FPGA Implementation Cost and Performance Evaluation of the IEEE 802.16e and IEEE 802.11i Security Architectures Based on AES-CCM

Ignacio Algredo-Badillo, Claudia Feregrino-Uribe, René Cumplido, Miguel Morales-Sandoval
Department of Computer Science, INAOE
Luis Enrique Erro 1, Puebla, México
{algredobadillo, cferegrino, rcumplido, mmorales}@inaoep.mx

Abstract

Software radios are communication devices with different configurations that enable to operate in different communication networks. Considering the OSI model, the main development of these radios is focused on the lower layers, which are implemented in hardware. Security is a key element for using software radios, because they can enter to different wireless networks and use the air like transmission medium, being vulnerable to possible attacks to the transmission of data. Several security architectures have been standardized for different networks, such as IEEE 802.11i-2004 for WLANs (Wireless Local Area Networks) and IEEE 802.16e-2005 for WMANs (Wireless Metropolitan Area Networks), operating on the MAC (Medium Access Control) sublayer. In this work, hardware implementations of these architectures are evaluated in terms of FPGA implementation costs and performance to be considered in a reconfigurable hardware platform, which supports both security architectures, working on the MAC sublayer. For the design of the reconfigurable platforms, it is required to examine characteristics such as hardware resources, throughput and reconfigurable/ nonreconfigurable modules with focus in the software-radio applications. These implementations of the proposed hardware architectures are based on the AES-CCM algorithm that is one of the most important cryptographic algorithms.

1. Introduction

In the world of the digital communications, there are many types of networks that have been widely developed, and mobility is a desirable feature that has extended the growth of the wireless communications. The wireless networks use different set of rules or protocols for governing the communication among diverse devices, and each network has applications that can use different protocols. Ideally, a device should operate in the diverse applications of the different wireless networks. This last idea is conceptualized by using software radios, which have different configurations for operating in different communication networks. Software radios have changed according to the technology advances, where it is possible to find a basic radio architecture, which has a key element, and it configures the radio to operate in the different networks. In this way, radios have been fixed designs, which have increased their flexibility, reporting transitions from software capable radios, transitioned into software programmable radios, and finally to software-defined radio (SDR). New capabilities for the software radios represent a great range for awareness, adaptability and the ability to learn, see Fig. 1 [1].

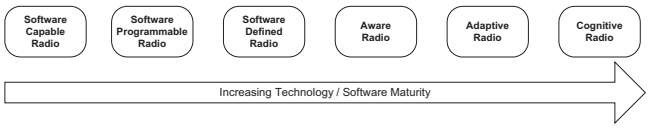

Figure 1. Evolution of the software radios.

The development of these radios, for example SDR, is focused on the lower layers of the OSI model, which are implemented in hardware [2]. At this point, it is important to highlight that software radios can enter to different networks and applications, furthermore, in these wireless communication networks, the transfer of the information uses the air like transmission medium, thus security attacks can appear, and these issues should be considered and solved. Nowadays, solutions are proposed to protect these networks through diverse mechanisms such as firewalls, cryptography, antivirus, intrusion detectors, secure routing, and security policy management, among others. One of the most important is the cryptography, which is based on algorithms and their operation modes. In this way, security based in cryptography is a key element in the recent standards of the communication networks, requiring modern enhancements, such as new cryptographic

IEEE Catalog Number: CFP08827-CDR
ISBN: 978-1-4244-2499-3
Library of Congress: 2008903800

algorithms, new operation modes of these algorithms and, considering these networks, their new security schemes that should solve other issues. Using cryptographic algorithms in demanding applications that communicate great amount of data requires computing complex operations. This computation causes that data flow slows down its speed. It is important to highlight that hardware cryptographic implementations have better performance than software implementations, exploiting advantages of the hardware design. Hardware architectures should consider the dataflow, the parallelization of processes, the specialized modules, and the synchronization of the modules and submodules.

In this work, two implementations for security protocols are evaluated to design a reconfigurable hardware platform, providing cryptographic services based on two security architectures of the IEEE 802.11i-2004 and IEEE 802.16e-2005. This platform is developed for software-radio applications operating in the MAC sublayer, which executes different configurations, and in this case, for two protocols of two different networks (WMAN and WLAN). This platform is based on a reconfigurable architecture, executing security services. To design this platform, characteristics such as hardware resources, throughput, efficiency and reconfigurable modules, are evaluated.

