A Hash Function Family *Luffa*

@The First SHA3 Candidate Conference
25th February 2009

Dai Watanabe
Hisayoshi Sato

Systems Development Laboratory,
Hitachi, Ltd.

Christophe De Canniére

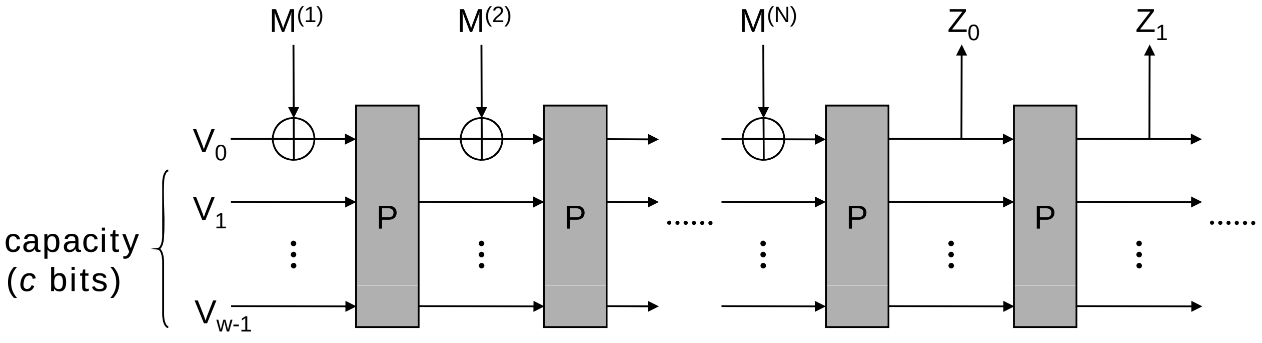
ESAT-COSIC,
Katholieke Universiteit Leuven

Outline

- Specification
  - Chaining
  - Non-linear components
- Security status
  - Generic attack
  - Differential based attack
- Implementations
  - Software
  - Hardware

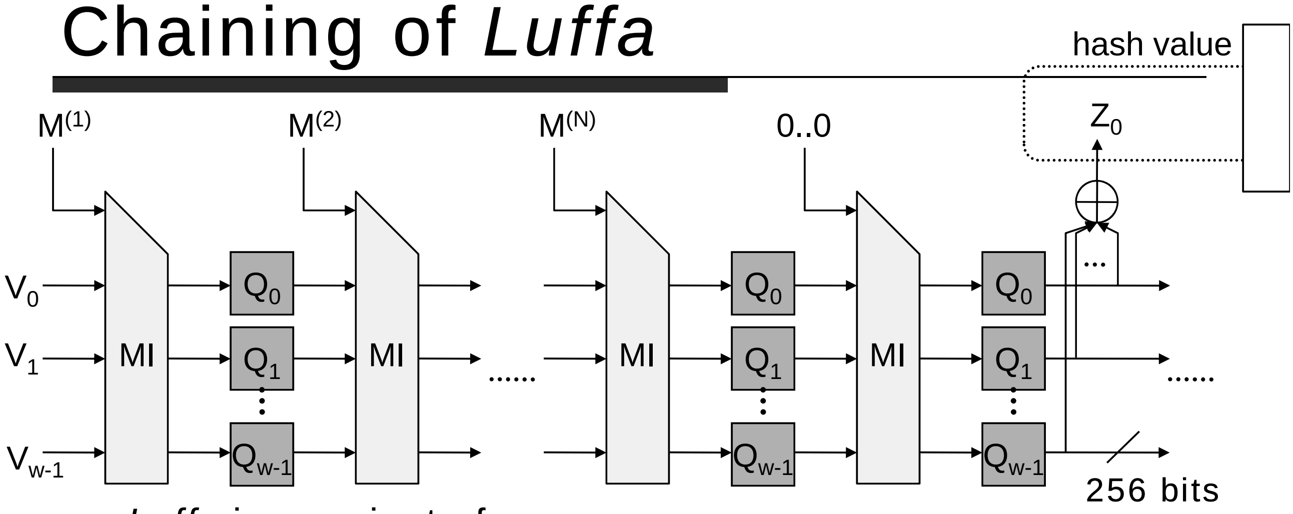
Introduction to *Luffa* (spec.)

