The ECHO hash function

Ryad Benadjila, Olivier Billet, Henri Gilbert, Gilles Macario-Rat, Thomas Peyrin, Matt Robshaw, and Yannick Seurin

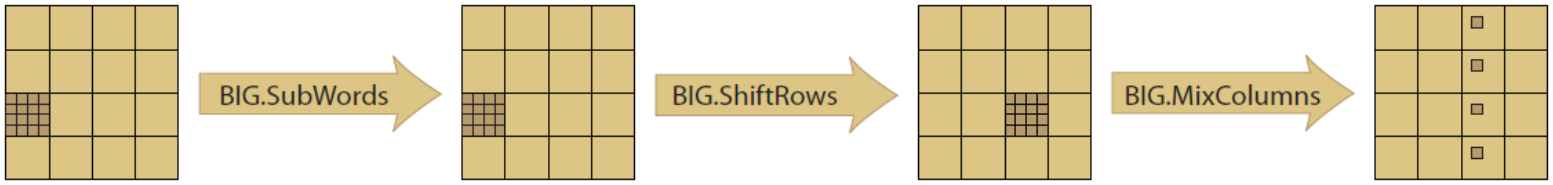
Second NIST SHA-3 conference

Santa Barbara – August 23, 2010

Outline

Outline

Description



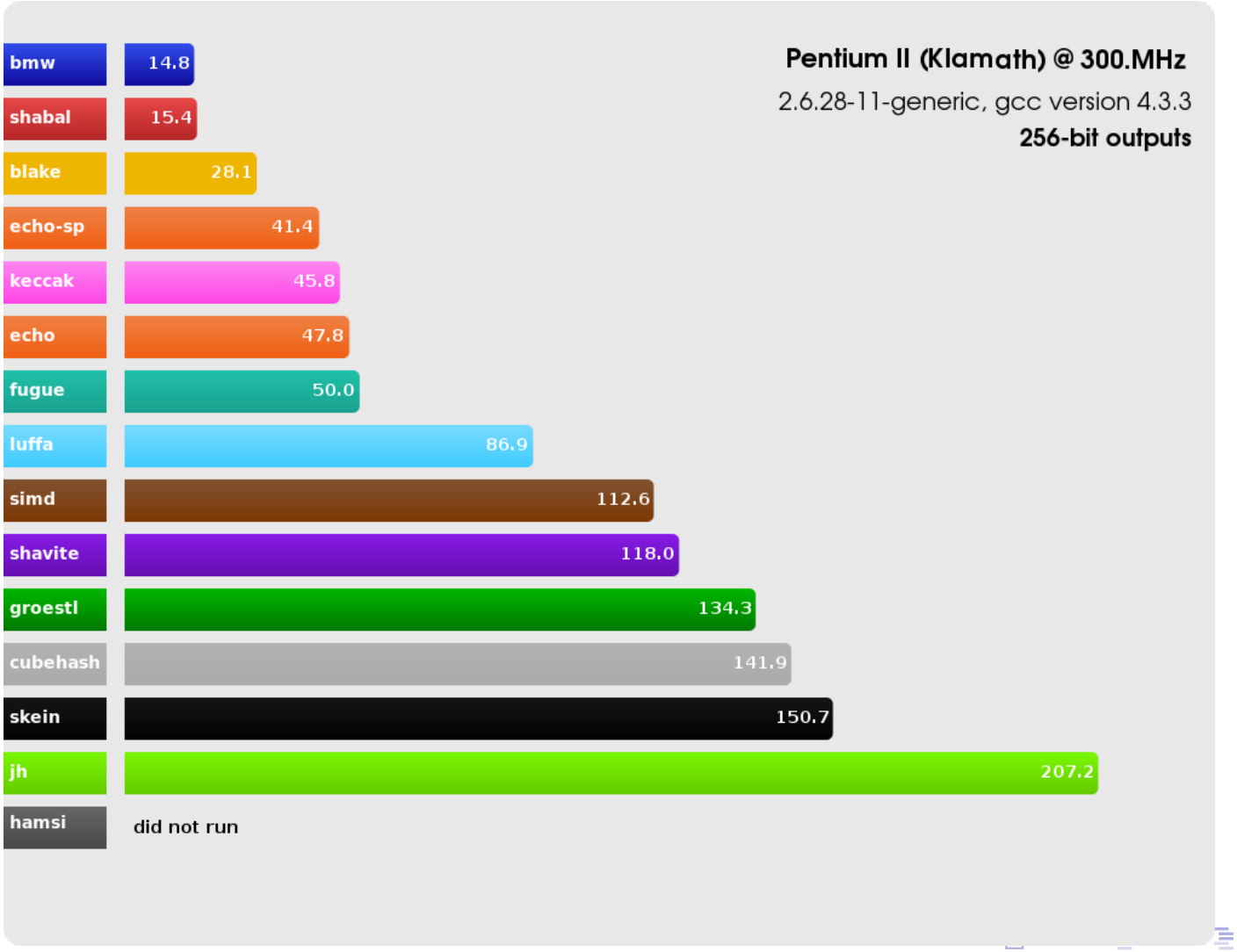
What is ECHO ?

