28 Nanometers FPGAs Support for High Throughput and Low Power Cryptographic Applications

Yaser Jararweh, Lo'ai Tawalbeh, Hala Tawalbeh
Cryptographic Hardware and information Security lab (CHiS)
Jordan University of Science and Technology, Irbid, Jordan
Email: {yijararweh, Tawalbeh}@just.edu.jo, hala.t.88@hotmail.com

Abidalrahman Moh'd
Engineering Mathematics and Internetworking
Dalhousie University, Halifax, Canada
Email: Abidalrahman.Mohd@dal.ca

***Abstract*—The current unprecedented advancements of communication systems and high performance computing urged for a high throughput applications with power consumption within a predefined budget. These advancements were accompanied with a crucial need for securing such systems and users critical data. Current cryptographic applications suffer from the limitations of their low throughput and extensive power consumption that severely impact the available power budget. Creating new algorithms to handle these issues will be a time consuming process. One viable solution is to use the new 28 Nanometers (nm) FPGAs devices that promise to provide less power consumption with a very competitive throughput and throughput to area ratio comparing to the older technologies. In this paper, we evaluate the 28 nm FPGAs technology and its impact in eight of the major cryptographic algorithms available today such as SHA2, SHA3, and AES. Our results revealed that using the 28 nm FPGAs reduced the power consumption to more than 50% and increase the throughput up to 100% compared to the older FPGs technologies. On the other hand, throughputs to area ratio results show about 71% improvement over other technologies.**

***Index Terms*—Hardware Evaluation, Power, Throughput, FPGA, 28 nm technology, AES, SHA.**

I. Introduction

During the previous decades, engineers and scientists kept trying to have as much as possible of transistors on a chip until computers became faster, more powerful, and very useful. Consequently computers became an important part of almost every single person on this earth and that's why all computer systems, applications, and networks must be secure, trusted, and safe in order to protect all data and information specially the sensitive ones from being accessed, stolen, or even shown to those who must not do so. Therefore it is very necessary and important to have methods that assure high level of security for the transmission of data and the communication between network's parties. The science of cryptography and its four services (confidentiality, integrity, authentication and non-repudiation) are both available for the purpose of assuring security over the different types of communications.

Cryptographic encryption algorithms and secure hash algorithm (SHA) functions are very important for many security applications, especially for the authentication related applications, such as message authentication codes, password protection and digital signature. Data integrity verification is another field in which cryptographic hashing takes place. It is used to make sure that the data transmitted within a message is not being accessed or modified [2].

In general, cryptographic systems and applications are slow and power consuming systems when implemented with software solutions. The viable alternative is using FPGAs hardware implementations of such critical systems. However, current FPGAs hardware devices also show some limitations in their throughput and power consumption. So what we are going to provide in this paper is an evaluation for the support provided by one of the newest FPGAs technologies for raising the amount of data encrypted in specific amount of time (throughput) and for reducing the consumed power. This technology is the 28 nm technology with its Xilinx 7 series FPGAs that includes Artix™-7, Kintex™-7, and Virtex-7 devices.

II. Related work

For SHA-1, and SHA-2, many works in literature focused on how to optimize speed and throughput such as in [11] [12] [13] [14] and many other works focused on improving the different implementations of SHA-2 like the one proposed in [12] and [15].

For the under development SHA-3 and its five final candidates (Blake, Grostl, JH, Keccak, and Skein), there are many works that studied each one of them and its implementation individually or compared them together under a certain criteria. The authors in [16] shows different architectures for each algorithm of the candidates which resulted in many tradeoffs between speed and area, and provides a ranking for the 5 candidates based on their performance and other features that differentiate each algorithm from the others.

doi:10.4304/jait.4.2.84-90

Researchers in [6] provided a comparative study for the five finalists and SHA2-256 using different FPGA families (Virtex-4, Virtex-5, Virtex-6 and Spartan-3). [1] and [2] provided a comparative study for the five finalists and SHA2-256 using different FPGA families (Virtex-5, Virtex-6 and Virtex-7).

