New Experimental Results for AES-CCMP Acceleration on Cyclone-II FPGA

Chakib Alaoui,

Taif University, KSA

Summary

This paper presents a possible solution for accelerating IEEE 802.11i. First, it offloads the process of AES-CCMP encryption from the master CPU onto a co-processor, which frees the master CPU resources for other uses. Second, its implementation on FPGA offers the possibility of using many threads to run the AES-CCMP encryption.

Different optimizations have been applied on the hardware architecture of AES and on the basic unit of AES-CCMP, in order to satisfy different constraints in terms of latency, area occupation and speed. Performance measurement of the hardware solution is compared to AES software implemented on a NIOS II processor. A strong focus is devoted to the achievement of high throughput, which is required to support security requirements for current and future high bandwidth applications**.**

Key words:

IEEE 802.11i, AES-CCMP, Cipher, WEP, FPGA Input.

1. Introduction

ENCRYPTION is becoming a fundamental building block to achieve security in data and telecommunication networks. It makes electronic commerce, payment systems and transactions over networks possible. It has become one of the main tools for privacy, trust, access control, corporate security and countless other areas [1].

Effective implementations of cryptographic algorithms are essential for the realization of many real time communication systems. Performance has always been one of the most critical issues of a cryptographic function, which determines its effectiveness. It is evaluated by many metrics like latency, size and power consumption. Cryptographic computations are intensive and therefore they influence the performance of the whole system.

Wi-Fi (IEEE 802.11) is a common example of wireless communication. Schools, hospitals and public buildings are becoming the major applications fields. However, the major drawback of current wireless LAN technology is the weak security measures in the standard 802.11 protocols (Wired Equivalent Privacy -WEP) [2].

The solutions for WLAN security are delivered in two stages:

The first is the Wi-Fi Protected Access (WPA), which has been designed to allow software upgrade for existing WLAN systems. The second is the standard IEEE 802.11i, which provides the best available security, but requires hardware support [2]

The AES protocol requires complex algorithms for encryption/decryption processes, which makes them computationally extensive (AES requires about 350 lines of code, WEP implement RC4 algorithm that require 50 lines of code [4]). At backbone communication channels or heavily loaded servers, it is possible to lose processing speed. This drops the efficiency of the overall system while running cryptography algorithms.

Moreover, the 802.11i standard specifies that AES should have its own coprocessor in order to speed up the encryption/decryption process [5]. This implies that older existing wireless hardware cannot be upgraded via firmware to support IEEE 802.11i.

IEEE 802.11i (also known as WPA2) is an enhancement of the 802.11 standard specifying security mechanisms of wireless networks. The draft standard was ratified on June 24, 2004, and supersedes the previous security specifications. In addition to the introduction of key management and establishment, it defines encryption and authentication improvement [6]. AES-CCMP is a mandatory implementation of 802.11i. It was designed by D. Whiting, N. Ferguson and R. Housley. AES may be implemented in sizes of 128 bits, 192 bits or 256 bits, but 802.11i supports 128 bit AES only.

There are several AES implementation on FPGA's available on the literature [8-23]. Its ASIC counterpart was also widely studied [24 - 31]. These implementations feature high speed and high costs suitable for high end applications only. Early AES designs featured pipelined architectures and limited resource utilization [14-18]. Later FPGA and ASIC implementations showed better optimization, using dedicated on-chip memories implementing S-Boxes [19-29].

The goal of this work is to design and evaluate an embedded coprocessor based on the NIOS II processor. It implements an efficient, cost-effective solution and optimized WiFi NIC. Different optimizations will be applied on the hardware architecture in order to satisfy different constrains in terms of latency, area occupation and security. This design uses Cyclone II FPGA using Quartus foundation series.

Manuscript received April 5, 2010
Manuscript revised April 20, 2010

From this section, input the body of your manuscript according to the constitution that you had. For detailed information for authors, please refer to [1].