- HAIFA domain extension algorithm + double pipe
- AES-based (reuses full AES rounds and mimics the AES structure)
- clean and simple (to understand, to implement, to analyze)
- same implementation for 256-bit and 512-bit versions
- same implementation for double/simple pipe mode

Outline

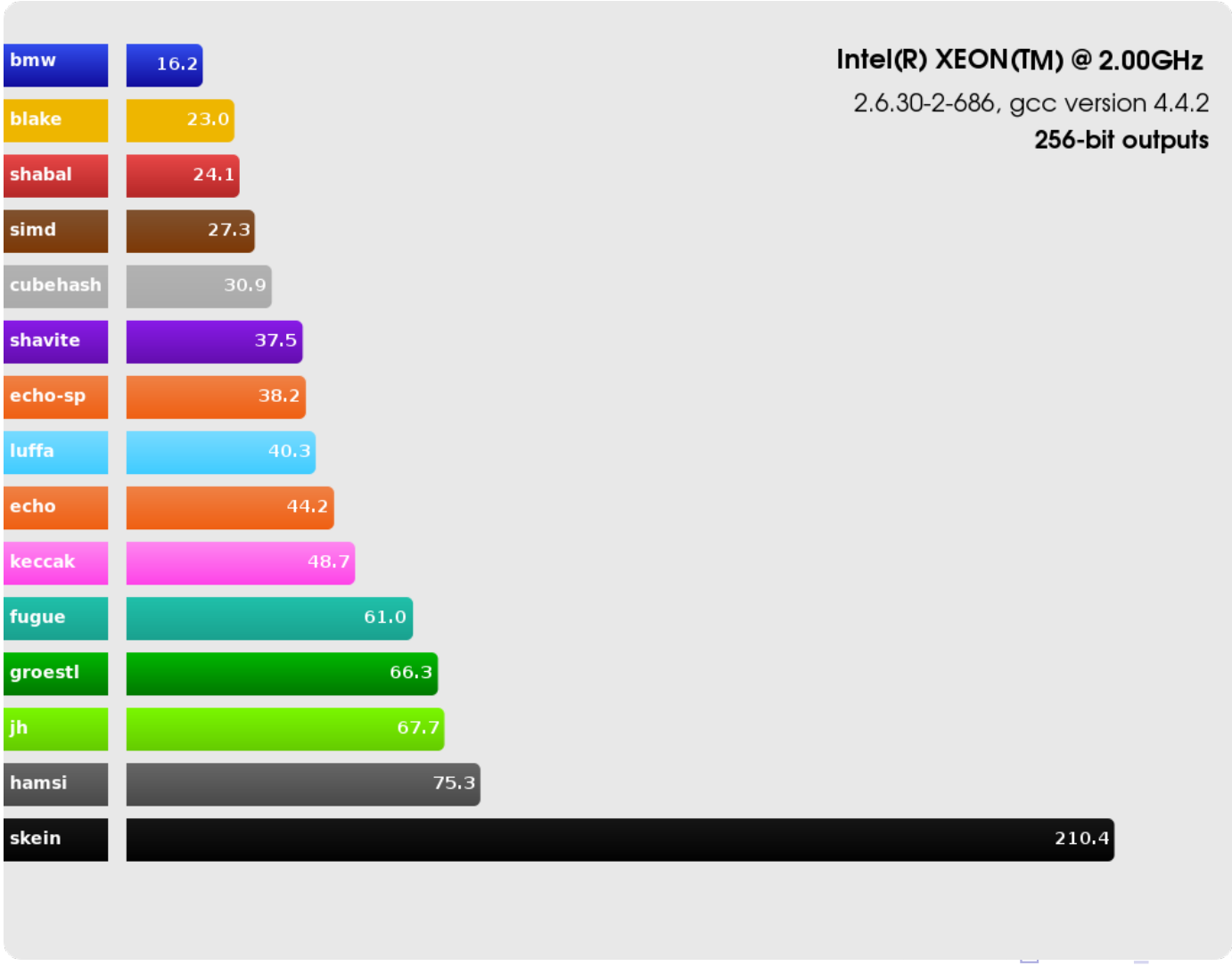
Software

- **legacy processors:**
  good performance (low cache overhead)



Software

- **legacy processors:**
  good performance (low cache overhead)



Software

- **legacy processors:** good performance (low cache overhead)
  - many candidates get good performance on the NIST platform (they exploit all the cache available) ...
  - ... but by going back just one generation of processors, some are severely penalized
- **Core 2 Duo:** average performance
- **current processors (AES-NI):** **one of the fastest candidates**

Example with Core i5 (see eBash or our AES-NI page):

ECHO-256: **6.8 c/B**, ECHO-512: **12.6 c/B**
ECHO-SP-256: **5.8 c/B**, ECHO-SP-512: **8.4 c/B**

Hardware

ECHO offers a wide range of HW size/speed tradeoffs:

- **high throughput:**
  one of the fastest FPGA candidates (26.5 Gbit/s - our website)
  one of the fastest ASIC candidates (14.8 Gbit/s - Lu et al.)