In Section 2, security architectures for IEEE 802.11i-2004 and IEEE 802.16e-2005 standards are described. In Section 3, hardware architectures are proposed based on modular designs focusing to the reconfigurable platform. These are implemented and their results are presented in Section 4. FPGA implementation cost and performance evaluation are described in Section 5. Finally, conclusions are drawn in Section 6.

2. Security Protocols

Security protocols for the widely-used wireless communication networks propose to use cryptographic solutions based on diverse cryptographic algorithms. This security is defined in the MAC sublayer, enabling communication networks to provide privacy, authentication, and confidentiality. These security services are based on cryptographic algorithms, which use several iterative mathematic operations. These algorithms protect data transmissions at the expense of high computational costs and cause bottlenecks in the data transmissions, thus architectures with high throughput are required, at least 1 Gbps, considering future data transmissions such as in the wireless networks [3] with application to transmit high-quality TV, movies in DVD, and great amount of digital files using personal computers, among others.

The AES algorithm in the CCM (Counter with Cipher Block Chaining - Messaging Authentication Code) mode is proposed to be implemented in the IEEE 802.11i-2004 and IEEE 802.16e-2005 standards. In the first standard, AES-CCMP (AES-CCM Protocol) presents the modern security architecture with advanced features based on AES-CCM algorithm, incorporating two cryptographic operation modes to provide a robust security protocol in the data transference. The IEEE 802.11i-2004 standard replaces Wired Equivalent Privacy in the original IEEE 802.11 standard with the Advanced Encryption Standard (AES) in CCM mode. In the same way, IEEE 802.16e-2005 standard has specified security mechanisms, using the AES-CCM algorithm to provide better security services, although it is required to execute a great number of operations, several iterations, and multiple processes. In this work, proposed hardware architectures are based on the AES-CCM, using parallelization and modular specialization, and reducing critical path without increasing the execution latency.

AES-CCM algorithm. Traditionally, two different cryptographic algorithms are used to provide privacy and authentication, but AES-CCM algorithm provides these two security services with the same algorithm, using the AES block cipher and the same key. CCM uses the CTR (Counter) mode and CBC-MAC (Cipher Block Chaining - Message Authentication Code) [4]. The privacy is provided by the AES algorithm in CTR mode, requiring a value that ensures uniqueness. The authentication is performed by the AES algorithm in CBC-MAC mode and provides additional capabilities; CBC-MAC is an integrity method that ensures that every cipher block depends on every preceding part of the plain text, where ciphering two identical blocks results in different cipher blocks.

IEEE 802.11i-2004 Standard. AES-CCMP provides data confidentiality, integrity, and replay-attack protection, operating on the MAC Protocol Data Unit (MPDU), see Fig. 2 [5]. MPDU contains several fields, including, for example, the payload, the length of payload, and header of the MAC sublayer. In general, the security architecture based on AES-CCMP ciphers data input (plaintext MPDU), using AES-CCM algorithm, and resulting the data output Cipher MPDU. AES-CCMP disassembles each packet in KeyID, packet number (PN) and plaintext MPDU (Medium Access Control Protocol Data Unit). Reuse of a PN with the same temporal key voids all security guarantees. A temporal key (TK) is required for every ciphering session. MPDU is expanded in several fields, such as payload DataP, Address 2 (A2), a priority octet, and the MAC Header. With these fields, a CCMP Header is constructed as well as a Nonce value (unique for each frame protected by a given TK and a 48-bit PN) and the additional authentication data (AAD). The payload, TK, Nonce value and ADD are input to the AES-CCM. It outputs the cipher data and message integrity code (MIC) that are used together with the CCMP and MAC headers to build the Cipher MPDU.

AES-CCM is the main cryptographic algorithm, which

IEEE Catalog Number: CFP08827-CDR
ISBN: 978-1-4244-2499-3
Library of Congress: 2008903800

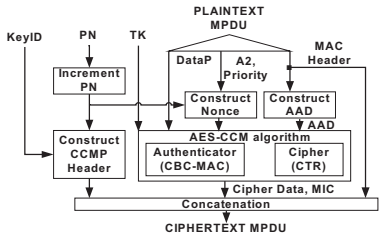

Figure 2. Security architecture based on the AES-CCM protocol for IEEE 802.11i networks.