For the Advanced Encryption Standard (AES), there are several hardware implementations that can be found in literature. These implementations were done for the original standard AES (not more than 256 bits key size), such as the work presented in [17] [18]. Before choosing Rijindael to be the AES in November of 2001, many related implementations were proposed to how much the structure of the proposed candidates for the AES competition is suitable for hardware implementation [19]. They provide a multiple architecture options for AES finalist candidates with an implementation analysis for each architecture based on both area and speed optimization with a detailed comparison of the FPGA hardware performance of the AES candidates. Many other implementations that target the Field Programmable Devices (FPD) for Rijndael with a comparison with Xilinx FPGA implementation are also available. The authors in [19] presented a new variation of the AES algorithm (called AES-512) with its hardware architecture. The goal of the AES-512 to be used when higher levels of security and throughput are required. The need for low power consumption systems such as in sensors networks [20] is continuously increasing, and this is our main motivation in this paper.

III. 28 NM TECHNOLOGY

Nanometer is a measure unit just like feet, inches and miles, but it is used to measure small things just like atoms. A meter is a billion (1000000000) of nanometers. So nanometer is a very small unit and things that are nanometers in size cannot be seen without using powerful microscopes. [3]

Inside someone's computer, thousands of tiny switches of 100 nanometers wide can be found. These stacked and packed tiny switches are manufactured by what is called nanometer technology or nanotechnology by which machines in factories can be used to take, move and mix ingredients that are nanometers big and turn them into materials that can be used to manufacture functional devices used in a wide range of complete and high performance applications and products just like electronics. Nm technology in computers refers to an individual transistor's size or the distance between the centers of two adjacent transistors on a chip. The smaller it could be made, the less energy it will use, and the more performance will be reached as more of them can be packed in a given space. [3]

Nanometer technology or the technology node selection for FPGA is passed through different stages and evolved from a version to another. Every newer version is specialized by its smaller size of transistor. The technology of node selection is started with transistors of thousands nanometers in size and kept evolving to be 150 nm by 2000, 130 nm by 2002, 90 nm by 2004, 65 nm by 2006, 45 nm by 2008 and 28 nm by 2010. In our research we are going to concentrate our efforts on the newest node selection technology that is the 28 nm technology as it is designed to efficiently and effectively manage both dynamic and static power and to raise the fundamental performance in a reasonable cost. [1]

What specializes the 28 nm technology's FPGAs is the optimized transistor mix of high threshold voltage transistors, low threshold voltage transistors, and regular threshold voltage transistors, with separate performance and leakage for each transistor in the mix. This optimized transistor mix is first introduced in Virtex-6 FPGA. Two voltages 1V and 0.9V at which 28 nm technology FPGAs operate are offered by Xilinx and this is what is called the voltage scaling option which result a 30% of static power reduction. [7]

The 7 series FPGAs of the 28 nm technology offered by Xilinx are created using the stacked silicon interconnect technology to avoid the problems caused by the different leakage components for each transistor specially for those large devices that contain billion of transistors. This technology creates large devices by using multiple dies with a recognized reduction in the static power and in the I/O interconnects power. [7]

High end, power sensitive and bandwidth sensitive applications need a very well suited nm technology. Low power process, high performance, and the different choices for cost effective mass production make the 28nm technology very appropriate and efficient for these applications.

Moreover, efficient management of current tunneling effects, which is a goal for all the process designers, utilizes 28nm technologies with the new gate dielectric material added by Xilinx such as super low-power (SLP) technology and high performance (HP) technology. These technologies are designed for applications such as graphics, wired networking and wireless mobile applications.

28nm node is a good choice for different projects since its performance variation will solve a many reliability challenges and problems by developing advanced processes and affordable techniques by which designers can detect correct reliability issues early in the custom and semi custom design phases. Furthermore, since the 28nm gate oxide is too thin, tunneling effect has to be addressed by a new gate material by making trade-offs in the overall transistor design. For this purpose a new gate with high dielectric constant for the dielectric material, called *hafnium dioxide* has been adopted by Xilinx. This material offers an increasing in the gate thickness, so the transistor will be more immune to the tunneling current effects [10]. Choosing the 28 nm HKMG (high-k metal gate) high performance and low-power process technology is performed by Xilinx after evaluating the 28 nm technology options including LP and HP variants [10].

After all the mentioned advantages of 28nm technology, Xilinx decided to merge the high performance and the low-power process technology in a new unified ASMBL (Advanced Silicon Modular Block)

in order to create a new FPGAs with lower power and higher performance.

