Partial-Collision Attack on the Round-Reduced Compression Function of Skein-256

Hongbo Yu, Jiazhe Chen, Xiaoyun Wang

Tsinghua University

Shandong University

Outline

- Brief description of Skein-256
- Previous results related to near(partial)-collision on Skein
- Our attacks

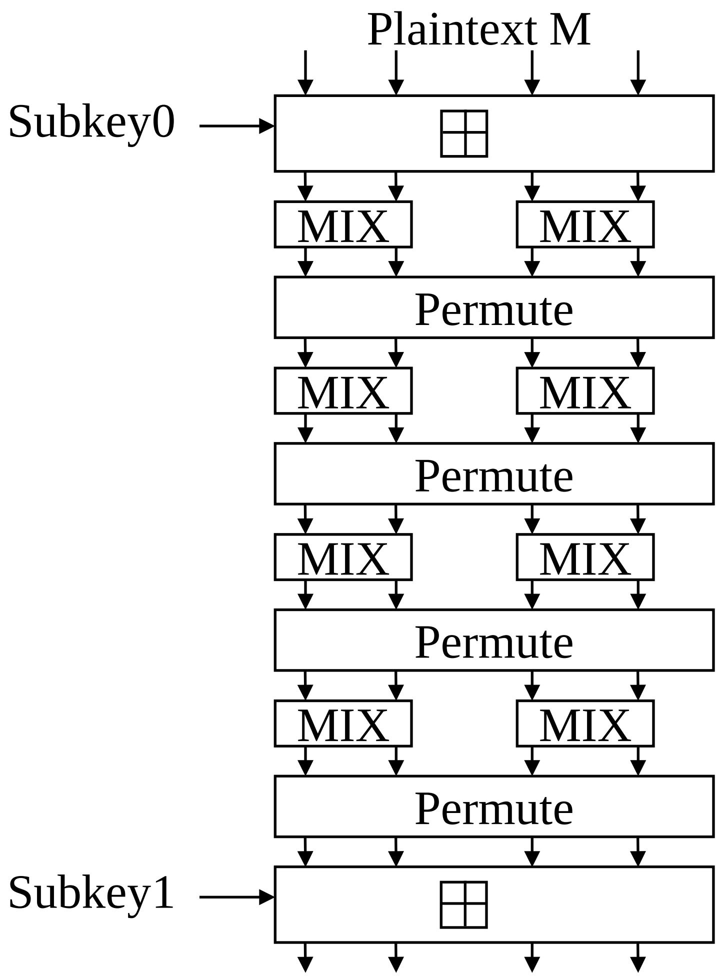
Skein

- One of the 5 finalists of SHA-3 competition
- Designers
  - Niels Ferguson , Stefan Lucks, Bruce Schneier, Doug Whiting, Mihir Bellare,Tadayoshi Kohno, Jon Callas, Jesse Walker
- Unique Block Iteration (UBI) based the block cipher Threefish
- The block size： 256/512/1024 bits
  - Skein-512 is primary proposal
  - Skein-256 is a low-memory variant
  - Skein-1024 is a ultra-conservative variant

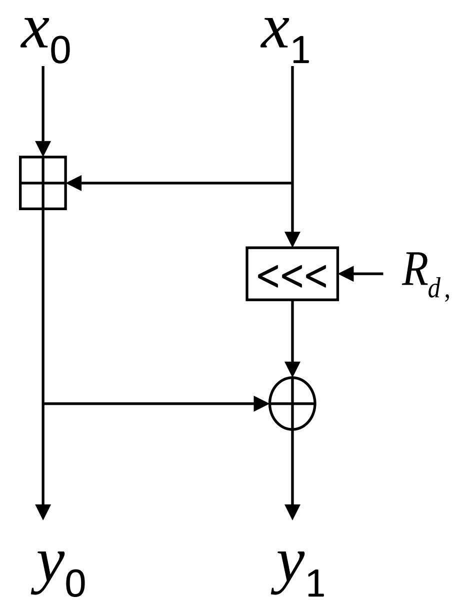
Skein

- Compression function $H_{i+1} = E(H_i, T, M_i) \oplus M_i$,
  - E( ): block cipher threefish
  - M_i: The plaintext, block size 256/512/1024 bits
  - H_i : The key, same size with M_i
  - $T=(t_0, t_1)$: the tweak of 128 bits

