Update on *Luffa*

@The Second SHA3 Candidate Conference
24th August 2010

Dai Watanabe
Hisayoshi Sato

Systems Development Laboratory,
Hitachi, Ltd.

Christophe De Cannière

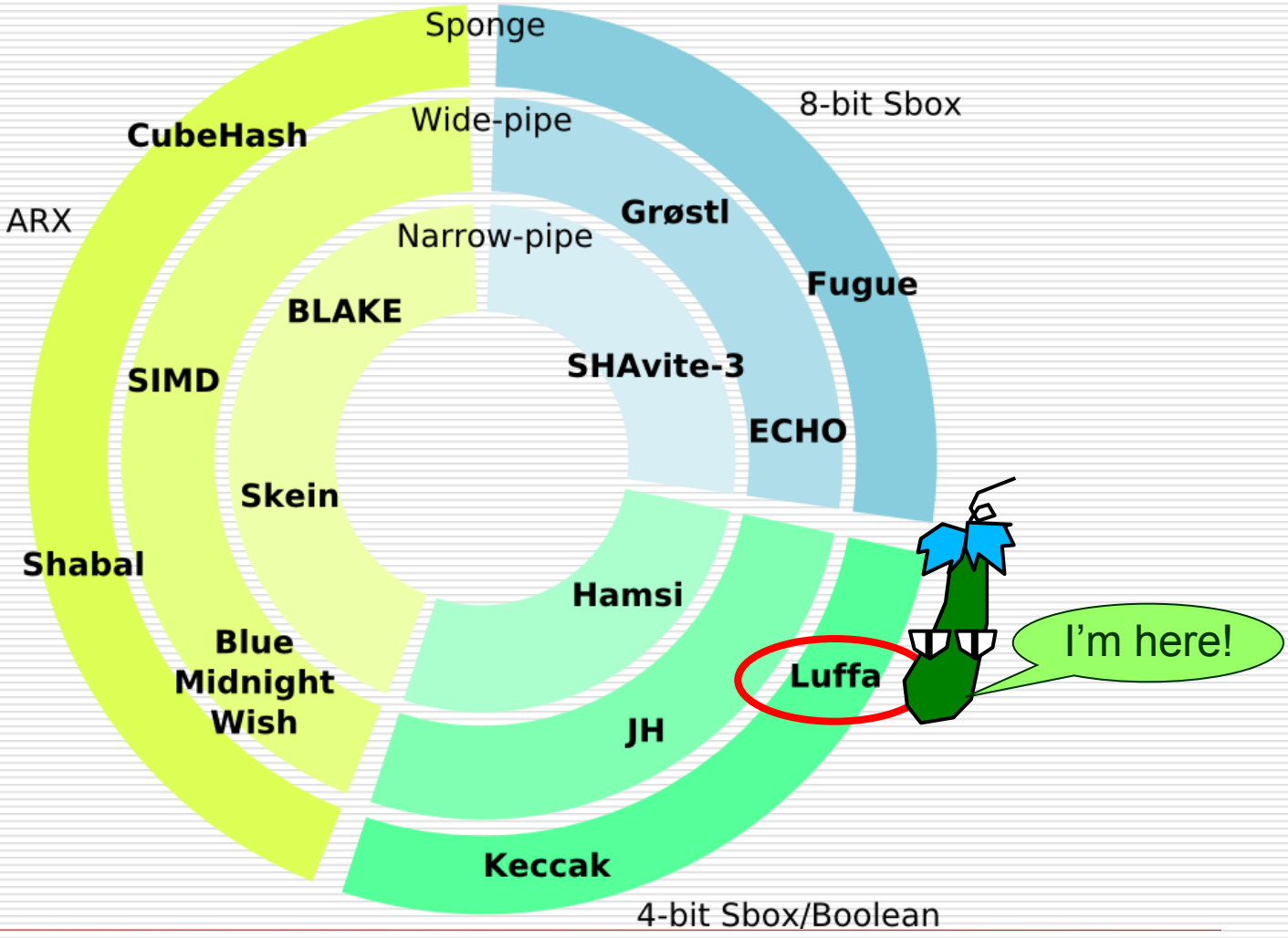
ESAT-COSIC,
Katholieke Universiteit Leuven

