Cryptographic Hash Function
BLUE MIDNIGHT WISH

Presented by
Prof. Svein Johan Knapskog

Centre for Quantifiable Quality of Service in Communication Systems (Q2S),
Norwegian University of Science and Technology - NTNU,
NORWAY
Outline

- Short history of BLUE MIDNIGHT WISH
- General characteristics of BLUE MIDNIGHT WISH
- Specific design characteristics
- SW/HW performance and memory requirements
Short history of **BLUE MIDNIGHT WISH**

  - Characteristics: design components from the SHA-2 family, more chaining variables, resistant against generic multi-block collision attacks, resistant against generic length extension attacks, 2 - 8 times faster than the original SHA-2, very fast diffusion and fast reaching the level of random Boolean function, has just 8 rounds in the iterative part (compared to 64 for SHA-256 and 80 for SHA-512).

  - “It follows that the only one remaining candidate from the hash family Turbo SHA is Turbo SHA-256 (and Turbo SHA-512) with 8 rounds. The original security reserve of 6 round has been lost.”
Short history of **Blue Midnight Wish** (cont.)

- Gligoroski and Klima started more intensively to investigate and improve Turbo SHA-2 hash function (in spring 2008).
- They put a working name of the new hash function: “Blue Wish”
- BUT ...
Short history of **BLUE MIDNIGHT WISH** (cont.)

Blue Wish International offers cleaning products that are environmentally friendly, safe for the skin, use no chemicals and create no odors.

**BLUE WISH® is registered trade mark for towels.**
Short history of **BLUE MIDNIGHT WISH** (cont.)

- In one occasion working very late (all night), exchanging emails, breaking and fixing numerous versions, one version that was produced after the midnight had the best characteristics that satisfied the designers.

What if we xor in the beginning, the message and the chaining value?

It seems that this MIDNIGHT version is strong enough. So the name will be “Blue Midnight Wish”

**BLUE MIDNIGHT WISH was defined**
Short history of **BLUE MIDNIGHT WISH** (cont.)

- Additionally, the following contributors joined the **BLUE MIDNIGHT WISH** team:
  - Svein Johan Knapskog (coordinating the synergy in the team, general comments and suggestions for improvements, proofreading)
  - Mohamed El-Hadedy (VHDL implementation)
  - Jørn Amundsen (Big-endian and endian-neutral implementation, suggestions for improvements)
  - Stig Frode Mjølsnes (contributed to an 8-bit implementation)
General design characteristics for **BLUE MIDNIGHT WISH**

<table>
<thead>
<tr>
<th>Algorithm: BLUE MIDNIGHT WISH</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> Message $M$ of length $l$ bits, and the message digest size $n$.</td>
</tr>
<tr>
<td><strong>Output:</strong> A message digest $Hash$, that is $n$ bits long.</td>
</tr>
</tbody>
</table>

1. **Preprocessing**
   
   (a) Pad the message $M$.
   
   (b) Parse the padded message into $N$, $m$-bit message blocks, $M^{(1)}, M^{(2)}, \ldots, M^{(N)}$.
   
   (c) Set the initial value of the double pipe $H^{(0)}$.

2. **Hash computation**

   For $i = 1$ to $N$
   
   
   
   \[
   \begin{align*}
   Q_a^{(i)} &= f_0(M^{(i)}, H^{(i-1)}) ; \\
   Q_b^{(i)} &= f_1(M^{(i)}, Q_a^{(i)}) ; \\
   H^{(i)} &= f_2(M^{(i)}, Q_a^{(i)}, Q_b^{(i)}) ;
   \end{align*}
   \]

   \}

3. $Hash = \text{Take}_{n}\text{ Least Significant Bits}(H^{(N)})$. 

*www.ntnu.no*

25-28 Feb 2009, Leuven, Belgium, The First SHA 3 Candidate Conference, *Cryptographic Hash Function BLUE MIDNIGHT WISH*
Compression function for **BLUE MIDNIGHT WISH**

Preneel-Govaerts-Vandewalle scheme

Nr. 6 (or PGV6):

\[
H_i = E(M_i, M_i \oplus H_{i-1}) \oplus M_i \oplus H_{i-1}
\]

**BLUE MIDNIGHT WISH** can be seen as generalized PGV6:

\[
H_i = f_2(M_i, H_{i-1}, E(M_i, M_i \oplus H_{i-1}))
\]

Note: Here the block cipher \( E(\cdot) \) is weak block cipher.
Another look at the compression function for BLUE MIDNIGHT WISH.
Specific design characteristics for **BLUE MIDNIGHT WISH** (cont.)