Cryptographic sponge function



- Newer coming construction of a hash function from a random permutation
- It is indifferentiable from a RO

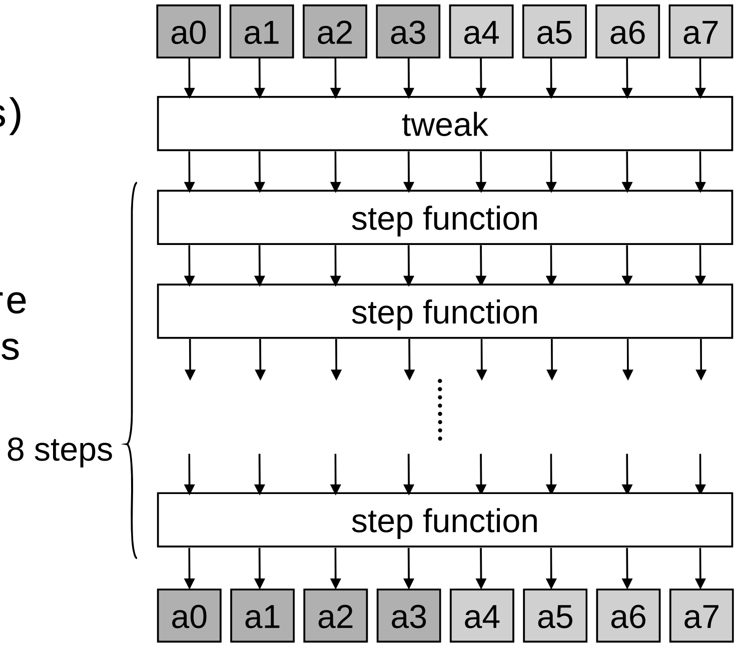
Chaining of *Luffa*



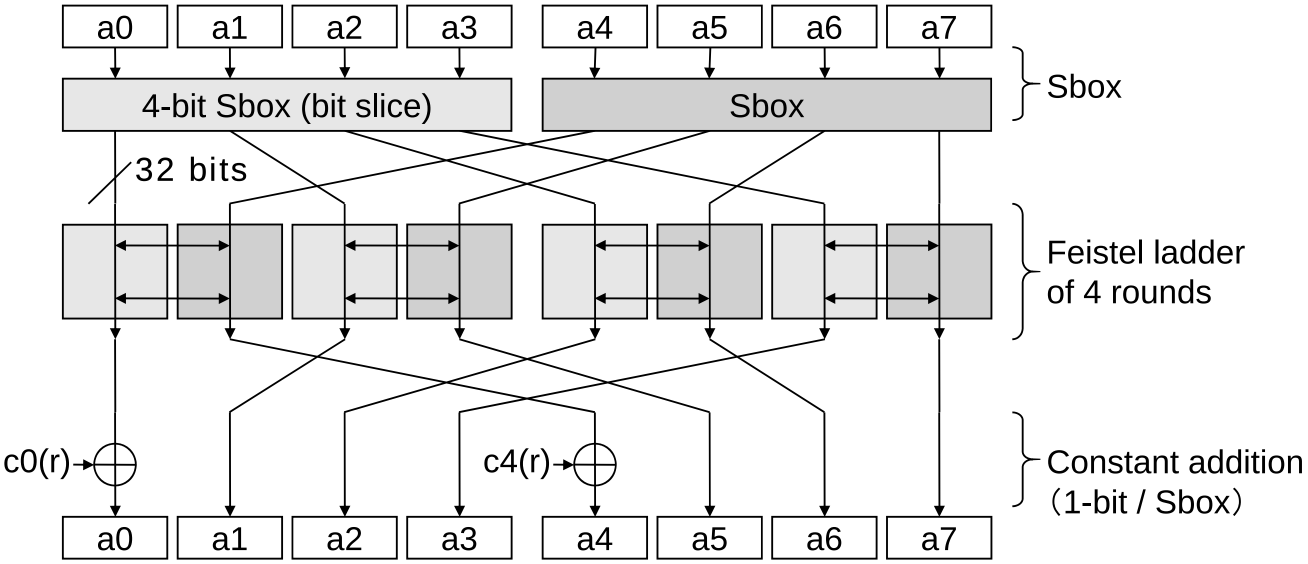
- *Luffa* is a variant of sponge
  - But, fixed length permutations for all hash length
    - The number of Qj increases if the hash length gets long (w=3, 4, 5 for hash_len=256, 384, 512)
  - Insert message and mix the state by the linear map MI
  - A blank round
  - The hash value is the sum of the outputs of Qj

Non-linear permutation Q

- Input/Output
  - 256 bits (8 32-bit words)
- Functions
  - tweak
    - Applied before step functions
  - Step functions
    - 8 steps



Step function



Sbox

Feistel ladder
of 4 rounds

Constant addition
（1-bit / Sbox）

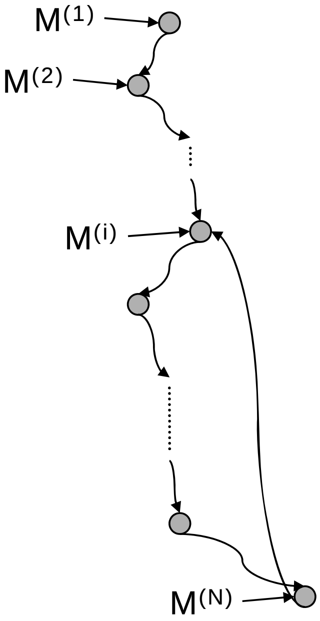
Security status

Summary of security status

- Sponge function features
  - Not based on CR compression function
  - Finding inner collision is the best attack
- Current security status of *Luffa*
  - No security proof for the chaining (yet)
  - Several generic attacks concerned, none of them are serious
  - Differential based attack
    - Seems secure under a reasonable assumption