Outline

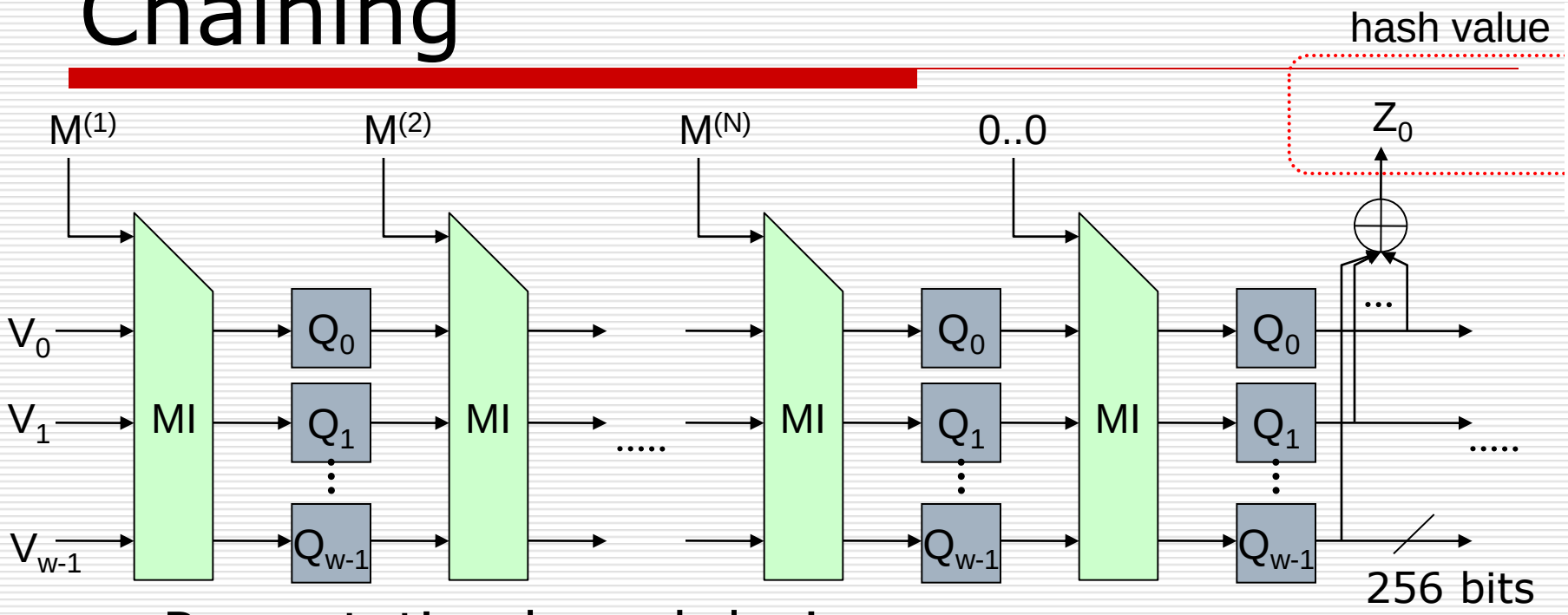
- Introduction to Luffa
- The specification changes
- Security status
- Implementation aspects

Running through *Luffa*

Where is Luffa?



