About MD4 differential paths.

Gaëtan Leurent

Laboratoire d'Informatique de l'École Normale Supérieure,
Département d'Informatique,
45 rue d'Ulm, Paris 75230 Cedex 05, France
Gaetan.Leurent@ens.fr

Fast Software Encryption 2007

A new algorithm

Overview

- Input: message difference
- Output: full differential path (∂Q_i and conditions)

Basic Idea

- Based on the sufficient condition algorithm.
- Goes from the last step to the first.
- Each step selects the difference on the state Q_i,
  the difference on the function Φ_i, and adds the conditions.
- Lots of recursivity, backtracking.
- Basic assumption: $\Phi'_i = \Phi_i$, *ie.* absorb the difference.
- When we have a path up to the first round,
  there might be a difference in the IV.

A new algorithm

Turning pseudo-collision path into collision path

- We run the algorithm again, using the previous path as a hint for the values of $\delta\Phi_i$.
- We try to modify the path on the bits that will become the IV differences.
- Indirect correction: if we can't cancel a difference, we introduce a new one that will allow to fix it.

Advantages

- No need to manually add some differences.
- Larger search space.
- Better results.

Results with Wang's message difference

Wang's path

- Eurocrypt 2005.
- Designed to find collisions very efficently.
- Improved by Oswald and Schläffer.
- Our algorithm finds a better path with the same message difference.

Comparison of paths using this message difference

Number of conditions	round 1	round 2	round 3	total
Wang	96	25	2	123
Schläffer and Oswald	122	22	2	146
Our path	72	16	2	90

Results with Yu's message difference

Yu *et al.*'s path

- CANS 2005.
- Designed to have a very low number of conditions (second-preimage).

Results on this path

- Authors claim 32 path using rotations of the path. Actually, only 28 paths (fails on bit 17,20,26 and 28).
- Using bit 25, only 58 conditions instead of 62. Good if you need only one path with very few conditions (eg. HMAC-MD4 attacks).