2. IEEE 802.11i NIC Architecture

2.1 WIFI Adapter Card IEEE 802.11

There are essentially four parts in a Wi-Fi LAN card shown in figure 1:

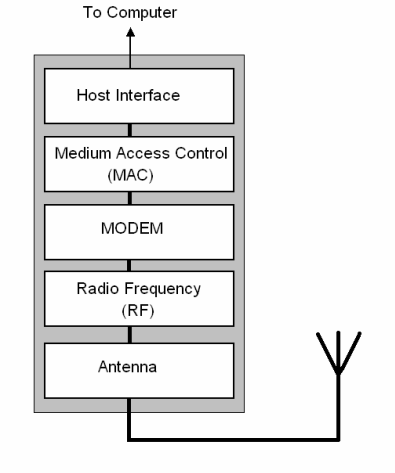

Figure1: NIC components in IEEE 802.11

1. Radio Frequency (RF) deals with the transmission and reception of the signal through the antenna.
2. MODEM extracts data from the received signal
3. Medium Access Control (MAC) is the heart of IEEE802.11 protocol. It has many functions like encryption/decryption of data, retransmission of lost data and data acknowledgement.
4. Host Interface is used to connect all the above to a computer like the USB or PCI bus.

Since IEEE 802.11i protocol is an enhancement to the MAC in terms of security, a closer look at the MAC components of IEEE802.11 is needed. Refer to figure 2.

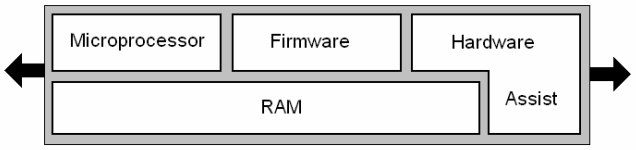

Figure 2: MAC Components [2]

MAC is made of a microprocessor who handles all the formatting and timing operations to control the protocol, the firmware is software that implements most functions and finally a hardware assist that speeds up the process of encryption/decryption of WEP. The hardware assist implemented in the existing NIC causes a critical problem for IEEE 802.11i; it cannot support AES-CCMP.

2.2 WIFI Adapter Card IEEE 802.11i

1.) WIFI Adapter Card IEEE 802.11i Block Diagram

The earlier NIC is static hardware and therefore its configuration could not be changed. The new design overcomes this issue and gives more flexibility for the longer term. FPGAs provide hardware reconfiguration possibility, i.e. flexible interconnect and short development time. They are very suitable as hardware accelerators for AES-CCMP. Another great improvement of the new WiFi adapter card is the network processor. It controls and processes all the network tasks so that the host CPU can be used for non-network related tasks such as video/audio processing. In this case, all networking tasks should be dropped into the FPGA (Encryption, Firewall, TCP|IP stack…). For evaluation purposes, NIOS II CPU from Altera Corporation was used as network processor.

Figure 3 shows a block diagram of the WiFi adapter card 802.11i

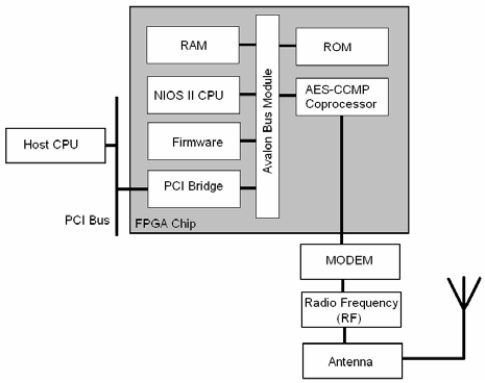

Figure 3: WiFi Adapter Card IEEE 802.11i

Avalon bus is an Altera's interface bus, used in NIOS II CPU. RAM contains unencrypted or decrypted data ready to be processed by AES-CCMP coprocessor. ROM contains all instructions necessary for the FPGA to work. During the boot-up phase, instructions are fetched from ROM since FPGA is volatile. PCI Bridge provides transparency between the host CPU and the NIOS II network processor. MODEM and Radio Frequency are off-chip.

2.) The Choice of Network Processor

It was shown that performance improvements made to general purpose processors do not translate necessarily

into improved network performance [32], because these processors are not optimized for network data processing. Recent processors incorporates several innovations in their architecture, like larger caches, out of order executions, deep pipelines, and super-scale executions, all of which cannot necessarily be exploited by networking code. It was also concluded that, even if the processor speed increases by Moore's law, network system speed increases in much lower pace [32]. So it is necessary to develop an efficient co-processor dedicated for network tasks.

3. AES Design And Implementation

3.1 Key Scheduling

Key scheduling expands a 128-bit cipher key into a 170 Byte key. It utilizes operations like word rotation, word substitution, and exclusive OR with round constant. Figure 4 shows AES key scheduling architecture.

