Blue Midnight Wish

May,12 2010

Liliya Andreicheva

Agenda

- SHA-3 competition
- Blue Midnight Wish design
- Tweaks to the 2nd round
- Security claims
- S.Thomsen attacks
- Rotational analysis
- Conclusion
- References

SHA-3 competition

- ”NIST has opened a public competition to develop a new cryptographic hash algorithm”
- Initially 64 entries
- 1st round : 51 candidates
- 2nd round : 14 candidates

Blue Midnight Wish(BMW)

- Authors:
  - Danilo Gligoroski, Vlastimil Klima and their team
- Norwegian University of Science and Technology
- Cryptographic hash function with output size of n-bits
- 32-bit version supports n ∈ {224, 256}
- 64-bit version supports n ∈ {384, 512}
- Using a block cipher of 16 rounds as part of the compression function

Algorithm: BLUE MIDNIGHT WISH

Input: Message M of length l bits, and the message digest size n.

Output: A message digest $Hash$, that is n bits long.

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

   {

   $$Q_a^{(i)} = f_0(M^{(i)}, H^{(i-1)});$$
   $$Q_b^{(i)} = f_1(M^{(i)}, H^{(i-1)}, Q_a^{(i)});$$
   $$H^{(i)} = f_2(M^{(i)}, Q_a^{(i)}, Q_b^{(i)});$$

