Alternative FPGA Implementations of SHA-3 Finalists

CryptArchi 2011

Julien Francq, Jean-Baptiste Rigaud
julien.francq@cassidian.com, rigaud@emse.fr

CASSIDIAN (Cyber Security Center), ENSMSE

2011, June the 17th

What is SHA?

Cryptographic Hash Functions

- play a fundamental role in modern cryptography
  - data integrity, message authentication, etc.
- map an arbitrary finite length bitstring to a fixed length digest
- should have desirable properties
  - preimage and collision resistance

- NIST Hash Function Standard = Secure Hash Algorithm
- Cryptanalysis of previous SHA families ⇒ SHA-3 Contest

SHA-3 Contest

- Similar to the past AES one.
- 11/2/2007: kick-off.
- 11/31/2008: 64 candidates submitted.
- 12/10/2008: 51 accepted in the 1st round.
- 07/24/2009: 14 semifinalists.

Selection Criteria

- Security, software/hardware cost (ASIC, FPGA), flexibility.

- 12/09/2010: 5 finalists.
  - BLAKE, Grøstl, JH, Keccak, Skein.
- 2012: and the winner is?

Strategies and Challenges

2 ways of studying SHA-3 candidates hardware cost on FPGA

- "Fair and comprehensive comparison" of all the candidates.
  - [Tillich *et al.*, ePrint 2009], [Henzen *et al.*, CHES 2010], [Gaj *et al.*, CHES 2010]
- Investigate hardware optimizations of some ones.

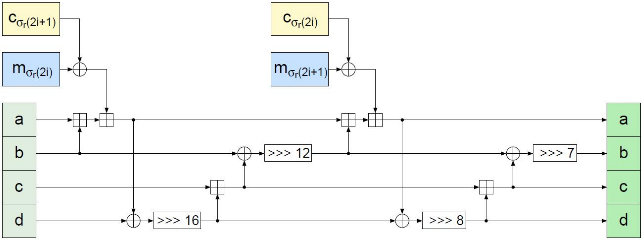
Challenges

- BLAKE: only 1 circuit for all the digest sizes.
- JH: improve throughput (TP) with FPGA Block RAMs (BRAMs).
- Keccak: improve the TP with the "unfolding method".

Outline

Main Characteristics

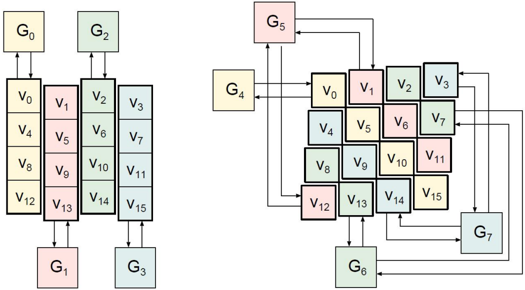
- BLAKE-224, 256: for 32-bit words and 32-byte digests.
- BLAKE-384, 512: for 64-bit words and 64-byte digests.
- Based on tweaked ChaCha
- G_i Function (for BLAKE-224 and 256)



- m: message block, c: constants, σ_r: permutations.
- BLAKE-384 and 512: replace 16 by 32, 12 by 25, 8 by 16, 7 by 11.

Round Function

- Column Step and Diagonal Step



- BLAKE-224, 256: 14 rounds per message block.
- BLAKE-384, 512: 16 rounds per message block.

Goals and Strategy

- Litterature: 2 different circuits for BLAKE-224, 256 and for BLAKE-384, 512.
  ⇒ Implementation cost issues
  ⇒ Goal: Merge them at a low-cost.

The Differences between the 2 BLAKEs

- Words Size
  - Solution: implement a mutualized 64-bit datapath.
  - Need to convert I/O in 32 or 64 bits.
  - Disable the unused part of the datapath (for BLAKE-224, 256).
- Initial Vectors (IVs)
  - Solution: all in ROM and selected with the size digest parameter.
- Rotation Distances
  - Solution: all implemented and selected with multiplexors.