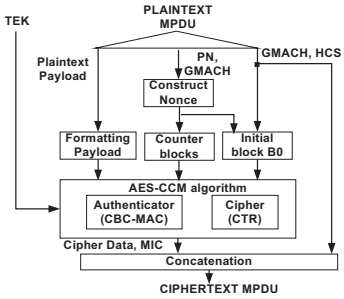

Figure 3. Related processes for ciphering in the IEEE 802.16e-2005 standard.

executes two related processes: generation-encryption and decryption-verification. For the purposes of this work, which is focused to the reconfiguration of a transmission platform, the generation-encryption process is considered to design the architecture. CBC-MAC process is applied to the payload DataP, the data associated AAD, and the nonce to generate a MIC (Message Integrity Code) whereas CTR mode is applied to the MIC and the payload DataP to obtain the ciphertext (Cipher MPDU).

IEEE 802.11e-2005 Standard. The IEEE 802.16e-2005 security scheme has two component protocols: management key (PKM) and encapsulation [6]. In the general operation of the encapsulation protocol, ciphering is applied to the MAC PDU payload for privacy service, whereas in the PKM, this protocol allows for authentication. In the encapsulation, data are protected by ciphering the information or plaintext payload, and by providing a value for the message integrity. Ciphering payload requires that two values shall be appended: packet number (PN) and message authentication code (MIC), and AES-CCM algorithm shall be applied to the plaintext payload, see Fig. 3. For applying AES-CCM algorithm, other related main functions should be executed, formatting data input such as plaintext payload, counter blocks, initial block, nonce value, packet number (PN), and generic MAC header (GHMAC). These functions are described in the security scheme of the standard.

In the Section 3, hardware architectures using the AES-CCM algorithm are proposed, which combine parallelized structures with low hardware resource requirements.

3. Proposed Hardware Architectures

The proposed hardware architectures are based on modular designs, focusing on high throughput. This is reached by making an analysis to reduce critical path by developing specialized modules, proposing compact control units, identifying parallelization of the data buses and modules, and balancing paths formed by the combinational and sequential elements. For evaluation purposes and for developing the reconfigurable platform, these architectures are implemented in FPGA devices, reporting high hardware implementation efficiency. The design of the architectures is written in VHDL and simulated using FPGA Advantage 6.3.

The used hardware design methodology in this work is based on designing a straightforward initial hardware architecture (considering specific parameters), and later, exploiting hardware advantages such as loop unrolling, pipelining, and using embedded hardware resources [7], and making trade-off analysis to decrement critical path. The aim is to get architectures with higher throughputs and lower hardware resources, i.e., a highly efficient hardware implementation or throughput/area ratio. The implementation efficiency (Gbps/slices) is a measurement of this type of cryptographic hardware implementations and it is defined as the ratio between the reached throughput and the number of slices that each implementation consumes [8].

AESCCMP Hardware Architecture. For the IEEE 802.11i-2004 standard, it is proposed the AESCCMP hardware architecture. The AES-CCMP hardware architecture is illustrated in Fig. 4. From Fig. 2, Increment PN and Construct CCMP Header blocks are considered to be executed in an upper layer. The AESCCMP hardware architecture is constituted by specialized modules to format data (Format_N&Q, Format_AAD, Format_Payload, and Format_CB), to compute AES-CCM algorithm (AESCCM) and main control (Control_CCMP). Each module to format data has its particular control submodule. The main control module is based on Finite State Machines (FSMs). AESCCM module executes AES-CBC-MAC and AES-CTR submodules in parallel, which compute AES-CBC-MAC and AES-CTR algorithm, respectively.

The general operation consists on processing two sources of data, parsed in 128-bit data blocks, and the same 128-bit key block through AESCCM module. The first source generates data blocks from three different modules (PAY_N&Q, PAY_AAD, and PAY_PAY) to compute the

IEEE Catalog Number: CFP08827-CDR
ISBN: 978-1-4244-2499-3
Library of Congress: 2008903800

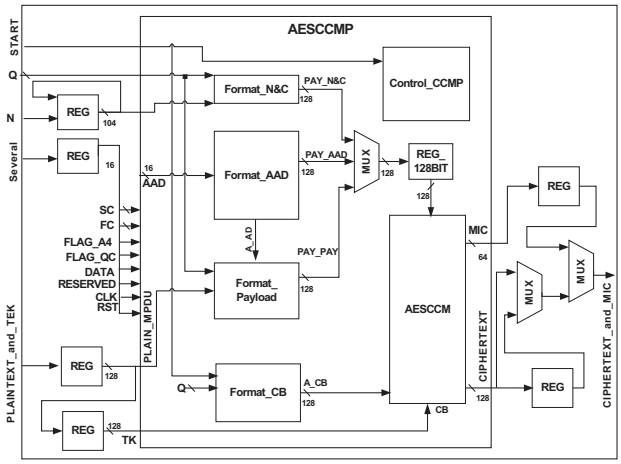

Figure 4. Block diagram of the AESCCMP.