- **lightweight:** only 127 slices + 1 memory block on Virtex 5 and even smaller for ECHO-AES coprocessors (Beuchat et al.)
- **balanced throughput/area:** use of BRAM allows high throughput for small/medium area (Francq et al.)

Note: in general, ECHO−SP, the simple pipe mode, is faster than the double pipe:

- by a factor 1.16 for the 256-bit version
- by a factor 1.5 for the 512-bit version

Outline

Security

- **untweaked** (only 6 other schemes untweaked)
- **double-pipe security** (only 6 other schemes with full double-pipe security)
- **well analyzed:** SAC 2009, FSE 2010, CRYPTO 2010, SAC 2010, SHA-3 conference
- **the simple design encourages the analyst to try a wide-range of old and new techniques:**
  - truncated differential paths
  - rebound attack
  - start-from-the-middle attack and improved variants
  - super-Sbox attack and improved variants
  - multiple inbounds attack
- **Unlike many other candidates, analysis confirms that the hash and the compression function offer a substantial margin for security**

Cryptanalysis

		ECHO		ECHO-SP	
		256-bit	512-bit	256-bit	512-bit
compression function	collision	**38%**	**25%**	**38%**	**30%**
	distinguisher	**87%**	**70%**	**75%**	**70%**
hash function	collision	**50%**	-	-	**40%**
	distinguisher	**63%**	-	-	**50%**

