Deterministic Differential Properties of the BMW Compression Function

GUO Jian

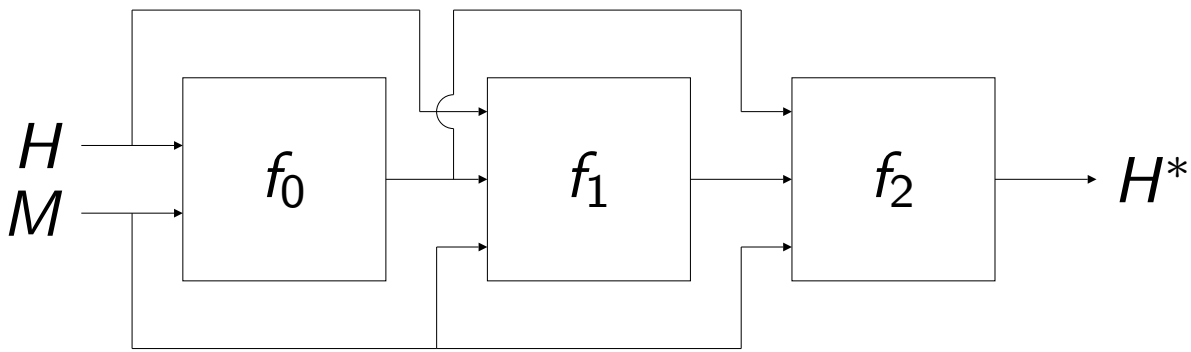
Søren S. THOMSEN

2nd SHA-3 Candidate Conference
University of California, Santa Barbara
August 23, 2010

BMW compression function overview

$$H^* \leftarrow \text{compress}(H, M)$$

1. $Y \leftarrow f_0(H, M)$
2. $Z \leftarrow f_1(H, M, Y)$
3. $H^* \leftarrow f_2(M, Y, Z)$

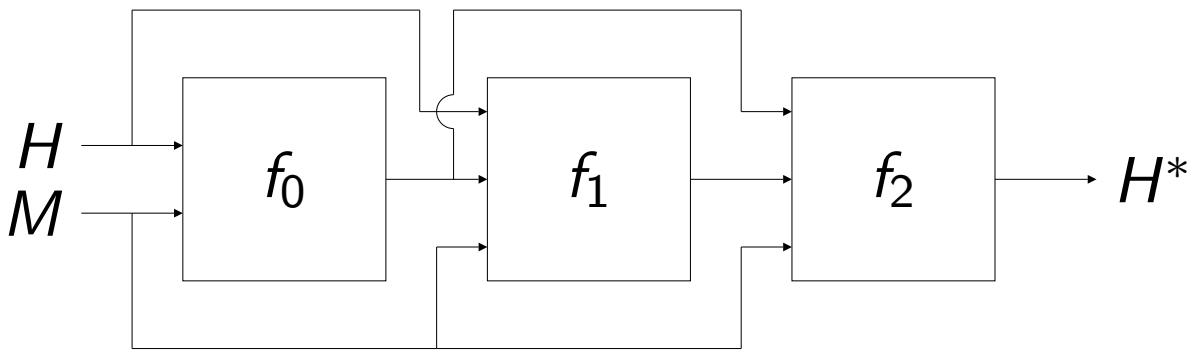


BMW compression function overview

$$H^* \leftarrow \text{compress}(H, M)$$

1. $Y \leftarrow f_0(H, M)$
2. $Z \leftarrow f_1(H, M, Y)$
3. $H^* \leftarrow f_2(M, Y, Z)$

- All values consist of 16 (32-/64-bit) words
- Let $Q = Y \| Z$
- Word i of X is denoted X_i.



The function f_0

$$Y \leftarrow f_0(H, M) = \begin{bmatrix} \text{Inv. matrix} \end{bmatrix} \cdot \begin{bmatrix} H \oplus M \end{bmatrix} + \begin{bmatrix} H^{\lll 1 \text{ word}} \end{bmatrix}$$

The function f_0

$$Y \leftarrow f_0(H, M) = \left[\text{Inv. matrix}\right] \cdot \left[H \oplus M\right] + \left[H^{\lll 1 \text{ word}}\right]$$

- Difference Δ in H_i and $M_i \Rightarrow$ difference $\approx \Delta$ in Y_{i-1}.

The function f_1

$$Q_{i+16} \leftarrow expand_{\{1,2\}}(Q_i, \ldots, Q_{i+15}, M_i, M_{i+3}, M_{i+10}, H_{i+7})$$

- Feedback shift register – each new word of Q depends on previous 16, and on 3 words of M and 1 word of H
- 2 types of rounds (feedback functions): $expand_1$ and $expand_2$
- 16 $expand_{\{1,2\}}$ rounds in total (default: 2/14)
- Diffusion more effective in $expand_1$ rounds

The function f_2 a single output bit

$$H_0^*[0] \leftarrow M_0[0] \oplus Q_0[0] \oplus Q_{16}[5] \oplus \bigoplus_{i=16}^{24} Q_i[0]$$

($X[i]$ means bit i of X, counting from LSB)

- Here, we concentrate on this single output bit
- Note:
  - no dependence on $Q_{25}, \ldots, Q_{31}$
  - dependence on 11 LSBs plus 1 additional bit

The function f_2 a single output bit

$$H_0^*[0] \leftarrow M_0[0] \oplus Q_0[0] \oplus Q_{16}[5] \oplus \bigoplus_{i=16}^{24} Q_i[0]$$

($X[i]$ means bit i of X, counting from LSB)

- Here, we concentrate on this single output bit
- Note:
  - no dependence on $Q_{25}, \ldots, Q_{31}$
  - dependence on 11 LSBs plus 1 additional bit
- Hence, by limiting difference propagation through the first 9 rounds of f_1, we may obtain a bias in $H_0^*[0]$

Idea

- Introduce a difference Δ in H_1 and M_1
- . . . leading to a difference Δ in $Y_0 = Q_0$
- Make sure Δ has many trailing '0' bits
- Differences propagate only slowly towards LSB in $expand_2$ rounds
- Consider now a variant with no $expand_1$ rounds. . .