MIC value in the AES-CBC-MAC submodule, whereas the second source takes data blocks from the same module (Format_CB) to compute cipher data in the AES-CTR submodule. After processing all data blocks, AESCCM generates the cipherdata Cipher_MPDU and the U value.

AESCCM6 Hardware Architecture. For the IEEE 802.16e-2005 security standard, it is proposed a hardware architecture based on the AES-CCM algorithm. The aim of this work is to implement a fast and simple iterative security hardware architecture with low FPGA resource requirements. The proposed hardware architecture, named AESCCM6, and it is illustrated in Fig. 5.

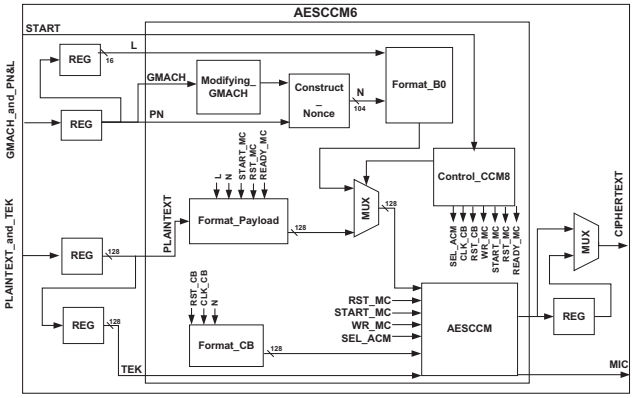

Figure 5. Block diagram of the AESCCM6.

This architecture is based on the security scheme of the standard, see Fig. 3. This architecture is constituted by specialized modules to format data (Modifying_GMACH, Construct_Nonce, Format_Payload, Format_B0, and Format_CB), to compute AES-CCM algorithm (AESCCM module), more details are in Section 2. The dataflow is managed by the main control. Format_Payload executes a complex process due to the variable length L of the plaintext payload, so, this module has a particular control submodule. Similar to AESCCMP hardware architecture, main control is based on an FSM, generating flag and control signals to the dataflow, whereas AESCCM module computes AES-CBC-MAC and AES-CTR processes in parallel form. The general operation consists on processing two sources of data, parsed in 128-bit data blocks, and the same 128-bit key block through AESCCM module. The first data source is taken from two different data blocks (Format_Payload and Format_B0) to compute the MIC value in the AES-CBC-MAC submodule, whereas the second data source is taken from the module Format_CB to compute ciphertext in the AES-CTR submodule. After processing all data blocks, AESCCM generates the Ciphertext and MIC value. Computation of the AES algorithm in the AESCCM blocks is executed by an iterative and compact module, which reports high performance based on several studies [9].

4. Implementations

The synthesis results of the AESCCMP and AESCCM6 hardware architecture are presented in this section. For the purpose of validation and comparison, these architectures were synthesized, mapped, placed and routed for three FPGA different technologies: Virtex-5, Virtex-4. And Spartan-3 The synthesized architectures were simulated and verified considering real-time operation condition by using the design conformance test data, which are provided by the IEEE 802.11i-2004 and IEEE 802.16e-2005 standards.

Data input loading and data blocks generation are performed in parallel. If these hardware architectures cipher data and they are maintained in the ciphering loop, their output buses will offer 128-bit cipher data every ten clock cycles for 128-bit plain data and 128-bit key data. The throughput of these iterative architectures is given by (1).

$$Throughput = \frac{Plain\_data\_block\_size \times Clock\_period}{Clock\_cycles} \quad (1)$$

Table 1 shows implementation results of these hardware architectures in three different FPGA devices, where the implementations on Virtex-5 and Virtex-4 support more than 1 Gbps, and the implementations on Spartan-3 is close to 1 Gbps. The designs reported in this work were implemented in configurable devices for evaluation and validation purposes. These architectures can be considered in the design of application-specific hardware devices that are aimed to meet standards in the new applications and be used in more demanding applications of cryptographic computational power in the wireless communications.

IEEE Catalog Number: CFP08827-CDR
ISBN: 978-1-4244-2499-3
Library of Congress: 2008903800

Table 1. Implementation results of the AESCCMP and AESCCM6 architectures for three technologies.

