Towards to SHA-3 Hashing Standard for Secure Communications: On the Hardware Evaluation Development

N. Sklavos, Member IEEE

Abstract—The most well known and officially used hash function is the Secure Hash Algorithm-1 (SHA-1) and Secure Hash Algorithm-2 (SHA-2). In recent years serious attacks have been published against SHA-1. This led the National Institute of Standard and Technology (NIST) to organize an effort to develop a modern and more secure hash algorithms through a hash function competition for usage in the following years in the near future. The selected new hash function will be called SHA-3. This keynote talk deals with the hardware implementation efficiency of SHA-3 candidates, which is one of the most critical issues, regarding the adoption of the SHA-3 standard. Comparisons, in terms of hardware terms are given in detail, through this keynote talk.

The most well known hash function is the Secure Hash Algorithm-1 (SHA-1). In recent years serious attacks have been published against SHA-1. After that, the transition to the stronger SHA-2 [3] family of hash functions (SHA-224/256, SHA-384 and SHA-512) was decided. SHA-2 functions are included in the same general family of hash functions. So, they could possibly be attacked with similar techniques, however theoretically they are much stronger than SHA-1. Also, a distinguishing attack on the full compression function of Whirlpool hash function is achieved. All the above mentioned results have been adopted by the International Organization for Standardization (ISO/IEC) 10118-3 standard. This led the National Institute of Standard and Technology (NIST) to organize an effort to develop more secure hash algorithms through a hash function competition for usage, in the following years of the near future. The selected new hash function will be called SHA-3 function.

The final submissions for this competition were due on October 31, 2008, at which time NIST received 64 submission packages. NIST announced the acceptance of 51 First-Round Candidates as meeting the minimum acceptance criteria on December 10, 2008, marking the beginning of the First Round of the SHA-3 competition. After that, NIST received much feedback from the cryptographic community and announced the selection of 14 algorithms as Second-Round Candidates on July 24, 2009 to move forward to the second round of the competition. Continuing with a similar process NIST is going to announce the winner at the end of 2012. The draft minimum acceptability requirements for candidate hash algorithms were: First, the algorithm must be publicly disclosed and available on a worldwide, non-exclusive, royalty-free basis, second, the algorithm must be implementable in a wide range of hardware and software platforms and thirdly, the algorithm must support 224,- 256-, 384-, and 512 -bit message digests, and must support a maximum message length of at least 264-bit.

The importance of hash functions, in modern cryptography is clearly proven by the different applications and multi-purposes that these are used, in cryptographic protocols. First, digital signatures are the first application of cryptographic secured hash functions. Hash functions serve a dual role in signature schemes: they expand the domain of messages that can be signed by a scheme and they are an essential element of the scheme's security. Second, message-authentication code (MAC) is a keyed hash function satisfying certain cryptographic properties. Third, a common method of client authentication is to require the client to present a password previously registered with the server. Storing passwords of all users on the server poses an obvious security risk. Although, the server need not to know the passwords—it may store their hashes (together with some salt to frustrate dictionary attacks) and use the information to match it with the hashes of alleged passwords. And last, one more usage of hash functions is to “destroy” any structure that may exist in the input, while preserving most of its entropy. Validity of using hash functions for entropy extraction is not based on their cryptographic properties but rather on our belief that a good hash function destroys most of the dependencies that may exist in the bits of its input.

One of the important criteria for the hash function selection is its efficiency on the hardware implementation. So, a comparison in term of implementation is much useful. The implementations are categorized into FPGA and standard-cell ASIC implementations. For FPGA implementation, it is desirable to compare implementations on the same target device or on devices of the same FPGA family. For ASIC implementation, the minimal gate length of the process should be agreed. For comparisons in many modules and different applications, three different hardware implementations are used (the fully autonomous implementation, implementation with external memory and implementation of core functionality) and are described, in the next paragraphs of this section. Candidate algorithms that meet the minimum acceptability requirements are going to comparing, based on the security, computational efficiency, memory requirements, hardware and software suitability, simplicity, flexibility, and licensing requirements. The security level provided by each submitted algorithm as compared to other submissions (of the same hash length), including first and second preimage resistance, collision resistance, and resistance to generic attacks. Also, if other security factors raised by the public comments during the evaluation process, including attacks which demonstrate that the actual security of the algorithm is less than the strength claimed by the submitter, this keynote talk deals with the evaluation of computational efficiency, applicable to hardware implementations. Computational efficiency essentially refers to the throughput of an implementation. The memory required for hardware and software implementations will be considered during the evaluation process. Memory requirements will include factors such as gate counts for hardware implementations, and code size and RAM requirements for software implementations. Algorithms with greater flexibility that meet the needs of more users are preferable. For example “flexibility” include, the algorithm parameterization (can