Example for BMW-256 with no $expand_1$ rounds

$\Delta = 20000000_h$

Diff. on Q_0:	`--x----------------------------`
Diff. on Q_{16}:	`??x----------------------------`
Diff. on Q_{17}:	`????x----------------------------`
Diff. on Q_{18}:	`??????x----------------------------`
Diff. on Q_{19}:	`????????x----------------------------`
Diff. on Q_{20}:	`??????????x----------------------------`
Diff. on Q_{21}:	`????????????x----------------------------`
Diff. on Q_{22}:	`??????????????x----------------------------`
Diff. on Q_{23}:	`????????????????x----------------------------`
Diff. on Q_{24}:	`??????????????????x----------------------------`

- Leads to a collision in $H_0^*[0]$
- Propagation towards LSB comes from $s_5(x) = x^{\gg 2} \oplus x$

Dealing with 1 $expand_1$ round

- In $expand_2$ rounds, propagation towards LSB comes from

$$s_5(x) = x^{\gg 2} \oplus x$$

- In $expand_1$ rounds, propagation towards LSB comes from (e.g.)

$$s_1(x) = x^{\gg 1} \oplus x^{\ll 2} \oplus x^{\ggg 9} \oplus x^{\ggg 24}$$

- With 1 $expand_1$ round: find Δ with many trailing '0' bits, such that $s_1(\Delta)$ also has many trailing '0' bits

Example for BMW-256 with 1 $expand_1$ round

$\Delta = 20404000_h$, $s_1(\Delta) = \texttt{d1710000}_h$

Diff. on Q_0:	`--x------x-------x--------------`
Diff. on Q_{16}:	`????????????????x---------------`
Diff. on Q_{17}:	`?????????????????x--------------`
Diff. on Q_{18}:	`??????????????????x-------------`
Diff. on Q_{19}:	`???????????????????x----------`
Diff. on Q_{20}:	`????????????????????x--------`
Diff. on Q_{21}:	`?????????????????????x------`
Diff. on Q_{22}:	`??????????????????????x----`
Diff. on Q_{23}:	`???????????????????????x--`
Diff. on Q_{24}:	`????????????????????????x`

- Leads to a difference with prob. 1 in $H_0^*[0]$

Dealing with 2 $expand_1$ rounds

- With 2 $expand_1$ rounds, Q_{16} goes through

$$s_0(x) = x^{\gg 1} \oplus x^{\ll 3} \oplus x^{\ggg 13} \oplus x^{\ggg 28}$$

- Now we need many trailing '0' bits in Δ and in $s_1(\Delta)$ and in $s_0(s_1(\Delta))$; no good Δ exists...
- New strategy: accept more differences in Δ and make them cancel other (LSB) differences in the last $expand_1$ round
- Requires some message modification...

Example for BMW-256 with 2 $expand_1$ rounds

$\Delta = \texttt{36fafbef}_h$, $s_1(\Delta) = \texttt{cdf60000}_h$, assuming proper message modification

Diff. on Q_0:	`--xx-xx-xxxxx-x-xxxxx-xxxxx-xxxx`
Diff. on Q_{16}:	`xx--xx-xxxxx-xx----------------`
Diff. on Q_{17}:	`??????????????x--------------`
Diff. on Q_{18}:	`???????????????????x------------`
Diff. on Q_{19}:	`????????????????????x----------`
Diff. on Q_{20}:	`?????????????????????x---------`
Diff. on Q_{21}:	`??????????????????????????x-------`
Diff. on Q_{22}:	`????????????????????????????x-----`
Diff. on Q_{23}:	`??????????????????????????????x--`
Diff. on Q_{24}:	`????????????????????????????????x`

- Leads to a collision in $H_0^*[0]$

Application to preimage search

- Assume we know Δ s.t. compress(H, M) and compress$(H \oplus \Delta, M \oplus \Delta)$ always differ in $H_0^*[0]$.
- Given target T, choose random (H, M), and compute $U =$ compress(H, M). If T and U agree on $H_0^*[0]$, compare remaining bits.
- Otherwise compare remaining bits of T and compress$(H \oplus \Delta, M \oplus \Delta)$.
- Complexity around $2^{\ell - 0.4}$ for ℓ-bit compression function...

Conclusions

- The BMW compression functions have differential weaknesses
- Difficult to extend weaknesses to full hash function for two reasons:
  - output bits affected are not used as output of the hash function
  - control of chaining input is required
- Future work:
  - apply more advanced message modification techniques
  - apply more advanced search for good characteristics over the $expand_1$ rounds
  - search for similar differential properties with fixed chaining input (would require difference in several message words)

Thank you for your attention!