In general, the 28nm technology and FPGAs products focus on 3 main goals, reducing the static and dynamic power, so we can have the total power reduced by half at the minimum, increasing the performance by the half too, and increasing the capacity.

A. Vitrex-7

In our research we are going to focus on one of Xilinx 7 series FPAG devices, this device is Virtex-7 as it is the World's Highest Capacity FPGA since it delivers greater than 2 x the capacity and bandwidth offered by other devices and integrates 2 million logic cells and 6.8 transistors. Virtez-7 is considered as Industry's Highest System Performance too since its FPGAs are optimized for advanced systems requiring the highest performance and highest bandwidth connectivity and delivers 2 x higher system performances at 50% lower power than previous generation FPGAs. [4]

IV. CRYPTOGRAPHIC ALGORITHMS

A. Advanced Encryption Standard (AES)

The Advanced Encryption Standard algorithm AES is the FIPS-197 stander that been in use since 2001 since it provides high level of security and can be implemented easily [17]. The AES is a symmetric cipher algorithm with block size of 128-bit supports key sizes of 128, 192, and 256 bits with 10, 12, or 14 iteration rounds, respectively. Four major operations are performed during each round: byte substitution, shifting rows, mixing columns, and finally adding the round key. AES 128-bit key is considered secure compared to the other existing symmetric cipher algorithms. It is widely used in many applications where the security is very important. Many new variations of AES algorithm were proposed to provide even more security and throughput. In AES, more security comes from using larger key size, and more throughputs come from using four times larger block size than the block size used in the original AES. The only disadvantage of larger block size AES is the need for more design area and power consumption which is the core of this paper. The top level architecture of the AES-128 and its variant AES-512 bits are similar to a certain extent. The plaintext and the key size are 128 or 512-bits respectively, each (organized in bytes). The same size will be for its output ciphertext.

AES operations are going through four steps, we summarized them as follow [17] [19].

a. .Byte Substitution

The input plaintext is organized in a set of arrays of fixed size of bytes and then substituted by values obtained from Substitution boxes (S-boxes). This is done to achieve more security according to diffusion-confusion Shannon's principles for cryptographic algorithms design.

b. Shift Row

After the original block data is substituted with values from the S-boxes, the rows of the resulting matrix are shifted in a process called *ShiftRow* transformation. The bytes in each row in the input data matrix will be rotated left.

c. Mix Colomn

The *MixColumn* transformation multiplies the columns of the data matrix by a pre-defined matrix over GF (2^8).

d. AddRound Key

To make the relationship between the key and the ciphertext more complicated and to satisfy the confusion principle, the *AddRound Key* operation is performed. This addition step takes the resulting data matrix from the previous step and performs on it a bitwise XOR operation with the sub key of that specific round (addition operation in GF (2^n)).

B. Secure Hashing Algorithms SHA

Secure hashing algorithms SHA take data as block (messages) and return a string of fixed and smaller size bits (hash value), so changes on data lead to changes on the hash value (digest). However the requirements for the cryptographic hash functions differ but at the same time there are common characteristics for all functions with messages as inputs. The following are some of these characteristics:

- Secure hash functions are very simple and easy. Therefore their hardware and software implementations are always efficient.
- Hashing functions are one way functions which means that it is impossible to generate a message from its digest.
- For a specific message m it is infeasible to find another specific message n such that H(m) = H(n). This is called weak collision resistance.
- It is infeasible too to find two different messages m and n such that H(m) = H(n). In other words two different messages do not lead to the same hash digest. This is called strong collision resistance.

Cryptographic hash functions are very important for many security applications, especially for the authentication related applications such as message authentication codes and digital signatures, message and file integrity secure login, and figureprints of keys.

Most of Secure Hash Algorithms (SHA) have common components which are: *Permutation* or the process of swapping data (input), *Substitution* or the process of nonlinear transformation of data using substitution-box or S-box, Logical functions just like AND, OR, NOT and the most desired XOR and the Modular arithmetic function (mod).

SHA is a group of hash functions published by NIST (stands for the National Institute of Standards and Technologies) and developed by National Security Agency NSA [6].

SHA0: 160-bit secure hash function published in 1993. Due to an undisclosed significant flaw, SHA0 was withdrawn shortly after its publication and replaced directly by SHA1.