1. Double size chaining (pipe) values
   - For \( n = 224, 256 \), chaining value has 512 bits
   - For \( n = 384, 512 \), chaining value has 1024 bits
2. Many entangled bijections
3. Very fast diffusion of initial differentials
Specific design characteristics for **BLUE MIDNIGHT WISH** (cont.)

1. Double size chaining (pipe) values $H^{(i)}$
   - For $n=224, 256$, chaining value has 512 bits
   - For $n=384, 512$, chaining value has 1024 bits
   - Gives resistance against length-extension attack
   - Gives resistance against multi-collision attack
Specific design characteristics for **BLUE MIDNIGHT WISH** (cont.)

2. Many entangled bijections

**Theorem 2 (in the documentation)**

1. When $H_{i-1}$ is fixed, $f_0(M_i, H_{i-1})$ is a bijection.
2. When $M_i$ is fixed, $f_0(M_i, H_{i-1})$ is a bijection.
3. When $Q_a$ is fixed, $f_1(M_i, Q_a)$ is a bijection.
4. When $M_i$ is fixed, $f_1(M_i, Q_a)$ is a bijection.
5. When $Q_b$ and $M_i$ are fixed, $f_2(M_i, Q_a, Q_b)$ is a bijection.
6. When $Q_b$ and $Q_a$ are fixed, $f_2(M_i, Q_a, Q_b)$ is a bijection.
7. When $Q_b$ is fixed, for every distinct value of $Q_a$ (resp. $M_i$), the equation $Q_b = f_1(M_i, Q_a)$ have a unique solution $M_i$ (resp. $Q_a$).
Specific design characteristics for **BLUE MIDNIGHT WISH** (cont.)

2. Many entangled bijections

- *The bijective entanglement, combined with the nonlinearity of the expressions in* $f_2$ *gives us confidence that it is infeasible to find collisions, preimages or second preimages of **BLUE MIDNIGHT WISH**.*

- *It is hard to find a way to change consistently all three inputs (tied together by non-linear bijective mappings) in such a way that these changes in the 3-times wider input of the compression function* $f_2$ *will cancel each other or will lead to controllable changes.*
Specific design characteristics for **BLUE MIDNIGHT WISH** (cont.)

2. Many entangled bijections

They give one unique property for **BLUE MIDNIGHT WISH**

**Theorem 4.** **BLUE MIDNIGHT WISH** could be seen as a generalization of any of the secure schemes PGV1, PGV2, . . . , PGV12.
Specific design characteristics for **BLUE MIDNIGHT WISH** (cont.)

3. Very fast diffusion of initial differentials

Normalized measure of the diffusion of initial differentials in variables $Q_b = f_1(M_i, Q_a)$.

In the first variable, one bit of the initial differential is not diffused as in an ideal Random Boolean function.
Specific design characteristics for BLUE MIDNIGHT WISH (cont.)

3. Very fast diffusion of initial differentials

The fast diffusion combined with entangled bijections – makes BLUE MIDNIGHT WISH resistant against differential cryptanalysis.
### SW/HW performance and memory requirements

<table>
<thead>
<tr>
<th>Software performances of the optimized C implementation on the NIST reference platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Visual Studio 2005, in 32-bit mode</td>
</tr>
<tr>
<td>BMW224/256 achieves 7.33 cycles/byte</td>
</tr>
<tr>
<td>Intel C++ v11.0.66, in 64-bit mode</td>
</tr>
<tr>
<td>BMW384/512 achieves 3.68 cycles/byte</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Memory requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMW224/256 needs 264 bytes</td>
</tr>
<tr>
<td>BMW384/512 needs 528 bytes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>HW – gate count</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMW224/256, ~15,000 gates</td>
</tr>
<tr>
<td>BMW384/512, ~30,000 gates</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>8-bit MCU (ATmega16, ATmega64)</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMW224/256, compiled C code produces ~10KB of machine instructions, speed 1369 cycles/bytes</td>
</tr>
<tr>
<td>BMW384/512, compiled C code produces ~55KB of machine instructions, speed 2793 cycles/bytes</td>
</tr>
</tbody>
</table>
Thank you for your attention!