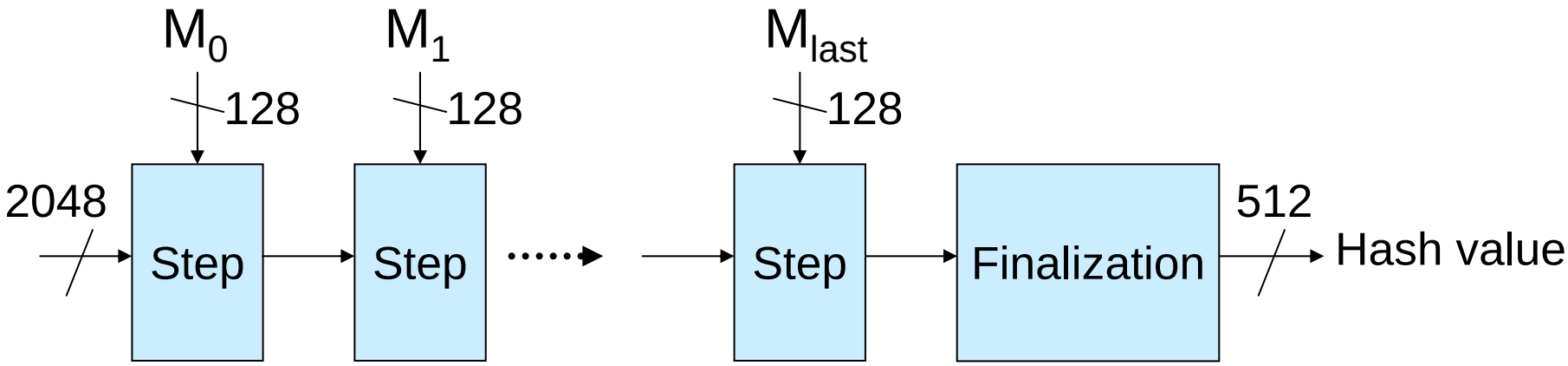
2nd preimage attack on SHAMATA-512

The first SHA-3 candidate conference@Leuven
28th February, 2009

Kota Ideguchi, Dai Watanabe
SDL, Hitachi, Ltd.