The path with Wang's message difference

step	s_i	δm_i	path	$\partial\Phi_i$	∂Q_i	Φ-conditions and $\lll$-conditions
0	3					
1	7	$\langle \blacktriangle^{[31]} \rangle$	$\langle \blacktriangledown^{[31]} \rangle$		$\langle \blacktriangle^{[6]} \rangle$	
2	11	$\langle \blacktriangledown^{[28]}, \blacktriangle^{[31]} \rangle$			$\langle \blacktriangledown^{[7]}, \blacktriangle^{[10]} \rangle$	$Q_0^{[6]} = Q_{-1}^{[6]}$
3	19					$Q_2^{[6]} = 0,\ Q_1^{[7]} = Q_0^{[7]},\ Q_1^{[10]} = Q_0^{[10]}$
4	3			$\langle \blacktriangle\blacktriangledown^{[6,7]} \rangle$	$\langle \blacktriangle\blacktriangle\blacktriangledown^{[9\ldots11]} \rangle$	$Q_3^{[6]} = 0,\ Q_3^{[7]} = 1,\ Q_3^{[10]} = 0$
5	7				$\langle \blacktriangle^{[13]} \rangle$	$Q_4^{[7]} = 1,\ Q_3^{[9]} = Q_2^{[9]},\ Q_3^{[10]} = 0,\ Q_3^{[11]} = Q_2^{[11]}$
6	11		$\langle \blacktriangledown^{[10]} \rangle$	$\langle \blacktriangle\blacktriangledown^{[10,11]} \rangle$	$\langle \blacktriangledown^{[18]} \rangle$	$Q_5^{[9]} = 0,\ Q_5^{[10]} = 1,\ Q_5^{[11]} = 1,\ Q_4^{[13]} = Q_3^{[13]}$
7	19					$Q_6^{[9]} = 1,\quad Q_6^{[10]} = 1,\quad Q_6^{[11]} = 1,\quad Q_6^{[13]} = 0,$ $Q_5^{[18]} = Q_4^{[18]}$
8	3		$\langle \blacktriangle^{[13]} \rangle$	$\langle \blacktriangle^{[13]} \rangle$	$\langle \blacktriangledown^{[12]}, \blacktriangle^{[16]} \rangle$	$Q_7^{[13]} = 0,\ Q_7^{[18]} = 0$
9	7		$\langle \blacktriangledown^{[12]} \rangle$	$\langle \blacktriangledown^{[12]} \rangle$	$\langle \blacktriangle^{[19]} \rangle$	$Q_7^{[12]} = 1,\ Q_6^{[12]} = 0,\ Q_7^{[16]} = Q_6^{[16]},\ Q_8^{[18]} = 1$
10	11				$\langle \blacktriangledown^{[29]} \rangle$	$Q_9^{[12]} = 0,\ Q_9^{[16]} = 0,\ Q_8^{[19]} = Q_7^{[19]}$
11	19					$Q_{10}^{[12]} = 1,\ Q_{10}^{[16]} = 1,\ Q_{10}^{[19]} = 0,\ Q_9^{[29]} = Q_8^{[29]}$
12	3	$\langle \blacktriangledown^{[16]} \rangle$	$\langle \blacktriangle^{[19]} \rangle$	$\langle \blacktriangle^{[19]} \rangle$	$\langle \blacktriangledown^{[15]}, \blacktriangle^{[22]} \rangle$	$Q_{11}^{[19]} = 0,\ Q_{11}^{[29]} = 0$
13	7				$\langle \blacktriangledown\blacktriangledown\blacktriangledown\blacktriangle^{[26\ldots29]} \rangle$	$Q_{11}^{[15]} = Q_{10}^{[15]},\ Q_{11}^{[22]} = Q_{10}^{[22]},\ Q_{12}^{[29]} = 1$
14	11		$\langle \blacktriangle^{[29]} \rangle$	$\langle \blacktriangle^{[29]} \rangle$		$Q_{13}^{[15]} = 0,\ Q_{13}^{[22]} = 0,\ Q_{12}^{[26]} = Q_{11}^{[26]},\ Q_{12}^{[27]} = Q_{11}^{[27]},$ $Q_{12}^{[28]} = Q_{11}^{[28]},\ Q_{12}^{[29]} = 1,\ Q_{11}^{[29]} = 0$
15	19		$\langle \blacktriangle^{[28]} \rangle$	$\langle \blacktriangledown\blacktriangle^{[28,29]} \rangle$	$\langle \blacktriangle^{[15]} \rangle$	$Q_{14}^{[15]} = 1,\quad Q_{14}^{[22]} = 1,\quad Q_{14}^{[26]} = 0,\quad Q_{14}^{[27]} = 0,$ $Q_{14}^{[28]} = 1,\ Q_{14}^{[29]} = 1$
16	3		$\langle \blacktriangle^{[15]} \rangle$	$\langle \blacktriangle^{[15]} \rangle$	$\langle \blacktriangle^{[25]} \rangle$	$Q_{14}^{[15]} \neq Q_{13}^{[15]},\quad Q_{15}^{[26]} = Q_{14}^{[26]},\quad Q_{15}^{[27]} = Q_{14}^{[27]},$ $Q_{15}^{[28]} = Q_{14}^{[28]},\ Q_{15}^{[29]} = Q_{14}^{[29]}$
17	5				$\langle \blacktriangle^{[31]} \rangle$	$Q_{16}^{[15]} = Q_{14}^{[15]},\ Q_{15}^{[25]} = Q_{14}^{[25]}$
18	9					$Q_{17}^{[15]} = Q_{16}^{[15]},\ Q_{17}^{[25]} = Q_{15}^{[25]},\ Q_{16}^{[31]} = Q_{15}^{[31]}$
19	13	$\langle \blacktriangledown^{[16]} \rangle$			$\langle \blacktriangledown^{[28]} \rangle$	$Q_{18}^{[25]} = Q_{17}^{[25]},\ Q_{18}^{[31]} = Q_{16}^{[31]}$
20	3	$\langle \blacktriangle^{[31]} \rangle$	$\langle \blacktriangledown^{[28]}, \blacktriangledown^{[31]} \rangle$	$\langle \blacktriangledown^{[28]}, \blacktriangle^{[31]} \rangle$	$\langle \blacktriangle^{[28]}, \blacktriangledown^{[31]} \rangle$	$Q_{18}^{[28]} \neq Q_{17}^{[28]},\ Q_{19}^{[31]} \neq Q_{18}^{[31]}$
21	5		$\langle \blacktriangledown^{[31]} \rangle$	$\langle \blacktriangledown^{[31]} \rangle$		$Q_{19}^{[31]} \neq Q_{18}^{[31]}$
22	9					$Q_{21}^{[31]} = Q_{19}^{[31]}$
23	13		$\langle \blacktriangle^{[28]} \rangle$	$\langle \blacktriangle^{[28]} \rangle$		$Q_{22}^{[28]} \neq Q_{21}^{[28]},\ Q_{22}^{[31]} = Q_{21}^{[31]}$
24	3	$\langle \blacktriangledown^{[28]}, \blacktriangle^{[31]} \rangle$				
25	5					
26	9					
27	13					
28	3					
29	5					
30	9					
31	13					