Threefish-256 (72 Rounds)



The MIX function



$$y_0 = (x_0 + x_1) \bmod 2^{64}$$

$$y_1 = (x_1 <<< (R_{(d \bmod 8), j}) \oplus y_0$$

Four of the 72 rounds of the Threesh-256 block cipher.

Key Schedule

- The key schedule starts with the 256-bit master key $K = (k_0, k_1, k_2, k_3)$ and the 128-bit tweak value $T = (t_0, t_1)$.
- First compute two additional words k_4 and t_2:

$$k_4 = C_{240} \oplus k_0 \oplus k_1 \oplus k_2 \oplus k_3 \quad \text{and} \quad t_2 = t_0 \oplus t_1$$

- Then the subkeys $K_s = (K_{s,a}, K_{s,b}, K_{s,c}, K_{s,d})$ are derived by:

for $s=0$ *to* 18

$$K_{s,a} = k_{(s+0)\, mod\, 5}$$
$$K_{s,b} = k_{(s+1)\, mod\, 5} + t_{s\, mod\, 3}$$
$$K_{s,c} = k_{(s+2)\, mod\, 5} + t_{(s+1)\, mod\, 3}$$
$$K_{s,d} = k_{(s+3)\, mod\, 5} + s$$

Near-collision and Partial- collision

- Near-collision resistance : It should be hard to find any two inputs m, m* with m≠m* such that H(m) and H(m*) differ in only a small number of bits. [Handbook]
- *w*-bit near-collision: a pair message m and m* collides such that $\left| H(M) \oplus H(M^*) \right| = w, \quad w \le n$
  - Generic attack: time complexity $2^{n/2}\sqrt{\sum_{i=0}^{w}\binom{n}{i}}$, memory $2^{n/2}$
- *w*-bit partial-collision: a pair message m and m* collides in the fixed *w* bits
  - Generic attack: $2^{w/2}$

Comparison of attacks related to (near)-collision on Skein-256

Target	Round	Time	Type	Authors
Skein-512	17(0-17)	2^{24}	434-bit free-start near-collision	[SWWD10]
Skein-256	20(0-20)	2^{97}	130-bit free-start near-collision	
Skein-512	20(20-40)	2^{52}	266-bit free-start near-collision	
Skein-512	22	$2^{253.7}$	Free-start collision	[LIS12]
Skein-512	37	$2^{255.7}$	Free-start collision	
Skein-256	24(4-28)	2^{42}	254-bit near-collision	This paper
Skein-256	28(0-28)	2^{44}	222-bit near-collision	
Skein-256	28(4-32)	2^{42}	228-bit near-collision	
Skein-256	32(0-32)	2^{85}	206-bit partial-collision	