Our Preliminary Results

- VHDL, Xilinx Virtex-5 330T -3, ISE Tools (v13.1i)
- TP (for long messages) $= \dfrac{\text{Message block length} \times \text{Frequency}}{\#\ \text{Clock Cycles per message block}}$
- Post-synthesis results
- Results given only for 4G, but 8G, 2G, 1G also implemented

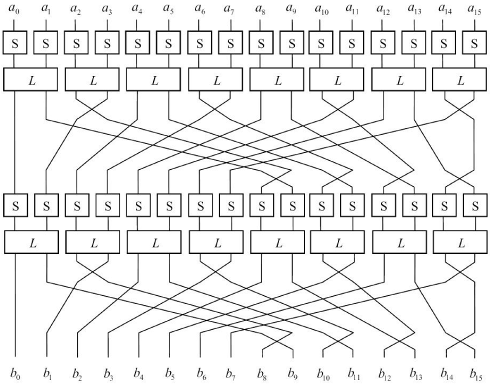
Reference	Size	Area (slices)	Freq. (MHz)	TP (Gbps)
Gaj's team	256	1523	128	3.143
Gaj's team	512	3064	99	3.520
Our work	256	4717	81	1.481
Our work	512	4717	81	2.592

- + 6Kb of ROM

Outline

Round Function

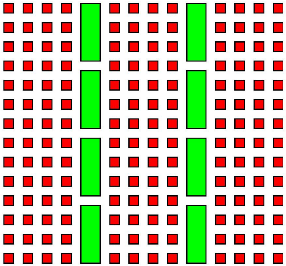
- E computes 42 rounds



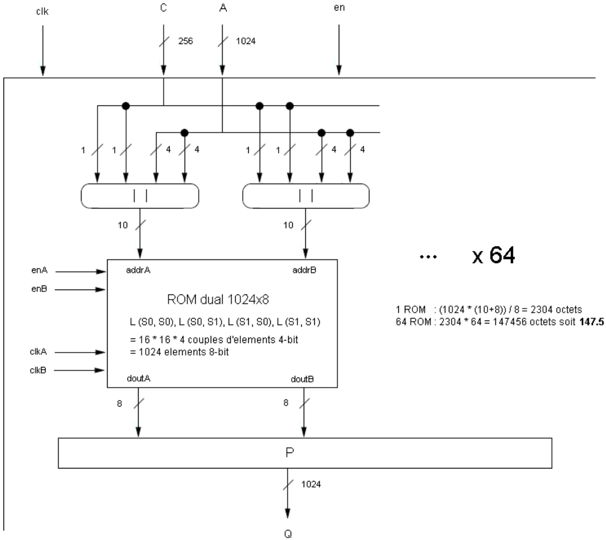
- S_0 and S_1 (4×4-bit Sboxes) chosen by round constants
- L implements a (4,2,3) Maximum Distance Separable (MDS) code over $GF(2^4)$

Goals and Strategy

- Litterature: bit-slice implementations, or only SBoxes stocked in BRAMs.
- JH looks like AES...
  $\Rightarrow$ Why not trying to use a "TBox-like" approach for JH?
- Slices can be used as distributed memory, but not efficient
  $\Rightarrow$ Intensive use of FPGA Dual-port BRAMs



JH Round Implementation



1 ROM : (1024 * (10+8)) / 8 = 2304 octets
64 ROM : 2304 * 64 = 147456 octets soit **147.5 Ko**

Our Preliminary Results

- VHDL, Xilinx Virtex-5 70T -3, ISE Tools (v11.5i)
- Post-place-and-route results

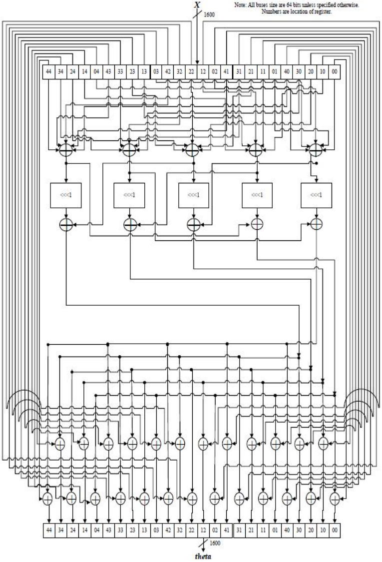
Reference	Area (slices)	Freq. (MHz)	TP (Gbps)	TP/Area (Mbps/slice)
Gaj's team	**1104**	**394**	**5.610**	**5.081**
Our work	1793	197	2.401	1.339