   }

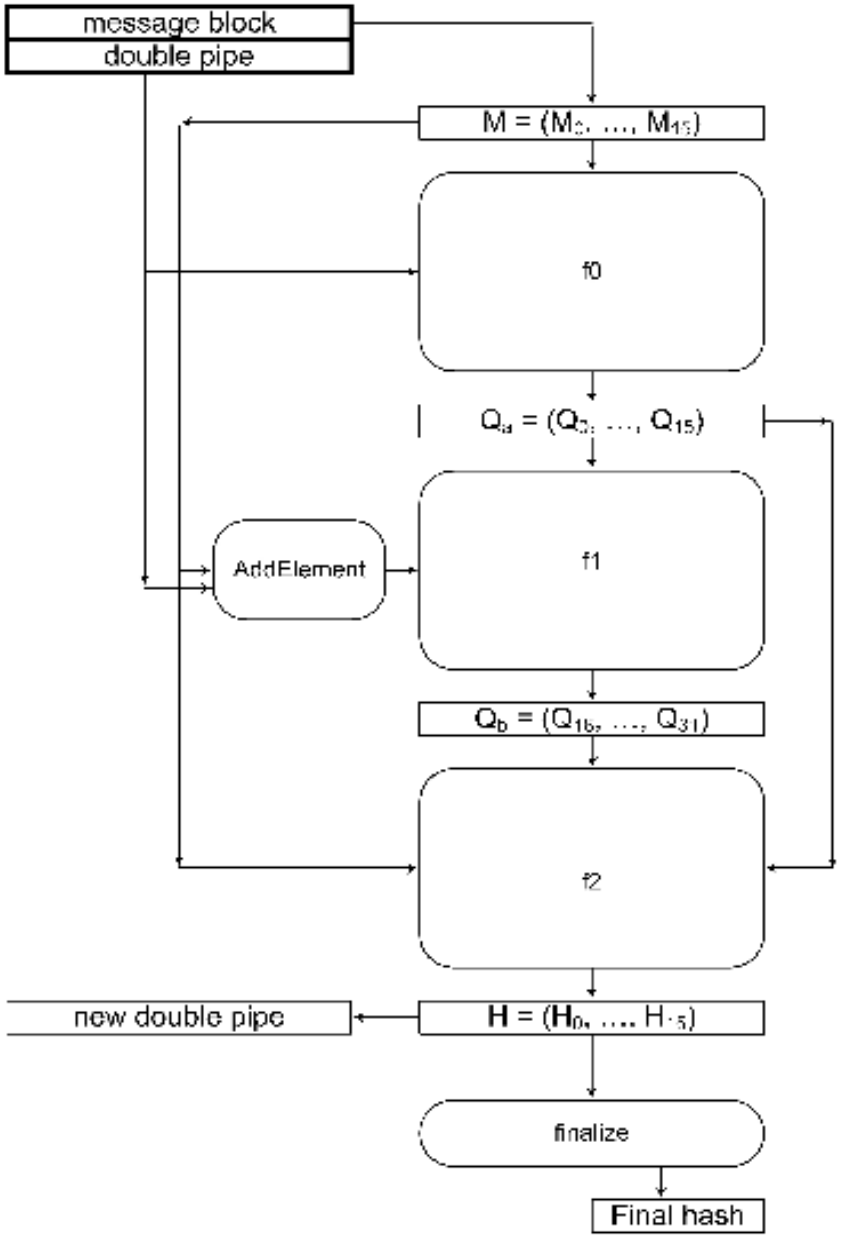
3. Finalization

   $$Q_a^{final} = f_0(H^{(N)}, CONST^{final});$$
   $$Q_b^{final} = f_1(H^{(N)}, CONST^{final}, Q_a^{final});$$
   $$H^{final} = f_2(H^{(N)}, Q_a^{final}, Q_b^{final});$$

4. $Hash$ =Take_n_Least_Significant_Bits(H^{final}).

BMW general scheme

- *M* – message block
- *H* - chaining input
- *f0* is a permutation with input M xor H = Q
- *f1* is a multi-permutation with inputs M and Q
- *f2* is a compression on input M and Q



Tweaks to the 2nd round

- Tweaks apllied to f_0 and f_1
- f_0 - rotation for chaining input H is added
- f_1 - chaining value H is added to the input

Compression function : f_0

$$f_0 : \{0,1\}^{2m} \rightarrow \{0,1\}^m$$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, and the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$.

Output: First part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$.

1. Bijective transform of $M^{(i)} \oplus H^{(i-1)}$:

$$\begin{aligned}
W_0^{(i)} &= (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_1^{(i)} &= (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_8^{(i)} \oplus H_8^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_2^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_3^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) \\
W_4^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_5^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_6^{(i)} &= (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) \\
W_7^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_8^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)}) - (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_9^{(i)} &= (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_3^{(i)} \oplus H_3^{(i-1)}) + (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{14}^{(i)} \oplus H_{14}^{(i-1)}) \\
W_{10}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_1^{(i)} \oplus H_1^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{15}^{(i)} \oplus H_{15}^{(i-1)}) \\
W_{11}^{(i)} &= (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_0^{(i)} \oplus H_0^{(i-1)}) - (M_2^{(i)} \oplus H_2^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_9^{(i)} \oplus H_9^{(i-1)}) \\
W_{12}^{(i)} &= (M_1^{(i)} \oplus H_1^{(i-1)}) + (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) \\
W_{13}^{(i)} &= (M_2^{(i)} \oplus H_2^{(i-1)}) + (M_4^{(i)} \oplus H_4^{(i-1)}) + (M_7^{(i)} \oplus H_7^{(i-1)}) + (M_{10}^{(i)} \oplus H_{10}^{(i-1)}) + (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) \\
W_{14}^{(i)} &= (M_3^{(i)} \oplus H_3^{(i-1)}) - (M_5^{(i)} \oplus H_5^{(i-1)}) + (M_8^{(i)} \oplus H_8^{(i-1)}) - (M_{11}^{(i)} \oplus H_{11}^{(i-1)}) - (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) \\
W_{15}^{(i)} &= (M_{12}^{(i)} \oplus H_{12}^{(i-1)}) - (M_4^{(i)} \oplus H_4^{(i-1)}) - (M_6^{(i)} \oplus H_6^{(i-1)}) - (M_9^{(i)} \oplus H_9^{(i-1)}) + (M_{13}^{(i)} \oplus H_{13}^{(i-1)})
\end{aligned}$$

