

Pseudo-cryptanalysis of the Original BMW

Søren S. Thomsen

Fast Software Encryption 2010

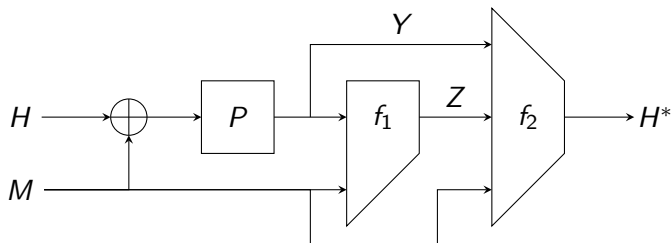
Seoul, Korea

February 9, 2010

Blue Midnight Wish

- Developed by Gligoroski et al.
- Four variants (224-, 256-, 384-, 512-bit)
- In the second round of the SHA-3 competition
- Was tweaked between first and second round
- My results are on the first version!

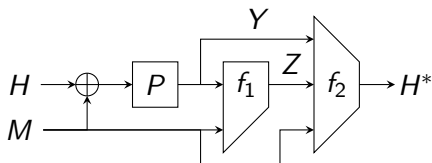
High-level design of the compression function



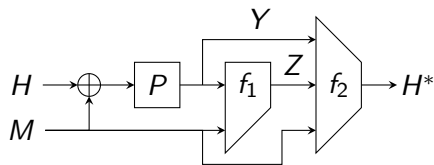
- H, M, Y, Z, H^* : 16 words each (e.g.: H_0, \dots, H_{15})
- Word size 32/64 (BMW-256/BMW-512).

The permutation P

- Easy to invert
- Given M and Y , compute $H = P^{-1}(Y) \oplus M$
- Details of P irrelevant here.



The function f_1



- Multipermutation
 - $f_1(Y, \cdot)$ a permutation
 - $f_1(\cdot, M)$ a permutation
- Permutations are invertible
- “Simple” and “complex” rounds (security parameter).

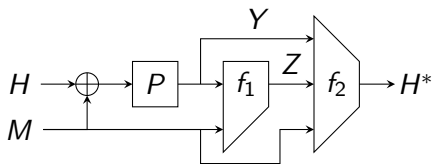
Example: a complex round

Let $Q = Y||Z$, with Z initially null.

$$\begin{aligned}
 Q_{i+16} \leftarrow & s_1(Q_i) + s_2(Q_{i+1}) + s_3(Q_{i+2}) + s_0(Q_{i+3}) + \\
 & s_1(Q_{i+4}) + s_2(Q_{i+5}) + s_3(Q_{i+6}) + s_0(Q_{i+7}) + \\
 & s_1(Q_{i+8}) + s_2(Q_{i+9}) + s_3(Q_{i+10}) + s_0(Q_{i+11}) + \\
 & s_1(Q_{i+12}) + s_2(Q_{i+13}) + s_3(Q_{i+14}) + s_0(Q_{i+15}) + \\
 & \underbrace{M_i + M_{i+3} - M_{i+10}}_{W_i} + K_i \pmod{2^{32}}
 \end{aligned}$$

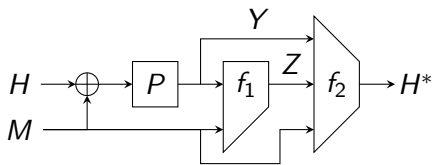
- Mapping from M to W corresponds to invertible matrix multiplication: $W = \mathbf{B} \cdot M$

The function f_2



- Details later

Preimages – idea of the attack



- Force $Z = 0$
- Now f_2 is very simple.

f_2 with $Z = 0$

$$\begin{aligned}H_0^* &= M_0 + Y_0 \\ &\vdots \\ H_7^* &= M_7 + Y_7 \\ H_8^* &= (M_4 + Y_4) \lll 9 + M_8 + Y_8 \\ H_9^* &= (M_5 + Y_5) \lll 10 + M_9 + Y_9 \\ H_{10}^* &= (M_6 + Y_6) \lll 11 + M_{10} + Y_{10} \\ H_{11}^* &= (M_7 + Y_7) \lll 12 + M_{11} + Y_{11} \\ H_{12}^* &= (M_0 + Y_0) \lll 13 + M_{12} + Y_{12} \\ H_{13}^* &= (M_1 + Y_1) \lll 14 + M_{13} + Y_{13} \\ H_{14}^* &= (M_2 + Y_2) \lll 15 + M_{14} + Y_{14} \\ H_{15}^* &= (M_3 + Y_3) \lll 16 + M_{15} + Y_{15}\end{aligned}$$

Inverting f_1

Remember: $Z = 0$

- After choosing W_{15} , we can compute Y_{15}
- ...or we can choose Y_{15} and compute W_{15}
- The same with W_{14} , W_{13} , ...

f_2 with $Z = 0$

$$\begin{aligned}H_0^* &= M_0 + Y_0 \\ &\vdots \\ H_7^* &= M_7 + Y_7 \\ H_8^* &= (M_4 + Y_4) \lll 9 + M_8 + Y_8 \\ H_9^* &= (M_5 + Y_5) \lll 10 + M_9 + Y_9 \\ H_{10}^* &= (M_6 + Y_6) \lll 11 + M_{10} + Y_{10} \\ H_{11}^* &= (M_7 + Y_7) \lll 12 + M_{11} + Y_{11} \\ H_{12}^* &= (M_0 + Y_0) \lll 13 + M_{12} + Y_{12} \\ H_{13}^* &= (M_1 + Y_1) \lll 14 + M_{13} + Y_{13} \\ H_{14}^* &= (M_2 + Y_2) \lll 15 + M_{14} + Y_{14} \\ H_{15}^* &= (M_3 + Y_3) \lll 16 + M_{15} + Y_{15}\end{aligned}$$

Choosing words in M and W concurrently

- Consider the definition of W_{15} :

$$W_{15} = M_{15} + M_2 - M_9$$

- We can “free” W_{15}
- Example: Replace everywhere M_2 by

$$W_{15} - M_{15} + M_9$$

Controlling output words

- I.e., we can choose some words in M , and some words in W (at most 16 in total)
- Example: choose Y_6, \dots, Y_{15} and $M_6, M_7, M_{10}, M_{11}, M_{14}, M_{15}$
- Allows to control:

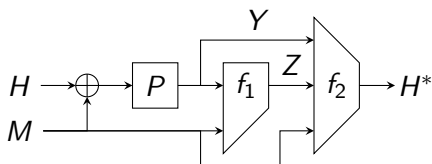
$$H_6^* = M_6 + Y_6$$

$$H_7^* = M_7 + Y_7$$

$$H_{10}^* = (M_6 + Y_6) \lll^{11} + M_{10} + Y_{10}$$

$$H_{11}^* = (M_7 + Y_7) \lll^{12} + M_{11} + Y_{11}$$

Summary



- We can control up to four output words
- Complexity ~ 1 compression function evaluation
- Reduces complexity of preimage, second preimage, collision attacks on compression function
- Can be extended to pseudo-attacks.

Pseudo-attack complexities

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})

(In brackets: birthday/brute force complexities)

Conclusion

- In the paper: near-collision attack in time $\sim 2^{15}$
- All results on Original BMW
- BMW tweaked – e.g., H now affects f_1 directly
- These attacks do not apply to Tweaked BMW

Thanks!