More Differential Paths for TIB3

Harry Wiggins, Phil Hawkes, Cameron McDonald, Greg Rose

Qualcomm Inc.

{hwiggins,phawkes,cameronm,ggr}@qualcomm.com

Motivation and achievements

- TIB3 closely resembled CHI (our SHA-3 submission)
- Mendel et al published a pseudo-collision differential path
  - No differences in messages.
- We discovered new properties in the key schedule and PHTX function
- This led to finding new differential paths with differences in messages
- We provide example message pairs

Message Expansion Differentials

- Key expansion uses $V = \psi(W, X, Y, Z)$ as defined below

$$\begin{aligned} V &:= (Y + (Z << 32)) \oplus W \oplus X \oplus (Z >> 32) \\ V &:= V + (V << 32) + (V << 43) \\ V &:= V \oplus (V >> 39). \end{aligned}$$

- If you modify W and X at bit i the effect can cancel out (same for pairs W, Y or X, Y)
  - Provides 16 possible message differentials
- If W, X, Y, Z has a difference in bit 31 so does V
  - Provides 16 more message differentials
  - Ex: $10, 15, 10, 15, 10, 15, 15, 10, 13, 13, 13, 7, 15, 15, 15, 15$
  - Note a "10" indicates a difference in 1st and 3rd word, no difference in 2nd and 4th word

1-Round Differential Paths

Round key differences allowing "Chain-able" 1-round differentials avoiding the PHTX

Input Difference	Output Difference			
	0	**1**	**6**	**7**
0	**0**	**8,10**		**8,10**
1		**13,15**	**5,7,13,15**	**5,7**
7		**8,10**	**0,2,8,10**	**0,2**
6	**7**	**13,15**		**13,15**

This produces three 16-round differentials for bit 31 with 2^{-32} probability. An example:

$$7 \xrightarrow{10} 6 \xrightarrow{15} 7 \xrightarrow{10} 6 \xrightarrow{15} 7 \xrightarrow{10} 1 \xrightarrow{15} 6 \xrightarrow{15} 7 \xrightarrow{10} 1,$$

$$1 \xrightarrow{13} 1 \xrightarrow{13} 6 \xrightarrow{13} 1 \xrightarrow{7} 6 \xrightarrow{15} 1 \xrightarrow{15} 1 \xrightarrow{15} 6 \xrightarrow{15} 1.$$

Example found by message modification

H_0		ΔH_0	
6a09e667f3bcc908	bb67ae8584caa73b	.....	.....8.....
3c6ef372fe94f82b	a54ff53a5f1d36f1	.....8.....	.....
M_1		ΔM_1	
f56ad25f5a340dc4	e312e89133026ab1	.....8.....	.....8.....
9be385032ee31661	f6ccfa026ff77ce2	.....	.....8.....
1211843cad836f81	aedde3d1398738bd	.....	.....8.....
fc9c7f1d4060f02a	c9ed13688251157c	.....8.....	.....
M_2		ΔM_2	
1bcf18aae23a931c	fa4a87b5d79ee354	.....8.....	.....
d4d1f1bd3115b211	2efffaa024671b11	.....8.....	.....
c99f87f3e75cbbbd	a6e8b08cb934285a	.....8.....	.....8.....
f4d27375524bacb3	c5bdd133f185bbe6	.....8.....	.....8.....
H_{16}		ΔH_{16}	
b79720b5985fc79c	f6189483b490e7e8	.....	.....
69bae9c1b45027bd	9eee2b2a1f459deb	.....	.....8.....

Differential Properties of the PHTX

- A short description of the PHTX function on 64-bit words:

$$\begin{aligned} D^* &= PHTX(D), \\ \tilde{D} &= D + (D << 32) + (D << 47), \\ D^* &= \tilde{D} \oplus (\tilde{D} >> 32) \oplus (\tilde{D} >> 43). \end{aligned}$$

The following table was observed:

Δ	$\Delta PHTX$
31	63,20
63	63,31,20
31,63	31

- This allows more 1-round paths to be considered
- Paper will be available on eprint soon