2. Further bijective transform of $W_j^{(i)}, j = 0, \ldots, 15$:

$$\begin{aligned}
&Q_0^{(i)} = s_0(W_0^{(i)}) + H_1^{(i-1)}; \quad Q_1^{(i)} = s_1(W_1^{(i)}) + H_2^{(i-1)}; \quad Q_2^{(i)} = s_2(W_2^{(i)}) + H_3^{(i-1)}; \quad Q_3^{(i)} = s_3(W_3^{(i)}) + H_4^{(i-1)}; \\
&Q_4^{(i)} = s_4(W_4^{(i)}) + H_5^{(i-1)}; \quad Q_5^{(i)} = s_0(W_5^{(i)}) + H_6^{(i-1)}; \quad Q_6^{(i)} = s_1(W_6^{(i)}) + H_7^{(i-1)}; \quad Q_7^{(i)} = s_2(W_7^{(i)}) + H_8^{(i-1)}; \\
&Q_8^{(i)} = s_3(W_8^{(i)}) + H_9^{(i-1)}; \quad Q_9^{(i)} = s_4(W_9^{(i)}) + H_{10}^{(i-1)}; \quad Q_{10}^{(i)} = s_0(W_{10}^{(i)}) + H_{11}^{(i-1)}; \quad Q_{11}^{(i)} = s_1(W_{11}^{(i)}) + H_{12}^{(i-1)}; \\
&Q_{12}^{(i)} = s_2(W_{12}^{(i)}) + H_{13}^{(i-1)}; \quad Q_{13}^{(i)} = s_3(W_{13}^{(i)}) + H_{14}^{(i-1)}; \quad Q_{14}^{(i)} = s_4(W_{14}^{(i)}) + H_{15}^{(i-1)}; \quad Q_{15}^{(i)} = s_0(W_{15}^{(i)}) + H_0^{(i-1)};
\end{aligned}$$

Compression function : f_1

$$f_1 : \{0,1\}^{3m} \rightarrow \{0,1\}^m$$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$, the previous double pipe $H^{(i-1)} = (H_0^{(i-1)}, H_1^{(i-1)}, \ldots, H_{15}^{(i-1)})$ and the first part of the quadruple pipe $Q_a^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)})$.

Output: Second part of the quadruple pipe $Q_b^{(i)} = (Q_{16}^{(i)}, Q_{17}^{(i)}, \ldots, Q_{31}^{(i)})$.