Parameter/Device	AESCCMP	AESCCM6	AESCCMP	AESCCM6	AESCCMP	AESCCM6
	Xc5vlx50-1ff676		Xc4vfx12-10ff668		Xc3s1000-4fg676	
Period (ns)	7.847	8.768	10.510	10.373	15.838	16.441
Clock(MHz)	127.43	114.05	95.14	96.40	63.13	60.82
IOBs	269	309	269	309	269	309
LUTs	2378	2324	5545	5447	5511	5336
Slices	1615 SRs	1221 SRs	3451	3228	3435	3205
	2932 SLs	2721 SLs				
BRAM	10	10	10	10	10	10
Throughput (Gbps)	1.631	1.459	1.217	1.233	0.808	0.778
Efficiency	1.009 /SRs	1.195 /SRs	0.352	0.381	0.235	0.242
(Gbps/slice x10^{-3})	0.556 /SLs	0.536 /SLs				

5. Comparisons and Evaluation

In this Section, FPGA implementation costs and performance evaluation are discussed for the design and development of the security software-radio platform with reconfigurable architecture. For implementation costs, characteristics such as utilized resources, period, clock frequency, and latency are considered, see Table 1. For performance evaluation, characteristics such as throughput and efficiency are considered. These studies and performance measurements of the AESCCMP and AESCCM6 implementations are used to design the security software-radio platform with reconfigurable architecture.

Firstly, considering only the AESCCMP or AESCCM6 hardware architecture, different device families (Virtex versus Spartan) will yield different implementation cost and performance, and where newer technologies (Virtex-5 versus Virtex-4) present shorter periods or higher operation clock frequencies.

Comparing AESCCMP against AESCCM6, the first one has a design, which uses slightly more hardware resources for the hardware platform. This is due to the specific modules, which execute different formatting of data and specifications. This difference in LUTs and slices is not very important, considering that a part of the FPGA will be selected for the reconfiguration. The two architectures for two different networks can be supported in the same reconfigurable platform. All implementations use ten BRAMs, situation that enables a consistency in the architectures. These BRAMs are used to implement S-boxes, which are required by the AES cipher. An important detail is the disparity on the use of the IOBs. These pins should be distributed, considering the reconfiguration of the device. The designs of these architectures for the reconfiguration should select tasks to be executed by the input/output data, evaluating reconfigurable/ nonreconfigurable modules, which require connections to the exterior. Excepting in Virtex-4, the AESCCMP implementation reports better performance than compared with AESCCM6 implementation. The minimized area resources of AESCCMP and AESCCM6 do not decrease the system performance, which reach throughput superior to 1 Gbps. This data rate is much higher compared with the highest specified by the IEEE 802.11 standards. These security architectures of the standards are the elements that execute more operations at high computational cost. According to (1), Plain_data_block_size and Clock_cycles have fixed values, 128 bits and 10 clock cycles, respectively, but Clock_period is defined by the implementation results, which produces different throughputs and efficiency for the implementations in the diverse technologies. If this value is to set a fixed value, both AESCCMP and AESCCM6 architectures will report the same throughput on the reconfigurable platform, where hardware resources are just selected for reconfiguration or configuration, where a similar efficiency can be obtained.

Comparing against related works, see Table 2, it is important to highlight that these implementations report high throughput and efficiency, characteristics that can be affected by implementing on a reconfigurable platform. There are many works reporting AES-CCM operations, but few works present complete security architectures executing operations based on AES-CCM. The period of each implementation should be analyzed to improve the performance of the platform, which is affected when reconfigurable architectures are mapped and reconfigurable modules are reused. For AESCCMP architecture, related works report different AES-CCMP implementations on FPGA [10] - [13], the proposed AESCCMP implementation reports the highest throughput and efficiency, allocating less area than [12] and [13], with higher operation frequency. For AESCCM6 architecture, few works have been reported, implemented on FPGAs [14]. The throughput values do not present any results, and diverse devices are considered to implement the architecture. Based on the above compar-

IEEE Catalog Number: CFP08827-CDR
ISBN: 978-1-4244-2499-3
Library of Congress: 2008903800

Table 2. Related works of 802.11i-2004 and 802.16e-2005 hardware architectures.

Work/ Standard	Slices	BRAM	Clock (MHz)	Throughput (Gbps)
[10]-802.11i	523	-	63.70	0.127
[11]-802.11i	3750	-	50.00	0.243
[12]-802.11i	3474	15	80.30	0.275
[13]-802.11i	5605	-	50.00	0.258
[14]-802.16e	-	-	93.00	-
[14]-802.16e	-	-	197.00	-

ison results, it can be mentioned that the AESCCMP and AESCCM6 implementations are proposed for applications with special needs in both, area resources and operation frequency.