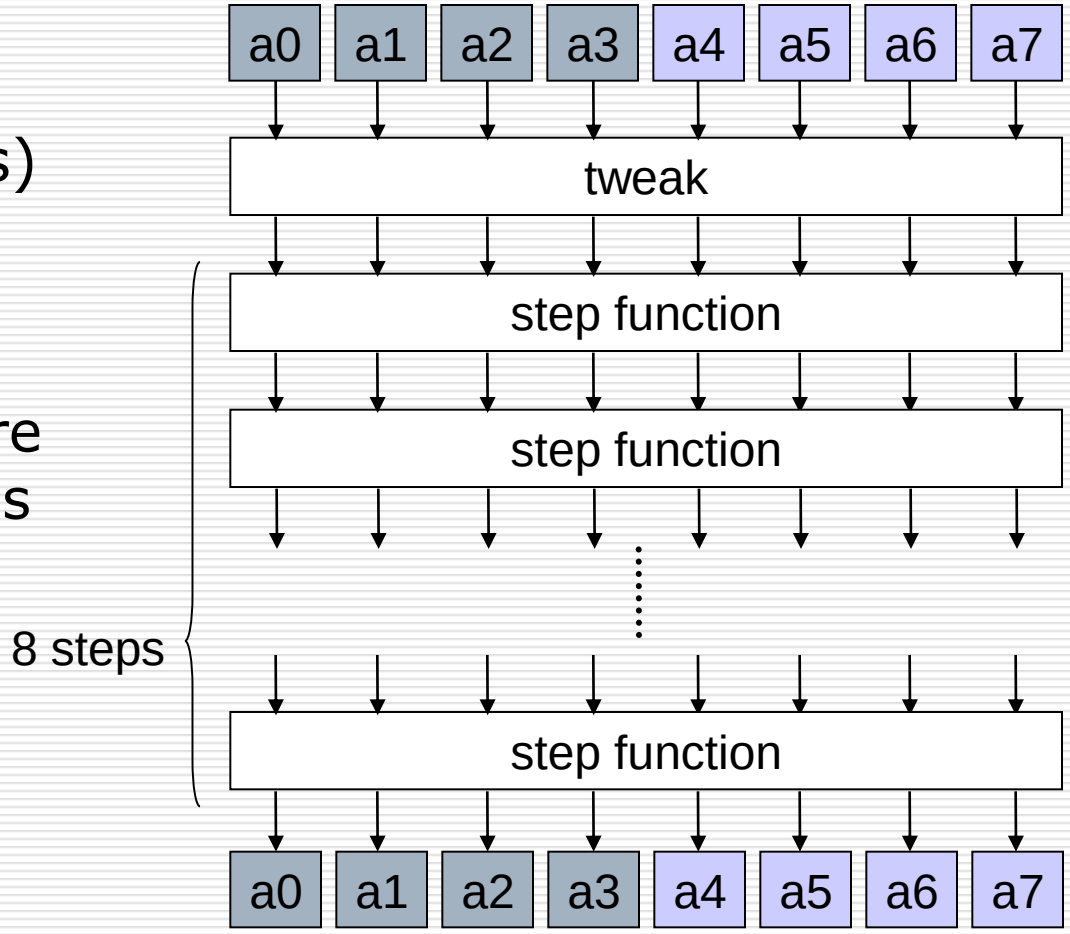
Chaining



- Permutation based design
- Fixed length permutations for all hash length
  - An MDS code is applied to mix the internal states and a message block
  - Similar to Knudsen-Preneel construction of a CF
- The hash value is the sum of the outputs of Qj

Non-linear permutation

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



Specification changes

- Application of a blank round
  - Ver.1: If the message length > 255
  - Ver.2: Always
- SubCrumb
  - The table
    - v1: {7, 13, 11, 10, 12, 4, 8, 3, 5, 15, 6, 0, 9, 1, 2, 14}
    - v2: {13, 14, 0, 1, 5, 10, 7, 6, 11, 3, 9, 12, 15, 8, 2, 4}
  - The order of the inputs
    - v1: SubCrumb(a[4], a[5], a[6], a[7]);
    - v2: SubCrumb(a[5], a[6], a[7], a[4]);

Updates on security status

Security of the permutation

- Not ideal from the beginning
  - Differential path with prob. 2^{-224} [in the proposal 2008]
- Later coming results
  - Zero-sum with 2^{82} comp. [Aumasson and Meier 2009]
  - Rotational property with $2^{116.3}$ comp. [Khovratovich et al. 2010]
  - Algebraic degree < 256 [Boura et al. 2010]

Attacks under relaxed settings

- Free-start setting
  - Second preimage attack (generic)
    - 1 comp. [Jia 2009]
  - Preimage attack (generic)
    - $2^{128}/2^{171}$ comp. for Luffa-256/512 [Jia 2009]
- Semi-free-start setting
  - Collision attack (generic) $2^{256*w/w-1}$ comp. [Ourselves 2009]
  - Collision attack (rebound) 2^{102} comp. for 7-steps of Luffa-256 [Khovratovich et al. 2010]

