

### Current Probability

1

Next step: $L_1, L_{16}$.

### Legend
- ✓ Known value and difference
- • Known difference
- ★ Guessed value and difference
- ▼ Highlight current step
Guess-and-Determine Algorithm

Current Complexity

$2^{256}$

Current Probability

1

Next step: $L'_4$.

Legend

- ✓ Known value and difference
- • Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Current Complexity

2^{256}

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Current Complexity

$2^{256}$

Current Probability

1

Next step: $L_{15}$.

Legend

✓ Known value and difference
OUTHKnown difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

\begin{array}{c}
\text{Current Complexity} \\
\hline
\text{2}^{256}
\end{array}

\begin{array}{c}
\text{Current Probability} \\
\hline
\text{1}
\end{array}

Next step: \( L_6 \).

Legend

- \( \checkmark \) Known value and difference
- \( \circ \) Known difference
- \( \star \) Guessed value and difference
- \( \blacksquare \) Highlight current step

Number of different differences in each \( L_i \)
Guess-and-Determine Algorithm

Current Complexity

\[2^{256} + 16\]

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each \(L_i\)

FSE’2012 – J. Jean, M. Naya-Plasencia, T. Peyrin – Improved Rebound Attack on the Finalist Grostl
**Guess-and-Determine Algorithm**

- **Current Complexity**
  \[2^{256+16}\]

- **Current Probability**
  1

- **Next step:** \(L'_9\).

**Legend**
- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each \(L_i\)
Guess-and-Determine Algorithm

| $L_i$ | \(1\) | \(2\) | \(3\) | \(4\) | \(5\) | \(6\) | \(7\) | \(8\) | \(9\) | \(10\) | \(11\) | \(12\) | \(13\) | \(14\) | \(15\) | \(16\) |
|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|-------|
|       | ✓     | ✓     | ✓     |       | ✓     | ✓     | ✓     |       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     |       |       |       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     |       |       |       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
|       | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |
| ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     | ✓     |

Current Complexity

\(2^{256+16}\)

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Next step: $L_{14}$.

Current Complexity

$2^{256+16}$

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Current Complexity

$2^{256+16}$

Current Probability

1

Next step: $L'_3$.

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Number of different differences in each $L_i$

Current Complexity

$2^{256+16}$

Current Probability

1

Legend

✓ Known value and difference
• Known difference
★ Guessed value and difference
■ Highlight current step
Guess-and-Determine Algorithm

Current Complexity

\[ 2^{256+16} \]

Current Probability

1

Next step: \( L_1 \).

Legend

- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each \( L_i \)
**Guess-and-Determine Algorithm**

![Diagram of the Guess-and-Determine Algorithm]

- **Current Complexity**: $2^{256+16}$
- **Current Probability**: 1

**Legend**:
- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each $L_i$
**Guess-and-Determine Algorithm**

Current Complexity: $2^{256+16}$

Current Probability: 1

Next step: $L'_1$.

Legend:
- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step
Guess-and-Determine Algorithm

Current Complexity

$2^{256+16+8}$

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

<table>
<thead>
<tr>
<th>Current Complexity</th>
<th>$2^{256+16+8}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Probability</td>
<td>1</td>
</tr>
</tbody>
</table>

Next step: $L_{13}$.

Legend
- ✓ Known value and difference
- ⬤ Known difference
- ★ Guessed value and difference
- ■ Highlight current step
### Guess-and-Determine Algorithm

|   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| L_i |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |   |
| 1  | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 2  | ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 3  | ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 4  | ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 5  | ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 6  | ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 7  | ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 8  | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 9  | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 10 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 11 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 12 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 13 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 14 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 15 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| 16 | ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

Number of different differences in each \( L_i \)

#### Current Complexity
\[ 2^{256+16+8} \]

#### Current Probability
1

Next step: \( L'_2 \).

#### Legend
- ✓ Known value and difference
- ★ Guessed value and difference
- ○ Known difference
- ■ Highlight current step
**Guess-and-Determine Algorithm**

**Current Complexity**

$2^{256+16+8}$

**Current Probability**

1

**Legend**

- ✓ Known value and difference
- ⬤ Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each $L_i$
**Guess-and-Determine Algorithm**

**Current Complexity**

$2^{256+16+8}$

**Current Probability**

1

Next step: $L_7, L_{16}$.

**Legend**

- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Current Complexity

$2^{256+16+8}$

Current Probability

1

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Grøstl & SHA-3 Cryptanalysis Techniques Grøstl-256 Grøstl-512 Conclusion

FSE'2012 – J. Jean, M. Naya-Plasencia, T. Peyrin – Improved Rebound Attack on the Finalist Grostl

25/27
**Guess-and-Determine Algorithm**

```
\begin{align*}
\text{Current Complexity} & \quad 2^{256+16+8} \\
\text{Current Probability} & \quad 1 \\
\text{Legend} & \\
\checkmark & \quad \text{Known value and difference} \\
\bigcirc & \quad \text{Known difference} \\
\star & \quad \text{Guessed value and difference} \\
\blacktriangle & \quad \text{Highlight current step}
\end{align*}
```

Next step: $L'_10; L'_11$.
Guess-and-Determine Algorithm

\[ L_i \]

Current Complexity

\[ 2^{256+16+8} \]

Current Probability

\[ 2^{-8\cdot(1)} \]

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step
Guess-and-Determine Algorithm

Current Complexity

\[2^{256+16+8}\]

Current Probability

\[2^{-8 \cdot (1)}\]

Next step: \(L_8, L_9, L_{11}, L_{15}\).