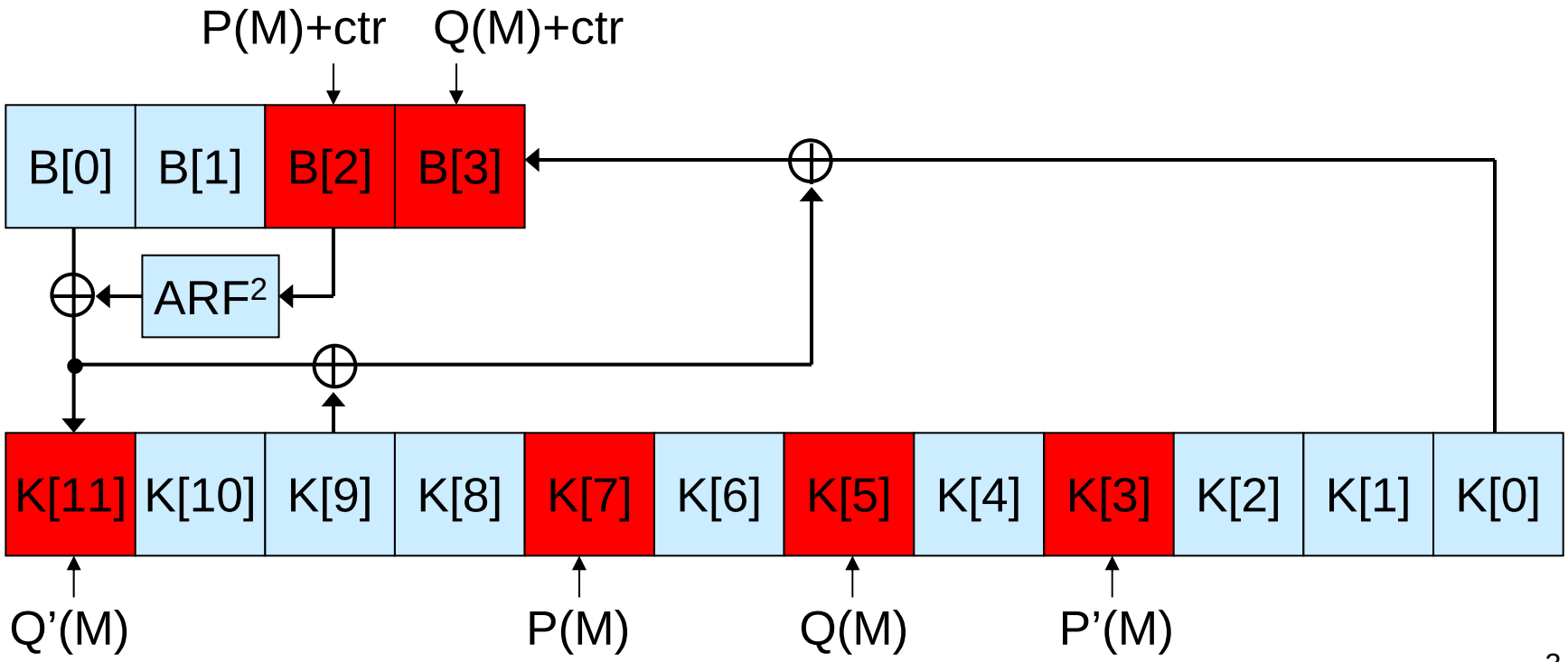
SHAMATA

- A first round candidate of SHA-3 Competition (withdrawn)
  - Designed by A. Atalay, O. Kara, F. Karakoc and C. Manap
- A register based hash function
- 2048-bit internal state
- Processing a 128-bit message block at each step

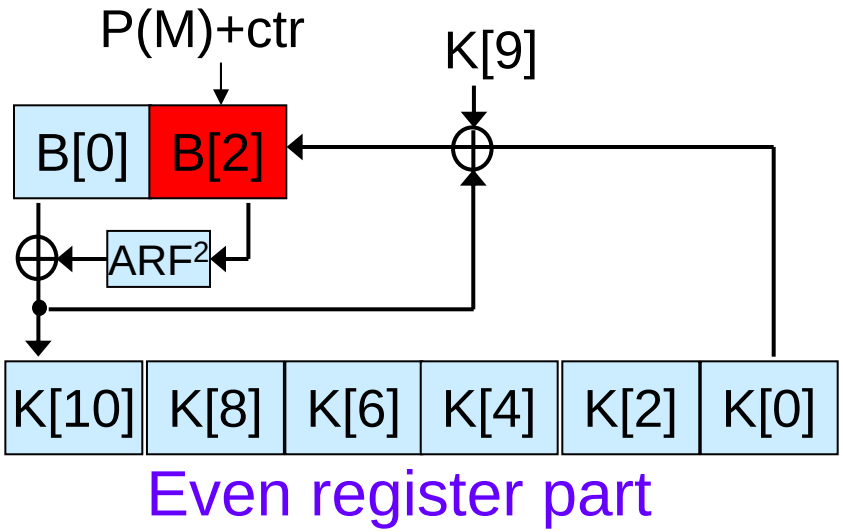


Step Function of SHAMATA-512

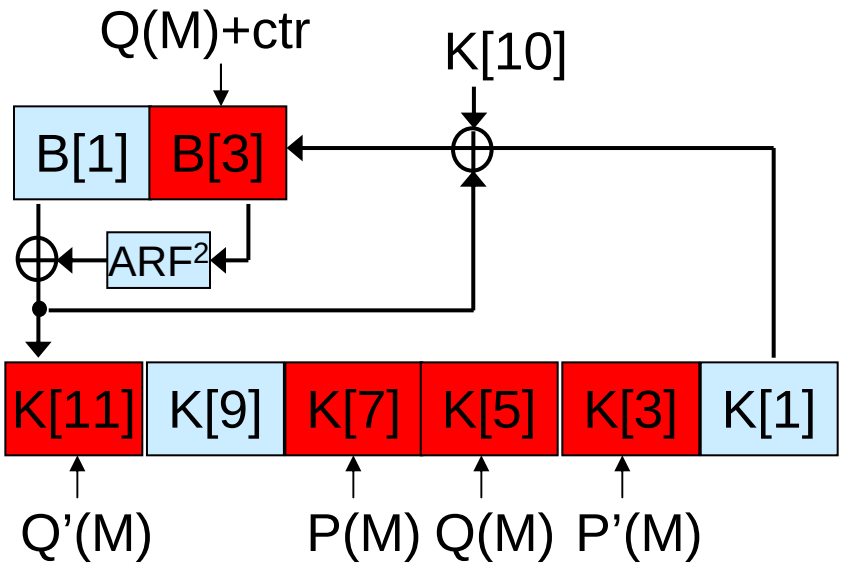
- 2048-bit internal state: 16 128-bit registers
- Step function:
  - Xoring a message block with the red registers
  - Clocking the shift register twice



