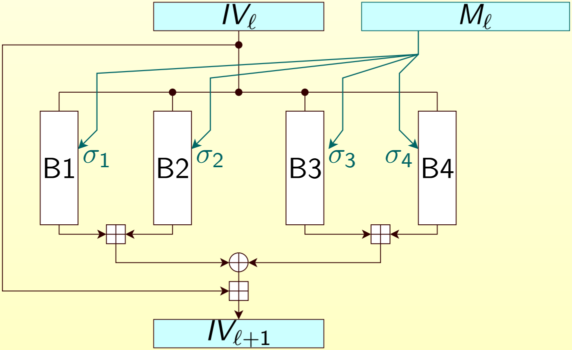
Weaknesses of the FORK-256 compression function

Krystian Matusiewicz, Scott Contini and Josef Pieprzyk

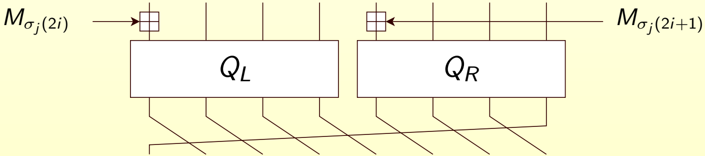
Macquarie University

Structure of FORK-256 :: four parallel branches



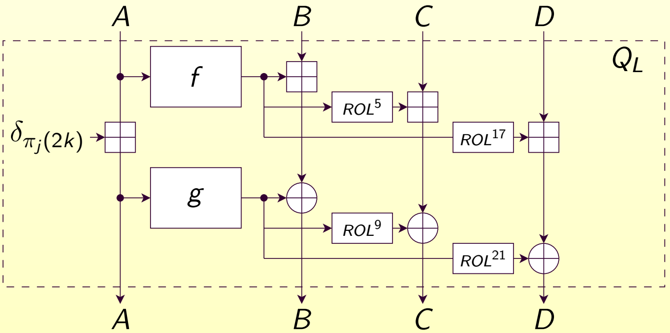
- 256 bits of chaining variable *IV*
- 512 bits of message *M*
- each branch B1, B2, B3, B4 consists of **8 steps**
- each branch uses a different permutation $(\sigma_1, \sigma_2, \sigma_3, \sigma_4)$ of message words $M_0, \ldots, M_{15}$

Structure of FORK-256 :: step transformation



- there are 8 steps in each branch
- each step uses two message words
- step transformation – a composition of three simple operations
  - addition of message words
  - two parallel **Q-structures**
  - rotation of registers

Structure of FORK-256 :: Q-structure (left)

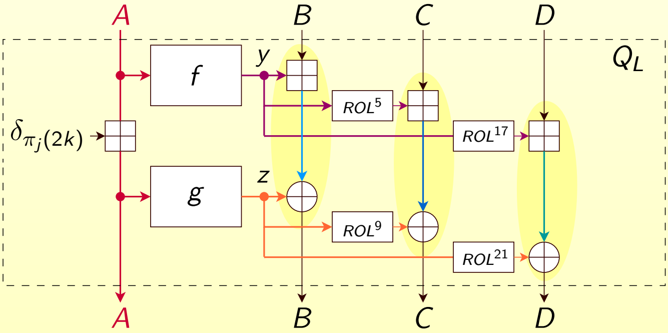


where

$$f(x) = x \boxplus (ROL^7(x) \oplus ROL^{22}(x)) \ ,$$
$$g(x) = x \oplus (ROL^{13}(x) \boxplus ROL^{27}(x))$$

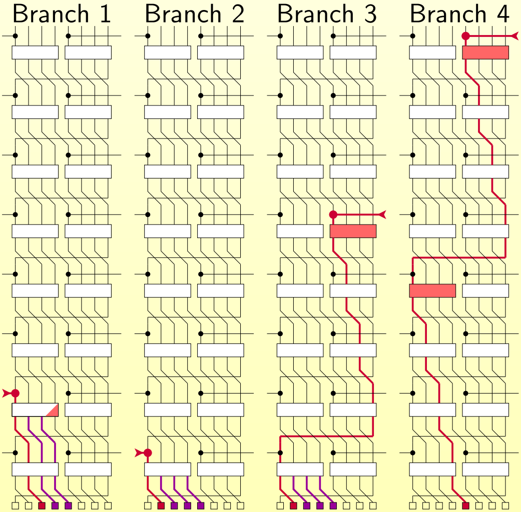
Q_R is similar : f swapped with g and different rotation amounts

“Microcollisions“ in Q-structures



- a difference in register A does not propagate to other registers
- differences cancel each other inside the Q-structure !
- we derived an efficent necessary and sufficent condition for $(y + B) \oplus z = (y' + B) \oplus z'$ to hold

High-level differential path



Using a special modular difference in M_{12} and three (and 1/3) micro-collisions we can restrict output differences to only **108** bits (part of register B and registers C, D, E).

Summary of results

- ”Near-near-collisions“: we managed to find an IV and two input messages that yield hashes different by only **28** out of 256 bits.

IV	6a09e667	db1bb914	3c6ef372	a54ff53a	510e527f	767b0824	66410f7d	90f7ce64
M	85a83e55	91d3ca9d	a6c2facb	027afd32	000000cb	00000000	9d4a6aba	00000000
	e649c148	4606ae35	6efb18d8	2d6ade8f	1dcb6936	ec995db1	d2ad257b	730f5bb4
M′	85a83e55	91d3ca9d	a6c2facb	027afd32	000000cb	00000000	9d4a6aba	00000000
	e649c148	4606ae35	6efb18d8	2d6ade8f	40c36936	ec995db1	d2ad257b	730f5bb4
diff	**00000000**	**8c300000**	**1d010204**	**52520104**	**c0908122**	**00000000**	**00000000**	**00000000**

- Full collisions faster than 2^{128} : With our method it is possible to find collisions with complexity not exceeding $\mathbf{2^{126.6}}$ hash evaluations (probably $\approx \mathbf{2^{125}}$). Moreover, as opposed to the birthday attack, our approach requires only very small storage (equivalent to less than 2^{20} hashes).

More details:

K.Matusiewicz, S.Contini and J.Pieprzyk, *Weaknesses of the FORK-256 compression function*, IACR ePrint Archive, Report **2006/317**

Thank you!