Legend

- ✓ Known value and difference
- ○ Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each \(L_i\)
Guess-and-Determine Algorithm

Current Complexity

\(2^{256+16+8}\)

Current Probability

\(2^{-8 \cdot (1+2)}\)

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each \(L_i\)
**Guess-and-Determine Algorithm**

<table>
<thead>
<tr>
<th>$L_i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>4</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>7</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>8</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>9</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>10</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>11</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>12</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>13</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>14</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>15</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>16</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Number of different differences in each $L_i$

**Current Complexity**

$2^{256+16+8}$

**Current Probability**

$2^{-8\cdot(1+2)}$

Next step: $L'_{12}$.

**Legend**

- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step
### Guess-and-Determine Algorithm

#### Current Complexity

\[ 2^{256+16+8} \]

#### Current Probability

\[ 2^{-8 \cdot (1+2+3)} \]

#### Legend

- ✓ Known value and difference
- □ Known difference
- ★ Guessed value and difference
- ■ Highlight current step

#### Number of different differences in each \( L_i \)
Guess-and-Determine Algorithm

\[ L_i \]

Current Complexity

\[ 2^{256+16+8} \]

Current Probability

\[ 2^{-8 \cdot (1+2+3)} \]

Next step: \( L_{10}, L_{12} \).

Legend

- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each \( L_i \)
**Guess-and-Determine Algorithm**

- **Current Complexity**: \(2^{256+16+8}\)
- **Current Probability**: \(2^{-8 \cdot (1+2+3)}\)

**Legend**
- ✓ Known value and difference
- ○ Known difference
- ★ Guessed value and difference
- ■ Highlight current step

### Number of different differences in each \(L_i\)

<table>
<thead>
<tr>
<th>(L_i)</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

- **Current Complexity**
- **Current Probability**

**FSE’2012 – J. Jean, M. Naya-Plasencia, T. Peyrin – Improved Rebound Attack on the Finalist Grostl**
**Guess-and-Determine Algorithm**

- **Current Complexity**: $2^{256+16+8}$
- **Current Probability**: $2^{-8 \cdot (1+2+3)}$
- **Next step**: $L'_2$.

**Legend**
- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step
Guess-and-Determine Algorithm

Current Complexity

$2^{256+16+8}$

Current Probability

$2^{-8\cdot(1+2+3+5)}$

Legend

✓ Known value and difference
● Known difference
★ Guessed value and difference
■ Highlight current step

Number of different differences in each $L_i$
Guess-and-Determine Algorithm

Current Complexity

\[ 2^{256+16+8} \]

Current Probability

\[ 2^{-8 \cdot (1+2+3+5)} \]

Next step: \( L'_{13}, L'_{14}, L'_{15} \).

Legend

- ✓ Known value and difference
- ⬜ Known difference
- ★ Guessed value and difference
- ■ Highlight current step
**Guess-and-Determine Algorithm**

<table>
<thead>
<tr>
<th>$L_i$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
<th>9</th>
<th>10</th>
<th>11</th>
<th>12</th>
<th>13</th>
<th>14</th>
<th>15</th>
<th>16</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**Current Complexity**

$2^{256+16+8}$

**Current Probability**

$2^{-8 \cdot (1+2+3+5+8+8+8+8)}$

**Legend**

- ✓ Known value and difference
- ● Known difference
- ★ Guessed value and difference
- ■ Highlight current step

Number of different differences in each $L_i$
**Guess-and-Determine Algorithm**

![Diagram of Grøstl & SHA-3 Cryptanalysis Techniques]

**Final Complexity**

\[ 2^{256+16+8} = 2^{280} \]

**Final Probability**

\[ 2^{-8\cdot(1+2+3+5+8+8+8)} = 2^{-280} \]

The End.

**Legend**

- ✓ Known value and difference
- ⬤ Known difference
- ★ Guessed value and difference
- ■ Highlight current step

---

FSE’2012 – J. Jean, M. Naya-Plasencia, T. Peyrin – Improved Rebound Attack on the Finalist Grostl
Summing Up

Inbound Phase

In total we try: $2^{256+16+8} = 2^{280}$ possibilities, and each gives a solution with probability

$$2^{-8 \times (1+2+3+5+8+8+8)} = 2^{-280}.$$  

Outbound Phase

Again: \( P(\text{outbound}) = 2^{-2 \times 56} = 2^{-112}. \)

Distinguisher

Finally, we distinguish the 10-round permutation in $2^{280+112} = 2^{392}$ operations and $2^{64}$ in memory.

This compares to a generic complexity of $2^{448}$ operations.
We have provided new rebound results on building blocks of both versions of Grøstl that improve the previous number of analysed rounds.

We propose a way to solve 3 fully active states in the middle.

The results do not threaten the security of Grøstl, but we believe they will help better understanding AES-based constructions and their bounds regarding rebound techniques.
Conclusion

► We have provided new rebound results on building blocks of both versions of Grøstl that improve the previous number of analysed rounds.

► We propose a way to solve 3 fully active states in the middle.

► The results do not threaten the security of Grøstl, but we believe they will help better understanding AES-based constructions and their bounds regarding rebound techniques.

Thank you!