Another Description of Step Function



Even register part



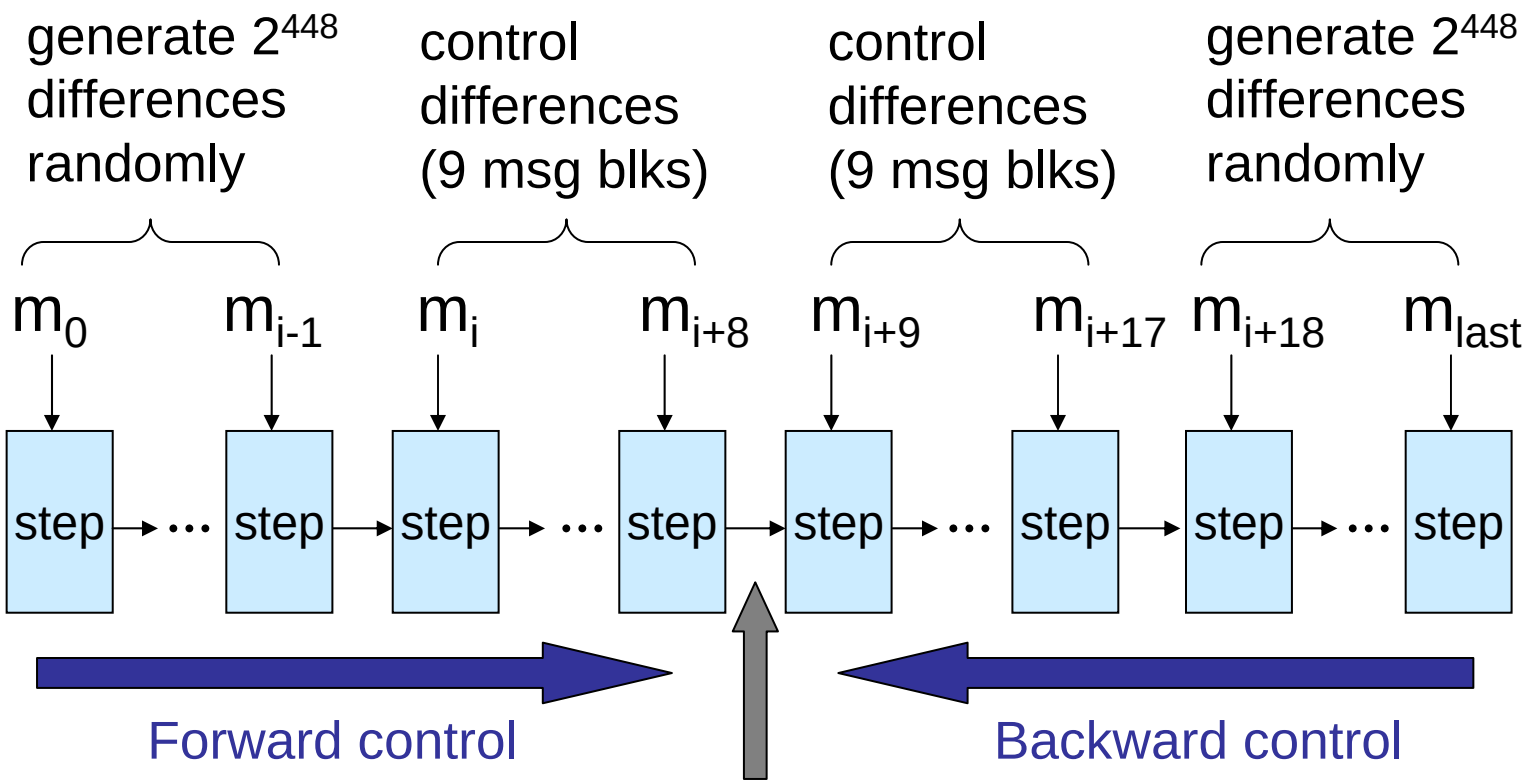
Odd register part

- Divided into two shift registers
  - Even / Odd register part
  - A message block is xored and clocked once.
  - These parts Interact at only two points.

Our attack uses the properties:

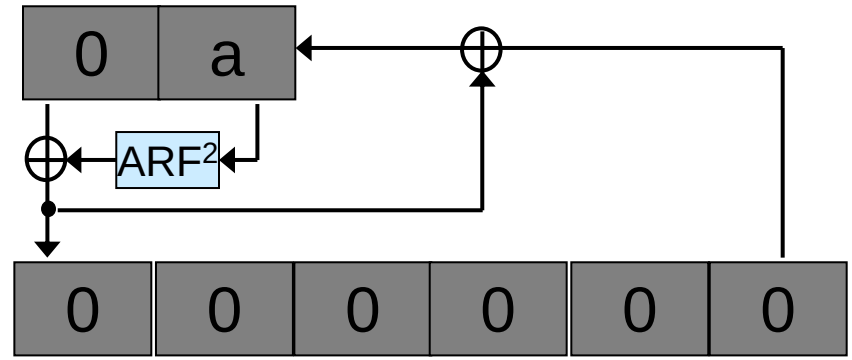
- Only one register is xored with a message block in the even register part.
  - The even register part can be controlled well.
- The same linear transf. of a message block is xored with B[2] and K[7].