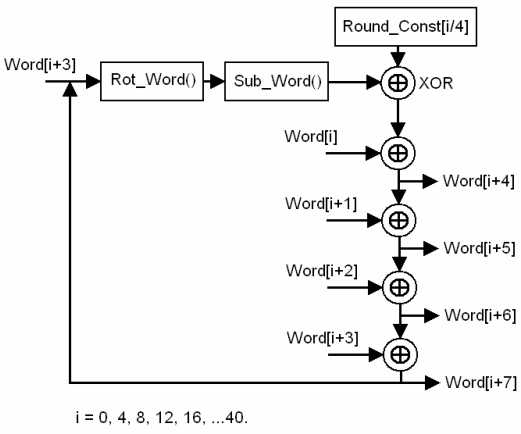

Figure 4: Key Scheduling Architecture.

First, the 128 bit cipher is divided into 4 sub-keys Word[0] to Word[3]. Then the shown operations are done to produce four new sub-keys Word[4] to Word[7]. Then this cycle is repeated 10 times in order to produce 160 Bytes. In total, a key of 176 Bytes is obtained.

In order to produce the new four sub-keys, the previous values of sub-keys are needed. So with this architecture, parallel execution is not possible.

In order to exploit the nature of parallelism offered by the hardware, an improved architecture is proposed using redundant computations. Refer to figure 5.

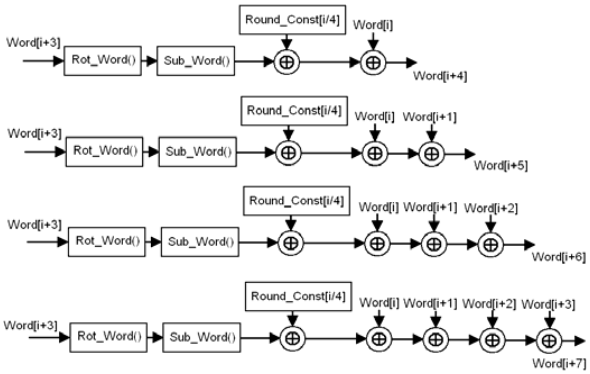

Figure 5: Modified Key Scheduling Architecture

3.2 AES Hardware Architecture:

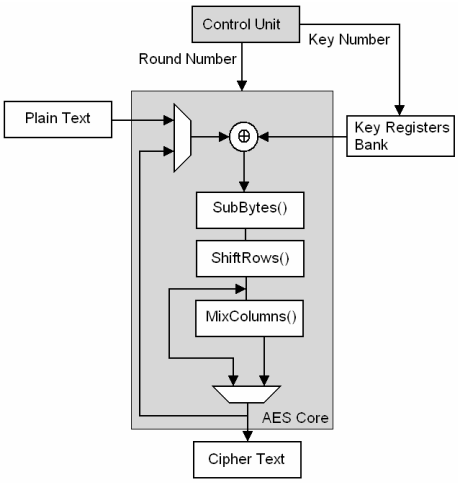

Figure 6: AES( ) Architecture

Control Unit: controls the components of the core (key registers bank and AES core). It also organizes the data flow by loading the specific data at the right round. After 10 rounds, the control unit will force the AES core to stop and output the cipher text.

Key registers bank: outputs the round keys. These sub-keys were computed offline.

AES Core: performs all the AES( ) modules.

3.3 Round Component Optimizations

Four different hardware/software optimizations have been developed. The first is based on the basic AES( ) unit which implements one round and executes ten times. This optimization employs the minimum hardware. The second optimization uses two AES( ) units and executes 5 times. The third implementation uses five AES( ) unites and executes them two times. Finally, the fourth implementation uses ten AES( ) units and executes them only one time. This last optimization uses the

maximum hardware. Figure 6 shows the four different AES implementations.

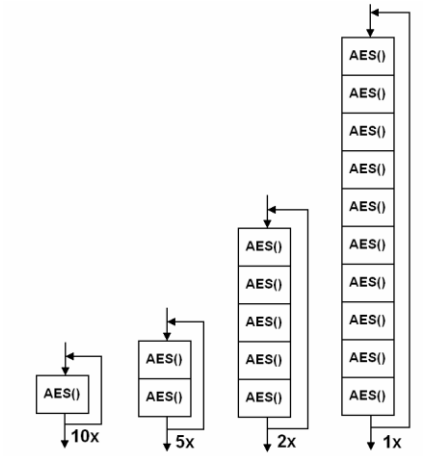

Figure 7: Four Different AES Implementations

4. AES Testing and Evaluation

The code has been synthesized using Altera's Quartus 6.1 development system. And Altera's Cyclone II chip was chosen for the implementation of the ciphers, because of its good performance among Altera's family and low cost.