Attacks on reduced round variants

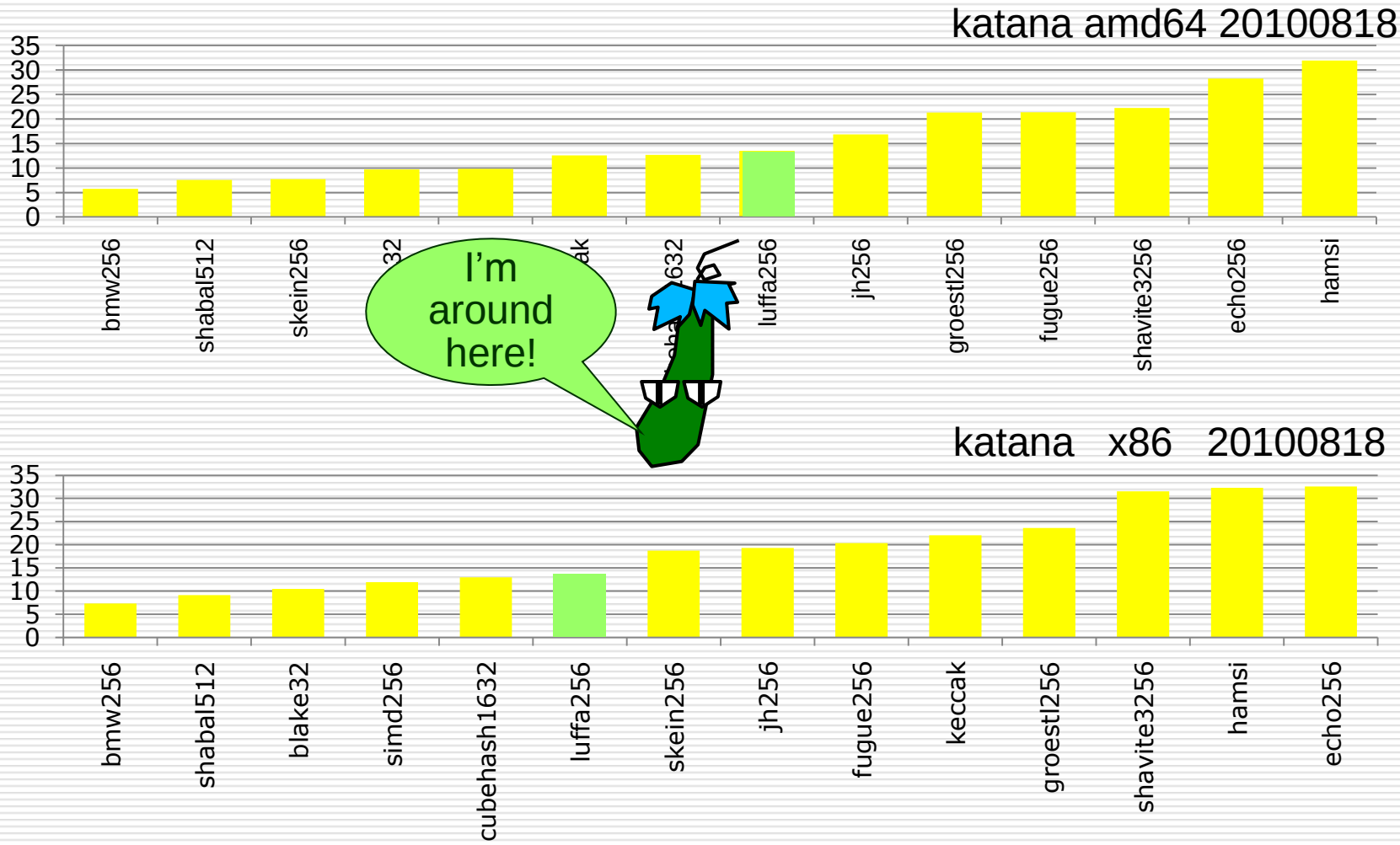
- Collision attack
  - Ongoing differential based analyses on Luffa-256 [Ourselves TBC]
    - 4 steps with 2^{90} comp.
    - 5 steps with $2^{216.2}$ comp.
- Distinguisher
  - HOD on 7 out of 8 steps of Luffa-256 v1 (no blank round) with 2^{216} comp. [Ourselves 2009]

Security margin?

- Differential probability of the permutation
  - If MDP < $2^{-170.7}$, it is hard to find an internal collision faster than the generic attacks for *n*-bit security.
  - MDP < 2^{-128} is sufficient for *n*/2-bit security.
  - For the best known differential path, dp=2^{-224}.
- Interpretation of a semi-free-start attack
  - Khovratovich's rebound attack (2^{102}) borrowed 512 bits of freedom from the internal state.