The Basic Idea of Our Attack

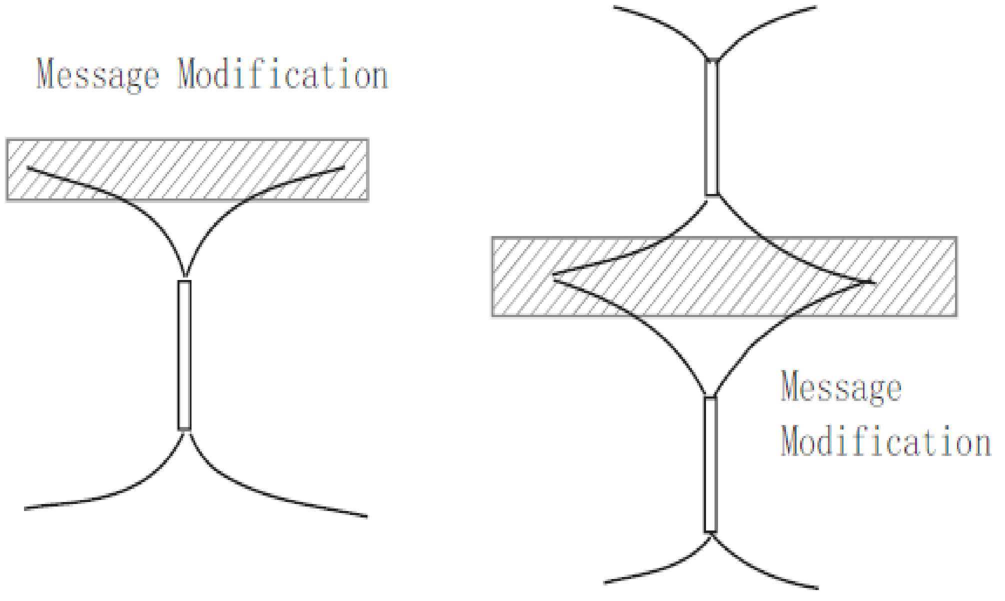


Fig. 1. Two Attack Models

- Long differential path
- Low Hamming Weight

The Subkey Difference

The subkey differences of 32-round Skein-256, given a difference $\delta = 2^{63}$ in k_3 and t_0

i	Rd	$K_{i,a}$	$K_{i,b}$	$K_{i,c}$	$K_{i,d}$
0	0	k_0	$k_1 + t_0$	$k_2 + t_1$	k_3
		0	δ	0	δ
1	4	k_1	$k_2 + t_1$	$k_3 + t_2$	$k_4 + 1$
		0	0	0	δ
2	8	k_2	$k_3 + t_2$	$k_4 + t_0$	$k_0 + 2$
		0	0	0	0
3	12	k_3	$k_4 + t_0$	$k_0 + t_1$	$k_1 + 3$
		δ	0	0	0
4	16	k_4	$k_0 + t_1$	$k_1 + t_2$	$k_2 + 4$
		δ	0	δ	0
5	20	k_0	$k_1 + t_2$	$k_2 + t_0$	$k_3 + 5$
		0	δ	δ	δ
6	24	k_1	$k_2 + t_0$	$k_3 + t_1$	$k_4 + 6$
		0	δ	δ	δ
7	28	k_2	$k_3 + t_1$	$k_4 + t_2$	$k_0 + 7$
		0	δ	0	0
8	32	k_3	$k_4 + t_2$	$k_0 + t_0$	$k_1 + 8$
		δ	0	δ	0

