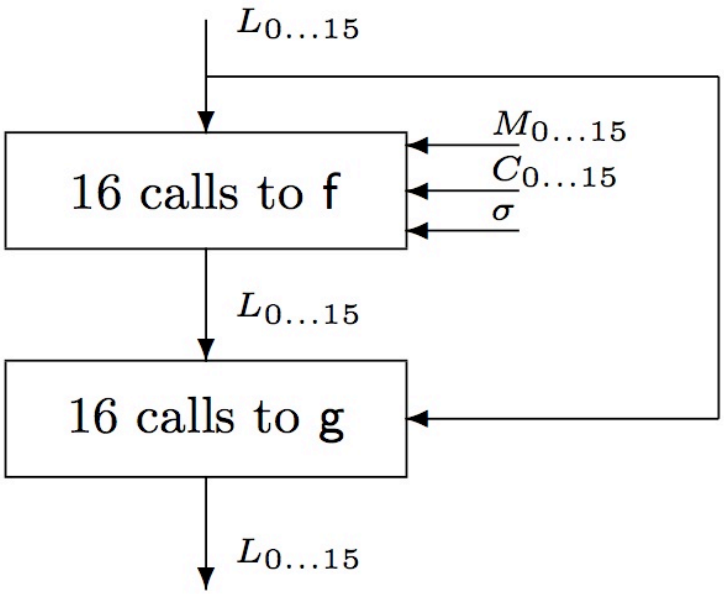
Update on Lake

Florian Mendel, Christian Rechberger,
and Martin Schläffer

Institute for Applied Information Processing and Communications (IAIK) - Krypto Group

Faculty of Computer Science
Graz University of Technology

Observation



- The Boolean function f used in Lake is not invertible

$$f(a,b,c,d) = (a + (b \vee C_0)) + (c + (a \wedge C_1)) \ggg 7) + ((b + (c \oplus d)) \ggg 13)$$
$$g(a,b,c,d) = ((a+b) \ggg 1) \oplus (c+d).$$

Collision in 1 round

- Since the function f is not invertible, we can find 2 message words m_k^* and m_k such that for both messages the output of f is equal

$$\Delta f = (\Delta m_k \ggg 7) + ((\Delta m_k \oplus C_i) \ggg 13) = 0$$

- Once, we have found a collision for f we have also a found collision for Lake reduced to 1 round

A Variant of Lake

- If we use the same constant in each round then we can easily construct collisions for Lake.

- Example $C_i = C_0$ (for i=1,…,15)

h_0	243F6A88 85A308D3 13198A2E 03707344 A4093822 299F31D0 082EFA98 EC4E6C89
M_0	7901FB66 7120239A 75018D7B 38EFC240 04BA14F4 54B5A198 60842D9A 05CE0AF7 1A31E11B 40B1C10C 55F91C02 559DF366 74D6D973 455E48F2 31072B72 4DB56283
M_0^*	7D11BC59 7120239A 75018D7B 38EFC240 04BA14F4 54B5A198 60842D9A 05CE0AF7 1A31E11B 40B1C10C 55F91C02 559DF366 74D6D973 455E48F2 31072B72 4DB56283
ΔM_0	0410473F 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000
h_1	289B5613 0295350F CA661380 699C892A 80CC3678 91B6F85B FD0332EB D89C925A
h_1^*	289B5613 0295350F CA661380 699C892A 80CC3678 91B6F85B FD0332EB D89C925A

The Lake hash function

- A different constant is used in each round

	m_0	m_1	m_2	m_3	m_4	m_5	m_6	m_7	m_8	m_9	m_{10}	m_{11}	m_{12}	m_{13}	m_{14}	m_{15}
R1	C_0	C_1	C_2	C_3	C_4	C_5	C_6	C_7	C_8	C_9	C_{10}	C_{11}	C_{12}	C_{13}	C_{14}	C_{15}
R2	C_3	C_0	C_{13}	C_{10}	C_7	C_4	C_1	C_{14}	C_{11}	C_8	C_5	C_2	C_{15}	C_{12}	C_9	C_6
R3	C_9	C_4	C_{15}	C_{10}	C_5	C_0	C_{11}	C_6	C_1	C_{12}	C_7	C_2	C_{13}	C_8	C_3	C_{14}
R4	C_0	C_7	C_{14}	C_5	C_{12}	C_3	C_{10}	C_1	C_8	C_{15}	C_6	C_{13}	C_4	C_{11}	C_2	C_9

- Hence constructing a collision gets more complicated

$$\Delta f_3 = (\Delta m_3 \ggg 7) + ((\Delta m_3 \oplus C_3) \ggg 13) = 0$$
$$\Delta f_{10} = (\Delta m_3 \ggg 7) + ((\Delta m_3 \oplus C_{10}) \ggg 13) = 0$$

Collision for 3 rounds

- Actual colliding message pair for 3 rounds of Lake

h_0	243F6A88	85A308D3	13198A2E	03707344	A4093822	299F31D0	082EFA98	EC4E6C89
M_0	2ED54018	259E7BED	6A7D12A0	12780007	57979D36	619A5DE1	2F1FA8A0	09D72979
	3428C041	1439951D	63537711	144840C4	7C75D35E	70C613E9	23DCA632	52DB6AB9
M_0^*	2ED54018	259E7BED	6A7D12A0	907FE827	57979D36	619A5DE1	2F1FA8A0	09D72979
	3428C041	1439951D	63537711	144840C4	7C75D35E	70C613E9	23DCA632	52DB6AB9
ΔM_0	00000000	00000000	00000000	8207E820	00000000	00000000	00000000	00000000
	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
h_1	0969AF41	101EA7CE	CBF3F2FE	E47832EB	60FFD511	DA156A75	150B3A20	F003BA7E
h_1^*	0969AF41	101EA7CE	CBF3F2FE	E47832EB	60FFD511	DA156A75	150B3A20	F003BA7E

Extending the attack to more rounds

- Problem: We have to find collisions in f for 4 different constants
- We found only characteristics with very low probability
- Example:
  - $\Delta m_4 = -1$
  - probability 2^{-47} for each round
  - 4 rounds => 2^{-188}
  - By using message modification this can be improved to 2^{-109}

Summary

- We show that the non-bijectiveness of the function f can be used to construct collisions for round reduced Lake
- We show a actual colliding message pair for 3 rounds of the hash function
- We present an attack on 4 rounds with a complexity of 2^{109}.
- We expect that the attack can be extended to 5 rounds by using advanced message modification techniques