The path with Yu's message difference

step	s_i	δm_i	$\partial \Phi_i$	∂Q_i	conditions
0	3				
1	7				
2	11				
3	19				
4	3	$\langle \blacktriangle^{[25]} \rangle$		$\langle \blacktriangle^{[28]} \rangle$	
5	7				$Q_3^{[28]} = Q_2^{[28]}$
6	11				$Q_5^{[28]} = 0$
7	19				$Q_6^{[28]} = 1$
8	3			$\langle \blacktriangle^{[31]} \rangle$	
9	7				$Q_7^{[31]} = Q_6^{[31]}$
10	11		$\langle \blacktriangle^{[31]} \rangle$	$\langle \blacktriangledown^{[10]} \rangle$	$Q_9^{[31]} = 1$
11	19				$Q_9^{[10]} = Q_8^{[10]},\ Q_{10}^{[31]} = 1$
12	3			$\langle \blacktriangle^{[2]} \rangle$	$Q_{11}^{[10]} = 0$
13	7				$Q_{11}^{[2]} = Q_{10}^{[2]},\ Q_{12}^{[10]} = 1$
14	11			$\langle \blacktriangledown^{[21]} \rangle$	$Q_{13}^{[2]} = 0$
15	19				$Q_{14}^{[2]} = 1,\ Q_{13}^{[21]} = Q_{12}^{[21]}$
16	3			$\langle \blacktriangle^{[5]} \rangle$	$Q_{15}^{[21]} = Q_{13}^{[21]}$
17	5	$\langle \blacktriangle^{[25]} \rangle$	$\langle \blacktriangle^{[5]} \rangle$	$\langle \blacktriangle^{[10]}, \blacktriangle^{[30]} \rangle$	$Q_{15}^{[5]} \neq Q_{14}^{[5]},\ Q_{16}^{[21]} = Q_{15}^{[21]}$
18	9			$\langle \blacktriangledown^{[30]} \rangle$	$Q_{17}^{[5]} = Q_{15}^{[5]},\ Q_{16}^{[10]} = Q_{15}^{[10]},\ Q_{16}^{[30]} = Q_{15}^{[30]}$
19	13				$Q_{18}^{[5]} = Q_{17}^{[5]},\ Q_{18}^{[10]} = Q_{16}^{[10]}$
20	3			$\langle \blacktriangle^{[8]} \rangle$	$Q_{19}^{[10]} = Q_{18}^{[10]}$
21	5		$\langle \blacktriangledown^{[30]} \rangle$	$\langle \blacktriangle^{[15]} \rangle$	$Q_{19}^{[8]} = Q_{18}^{[8]},\ Q_{20}^{[30]} \neq Q_{19}^{[30]}$
22	9			$\langle \blacktriangle\blacktriangledown^{[7,8]} \rangle$	$Q_{21}^{[8]} = Q_{19}^{[8]},\ Q_{20}^{[15]} = Q_{19}^{[15]}$
23	13				$Q_{21}^{[7]} = Q_{20}^{[7]},\ Q_{22}^{[15]} = Q_{20}^{[15]}$
24	3		$\langle \blacktriangledown^{[8]} \rangle$		$Q_{23}^{[7]} = Q_{21}^{[7]},\ Q_{23}^{[8]} \neq Q_{21}^{[8]},\ Q_{23}^{[15]} = Q_{22}^{[15]}$
25	5			$\langle \blacktriangle^{[20]} \rangle$	$Q_{24}^{[7]} = Q_{23}^{[7]},\ Q_{24}^{[8]} = Q_{23}^{[8]}$
26	9			$\langle \blacktriangledown^{[16]} \rangle$	$Q_{24}^{[20]} = Q_{23}^{[20]}$
27	13				$Q_{25}^{[16]} = Q_{24}^{[16]},\ Q_{26}^{[20]} = Q_{24}^{[20]}$
28	3				$Q_{27}^{[16]} = Q_{25}^{[16]},\ Q_{27}^{[20]} = Q_{26}^{[20]}$
29	5			$\langle \blacktriangle^{[25]} \rangle$	$Q_{28}^{[16]} = Q_{27}^{[16]}$
30	9			$\langle \blacktriangledown^{[25]} \rangle$	$Q_{28}^{[25]} = Q_{27}^{[25]}$
31	13				
32	3				
33	9		$\langle \blacktriangledown^{[25]} \rangle$		$Q_{32}^{[25]} = Q_{31}^{[25]}$
34	11	$\langle \blacktriangle^{[25]} \rangle$			
35	15				
36	3				
37	9				
38	11				

58 conditions: $20 + 37 + 1$