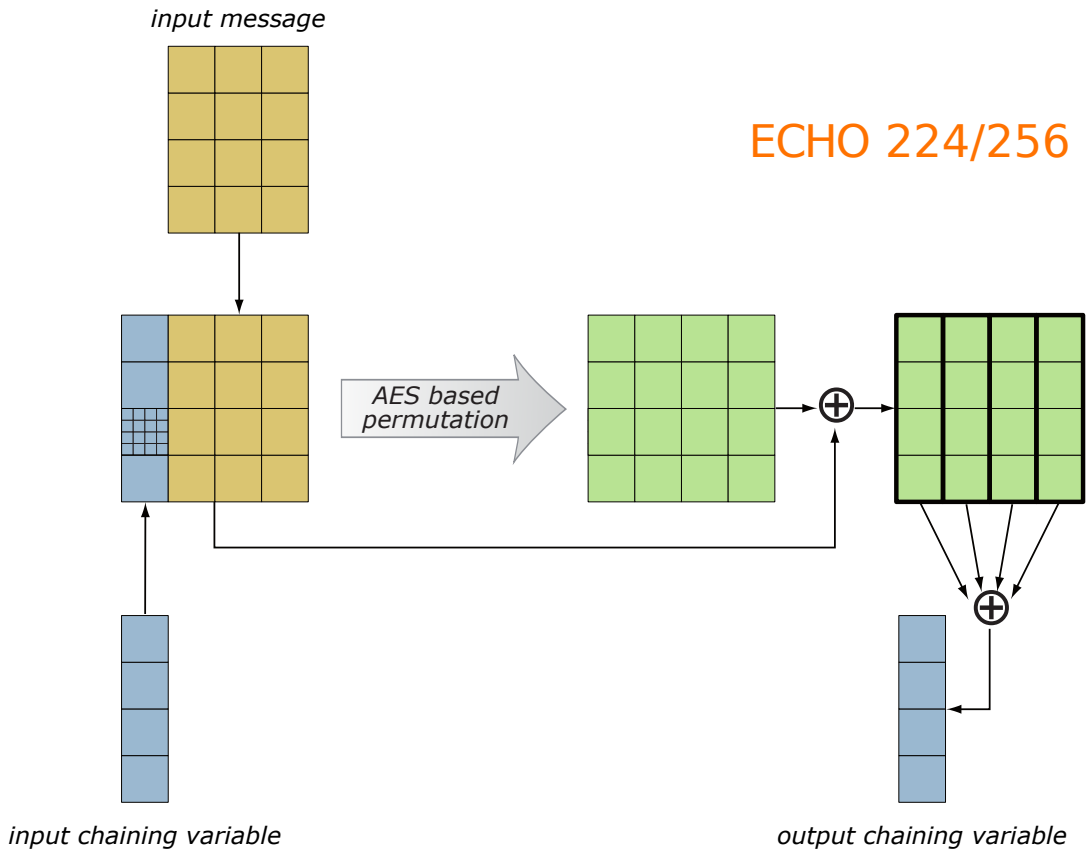
Current best cryptanalysis

In chosen-salt setting:

- collision attack against ECHO-512 compression function reduced to 3 rounds

Cryptanalysis

Distinguishers on internal permutation are interesting, but absolutely not a danger (because of the final folding phase)



Cryptanalysis

We improved our active Sboxes proofs:

number of rounds	best known diff. path	old		new	
		bound	gap	bound	gap
1	5	5	0	5	0
2	40	25	15	40	0
3	60	45	15	60	0
4	200	125	75	200	0
5	250	130	120	205	45
6	285	150	135	240	45
7	320	170	150	260	60
8	445	250	195	400	45

The paths used for the attacks are almost optimal.

Outline

Summary

- **Simple**, **elegant**, **flexible**, easy to understand/implement
- **Performance:** good in every situation, exceptional in some
  - current processors (AES-NI)
  - high throughput hardware
- **Security:**
  - untweaked
  - double-pipe security
  - one of the most studied SHA-3 candidates
  - compression function and hash function offer good margin for security
  - strong security arguments: new analysis shows that attackers are already using paths very close from being the best ones ($>$ 400 active AES S-boxes over 8 rounds)