Outline of Our Attack

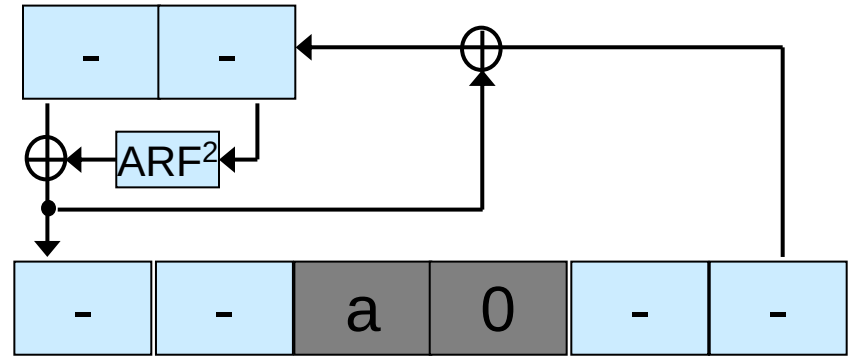


m_i : message block difference between the target message and a 2^{nd} preimage

Internal State Difference at the Meeting Point



Differences of even registers

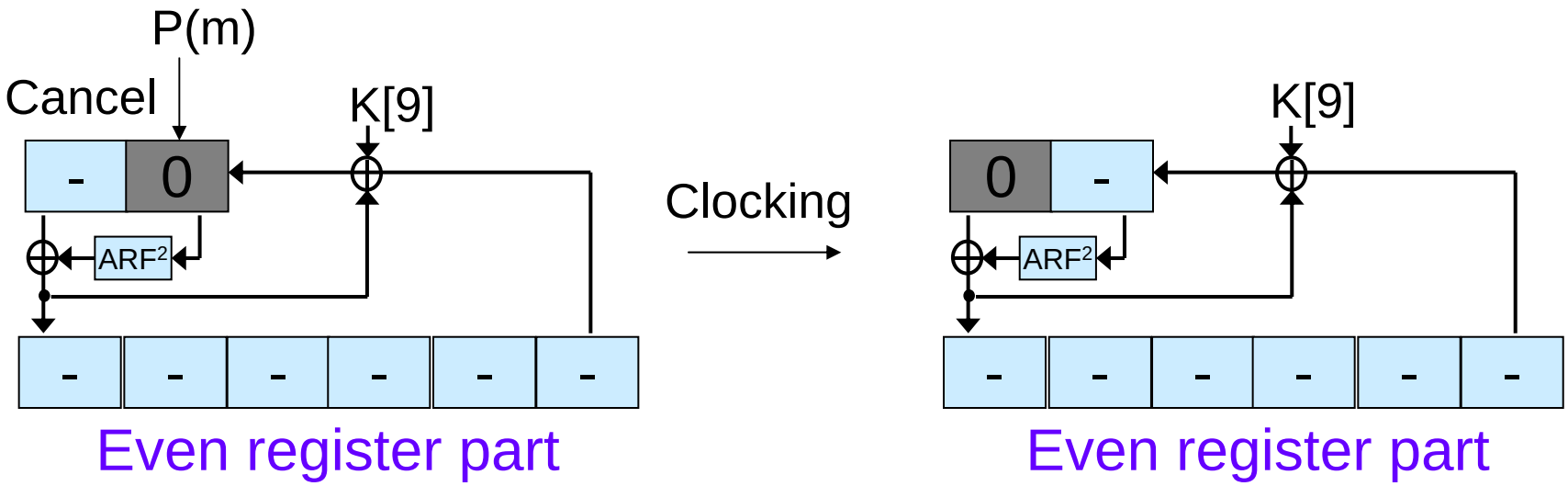


Differences of odd registers

- Eight 128-bit block differences are zero.
- Two block differences are the same as each other.
- Degrees of freedom of the internal state difference is 896 bits.
  - MIM attack can be applied because 896/2 < 512.

Difference Control: Forward

- A message block is set to cancel the value of the register B[2].
- Repeating this 9 times in total, the internal state difference becomes the form of the previous page.



Summary

- Observations
  - The even registers can be controlled well.
  - The same message differences $P(m_i)$ are xored with B[2] and K[7].
- Forward control is simple. Backward control is more complicated, but possible.
- Complexity of the attack
  - Cost to control the difference is negligible.
  - Cost for MIM (DOF of differences: 896 bits)
    - time: $2^{452.7}$ step function evaluations
    - memory: $2^{452.7}$ 128-bit blocks
- More details:

  http://www.sdl.hitachi.co.jp/crypto/eval/shamata_2ndPI.pdf