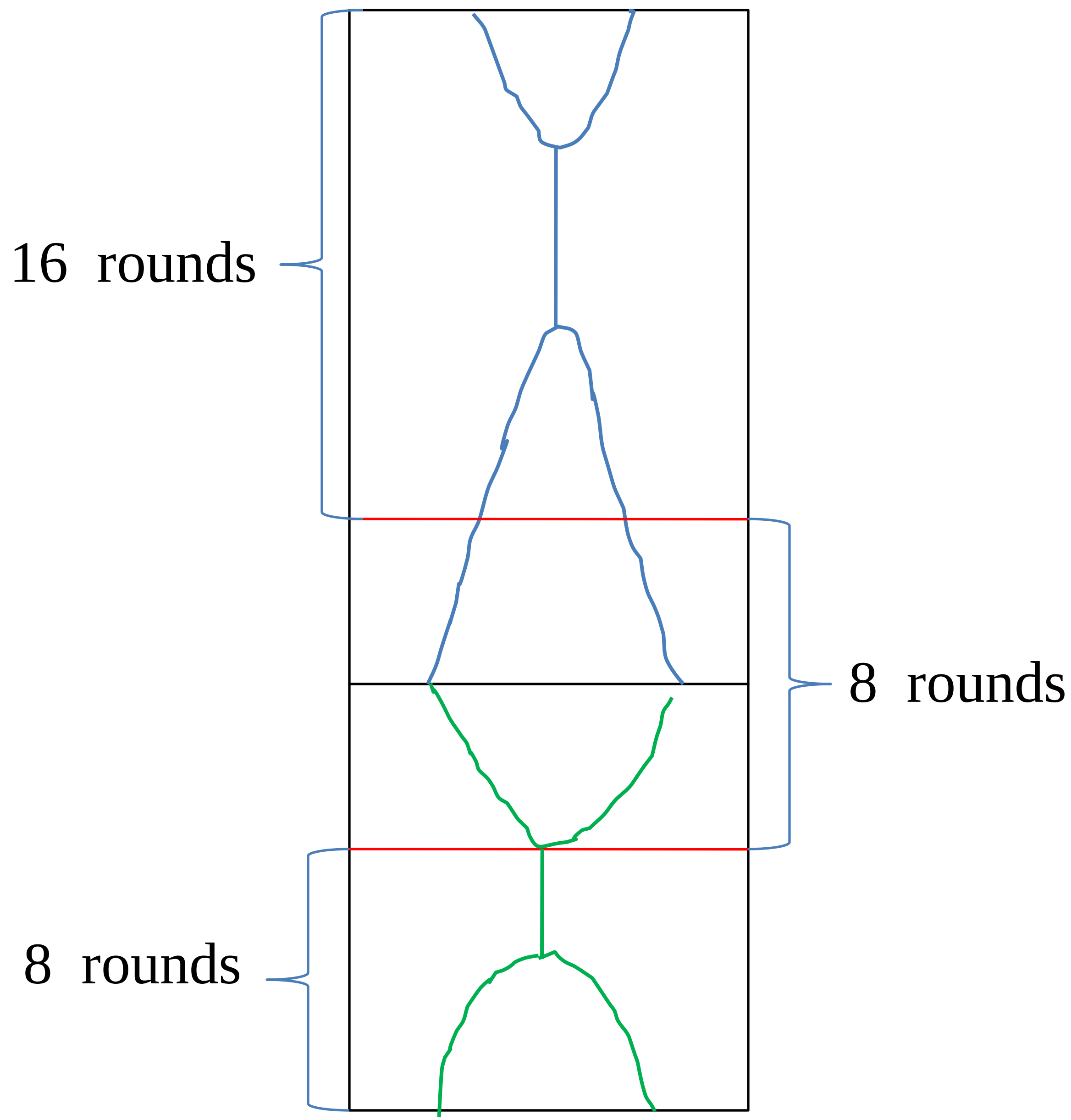