SHA1: 160-bit secure hash function which is nearly similar to the MD5 but much more moderate. SHA1 was designed, developed, and published by the NSA. And among the SHA families, SHA1 is the most widely used one.

SHA2: consists of two hash functions with 4 different size blocks for the output, 224, 256, 384, and 512 bits. SHA-224 and the SHA-256 are truncated versions of the SHA-384 and SHA-512. Same as SHA1, all SHA2 families were designed, developed, and published the NSA.

SHA3: The upcoming hash function which is still under development and supposed to be published by March 2012 through a public competition held by NIST, in order to choose the best algorithm among all the candidates. The five candidates are Blake, Grostl, JH, Keccak, and Skein.

V. Evaluation Metrics

As we are studying the 28 nm FPGAs support for high throughput and low power cryptographic applications, we are going to evaluate the new technology's effect in term of power and throughput.

Throughput: is an important metric, which means the amount of processed data by a design within a fixed amount of time. The importance of throughput is coming from being a number that weights: the block size which is a characteristic for the algorithm used in an application, the frequency which is a characteristic for the hardware design performance and the latency which is a characteristic for the hardware design architecture [5] [6].

Power: Power consumption is one of the most important factors that can be used for the FPGA selection, and that's why Xilinx tries always to reduce it, starting from Virtex-4 FPGAs, until the development of Xilinx 28 nm 7 series FPGAs that includes Artix-7, Kintex-7, and Virtex-7 devices, which all have been evaluated according to their impact on static power, dynamic power, and I/O power [7]. The power of any design is presented as a summation of dynamic power and static power, and the power of any design we are going to present in this research is calculated using Xilinx Xpower estimator tool.

VI. Results and Evaluation

In this section a detailed description about all experiments that have been done will be presented. Our Experiments depend on the hardware implementation for SHA3 candidates. We have got these implementations from George Mason University (GMU) website and synthesized them on FPGAs for different families. [8]

A. Framework

We have used VHDL implementation from the GMU for the 5 candidates since they are all described in this language, where if different languages are used to describe different candidates may lead to unneeded bias. So the VHDL is a perfect choice for the implementations and comparisons of the candidates.

For FPGA devices, we decided to concentrate on those from Xilinx, so we have chosen 3 families of Xilinx FPGA devices optimized for high performance, Virtex-5 (xc5vlx20t-2ff323), Virtex-6 (xc6vcx75t-2ff484), and the 28 nm technology's Virtex-7 (xc7v285t-2ffg1157).

For throughput results we have used the Xilinx ISE synthesizer and design suit (version 13.1). For power results evaluation, XPower estimator was used. XPower estimator is a spreadsheet estimation tools that is used after applying the XPower analyzer tool of Xilinx ISE design software for more accurate estimations and power analysis, by mapping the results of the analyzer to the sheets [9]. We calculate throughput firstly by finding T, which stands for the period that is the length of time taken by one cycle. The formula for T is:

$$\mathrm{T} = 1/\mathrm{frequency}$$

Then, the throughput will be calculated using:

$$\mathrm{TP} = \mathrm{block\ size}/(\mathrm{latency} * \mathrm{T})$$

The block size is a fixed amount of data that the algorithm will process at a time. The latency is the number of cycles that are needed to hash a message and we have got the values for the latency ready from the GMU website. [8]

So throughput equations will be as follow:

- For Blake algorithm: $TP = 512/(21 * T)$.
- For Groestle algorithm: $TP = 512/(21 * T)$.
- For JH algorithm: $TP = 512/(36 * T)$.
- For Keccak algorithm: $TP = 1088/(24 * T)$.
- For Skein algorithm: $TP = 512/(19 * T)$.
- For SHA2 algorithm: $TP = 512/(65 * T)$.

Then, we use the XPower analyzer tool from Xilinx ISE to generate the thermal and power summery for each algorithm. Also, we have a mapping between the XPower analyzer and the XPower estimator to work on the power experiments after extracting the map reports of the analyzer using the estimator.

