RadioGatún, a belt-and-mill hash function

Guido Bertoni, Joan Daemen, Michaël Peeters* and Gilles Van Assche

STMicroelectronics *De Valck Consultants
Introduction

• New hash function (family)
• Alternative design
  • Not based on fixed-length comp. function (Damgård-Merkle)
  • Not based on reduction
  ⇒ Variable-length input, variable-length output
• Diversity
• Building upon PANAMA
  • Generalizing collision-generating attack [Rijmen et al.]
  • Simplify and strengthen
  • Performance in SW and HW
Alternating-input construction

• State
  • Starts from 0
• Iterate with input blocks
  • Input mapping
  • State size > input block size ($l_i$)
• Do blank iterations
• Iterate with output blocks
  • Output mapping
  • Fixed number for hash function
**Belt-and-mill structure**

- **State** = (mill, belt)
- **Mill function**
  - **Non-linear** function
  - Diffusion and confusion
- **Belt function**
  - Linear function
  - **Long-term diffusion**
- **Belt-to-mill** + **mill-to-belt**
  - **Bell** + **milt**
  - Linear mappings
**RadioGatún**

- Parameter: *word size*
  - *RadioGatún*[32]
  - *RadioGatún*[64]
The mill function contains:
- Bitwise logical operations (XOR, AND, NOT)
- Cyclic shifts
The mill function contains:
- Bitwise logical operations (XOR, AND, NOT)
- Cyclic shifts
RadioGatúN

Input Block

<table>
<thead>
<tr>
<th>2</th>
<th>1</th>
<th>0</th>
</tr>
</thead>
</table>

Input Mapping

Mill Function

Belt Function

Mill 16 17 18 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15

Belt

Mill Function
Differential trails

- Differential trail
  - State differences + input differences
  - Used to find an internal collision

- Weight
  - Negative (binary) logarithm of probability
Trail backtracking

- Propagate difference
  - Through each round
  - Only if right pair
  - weight > \( l_i \) : fraction thru
  - weight \( \leq l_i \) : pair creation

- Complexity
  - Lonesome round
  - Crowded round
  - Backtracking cost
    - Also for algebraic attacks
**Analysis**

- **\textsc{RadioGatún}[1, 2, 4, …]** useful for analysis
  - *Explicit* search of collisions
  - Differential trails with lowest complexity
    - Trail for \textsc{RadioGatún}[1] extends to \textsc{RadioGatún}[n]
  - Symmetry destroyed in the mill
    - Specific trails for \textsc{RadioGatún}[n] may exist with lower cost

- **Other aspects**
  - Fixed points
  - Algebraic attacks on \textsc{RadioGatún}[1, 2, 3, 4, …, 64]

- **Ongoing**
  - Prove bounds

Second Cryptographic Hash Workshop
Performance

- Extremely fast in hardware
- Fast in software

<table>
<thead>
<tr>
<th>Dell Precision 670 with Intel Xeon 3GHz (in Mbyte/sec)</th>
<th>Windows (32 bits) Visual Studio 2005</th>
<th>Linux (x86_64) GCC 3.3.5</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-1</td>
<td>90</td>
<td>91</td>
</tr>
<tr>
<td>SHA-256</td>
<td>65</td>
<td>80</td>
</tr>
<tr>
<td>PANAMA</td>
<td>480</td>
<td>288</td>
</tr>
<tr>
<td>RADIOGATÚN[32]</td>
<td>120</td>
<td>175</td>
</tr>
<tr>
<td>RADIOGATÚN[64]</td>
<td>55</td>
<td>270</td>
</tr>
</tbody>
</table>
Conclusion

• Belt-and-mill structure
  • Simplicity (analysis)
• RADIOGATÚN
  • Performance
  • Existence of toy cipher (analysis)
  • No patent
• Analysis ongoing
• Do not hesitate to attack!
  • See security claims in RADIOGATÚN paper

http://radiogatun.noekeon.org