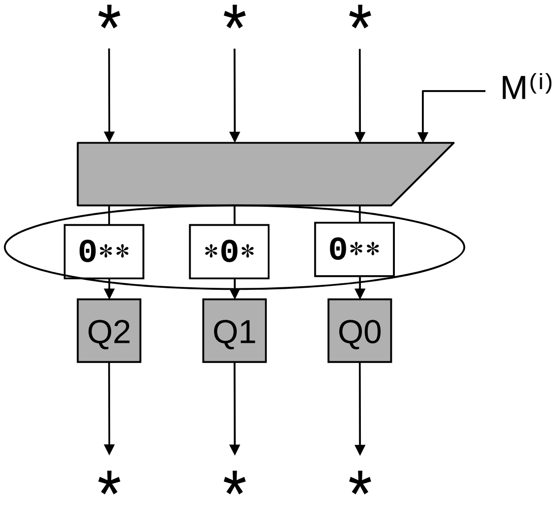
Long message attack

- Sponge's case
  - Finding a message s.t. $S^{(i)}=S^{(N)}$
  - Prob. of the event
    - capacity: c=len(S)–len(M)
    - prob=$2^{-c/2}$
  - Complexity
    - Queries to the permutation: $2^{c/2}$
    - Num. of nodes: $2^{c/2}$



Long message attack (conti.)

- Luffa’s case
  - 1/w of input bits to each Qj is controllable by message injection
- Complexity
  - Queries to Qj
    - $2^{(w-1)/w*256}$
  - Num. of nodes
    - $2^{(w-1)/2*256}$
  - Calc. Complexity
    - MA: $2^{(w-1)/2*256}$
    - MI calls: $2^{(w-1)/2*256}$

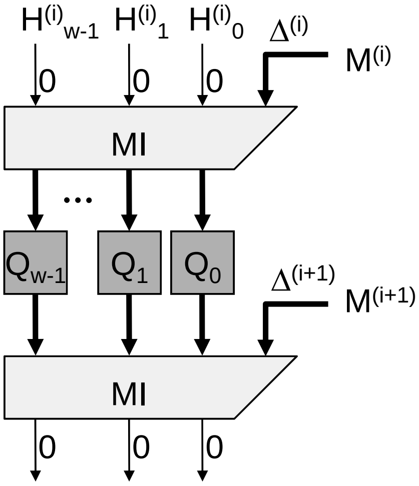


Differential characteristics of Qj

- 4 steps (half-block)
  - Approach: exhaustive truncated path search
  - Possible min. num. of active Sbox: 31
  - MDCP $\leq 2^{-62}$
- 8 steps (full)
  - Approach: Leon’s algorithm to find the lowest code word
  - Min. active Sbox = 112
  - DCP = 2^{-224} ($>2^{-256}$)
  - Not useful to find an inner collision

Differential based attack scenario

- (Seems) the best scenario
  - 2 rounds attack to find an inner collision
- Limitation of modification technique
  - Assumption
    - 1 bit modification doubles the diff. prob.
  - Message block $M^{(i)}$
    - Any, up to 256 bits
  - State $H^{(i)}$
    - Assumed random, up to (w-1)/2*256 bits
- (Our) conclusion
  - *Luffa* is secure against this attack if MDCP(Qj)<2^{-171}



Implementation aspects

Software implementations

hash length	ANSI C (cycle/byte)		assembly with SSE2 (cycle/byte)	
	32-bit	64-bit	32-bit	64-bit
224	33.9	32.0	13.9	13.4
256	33.4	32.0	13.9	13.4
384	45.2	39.0	15.7	15.2
512	59.7	50.3	25.5	23.2

- Evaluation environment
  - CPU：Intel Core2Duo E6600 (2.4GHz)
  - Memory: 2GB
  - ANSI-C: Windows Vista + Visual Studio 2005
  - Assembly: Ubuntu Linux 8.04 + gas

Hardware implementations (ASIC)

Hash length (bit)	Opt.	Gate count (gate)	Frequency (MHz)	Cycles	Throughput (Mbps)
256/224	size	10,157	100	891	28.7
256/224	speed	26,849	444	9	12,642
384	speed	34,985	444	9	12,642
512	speed	44,163	444	9	12,642

- Evaluation environment
  - 0.13μm CMOS standard cell library
- Optimization
  - Small gate size: with 1 Sbox and 1 MixWord
  - Speed: 3 step functions in parallel