- At first sight, not so good results, but DSPs not used
- + 2.448MB of Dual-Ported ROM (45% of FPGA resources)

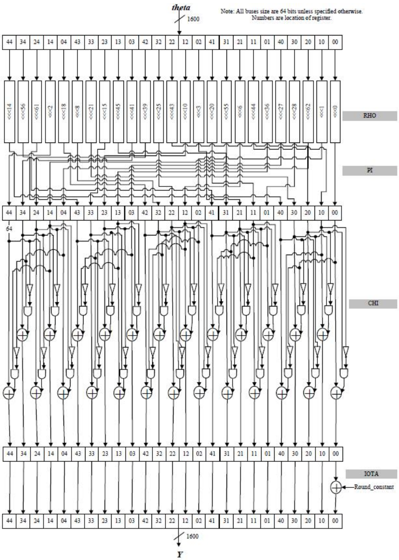
Outline

1. Our BLAKE Implementation
2. Our JH Implementation
3. Our Keccak Implementation
4. Conclusion and Future Works

Hardware View of the Keccak Round (1/2)



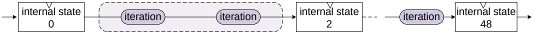
Hardware View of the Keccak Round (2/2)



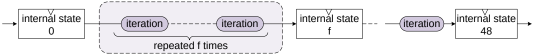
Unfolding Method

- Unroll the Keccak core
- Method already used for Shabal [Francq *et al.*, ReConFig 2010].
- Factor 1

- Factor 2



- ...
- Factor f



- For Keccak: 24 rounds

Benefits of Using Unfolding Method?

1. Save register loading time.
   $\Rightarrow$ Impact on Frequency.
2. $\searrow$ # Clock Cycles per message block

- Yet, TP (for long messages) $= \dfrac{\text{Message block length} \times \text{Frequency}}{\#\ \text{Clock Cycles per message block}}$.
- How can we explain an hypothetical gain?
- Ex.: when $f = 1 \rightarrow 2$, # Clock Cycles per message block/2.
  $\rightarrow$ To get TP $\nearrow$, Frequency ($f = 2$) $>$ Frequency ($f = 1$) / 2.

Our Preliminary Results

- VHDL, Xilinx Virtex-5 330T -3, ISE Tools (v13.1i)
- Post-place-and-route results
- Generic parameter for unfolding factor

Reference	Area (slices)	Freq. (MHz)	TP (Gbps)	TP/Area (Mbps/slice)
Homsi. *et al.*	**1257**	**285**	**6.845**	**5.445**
Our work (f=1)	2864	228	5.472	1.910
Our work (f=2)	3458	125	6.000	1.735
Our work (f=3)	TBA	TBA	TBA	TBA
Our work (f=4)	TBA	TBA	TBA	TBA

- More complex place and route step (TBA = To Be Announced)
- Is f=2 the best unfolding factor?
- + 1.576Kb of ROM

Outline

Conclusion and Future Works

- Previous Hardware Implementations of SHA-3 candidates are basic $\Rightarrow$ Alternatives
- BLAKE: only 1 circuit for all digest sizes, dual-mode.
  - Improve frequency with optimized adders
- JH: extensive use of BRAMs.
  - Implement a more regular architecture with DSPs
- Keccak: unfolding method for improving TP.
  - Needs final results
- For all: ATHENa tool.
- For allowing public scrutiny, VHDL sources and ISE projects will be available on SAPHIR2 website
- Significant contribution in the benchmarking of the SHA-3 finalists

Calendar

- September, 2011:
  - implement low-area JH and Keccak,
  - implement Grøstl and Skein.
- Then, implement countermeasures against side-channel attacks when HMAC is computed
- February, 2012: 3rd SHA-3 Conference, CHES.
- June, 2012: SHA-3 announced by NIST.
- March, 2013: End of SAPHIR2 project.

SAPHIR2 Partners

CRYPTOLOG
Créateur de confiance

ANSSI

EADS
DEFENCE
& SECURITY

Ens

france telecom

gemalto
security to be free

INRIA

Sagem Sécurité
SAFRAN Group

UNIVERSITÉ DE VERSAILLES
SAINT-QUENTIN-EN-YVELINES