N. Sklavos, Security & Systems Design Group, Informatics & MM Department, Technological Educational Institute of Patras, HELLAS, nsklavos@ieee.org.
accommodate additional rounds), parallel implementations of the
algorithm in order to achieve higher performance efficiency and
efficiency algorithm implementations for wide variety of platforms,
including constrained environments such as smart cards. The
algorithms will be judged according to relative simplicity of design.

Keywords—SHA-3, cryptographic hardware, system design,
FPGA, embedded system.

REFERENCES

[1] SHA-1 Standard, National Institute of Standards and Technology
(NIST), Secure Hash Standard, FIPS PUB 180-1, available on line at
www.itl.nist.gov/fipspubs/ fip180-1.htm

[2] Secure Hash Standard (SHS), National Institute of Standards and
Technology (NIST), FIPS PUB 180-3, available on line at

Information technology – Security techniques – Hash functions – Part 3:


From the Fastest to the Smallest", IEEE Computer Society Annual
Symposium on VLSI (IEEE ISVLSI’10), Kefalonia, Greece, July 5-7,
2010.

[6] N. Sklavos, "On the Hardware Implementation Cost of Crypto-
Processors Architectures", Information Systems Security, The official
journal of (ISC)2, A Taylor & Francis Group Publication, Vol. 19, Issue:
2, pp. 53-60, 2010.

Family Standard Using FPGAs", Journal of Supercomputing, Springer-

[8] Nicolas Sklavos, "Multi-module Hashing System for SHA-3 & FPGA
Integration", proceedings of 21st International Conference on Field
Programmable Logic (FPL’11) and Applications, Chania, Greece,
September 5-7, 2011.

[9] P. Kitsos, N. Sklavos, "On the Hardware Implementation Efficiency of
SHA-3 Candidates", proceedings of 17th IEEE International Conference
on Electronics, Circuits, and Systems, (IEEE ICECS’10), December 12-
15, Athens, Greece, 2010.

Dr. Nicolas Sklavos received the Ph.D. Degree in
Electrical & Computer Engineering, and the Diploma in
Electrical & Computer Engineering, in 2004 and in
2000 respectively, both from the Electrical & Computer
Engineering Dept., University of Patras, Hellas. Since
2008, he is an Assistant Professor with the Informatics &
MM Dept, Technological Educational Institute of
Patras, Hellas. He is the Head of Security and Systems
Design. Research Group. He is also adjunct faculty,
Assistant Professor, with the Computer Engineering & Informatics Dept.,
University of Patras, Hellas from 2007. He holds an award for his PhD thesis
on “VLSI Designs of Wireless Communications Security Systems”, from IFIP
VLSI SOC 2003. His research interests include System on Chip Design,
N. Sklavos has participated to a great number of European and National
projects both research & development, in the areas of his research. He serves
as evaluator of both European Commission Projects (FP7) and General
Secretary of Research and Development, Hellas. Since 2007, he is the
Council’s Chair of IEEE Hellas GOLD Affinity Group. He is the Editor-in-
Chief for the Information Security Journal: A Global Perspective Journal,
Taylor & Francis Group. He serves as Associate Editor for IEEE Latin
America Transactions, IEEE Press, and Computers & Electrical Engineering
Journal, Elsevier. He has been Guest Editor of Special Issues for Elsevier &
Springer publishers. He was the General Co-Chair of ACM MobiMedia 2007
and General Chair of ATHENA 2011 Summer School. He has participated to
the organization of up to 100 conferences organized by IEEE/ACM/IFIP, as
Publicity, Publication Chair, Program Chair and Program Committee member.
He has authored or co-authored up to 100 scientific articles, books, chapters,
tutorials, in the areas of his research. His published works has received up to
750 citations.