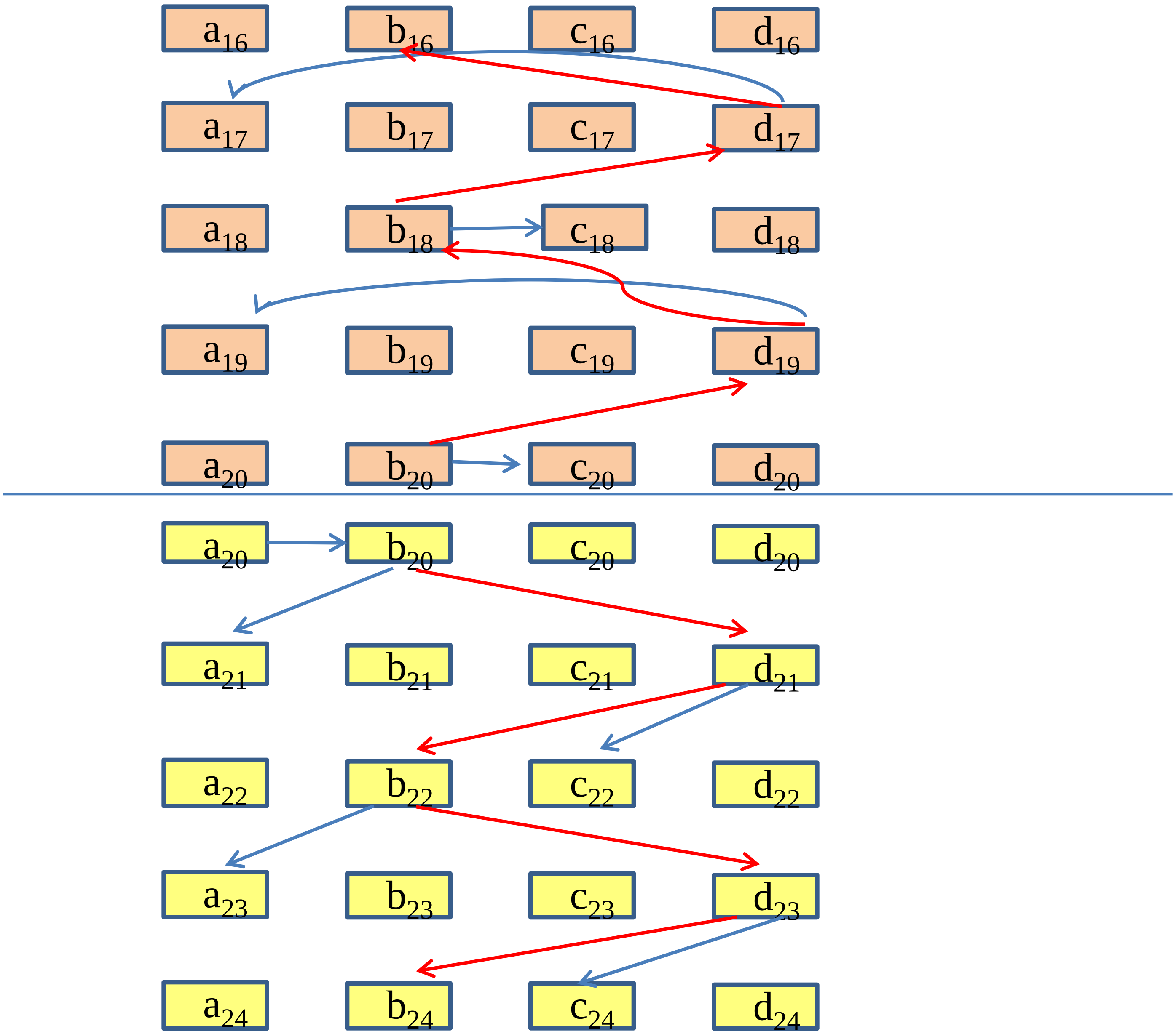