Implementation aspects

Some eBASH results



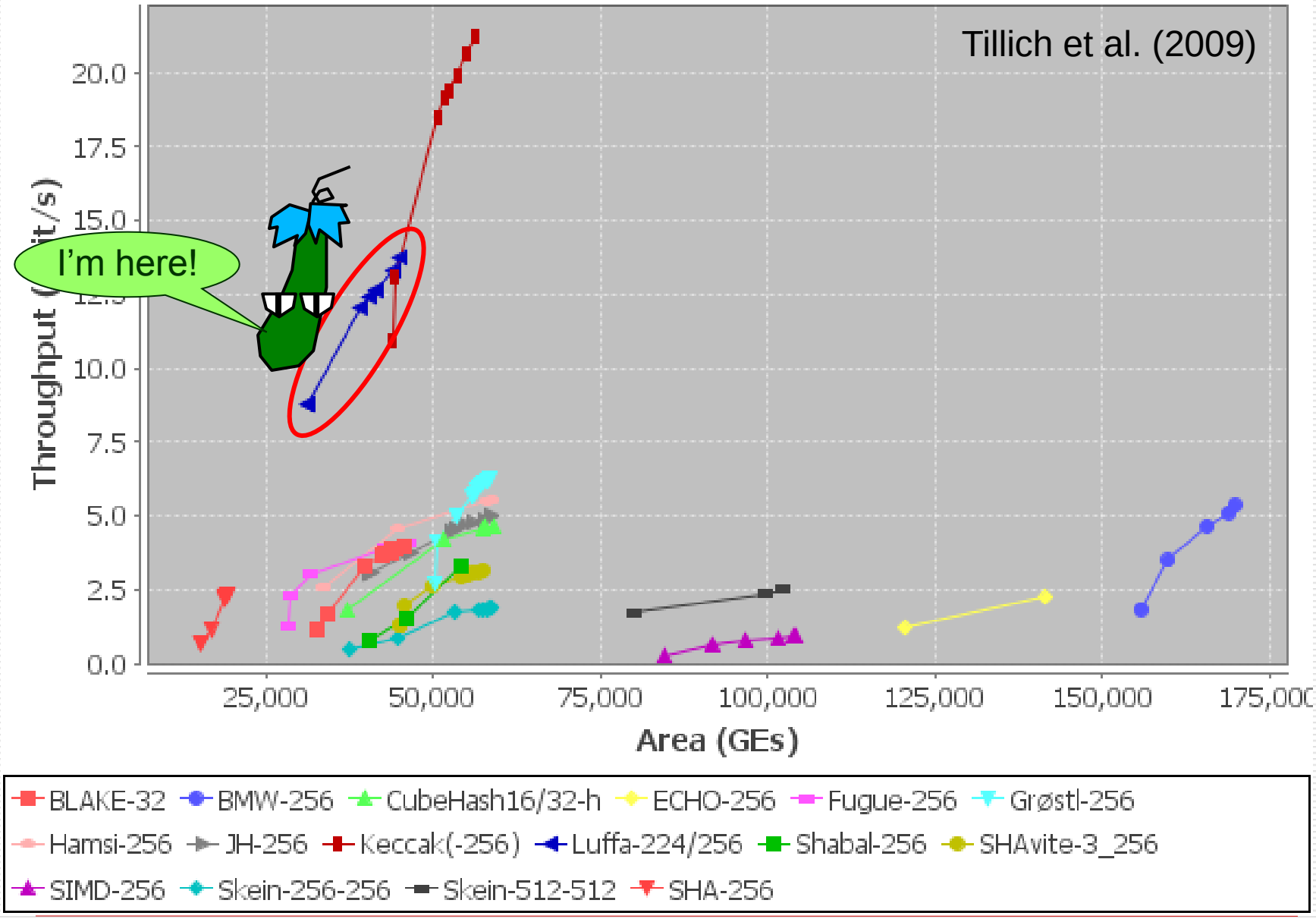
More on software performances

- NIST platform (64-bit mode)

	[Ourselves 2009]	[Oliveira and López TBC]
	ASM	C with SSE intrinsics
Luffa-256	13.3	11.75
Luffa-384	15.0	14.78
Luffa-512	23.8	19.81

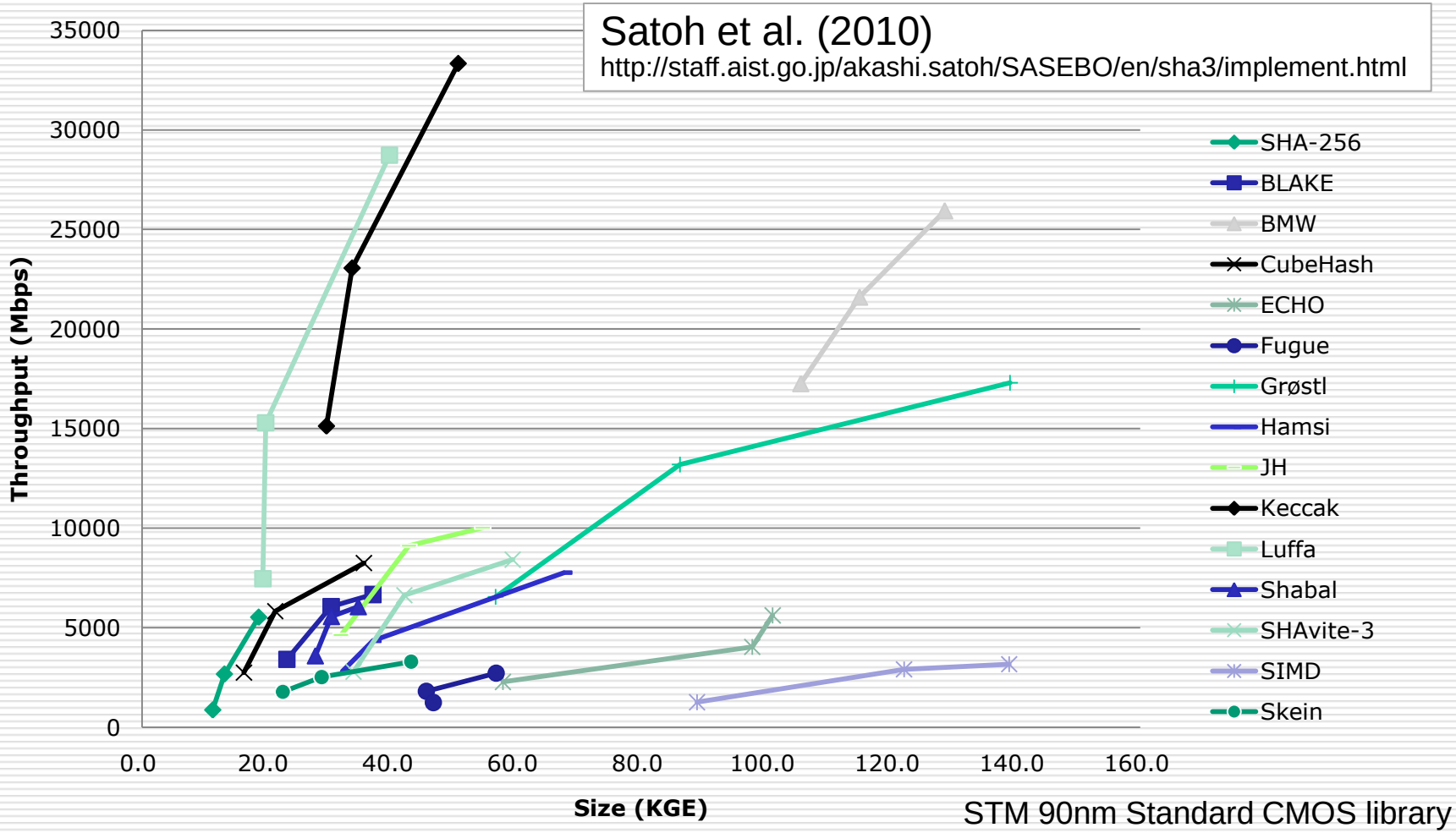
- 8-bit microprocessor [Ourselves 2009]
  - Luffa-256 on Atmel ATmega8515
  - Speed: 732.1 cycles/byte
  - Memory: 688 bytes code, 120 bytes constants, 134 bytes RAM