4.1) AES Modules Synthesis

Table 1 shows the synthesis of the main components of AES, which are MixColumns() ver1, MixColumns() ver2, ShiftRows(), SubBytes() and SubBytes that implements RAM.

Table1: Synthesis of the Main Components Of AES

Total	MixColumns() ver1	MixColumns() ver2	SubBytes()	SybBytes() RAM
Logic Elements	**212**	**196**	**196**	**0**
Registers	**0**	**0**	**0**	**0**
Memory bits	**0**	**0**	**0**	**2048**
Cell Delay (ns)	**4.275**	**4.446**	**5.777**	**4.292**
Interconnect Delay (ns)	**11.263**	**11.394**	**9.090**	**7.955**
Worst Case tpd (ns)	**15.538**	**15.840**	**14.867**	**14.04**

There are two choices SubBytes() look-up table in the target device:

RAM: The values of the S-Box are loaded at the embedded RAM at configuration time.

Logic: S-Box can also be converted into logical representations and therefore implemented with logic elements. This option consumes chip area.

Data from table1 shows that the implementation of SubBytes() with embedded RAM gives significant improvements in the area/delay performance. Each 8 bits require 2048 bit of RAM, so in order to process 128 bits, 32768 bits for a 16x16 S-Box.

4.2) AES Cores Synthesis

Table 2 shows the synthesis results of AES key scheduling in Cyclone II

Table2: Synthesis Results Of An Aes Key Scheduling With Cyclone Ii

Implementation	Total
Logic Elements	**1102**
Registers	**269**
Clock Frequency (MHz)	**167.81**
Clock Cycles per Block	**11**
Period (ns)	**5.96**
Throughput (Mbits/s)	**1952.7**

Table 3 shows the synthesis results of AES without exploring the embedded RAM in Cyclone II

Table 3: Synthesis Results of n AES Without Exploiting Embedded RAM In Cyclone II

Implementations	1 AES( ), 10 Iterations	2 AES( ), 5 Iterations	5 AES( ), 2 Iterations	10 AES(), 1 Iteration
Logic Elements	**4190**	**7385**	17991	35624
Registers	**270**	**151**	134	132
Memory Bits	**0**	**0**	0	0
Clock Frequency (MHz)	**61.69**	**56.30**	21.67	10.47
Clock Cycles per block	**12**	**7**	4	3
Period (ns)	**16.69**	**17.762**	46.157	95.51
Throughput Mbits/sec	**658.07**	**1029.48**	693.44	446.72
Throughput/Area (Mbps/TLE)	**0.157**	**0.139**	0.038	0.012

Table 3 shows that having 2 AES( ) units and executing them 5 times yields the highest throughput of 1029.48 Mbits/sec.

In order to exploit the RAM blocks that exist in FPGA, the four implementations were re-synthesized by allowing the tool to use the embedded RAM. This reduces the total logic elements used in the four implementations. Table 4 shows the synthesis results of AES that exploits the embedded RAM in Cyclone II

Table4: Synthesis Results of an AES Exploiting Embedded RAM In Cyclone II

Implementations	1 AES( ), 10 Iterations	2 AES( ), 5 Iterations	5 AES( ), 2 Iterations	10 AES(), 1 Iteration
Logic Elements	**828**	**4156**	14754	32322
Registers	**270**	**151**	134	134
Memory Bits	**32768**	**32768**	32768	32768
Clock Frequency (MHz)	**62.83**	**61.32**	23.01	11.17
Clock Cycles per block	**12**	**7**	4	3
Period (ns)	**15.92**	**16.32**	43.457	89.526
Throughput Mbits/sec	**670.19**	**1121.28**	736.32	476.58

Since each S-Box needs 2K bits, 32768 bits are needed for 16 S-Boxes. Also, 16 blocks of RAM is exactly 32768 memory bits. Inferring S-Box as RAM blocks saves chip area in FPGA and improves the speed of the overall architecture.

5. AES-CCMP Accelerator: Architecture, Implementation & Results

5.1) Hardware Encryption of AES-CCM

CCMP computes the message authentication code and performs encryption in a single pass. That is encryption and authentication work in parallel.

Figure 7 shows the AES-CCMP algorithm used in the 802.11i security protocol. It is responsible for the authentication that produces a 64-bit long MIC (Message Integrity Check). IV in the Initialization Vector, it contains the source address, the length of packet during the session and other fields. PN: Packet Number.