1. Double pipe expansion according to the tunable parameters $ExpandRounds_1$ and $ExpandRounds_2$.

   1.1 For $ii = 0$ to $ExpandRounds_1 - 1$

   $$Q_{ii+16}^{(i)} = expand_1(ii + 16)$$

   1.2 For $ii = ExpandRounds_1$ to $ExpandRounds_1 + ExpandRounds_2 - 1$

   $$Q_{ii+16}^{(i)} = expand_2(ii + 16)$$

BMW224/BMW256	BMW384/BMW512
$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{19}(x)$	$s_0(x) = SHR^1(x) \oplus SHL^3(x) \oplus ROTL^4(x) \oplus ROTL^{37}(x)$
$s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^8(x) \oplus ROTL^{23}(x)$	$s_1(x) = SHR^1(x) \oplus SHL^2(x) \oplus ROTL^{13}(x) \oplus ROTL^{43}(x)$
$s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{12}(x) \oplus ROTL^{25}(x)$	$s_2(x) = SHR^2(x) \oplus SHL^1(x) \oplus ROTL^{19}(x) \oplus ROTL^{53}(x)$
$s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{15}(x) \oplus ROTL^{29}(x)$	$s_3(x) = SHR^2(x) \oplus SHL^2(x) \oplus ROTL^{28}(x) \oplus ROTL^{59}(x)$
$s_4(x) = SHR^1(x) \oplus x$	$s_4(x) = SHR^1(x) \oplus x$
$s_5(x) = SHR^2(x) \oplus x$	$s_5(x) = SHR^2(x) \oplus x$
$r_1(x) = ROTL^3(x)$	$r_1(x) = ROTL^5(x)$
$r_2(x) = ROTL^7(x)$	$r_2(x) = ROTL^{11}(x)$
$r_3(x) = ROTL^{13}(x)$	$r_3(x) = ROTL^{27}(x)$
$r_4(x) = ROTL^{16}(x)$	$r_4(x) = ROTL^{32}(x)$
$r_5(x) = ROTL^{19}(x)$	$r_5(x) = ROTL^{37}(x)$
$r_6(x) = ROTL^{23}(x)$	$r_6(x) = ROTL^{43}(x)$
$r_7(x) = ROTL^{27}(x)$	$r_7(x) = ROTL^{53}(x)$
$AddElement(j) = \left(ROTL^{(j+1)}(M_j^{(i)}) + ROTL^{(j+4)}(M_{j+3}^{(i)}) - ROTL^{(j+11)}(M_{j+10}^{(i)}) + K_{j+16}\right) \oplus H_{j+7}^{(i)}$	$AddElement(j) = \left(ROTL^{(j+1)}(M_j^{(i)}) + ROTL^{(j+4)}(M_{j+3}^{(i)}) - ROTL^{(j+11)}(M_{j+10}^{(i)}) + K_{j+16}\right) \oplus H_{j+7}^{(i)}$
$expand_1(j) = s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)}) + s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)}) + s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)}) + s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)}) + AddElement(j-16)$	$expand_1(j) = s_1(Q_{j-16}^{(i)}) + s_2(Q_{j-15}^{(i)}) + s_3(Q_{j-14}^{(i)}) + s_0(Q_{j-13}^{(i)}) + s_1(Q_{j-12}^{(i)}) + s_2(Q_{j-11}^{(i)}) + s_3(Q_{j-10}^{(i)}) + s_0(Q_{j-9}^{(i)}) + s_1(Q_{j-8}^{(i)}) + s_2(Q_{j-7}^{(i)}) + s_3(Q_{j-6}^{(i)}) + s_0(Q_{j-5}^{(i)}) + s_1(Q_{j-4}^{(i)}) + s_2(Q_{j-3}^{(i)}) + s_3(Q_{j-2}^{(i)}) + s_0(Q_{j-1}^{(i)}) + AddElement(j-16)$
$expand_2(j) = Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)}) + Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)}) + Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)}) + Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)}) + AddElement(j-16)$	$expand_2(j) = Q_{j-16}^{(i)} + r_1(Q_{j-15}^{(i)}) + Q_{j-14}^{(i)} + r_2(Q_{j-13}^{(i)}) + Q_{j-12}^{(i)} + r_3(Q_{j-11}^{(i)}) + Q_{j-10}^{(i)} + r_4(Q_{j-9}^{(i)}) + Q_{j-8}^{(i)} + r_5(Q_{j-7}^{(i)}) + Q_{j-6}^{(i)} + r_6(Q_{j-5}^{(i)}) + Q_{j-4}^{(i)} + r_7(Q_{j-3}^{(i)}) + s_4(Q_{j-2}^{(i)}) + s_5(Q_{j-1}^{(i)}) + AddElement(j-16)$

Compression function: f_2

Folding $f_2 : \{0,1\}^{3m} \rightarrow \{0,1\}^m$

Input: Message block $M^{(i)} = (M_0^{(i)}, M_1^{(i)}, \ldots, M_{15}^{(i)})$,
quadruple pipe $Q^{(i)} = (Q_0^{(i)}, Q_1^{(i)}, \ldots, Q_{15}^{(i)}, Q_{16}^{(i)}, \ldots, Q_{31}^{(i)})$.
Output: New double pipe $H^{(i)} = (H_0^{(i)}, H_1^{(i)}, \ldots, H_{15}^{(i)})$.