SHA-3 High-Speed Hardware



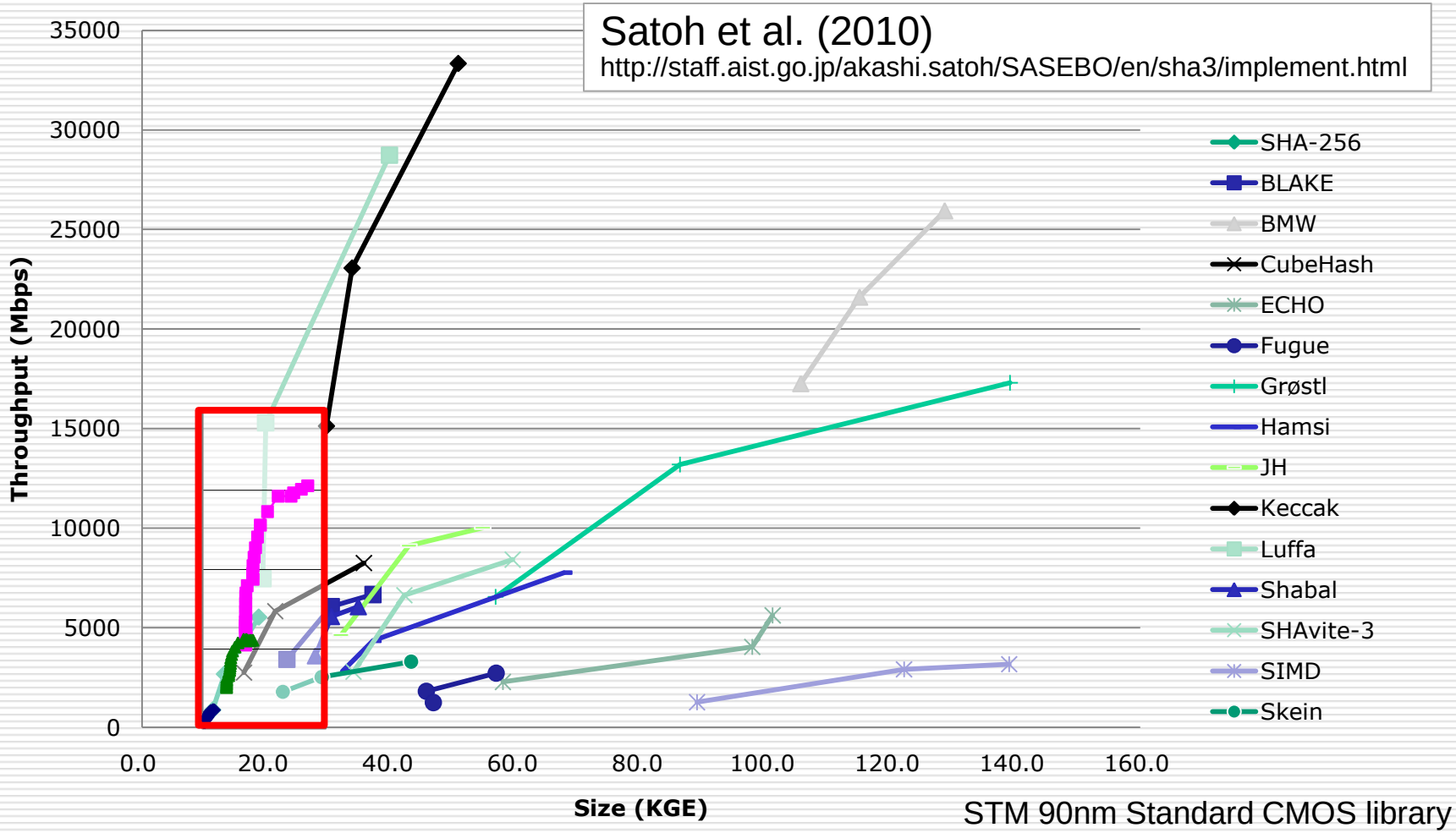
Update on *Luffa*
C. De Cannière, H. Sato, D. Watanabe