Fig. Near(partial)-collision path

Strategy to Connect two Short Parths

- Select the round 20 as the connection point
  - the subkey is involved
- Connect a_{20} and c_{20}
  - adjust the difference from h_{21} to h_{24},
- Connect b_{20} and d_{20}
  - adjust the difference from h_{16} to h_{19}
- Using two kinds of difference modes
  - XOR differential
  - '+' the integer modular subtraction difference


a16 b16 c16 d16
a17 b17 c17 d17
a18 b18 c18 d18
a19 b19 c19 d19
a20 b20 c20 d20
a20 b20 c20 d20
a21 b21 c21 d21
a22 b22 c22 d22
a23 b23 c23 d23
a24 b24 c24 d24

32 round Skein-256 Differential path

Round	Δa_i	Δb_i	Δc_i	Δd_i
0	0500900a50210840	8100100210210800	0040040082044204	8040000084004204
$\overline{0}$:$+K_0$	$\Delta^+ a_0$	0100100210210800	$\Delta^+ c_0$	0040000084004204
1	0400800840000040	0000800040000040	0000040002040000	0000040002000000
2	0400000800000000	0000000800000000	0000000000040000	0000000000040000
3	0400000000000000	0400000000000000	0000000000000000	0000000000000000
4	0000000000000000	0000000000000000	0000000000000000	8000000000000000
$\overline{4}$:$+K_1$	0000000000000000	0000000000000000	0000000000000000	0000000000000000
$5-12$	0000000000000000	0000000000000000	0000000000000000	0000000000000000
$\overline{12}$:$+K_3$	8000000000000000	0000000000000000	0000000000000000	0000000000000000
13	8000000000000000	0000000000000000	0000000000000000	8000000000000000
14	8000000000000000	8000000000000800	8000000000000000	8000000000000000
15	0000000000000800	0000000000200000	0000000000000000	0200000000000820
16	0000000000200800	0600082002000820	0600000000000820	0020000000200800
$\overline{16}$:$+K_4$	$\Delta^+ a_{16} + 2^{63}$	0600182006000820	$\Delta^+ c_{16} + 2^{63}$	0020000000600800
17	8600182002200020	8260006008200000	8260000000200020	800819a0002801a0
18	08a0080006000020	4328099340d85f83	022819a000d80f80	08a82e0000008220
19	7898108fc7e9d4a1	0a4230a8a86980a0	0ac010a0004780a0	b1387ca0064840a5
20	d146001565005501	800001b6251fd503	4908150002104103	9900150068304100
$\overline{20}$:$+K_5$	$\Delta^+ a_{20}$	0000019fe700f703	$\Delta^+ c_{20} + 2^{63}$	39001f01ebf3ff00
21	dfc601eff8000000	f7fe000008000000	2019fe007a003e03	e0080001fe000003
22	00003fff80000000	000001e000000000	80001e0000003e00	0000020000000200
23	0000000780000000	0000000080000000	8000000000000000	0000000000000000
24	0000000000000000	8000000000000000	8000000000000000	8000000000000000
$\overline{24}$:$+K_6$	0000000000000000	8000000000000000	8000000000000000	8000000000000000
25-28	0000000000000000	0000000000000000	0000000000000000	0000000000000000
$\overline{28}$:$+K_7$	0000000000000000	8000000000000000	0000000000000000	0000000000000000
29	8000000000000000	0000000000000000	0000000000000000	8000000001000000
30	8000000000000000	8000001001000800	8000000001000000	8000000000000000
31	0000001001000800	0000000001200000	0000000001000000	0200001041040820
32	0000001000200800	4304083042040830	0200001040040820	0120001000200800
$\overline{32}$:$+K_8$	8000001000200800	c104081042040810	8200001040040820	0120001000200800
Output Difference	8500901a50010040	4004181250250010	82400410c2004a24	8160001084204a04

The Conditions Distribution

Groups	Conditions	Modified Conditions	Used message/IV
1	216	174	$a_{20}, b_{20}, c_{20}, d_{20}$
2	168	150	$K_{5,a}$, $K_{5,b}$, $K_{5,c}$, $K_{5,d}$
3	104	15	$K_{4,b}$, $K_{4,d}$

Group-1: conditions in round 16 to 20
Group-2: conditions in round 20 to 24, and c16
Group-3: other conditions

Partial(near)-Collision Attack

Phase 1:

- Search 256-bit $h_{20}=(a_{20},b_{20},c_{20},d_{20})$ to fulfil rounds 16-20
  - Message modification technique
  - Time complexity: 2^{42}

Phase 2:

- Search 256-bit $K_5=(K_{5,a}, K_{5,b}, K_{5,c}, K_{5,d})$ to fulfil rounds 20 to 24 and conditions in c_{16}
  - Message modification technique
  - Time complexity: 2^{18}

Partial(near)-Collision Attack

Phase 3:

- Search 128-bit $K_{4,b}$, $K_{4,d}$ to fulfil other rounds (0-16, 24-32)
  - Message modification technique
  - Time complexity: 2^{85}

The complexity of our attack

- 32 rounds(0-32): $2^{42}+2^{18}+2^{85} \approx 2^{85}$
- 24 rounds(4-28): $2^{42}+2^{26} \approx 2^{42}$
- 28 rounds(0-28): $2^{42}+2^{18}+2^{44} \approx 2^{44}$
- 28 rounds(4-32): $2^{42}+2^{18}+2^{41} \approx 2^{42}$

Degrees of Freedom Analysis

- The total degrees of freedom
  - come from the messge M, the master Key K and the tweak T: 256+256+128=640
  - Number of conditions: 488
- The degrees of freedom in rounds 16-20 (Phase 1)
  - Come from h_{20}: 256
  - Number of conditions: 216
- The degrees of freedom in rounds 20-24 (Phase 2)
  - Come from K_5: 256
  - Number of conditions: 168
- The degrees of freedom in other rounds (Phase 3)
  - Come from K_5: 128
  - Number of conditions: 104