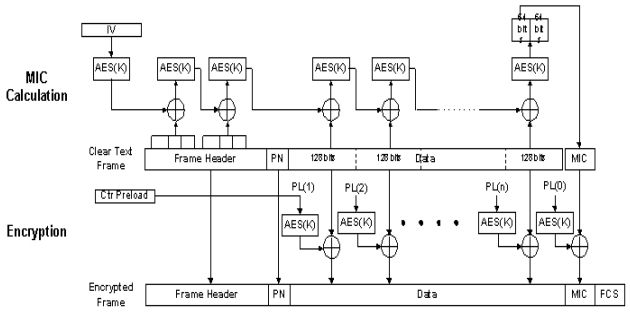

Figure 8: AES-CCMP Algorithm [13]

5.2) AES-CCMP Results

In order to implement the AES-CCMP core, the design that meets the lowest area with the highest throughput must be selected. The lowest area achieves a throughput of 670.19 Mbps (1 AES( ), 10 executions), while the second design (2 AES( ), 5 executions) achieves 1121.28 Mbps. Therefore these two different designs have been used to implement AES-CCMP algorithm.

Table 5 shows the performance and the cost comparison of these 2 implementations.

Table5: Performance and Cost Comparison of AES-CMP Implementations

AES-CCMP Implementation	1 AES( ) unit, 10 executions	2 AES( ) units, 5 executions
Total Logic Elements	1624	8438
Total Registers	589	471
Total Memory Bits	65536	65536
Clock Frequency (MHz)	66.31	55.68
Number of clock cycles per 3*128 bits	52	32
Period (ns)	15.08	17.96
Throughput (Mbits/s)	499.67	688.16
Surface area occupation	134	560
Throughput/Area	3.72	1.23

6. Conclusion

This project shows that Altera's Cyclone II series FPGA and NIOS II CPU make a low-cost and compact solution that adds high-speed features at lower cost and high degree of flexibility. Various architectures of AES unit and AES-CCMP were implemented with strong emphasis on high speed performance. FPGA technology has matured to the point where high throughput can be easily obtained. The most interesting result achieved in this paper is a data rate of 688.16 Mbits/sec by using the standard and low cost Cyclon II FPGA chip of Altera. This encryption rate meets the performance requirements of the emerging cryptographic applications such as the high speed standard IEEE 802.11n which supports a data rate of 600 Mbps [32].

References

[1] National Institute of Standards and Technology (U.S.), Advanced Encryption Standard. Available at: http://csrc.nist.gov/publication/drafts/dfips-AES.pdf

[2] Simon James Graham, "Hardware-Based Secure WLAN Solution", The University of Auckland, Part IV, September 15, 2003

[3] Web-site: "Time Controlled Communication and the 802.11 Recommendation', http://swedetrack.com/ieee802.htm, 2004