B. Throughput results for different FPGAs devices

Table 1 shows two things, the first point is that the use of Virtex-7 provides a higher operating frequency compared with Virtex-5 and Virtex-6. JH and KECCAK algorithms show a higher frequency than SHA-3 candidates, SHA-2, AES-128 and AES-512. In contrast, BLAKE and SKEIN results show lower frequency when compared to SHA2 and AES-128 and AES-512. The second point is that using Virtex-7 has a little impact on the throughput compared with Virtex-5 and Virtex-6 except for KECCAK algorithm. JH and KECCAK algorithms show higher throughput than other SHA-3 and SHA-2 algorithms. KECCAK algorithm shows the best results in terms of throughput and AES-128 and AES-512 show the worst results in term of throughput [1]. The Throughput results that most of the algorithms gain about 100% increase in its throughput compared with other technologies. Table 2 shows the improvements achieved by implementing designs on Virtex-7 FPGA family as it is one of the 28nm technologies compared to Vertix-5 for SHA-3 candidates, SHA-2, AES-128 and AES-512 [1]. The results show that even the throughput to area ration is

also improved with using 28nm technologies (Virtex-7 FPGA).

TABLE I.
THROUGHPUT RESULTS FOR SHA2 AND THE CANDIDATES

FPGA Family	Algorithm	Block Size[bits]	Max Freq. [MHz]	TP **[Mbit/s]**
Virtex-5	BLAKE	512	131.576	3207.9
	GROESTL	512	212.648	5184.6
	JH	512	314.125	4467.6
	KECCAK	1088	270.944	12282.8
	SKEIN	512	121.312	3269.0
	SHA2	512	179.509	1414.0
	AES-128	128	204.4	254
	AES-512	512	194.6	585
Virtex-6	BLAKE	512	146.709	3576.9
	GROESTL	512	242.242	5906.1
	JH	512	426.314	6063.1
	KECCAK	1088	333.361	15112.4
	SKEIN	512	153.418	4134.2
	SHA2	512	225.739	1778.1
	AES-128	128	250.4	320
	AES-512	512	261.1	954
Virtex-7	BLAKE	512	151,253	3687.7
	GROESTL	512	233.111	5683.5
	JH	512	426.13	6060.5
	KECCAK	1088	403.388	18286.9
	SKEIN	512	157.222	4236.7
	SHA2	512	232.631	1832.4
	AES-128	128	378.4	495
	AES-512	512	318.7	1163

TABLE II.
IMPROVEMENTS OF VIRTEX7 OVER VIRTEX5 REGARDING THE RATIO BETWEEN THE TP AND THE NUMBER OF SLICES

Algorithm name	**FPGA families**	**TP/number of Slices**	**Improvement of v7 over v5**
BLAKE	Virtex5	1.79	1.32
	Virtex6	2.26	
	Virtex7	2.36	
GROESTL	Virtex5	2.41	1.33
	Virtex6	3.69	
	Virtex7	3.20	
JH	Virtex5	3.51	1.62
	Virtex6	6.24	
	Virtex7	5.71	
KECCAK	Virtex5	8.69	1.67
	Virtex6	12.79	
	Virtex7	14.51	
SKEIN	Virtex5	2.24	1.60
	Virtex6	3.70	
	Virtex7	3.58	
SHA2	Virtex5	3.33	1.71
	Virtex6	4.68	
	Virtex7	5.71	
AES-128	Virtex5	0.083	1.36
	Virtex6	0.108	
	Virtex7	0.113	
AES-512	Virtex5	0.119	1.45
	Virtex6	0.171	
	Virtex7	0.173	