Examples

Near-Collision 1: a near collision with Hamming distance 2 from rounds 4 to 28	
Message of Round 4	
$M^{(1)}$	e06dae5ef2a07f47 ab4a1eb0d3ca9657 2df69dff1cf902f7 <u>9</u>4f1d26c1640e047
$M^{(2)}$	e06dae5ef2a07f47 ab4a1eb0d3ca9657 2df69dff1cf902f7 <u>1</u>4f1d26c1640e047
Key	
$K^{(1)}$	276233eabba1aee6 66468bf4f9186874 4c1044cb8ebdb40 <u>7</u>1b6c3354128213a
$K^{(2)}$	276233eabba1aee6 66468bf4f9186874 4c1044cb8ebdb40 <u>f</u>1b6c3354128213a
Tweak	
$T^{(1)}$	<u>0</u>000000000000000 0000000000000000
$T^{(2)}$	<u>8</u>000000000000000 0000000000000000
Output: $a_4 \oplus \overline{a_{28}}$	
Output1	7d750ef8ccb0bbd0 <u>1</u>cc1e98ec9f9a18a eab66d1642a6c3f1 <u>f</u>a19cc4783700f1c
Output2	7d750ef8ccb0bbd0 <u>9</u>cc1e98ec9f9a18a eab66d1642a6c3f1 <u>7</u>a19cc4783700f1c

Near-Collision 2: a near collision with Hamming distance 34 from rounds 0 to 28	
Message of Round 0	
$M^{(1)}$	75567a6722e984c1 6aa74b49b44a4b0e 8dc87c2235fe4944 910233d1a5628f29
$M^{(2)}$	7056ea6d72c88c81; eba75b4ba46b430e 8d887822b7fa0b40 114233d12162cd2d
Key	
$K^{(1)}$	174b482acb8192de d581ea180039c605 6a83af6bc11fb1ca 73aaa3494528212f
$K^{(2)}$	174b482acb8192de d581ea180039c605 6a83af6bc11fb1ca f3aaa3494528212f
Tweak	
$T^{(1)}$	204974d2f898e9cd 0085794e10264ba2
$T^{(2)}$	a04974d2f898e9cd 0085794e10264ba2
Output: $a_0 \oplus \overline{a_{28}}$	
Output1	9ba9ee20f9e4dbfb d99ef6dbe703fd1b 567033e47cd85ebe bfa917f64a5f8926
Output2	9ea97e2aa9c5d3bb d89ee6d9f722f51b 563037e4fedc1cba 3fe917f6ce5fcb22

Near-Collision 3: a near collision with Hamming distance 28 from rounds 4 to 32	
Message of Round 4	
$M^{(1)}$	7c4d70e0bb911686 126e7d70b549e195 687401fcfdda8a32 74d4ba53d43c8f4b
$M^{(2)}$	7c4d70e0bb911686 126e7d70b549e195 687401fcfdda8a32 f4d4ba53d43c8f4b
Key	
$K^{(1)}$	174b482acb8192de f80431a5cb0dcdc8 43f0a9b602dfc4e2 73aaa3494528212f
$K^{(2)}$	174b482acb8192de f80431a5cb0dcdc8 43f0a9b602dfc4e2 f3aaa3494528212f
Tweak	
$T^{(1)}$	46dc7a88b6d8d6b5 b895bc87ab324c19
$T^{(2)}$	c6dc7a88b6d8d6b5 b895bc87ab324c19
Output: $a_4 \oplus \overline{a_{32}}$	
Output1	e5e0fd7e130df9ae cd8f77d82cf70926 abd50d673bc9fab1 feca27355d91f45d
Output2	65e0fd6e132df1ae 0c8b7fc86ef30136 29d50d777bcdf291 7fea27255db1fc5d

Thanks you for your attention!