1. Compute the cumulative temporary variables XL and XH.

$$XL = Q_{16}^{(i)} \oplus Q_{17}^{(i)} \oplus \ldots \oplus Q_{23}^{(i)}$$
$$XH = XL \oplus Q_{24}^{(i)} \oplus Q_{25}^{(i)} \oplus \ldots \oplus Q_{31}^{(i)}$$

2. Compute the new double pipe $H^{(i)}$:

$$H_0^{(i)} = \left(SHL^5(XH) \oplus SHR^5(Q_{16}^{(i)}) \oplus M_0^{(i)}\right) + \left(XL \oplus Q_{24}^{(i)} \oplus Q_0^{(i)}\right)$$
$$H_1^{(i)} = \left(SHR^7(XH) \oplus SHL^8(Q_{17}^{(i)}) \oplus M_1^{(i)}\right) + \left(XL \oplus Q_{25}^{(i)} \oplus Q_1^{(i)}\right)$$
$$H_2^{(i)} = \left(SHR^5(XH) \oplus SHL^5(Q_{18}^{(i)}) \oplus M_2^{(i)}\right) + \left(XL \oplus Q_{26}^{(i)} \oplus Q_2^{(i)}\right)$$
$$H_3^{(i)} = \left(SHR^1(XH) \oplus SHL^5(Q_{19}^{(i)}) \oplus M_3^{(i)}\right) + \left(XL \oplus Q_{27}^{(i)} \oplus Q_3^{(i)}\right)$$
$$H_4^{(i)} = \left(SHR^3(XH) \oplus Q_{20}^{(i)} \oplus M_4^{(i)}\right) + \left(XL \oplus Q_{28}^{(i)} \oplus Q_4^{(i)}\right)$$
$$H_5^{(i)} = \left(SHL^6(XH) \oplus SHR^6(Q_{21}^{(i)}) \oplus M_5^{(i)}\right) + \left(XL \oplus Q_{29}^{(i)} \oplus Q_5^{(i)}\right)$$
$$H_6^{(i)} = \left(SHR^4(XH) \oplus SHL^6(Q_{22}^{(i)}) \oplus M_6^{(i)}\right) + \left(XL \oplus Q_{30}^{(i)} \oplus Q_6^{(i)}\right)$$
$$H_7^{(i)} = \left(SHR^{11}(XH) \oplus SHL^2(Q_{23}^{(i)}) \oplus M_7^{(i)}\right) + \left(XL \oplus Q_{31}^{(i)} \oplus Q_7^{(i)}\right)$$
$$H_8^{(i)} = ROTL^9(H_4^{(i)}) + \left(XH \oplus Q_{24}^{(i)} \oplus M_8^{(i)}\right) + \left(SHL^8(XL) \oplus Q_{23}^{(i)} \oplus Q_8^{(i)}\right)$$
$$H_9^{(i)} = ROTL^{10}(H_5^{(i)}) + \left(XH \oplus Q_{25}^{(i)} \oplus M_9^{(i)}\right) + \left(SHR^6(XL) \oplus Q_{16}^{(i)} \oplus Q_9^{(i)}\right)$$
$$H_{10}^{(i)} = ROTL^{11}(H_6^{(i)}) + \left(XH \oplus Q_{26}^{(i)} \oplus M_{10}^{(i)}\right) + \left(SHL^6(XL) \oplus Q_{17}^{(i)} \oplus Q_{10}^{(i)}\right)$$
$$H_{11}^{(i)} = ROTL^{12}(H_7^{(i)}) + \left(XH \oplus Q_{27}^{(i)} \oplus M_{11}^{(i)}\right) + \left(SHL^4(XL) \oplus Q_{18}^{(i)} \oplus Q_{11}^{(i)}\right)$$
$$H_{12}^{(i)} = ROTL^{13}(H_0^{(i)}) + \left(XH \oplus Q_{28}^{(i)} \oplus M_{12}^{(i)}\right) + \left(SHR^3(XL) \oplus Q_{19}^{(i)} \oplus Q_{12}^{(i)}\right)$$
$$H_{13}^{(i)} = ROTL^{14}(H_1^{(i)}) + \left(XH \oplus Q_{29}^{(i)} \oplus M_{13}^{(i)}\right) + \left(SHR^4(XL) \oplus Q_{20}^{(i)} \oplus Q_{13}^{(i)}\right)$$
$$H_{14}^{(i)} = ROTL^{15}(H_2^{(i)}) + \left(XH \oplus Q_{30}^{(i)} \oplus M_{14}^{(i)}\right) + \left(SHR^7(XL) \oplus Q_{21}^{(i)} \oplus Q_{14}^{(i)}\right)$$
$$H_{15}^{(i)} = ROTL^{16}(H_3^{(i)}) + \left(XH \oplus Q_{31}^{(i)} \oplus M_{15}^{(i)}\right) + \left(SHR^2(XL) \oplus Q_{22}^{(i)} \oplus Q_{15}^{(i)}\right)$$