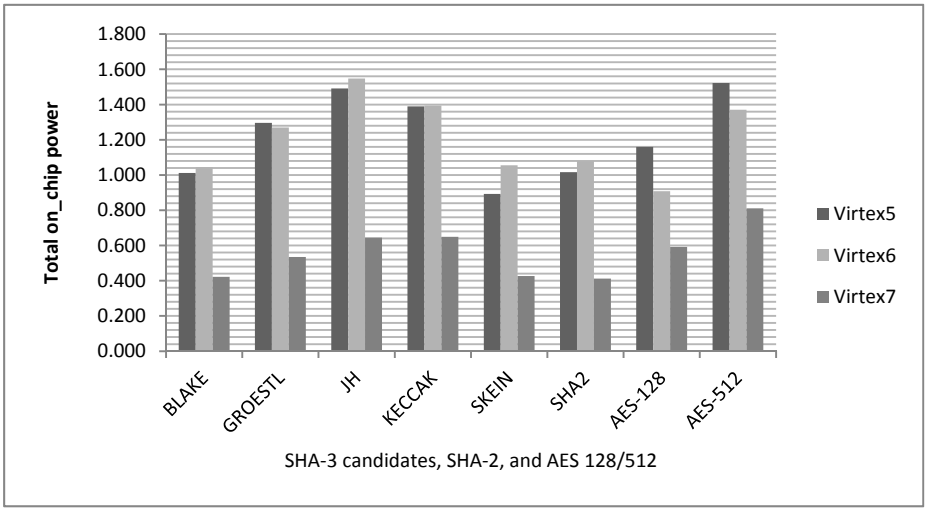

Figure 1: Total on chip power results for hash candidates and SHA2

C. FPGA Results for Power

FPGA results for power is going to be presented, analyzed and evaluated in this section using XPower estimator for Virtex-5 (XC5VLX20T-FF323), Virtex-6 (VC6VCX75T-FF484), and Virtex-7 (XC7VX485T-FFG1157).Figure 1 shows remarkable power efficiency up to 50% of power saving when implementing designs on Virtex-7 compared to Virtex-6 and Virtex-5 for SHA-3 candidates, SHA-2, AES-128 and AES-512 [1] [2]. These promising power results made using 28 nm FPGAs a viable alternative in power limited devices such as Wireless sensor networks (WSN).

VII. CONCLUSION

The demands on securing information and communications systems are increasing continuously. This fact is accompanied by the unprecedented increase in applications throughput and power requirements. Current security algorithms e.g. AES and SHA suffer from their limitations in supporting high throughput applications. Furthermore, limited power budget of many devices such mobile phones and WSN add more challenges to adopting them in current communication systems. In this paper, we evaluate the current new advancement in FPGAs design technology. The 28 nm transistor design technology promises to increase applications throughputs while decrease their power consumption. Based on our comparative evaluation of the 28 nm devices with older technologies e.g. 45 nm and 65 nm, the 28 nm FPGAs technology devices achieved a one fold increase in throughput and throughput to area ration with 50% power saving gain. These results are very promising and can be exploited in many emerging applications such as cloud computing, high throughput network, and smart mobile devices.

ACKNOWLEDGMENT

The authors would like to thank their Universities and the Scientific Research Support Fund at the Ministry of High Education in Jordan for supporting this research. Also, we would to thank the Cryptographic Engineering Research Group (CERG) at George Mason University for their valuable supports and providing the HDL resources.

