(Pseudo) Preimage Attack on Reduced-Round Grøstl Hash Function and Others

Shuang Wu, Dengguo Feng, Wenling Wu, Jian Guo, Le Dong, Jian Zou
March 20, 2012
Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion
Introduction

Meet-in-the-Middle pre-image attacks

- Applied to full MD4, MD5, HAVAL-3/4, Tiger and reduced-round HAS-160, RIPEMD, SHA-0/1, SHA-2 etc.

- Tricks:
  - Splice and Cut Techniques
  - Bicliques, Initial Structure (Message Stealing), local collision
  - Partial-Matching (Relations between deterministic values)
Meet-in-the-Middle pre-image attacks

- Yu Sasaki proposed the MitM preimage attack on AES-like structures for the first time at FSE 2011
  - Target: Whirlpool and AES hash modes
- Use freedom degrees of the state for chunk separation
Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion
Pseudo-Preimage Attack on 5-round Grøstl-256

Specification of Grøstl hash function

- Wide-pipe MD structure with output transformation
- Permutations P and Q are AES-like structures with
  - $8 \times 8$ states (Grøstl-256) and $8 \times 16$ states (Grøstl-512)
  - 10 rounds for Grøstl-256 and 14 rounds for Grøstl-512
Properties of the compression function

- 2n-bit state, \( F(H, M) = P(H \oplus M) \oplus Q(M) \oplus H \)
  - With \( H' = H \oplus M, F(H', M) = P(H') \oplus H' \oplus Q(M) \oplus M \)

Bounds for generic attacks

- Pre-image attack: \( 2^n \)
  - \( P(H') \oplus H' \oplus Q(M) \oplus M = T \)
  - birthday attack on 2n-bit state

- Collision attack: \( 2^{2n/3} \)
  - \( P(H'_1) \oplus H'_1 \oplus Q(M_1) \oplus M_1 \oplus P(H'_2) \oplus H'_2 \oplus Q(M_2) \oplus M_2 = 0 \)
  - generalized birthday attack on 2n-bit state with four entries
Outline of the attack
Pseudo-Preimage Attack on 5-round Grøstl-256

Attack outline

- Pseudo pre-image \((H, M)\)
  - \(F(H, M) = X, P(X) \oplus X = \ast \parallel T\)
  - \(X\) is a pre-image of the output transformation

- With \(H' = H \oplus M\),
  
  \[
P(H') \oplus H' \oplus Q(M) \oplus M \oplus X = 0
  \]
How to convert the partial pre-images of $P(X) \oplus X$ into pseudo pre-image of the hash function

$P(H') \oplus H' \oplus Q(M) \oplus M \oplus X = 0$

$2^{x_3} \times b \times 2^{n-b}$

Lookup table 2

$2^{x_2} \times 2^n$

$2^{x_1} \times 2^n$

Lookup table 1

$2^{x_1 + x_2 - b} \times b \times 2^{n-b}$

$2^{x_1 + x_2 + x_3 - 2n} \times 2^n$

$2^{x_1 + x_2 + x_3 - 2n} \geq 1$

$\Rightarrow x_1 + x_2 + x_3 \geq 2n$

zero

unknown
Complexity evaluation

- **X**: Fixed position partial preimage (n-bit) of $P(X) \oplus X$
  - Let complexity to find one $X$ be $2^{C_1(2n,n)}$

- **M**: Randomly chosen message with padding
  - Complexity = one Q call = 1/2 compression function call

- **H’**: Chosen position partial preimage (b-bit) of $P(H') \oplus H'$
  - Let complexity to find one $H'$ be $2^{C_2(2n,b)}$
Overall complexity of the attack is

\[ 2^{x_1 + C_1(2n,n)} + 2^{x_3 + C_2(2n,b)} + 2^{x_2-1} + 2^{x_1+x_2-b}C_{TL} \]

\[ 2^{x_2-1}(1 + C_{TL}) \]

\[ P(H') \oplus H' \oplus Q(M) \oplus M \oplus X = 0 \]
Partial preimage attacks on $P(X) \oplus X$
Evaluation of $C_1(2n, n)$ (fixed position partial preimage)

- Freedom degrees in blue and red bytes: 64 and 48 bits
- Size of the matching point: 64 bits
- Size of the full match: 256 bits
- Complexity: $2^{207}$ $P(X)$ calls = $2^{206}$ compression function calls
Evaluation of $C_2(2n, b)$ (chosen position partial preimage)

- Note: we can choose the positions of the target zero bits
- Choose optimal positions to maximize the size of the matching point
Graphs of $m(b)$ and $C_2(2n, b)$ for different $b$
Overall complexity of pseudo-preimage attack on 5-round Grøstl-256

- When \( b = 35 \), the overall complexity reaches its minimum value \( 2^{244.85} \)
Results on Grøstl-512
Pseudo-Preimage Attack on 8-round Grøstl-512