Security claims

- Collision resistance of approximately bits, n/2
- Preimage resistance of approximately n bits
- Second-preimage resistance of approximately n – k bits for any message shorter than 2^k bits
- Resistance to length-extension attacks
- Resistance to multicollision attacks

S.Thomsen attacks

- Pseudo-cryptanalysis on original BMW
- Showed the scenario how to attack BMW with the following complexities:
  - Near-collision attack 2^14
  - Pseudo-collision attack 2^(3n/8 +1)
  - Pseudo-(second) preimage attack 2^(3n/4+1)

where n is the length of the input

S.Thomsen attacks(cont.)

- Near-collision attacks
  - The strategy is to search for difference patterns of the last few words of W, such that these differences do not spread too much in the last few rounds of f_1 and f_2
- Pseudo attacks
  - The idea is to fix some of the output words Q(16,...,31),then *f2* becomes simple. Thus fixing one of the input value attacker is controlling some of the words of chaining input H.

S.Thomsen attacks(cont.)

- Complexity:

- Controlling 2 output words:
  - Pseudo-collision attack 2^(7n/16)
  - Pseudo-preimage attack 2^(7n/8)
- Controlling 4 output words:
  - Pseudo-collision attack 2^(3n/8 +1)
  - Pseudo-preimage attack 2^(3n/4 +1)

Variant	Pseudo-collision	Pseudo-(second) preimage
BMW-224	2^{81} (2^{112})	2^{161} (2^{224})
BMW-256	2^{97} (2^{128})	2^{193} (2^{256})
BMW-384	2^{128} (2^{192})	2^{256} (2^{384})
BMW-512	2^{192} (2^{256})	2^{384} (2^{512})

Rotational analysis

- Relatively new type of analysis
- Looking at the propagation of rotational pair((x,x <<<r)) through some transformation.
- Rotational input produces rotational output with some probability
- Reduces the complexity of obtaining the original message
- BMW-512 : 2 ^ 223.5

Conclusion

- Attacks presented by Thomsen are infeasible
- Further investigation concerning rotational analysis is needed

References

- Soren S. Thomsen - Pseudo-cryptanalysis of Blue Midnight Wish. Available online, 2009
- Jian Guo, Soen S. Thomsen - Distinguishers for the Compression Function of Blue Midnight Wish with Probability 1. Available online, 2010
- Soren S. Thomsen - Pseudo-cryptanalysis of the Original Blue Midnight Wish. In S.Hong and T.Iwata, editors, Fast Software Encryption, LNCS, Seoul, South Korea, 2010. To appear
- Ivica Nikolic, Josef Pieprzyk, Przemyslaw Sokolowski, Ron Steinfeld - Rotational Cryptanalysis of (Modified) Versions of BMW and SIMD. Available online, 2010 Soren S. Thomsen - A near-collision attack on the Blue Midnight Wish compression function. Version 2.0, available online, 2008

Thank you!

Questions?