Another High-Speed Hardware

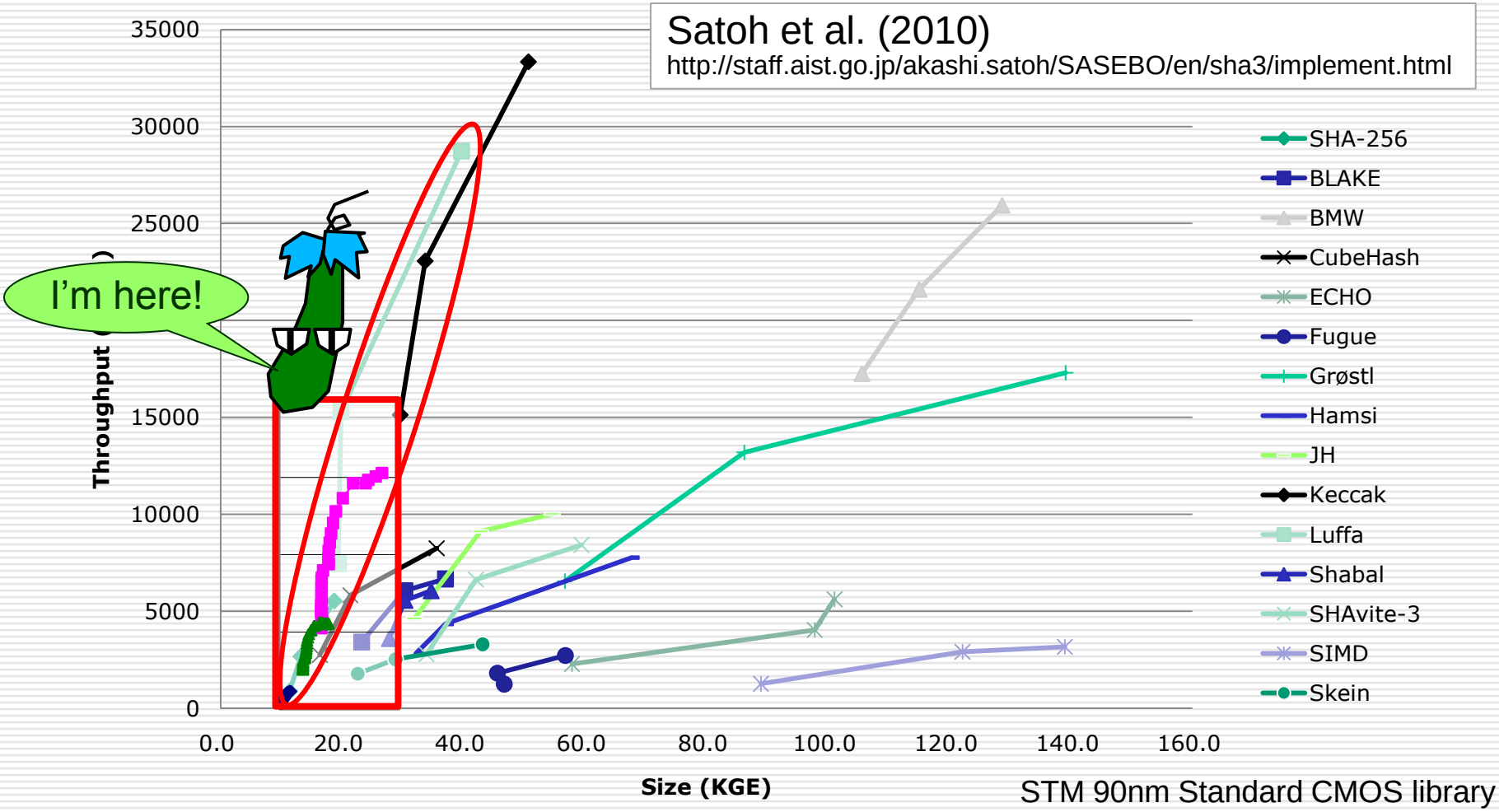


STM 90nm Standard CMOS library

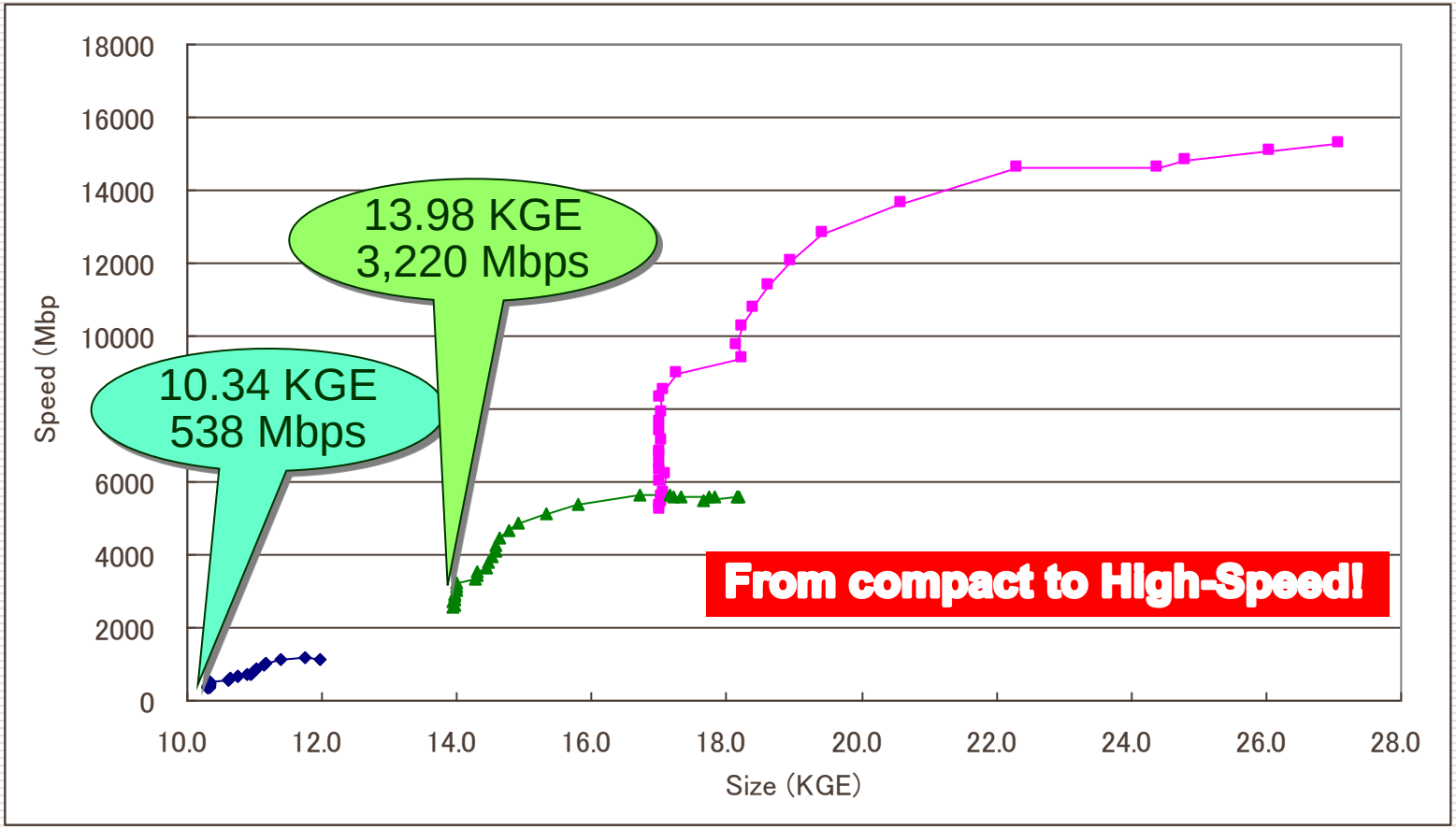
Another High-Speed Hardware



Another High-Speed Hardware



Compact HW implementations



TSMC 90nm Standard CMOS library

Summary


No security flaw


Moderate software speeds


Very good hardware performances

- 
  Fast!
- 
  Compact!

Summary

- No security flaw
- Moderate software speeds
- Very good hardware performances
  - Fast!
  - Compact!

Thank you for attention!

See our web site for the most recent results.
http://www.sdl.hitachi.co.jp/crypto/luffa/