[4] Web-site: Advanced Encryption Standard (AES), http://www.informit.com/guides, Jan 1, 2004
[5] Web-site: "802.11i, WPA, RSN and what it all means to Wi-Fi Security", http://www.windowsecurity.com/articles/80211i-WPA-RSN-Wi-Fi-Security.html, April 06, 2005
[6] Web-site: "802.11i", http://wirelesslibraries.blogspot.com/2005/04/80211i.html, April 01, 2005
[7] J¨arvinen K.U., Tommiska M.T., Skytt¨a J.O.: A fully pipelined memoryless 17.8 Gbps AES-128 encryptor, International Symposium on Field-Programmable GateA rrays (FPGA 2003), Monterey, CA, 2003
[8] Chodowiec P., Gaj K., Bellows P., Schott B.: Experimental Testing of the Gigabit IPSec-Compliant Implementations of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board, Information Security Conference (ISC 2001), Malaga, Spain, 2001
[9] Elbirt A.J., Yip W., Chetwynd B., Paar C.: An FPGA-based performance evaluation of the AES block cipher candidate algorithm finalists, IEEE Transactions on Very Large Scale Integration (VLSI) Systems, Volume: 9 Issue: 4, August 2001
[10] Fischer V. and Drutarovsk´y M.: Two Methods of Rijndael Implementation in Reconfigurable Hardware, Cryptographic Hardware and Embedded Systems (CHES 2001), Paris, France, 2001
[11] McLoone M. and McCanny J.V.: High Performance Single-Chip FPGA Rijndael Algorithm Implementations, Cryptographic Hardware and Embedded Systems (CHES 2001), Paris, France, 2001
[12] McLoone M. and McCanny J.V.: Single-Chip FPGA Implementation of the Advanced Encryption Standard Algorithm, Field-Programmable Logic and Applications (FPL 2001), Belfast, Northern Ireland, UK, 2001
[13] McLoone W., McCanny J.V.: Rijndael FPGA implementation utilizing look-up tables, IEEE Workshop on Signal Processing Systems, 2001 [14] Dandalis A., Prasanna V.K., Rolim J.D.: A Comparative Study of Performance of AES Final Candidates Using FPGAs, Cryptographic Hardware and Embedded Systems Workshop (CHES 2000), Worcester, Massachusetts, 2000
[15] Elbirt A.J., Yip W., Chetwynd B., Paar C.: An FPGA Implementation and Performance Evaluation of the AES Block Cipher Candidate
Algorithm Finalists, Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000
[16] Gaj K. and Chodowiec P.: Comparison of the hardware performance of the AES candidates using reconfigurable hardware, Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000
[17] Gaj K. and Chodowiec P.: Hardware performance of the AES finalists-survey and analysis results, Technical Report, George Mason University, 2000, available at http://ece.gmu.edu/crypto/AES survey.pdf
[18] Ichikawa T. and Matsui T.: Hardware Evaluation of the AES Finalists Third Advanced Encryption Standard (AES3) Candidate Conference, New York, 2000
[19] Alireza Hodjat, Ingrid Verbauwhede, "A 21.54 Gbit/s Fully Pipelined AES Processor on FPGA", IEEE Symposium on Field Programmable Custom Computing Machines, April 2004.
[20] Kimmo U. Jarvinen, Matti Tommiska, Jorma Skytta, " A Fully Pipelined Memory less 17.8 Gbps AES-128 encryptor", FPGA 2003, Proceedings of the ACM/SIGDA International Symposium on Field Programmable Gate Arrays, February 23-25 2003, Monterey, CA.
[21] Alizera Hodjat, Ingrid Verbauwhede, "Minimum area Cost for a 30 to 70 Gbits/s AES Processor", Proceedings of IEEE Computer Society Annual Symposium on VLSI, Pages 83-88, February 2004
[22] Jon Edney, William A. Arbaugh, "Real 802.11 security: Wi-Fi Protected Access and 802.11i", ISBN 0-321-13620-9 , Chap9, July 15, 2003
[23] Tzi-Cker Chiueh, Prashant Pradhan, "Cache Memory Design for Network Processors" Proceedings of the Sixth International Symposium on High-Performance Computer Architecture, Pages 409-418, 2000
[24] Verbauwhede I., Schaumont P., Kuo H.: Design and performance testing of a 2.29-GB/s rijndael processor, IEEE Journal of Solid-State Circuits, Volume: 38 Issue:3, March 2003
[25] Lin T.F., Su C.P., Huang C.T., Wu C.W.: A high-throughput low-cost AES cipher chip, IEEE Asia-Pacific Conference on ASIC, 2002
[26] Lutz A.K., Treichler J., G¨urkaynak F.K., Kaeslin H., Basler G., Erni A., Reichmuth S., Rommens P., Oetiker S., Fichtner W., 2Gbit/s Hardware Realizations of RIJNDAEL and ERPENT: A Comparative Analysis, Cryptographic Hardware
[27] and Embedded Systems (CHES 2002), San Francisco Bay, CA, 2002
[28] Mayer U., Oelsner C., Kohler T.: Evaluation of different rijndael implementations for high end servers, IEEE International Symposium on Circuits and Systems (ISCAS 2002), 2002
[29] Morioka S. and Satoh A., An Optimized S-Box Circuit Architecture for Low Power AES Design, Cryptographic Hardware and Embedded Systems (CHES 2002), San Francisco Bay, CA, 2002
[30] Morioka S. and Satoh A.: A 10 Gbps full-AES crypto design with a twisted-BDD S-Box architecture, IEEE International Conference on Computer Design: VLSI in Computers and Processors, 2000
[31] Evangelos P. Markatos, Speeding up TCP/IP: Faster Processors are not Enough, The 21st IEEE International Performance, Computing and Communication Conference, 2001
[32] "Testing IEEE 802.11n", Test & Measurement World, April 1, 2007

BIOGRAPHY

Chakib Alaoui has obtained his Ph.D. om the University of Massachusetts at owell, USA, in 2001. He joined Taif niversity in January 2009 where he works s Assistant Professor. His research interests e in the area of VLSI and Embedded ystems.