6. Conclusions

Software radio is a hot research topic with focus on designing and developing hardware elements that present capabilities of high flexibility and performance. In these radios, security is a key characteristic to protect the transmissions of data in the wireless networks. The implementation costs and performance evaluation of the proposed security architectures from two different networks, such as WMAN and WLAN, enable to design and propose a reconfigurable platform, which support these implementations, using similar hardware resource and reporting efficiency. Due to the latency of ten clock cycles in both implementations, the same throughput is reached by establishing a clock for the reconfigurable platform. Finally, efficiency is a characteristic, which is affected by the throughput and hardware resources used for each implementation. If the same resources are used to partition reconfigurable and nonreconfigurable elements, and the throughput is the same, a similar efficiency is obtained.

References

[1] B. A. Fette, "Cognitive Radio Technology: Using TPM in Embedded Systems", Newnes, ISBN 0750679522, 2006, ch 4, pp. 119-133.

[2] Center for Software Defined Radio, "Software Defined Radio: Terms, Trends and Perspectives", White Paper, January 2007. Available: www.csdr.ck.

[3] ICT-Centre, "Multi Gigabit Millimeter Wave Wireless", Innovative ICT transforming Australian industries, 2008. Available: www.ict.csiro.au/index.php.

[4] M. Dworkin, "NIST Special Publication 800-38C. Recommendation for Block Cipher Operation modes: The CCM Mode for Authentication and Confidentiality", National Institute of Standards and Technology (NIST), May 2004.

[5] LAN/MAN Standards Committee, "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications" IEEE Std 802.11i-2004, IEEE Computer Society, July 2004.

[6] LAN/MAN Standards Committee of the IEEE Computer Society and the IEEE Microwave Theory and Techniques Society, "Part 16: Air Interface for Fixed and Mobile Broadband Wireless Access Systems", IEEE Std 802.16e-2005, IEEE Standard for Local and Metropolitan Area Networks, February 2006.

[7] R. Chaves, G. K. Kuzmanov, S. Vassiliadis, and L. A. Sousa, "Reconfigurable Memory Based AES Co-processor", International Parallel and Distributed Processing Symposium 2006 (IPDPS 2006), IEEE Computer, pp. 446-455, 2006.

[8] N. Sklavos, G. Selimis and O. Koufopavlou, "FPGA Implementation Cost and Performance Evaluation of IEEE 802.11 Protocol Encryption Security Schemes", Journal of Physics: Conference Series 10 (2005), pp. 361-364, Second Conference on Microelectronics, Microsystems and Nanotechnology, 2005.

[9] Algredo-Badillo I., Feregrino-Uribe C., Cumplido-Parra R., "Design and Implementation of an FPGA-Based 1.452-Gbps Non-pipelined AES Architecture", ICCSA 2006, Lecture Notes in Computer Science 3982, pp. 446-455, Springer-Verlag, 2006.

[10] A. Aziz, A. Samiah, and N. Ikram, "A Secure Framework for Robust Secure Wireless Network (RSN) using AES-CCMP", 4th International Bhurban Conference on Applied Sciences and Technology, June 2005.

[11] J. H. Shim, T. W. Kwon, D. W. Kim, J. H. Suk, Y. H. Choi, and J. R. Choi, "Compatible Design of CCMP and OCB AES Cipher Using Separated Encryptor and Decryptor for IEEE 802.11i", Proceedings of the International Symposium on Circuits and Systems, 2004. ISCAS '04, pp. III- 645-8 vol. 3, ISBN: 0-7803-8251-X, 2004.

[12] N. Smyth, M. McLoone, and J. V. McCanny, "WLAN Security Processor", IEEE Transactions on Circuits and Systems I: Fundamental Theory and Applications, Vol. 53, Issue 7, pp: 1506- 1520, ISSN: 1057-7122, 2006.

[13] D. Bae, G. Kim, J. Kim, S. Park, and O. Song, "An Efficient Design of CCMP for Robust Security Network", ICISC 2005, Lecture Notes in Computer Science 3935, pp. 352-361, Springer-Berlin, 2006.

[14] Jetstream Media Technologies, "JetCCM-6: 802.16e WiMAX AES-CCM Core", Datasheet, 2006. Available: www.security-cores.com.

IEEE Catalog Number: CFP08827-CDR
ISBN: 978-1-4244-2499-3
Library of Congress: 2008903800