REFERENCES

[1] H. Tawalbeh," Hardware Performance Evaluation Of Sha-3 Candidate Algorithms," Master thesis, Jordan University of Science and Technology, June 2012.
[2] Y. Jararweh, L. Tawalbeh, H. Tawalbeh, and Moh'd A. "Hardware Performance Evaluation of SHA-3 Candidate Algorithms," Journal of Information Security (JIS), vol. 3, pp. 69-76, 2012.
[3] http://www.nanooze.org/english/pdfs/nanoozeissue01.pdf. Online Access [August 2012]
[4] http://www.xilinx.com/products/technology/dsp/
[5] R. McEvoy, M. Tunstall, C. Murphy, and W. Marnane. "Differential Power Analysis of HMAC based on SHA-2, and Countermeasures," Proceedings of Workshop on Information Security Applications-WISA. Vol. 4867, Pp. 317–332, 2007.
[6] S. Huang. "Hardware Evaluation of SHA-3 Candidates," Master Thesis, Virginia Tech Polytechnic Institute and State University. 2011.
[7] Hussein J, Klein M, and Hart M. Lowering Power at 28 nm with Xilinx 7 Series FPGAs. February 24, 2011.
[8] George Mason University: http://www.gmu.edu/
[9] Xilinx. "XPower Estimator User Guide," March 2011.
[10] X. Wu, P. Gopalan, and G. Lara, "Xilinx Next Generation 28 nm FPGA Technology Overview," March 2011.
[11] R. Lien, T. Grembowski, and K. Gaj. "A 1 Gbit/s partially unrolled architecture of hash functions SHA-1 and SHA-512," In Proceedings of CT-RSA, vol. 2964, pp. 324–338, 2004.
[12] R. Chaves, G. Kuzmanov, L. Sousa, and S. Vassiliadis. "Improving SHA-2 hardware implementations," Proceeding of Workshop Cryptograph. Hardw. Embedded Syst. (CHES), pp. 298-310, 2006.
[13] L. Dadda, M. Macchetti, and J. Owen. "An ASIC design for a high speed implementation of the hash function SHA-256," Proceedings of the ACM Great Lakes Symposium on VLSI 2004. Boston, MA, USA, pp. 421–425, 2004.
[14] N. Sklavos and O. Koufopavlou. "Implementation of the SHA-2 Hash Family Standard Using FPGAs," The Journal of Supercomputing, vol. 31, pp. 227–248, 2005.
[15] NIST, FIBS-PUB 180-2. "Secure Hash Standardm," August 2012. http://csrc.nist.gov/publications/fips/fips180-2/.
[16] E. Homsirikamol, M. Rogawski, and K. Gaj. "Comparing Hardware Performance of Round 3 SHA-3 Candidates using Multiple Hardware Architectures in Xilinx and Altera FPGAs," Proceedings of Ecrypt II Hash workshop, Tallinn Estonia; May 19-20 2011.
[17] J. Daemen and V. Rijmen, "The Rijndael Block Cipher: AES Proposal," Proc. 1st AES Candidate Conf., 1998;
[18] H. Kuo and I. Verbauwhede, "Architectural Optimization for a 1.82-Gbits/sec VLSI Implementation of the AES Rijndael Algorithm" Cryptographic Hardware and Embedded Systems (CHES 2001), Lecture Notes in Computer Science 2162, Springer-Verlag, Heidelberg, Germany, pp. 53-67, 2001.
[19] A. Moh'd, Y. Jararweh, L. Tawalbeh: AES-512: 512-bit Advanced Encryption Standard algorithm design and evaluation. IAS, pp. 292-297, 2011.
[20] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, E. Cayirci, Wireless sensor networks: a survey, Computer Networks, Volume 38, Issue 4, 15 March 2002, Pages 393-422.

Yaser Jararweh received his Ph.D. in electrical and computer engineering from the University of Arizona in August 2010. He is currently an assistance professor of computer science at Jordan University of Science and Technology (JUST). He is working in different research areas such as cloud computing, high performance computing, and systems security. He is the co-director of the CHiS research lab at JUST.

Lo'ai A. Tawalbeh is the Director of the Cryptographic Hardware and Information Security (CHiS) lab at Jordan University of Science and Technology (JUST). He is a full time assistant professor at the computer engineering department at JUST, Jordan, and part time professor at New York Institute of Technology (NYIT)-Amman's campus, and DePaul's University.-Amman since 2005. He got his BSc. in electrical and computer eng. form (JUST) in 2000, and his Masters and PhD in computer engineering from Oregon State University (OSU) , USA in 2002 and 2004 respectively, under the supervision of Dr. Cetin K. Koc , with GPA 4.0/4.0. Dr. Tawalbeh has many research publications in many refereed international Journals and conferences. His research interests includes: information security, hardware for cryptography and dedicated arithmetic algorithms for cryptographic applications, intrusion detection and computer forensics. Dr. Tawalbeh is a reviewer and a member of the editorial boards of many international journals and conferences in the area of the information security. For more details, please see his website: www.just.edu.jo/~tawalbeh

Hala Tawalbeh is a lecturer at the computer science department at Jordan University of Science and Technology (JUST), and a member of the Cryptographic Hardware and Information Security (CHiS) lab at JUST. She took part in the IT security research lab activities as a tester at the department of EE and CS at Muenster University of Applied Sciences, Germany. Ms Tawalbeh received a BSc in computer information systems from JUST, Jordan in 2010 and an M.S. in computer science from JUST too in 2012. Her research interests are in information security and cryptograph, cloud computing, trusted computing, and management of business processes.

Abidalrahman Moh'd is currently a Ph.D candidate in Engineering Mathematics & Internetworking Department at Dalhousie University, Canada, under the supervision of Dr. William J. Phillips and Dr. Nauman Aslam. His main research concern is to develop energy efficient security protocols and cryptographic algorithms for energy efficient and low-power architectures such as wireless sensor networks. He received both his B.Sc. and M.Sc. Degrees in Computer Engineering from Jordan University of Science and Technology (JUST) in February, 2006 and July, 2007 respectively.