Preimage attack on the output transformation
## Summary of results

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Target</th>
<th>Type</th>
<th>Rounds</th>
<th>Time</th>
<th>Memory</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Grøstl-256</td>
<td>Hash Function</td>
<td>Collision</td>
<td>3</td>
<td>$2^{64}$</td>
<td>-</td>
<td>Martin Schlæffer</td>
</tr>
<tr>
<td></td>
<td>Compression Function</td>
<td>Semi-Free-Start</td>
<td>6</td>
<td>$2^{112}$</td>
<td>$2^{64}$</td>
<td>Martin Schlæffer</td>
</tr>
<tr>
<td></td>
<td>Permutation</td>
<td>Distinguisher</td>
<td>9</td>
<td>$2^{368}$</td>
<td>$2^{64}$</td>
<td>Jérémy Jean et al.</td>
</tr>
<tr>
<td></td>
<td>Permutation</td>
<td>Zero-Sum Distinguisher</td>
<td>10</td>
<td>$2^{509}$</td>
<td>-</td>
<td>Christina Boura et al.</td>
</tr>
<tr>
<td></td>
<td>Output Transformation</td>
<td>Preimage</td>
<td>5</td>
<td>$2^{206}$</td>
<td>$2^{48}$</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>Hash Function</td>
<td>Pseudo Preimage</td>
<td>5</td>
<td>$2^{244.85}$</td>
<td>$2^{230.13}$</td>
<td>Ours</td>
</tr>
<tr>
<td>Grøstl-512</td>
<td>Hash Function</td>
<td>Collision</td>
<td>3</td>
<td>$2^{192}$</td>
<td>-</td>
<td>Martin Schlæffer</td>
</tr>
<tr>
<td></td>
<td>Compression Function</td>
<td>Semi-Free-Start</td>
<td>7</td>
<td>$2^{152}$</td>
<td>$2^{56}$</td>
<td>Yu Sasaki</td>
</tr>
<tr>
<td></td>
<td>Permutation</td>
<td>Distinguisher</td>
<td>10</td>
<td>$2^{392}$</td>
<td>$2^{64}$</td>
<td>Jérémy Jean et al.</td>
</tr>
<tr>
<td></td>
<td>Output Transformation</td>
<td>Preimage</td>
<td>8</td>
<td>$2^{495}$</td>
<td>$2^{16}$</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>Hash Function</td>
<td>Pseudo Preimage</td>
<td>8</td>
<td>$2^{507.32}$</td>
<td>$2^{507.00}$</td>
<td>Ours</td>
</tr>
</tbody>
</table>
Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion
## Other results in this paper

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Target</th>
<th>Type</th>
<th>Rounds</th>
<th>Time</th>
<th>Memory</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whirlpool</td>
<td>Hash Function</td>
<td>2\textsuperscript{nd} Preimage</td>
<td>5</td>
<td>$2^{504}$</td>
<td>$2^8$</td>
<td>Yu Sasaki</td>
</tr>
<tr>
<td></td>
<td>Hash Function</td>
<td>2\textsuperscript{nd} Preimage</td>
<td>5</td>
<td>$2^{448}$</td>
<td>$2^{64}$</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>Hash Function</td>
<td>Preimage</td>
<td>5</td>
<td>$2^{481.5}$</td>
<td>$2^{64}$</td>
<td>Ours</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Hash Mode</th>
<th>Type</th>
<th>Rounds</th>
<th>Time</th>
<th>Memory</th>
<th>Message Length</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>AES</td>
<td>MMO,MP</td>
<td>2\textsuperscript{nd} Preimage</td>
<td>7</td>
<td>$2^{120}$</td>
<td>$2^8$</td>
<td>-</td>
<td>Yu Sasaki</td>
</tr>
<tr>
<td></td>
<td>MMO,MP,DM</td>
<td>2\textsuperscript{nd} Preimage</td>
<td>7</td>
<td>$2^{128-k}$</td>
<td>$2^k$</td>
<td>$2^k$ blocks</td>
<td>John Kelsey et at.</td>
</tr>
<tr>
<td></td>
<td>MMO,MP,DM</td>
<td>2\textsuperscript{nd} Preimage</td>
<td>7</td>
<td>$2^{120-\min(k,24)}$</td>
<td>$2^{16}$</td>
<td>$2^k$ blocks</td>
<td>Ours</td>
</tr>
<tr>
<td></td>
<td>DM</td>
<td>Preimage</td>
<td>7</td>
<td>$2^{125}$</td>
<td>$2^8$</td>
<td>-</td>
<td>Yu Sasaki</td>
</tr>
<tr>
<td></td>
<td>DM</td>
<td>Preimage</td>
<td>7</td>
<td>$2^{122.7}$</td>
<td>$2^{16}$</td>
<td>&gt;$2^8$ blocks</td>
<td>Ours</td>
</tr>
</tbody>
</table>
Converting partial pre-images into pseudo collisions

- The technique is proposed by Ji Li et al.
- Target: 8-round Grøstl-512 output transformation
- The complexity is $2^{248}$
Outline

- Introduction
- Attack on Grøstl
- Other results
- Conclusion
Conclusion

We proposed:

- Pseudo preimage attack on 5-round Grøstl-256 and 8-round Grøstl-512 for the first time

- We found that partial preimage attack on \( P(X) \oplus X \) (n-bit size) can be converted into pseudo preimage attack on the hash function

- An interesting observation: Properties of the permutation \( Q \) are not concerned in this attack, i.e. this attack works with any \( Q \).
  - So, our attack works on Grøstl-256 with 5-round \( P \) and full 10-round \( Q \) and Grøstl-512 with 8-round \( P \) and full 14-round \( Q \).
Thank you!

Any questions?