Secure Multicarrier Modem on FPGA

Galia Marinova, Vassil Guliashki, Didier LeRuyet and Maurice Bellanger

Abstract — **The paper deals with the design and realization of a secure multicarrier modem on FPGA. The crypto-modem principle is adopted. An encryption block is integrated in the modem transmitter and a decryption block is integrated in the modem receiver. Different Encryption/Decryption IPs (Intellectual Properties) implementing DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advanced Encryption Standard) algorithms are developed and/or adapted in order to estimate the feasibility as well as the time and area efficiency of the crypto-modem. The design language used is VHDL and the crypto-modem system is validated in ISE environment, using Xilinx development board with XC4VSX35 circuit from VIRTEX-4 family.**

Index Terms— **Secure multicarrier modem, DES, 3DES, AES crypto-processing cores, FPGA realization**

I. Introduction

Modem-based attacks are occurring with increasing frequency due to the Internet Protocol-based security [6], that most organizations have applied to their Internet Protocol networks. In [23] it's stated that dialup Internet access from desktop systems using modems is in fact the second biggest security risk in corporations, after the internal threat posed by employees. Security needs of geographically or globally distributed enterprises are not guaranteed by traditional methods. Crypto-modems are the best solution for modem security, but it has the highest cost in terms of time latency and surface area on FPGA [11, 19-22]. Secure encrypting modems work between pairs (or groups) of similarly configured modems which not only restrict access to authorized connections, but they encrypt all data transmission to safeguard against eavesdropping on phone lines.

There are some realizations of secure modems as crypto-modems for mobile data security, described in [25]. The Palladium Secure Modem [12] is a credit-card size modem that uses the Skipjack algorithm to combine V.34 data communications with encryption and decryption. The Secure Telephone Unit Third Generation (STU - III) uses a Secure Access Control System (SACS) [18]. The Secure Terminal STE cryptographic engine is on a removable PC Memory Card [18]. More about different crypto-core algorithms and applications can be found in [5].

Our research concerns the security of a multicarrier filter bank based modem which main core is described in details in [14]. In [15] some commercial IP crypto-cores from Xilinx Corp. (X_DES from [2], X_3DES from [3] and XF_DES from [4]) were integrated in the secure modem design and their performance was estimated. Those cores are not suitable for design optimization and we continued the research in order to develop a flexible IP crypto-core library by studying and adapting some open crypto-core solutions [1,13,24] and by developing proprietary IP blocks for DES, 3DES and AES [8-10] encryption standard implementations. The paper presents the results from this study. First we present the specification of the secure multicarrier modem, then we consider the integration of different crypto-processing IP blocks in the multicarrier modem and finally we present results for efficiency estimations in time and surface area for the FPGA-based secure modem realizations integrating different crypto-cores.

II. Specification of the Secure Multicarrier Modem

The IP blocks from the filter bank based multicarrier modem core are developed in VHDL, validated on FPGA and stored in a Data Base with IP blocks for modem design – OQAM modulation in transmitter, Synthesis Filter Bank which integrates an IFFT and a Polyphase Network, Interpolator, Decimator, Analysis Filter Bank which integrates Polyphase Network and FFT, Equalizer with channel coefficient estimation, OQAM demodulation in receiver. The Low Density Parity Check (LDPC) Encoder and Decoder blocks [26] are available in proprietary VHDL realizations.

The security of the modem follows the crypto-modem principle and it is realized through the integration of an encrypting block in the transmitter and a decrypting block in the receiver. Encryption and decryption in secure modem couples (or groups) are realized through key exchange. Three types of encryption and decryption blocks are adapted, developed and studied – DES, 3DES and AES IPs. The type of the encryption algorithm determines the key length and the encrypted/decrypted data organization. . It determines also the time latency and the surface area on the FPGA added by the

Manuscript received March 22, 2007. This work was partly supported by NATO grant CLG 981551/2005.

Galia Marinova is with the Faculty of Telecommunications in Technical University - Sofia, 8, bul. Kliment Ohridski, Sofia-1000, Bulgaria,
phone: 3592 965 31 88, e-mail: gim@tu-sofia.bg

Vassil Guliashki is with the Institute of Information Technologies, BAS, Sofia, Bulgaria,
e-mail: vggul@yahoo.com

Didier Le Ruyet is with the Laboratory Electronics and communications, CNAM-Paris, France,
e-mail: leruyet@cnam.fr

Maurice Bellanger is with the Laboratory Electronics and communications, CNAM-Paris, France,
e-mail: bellang@cnam.fr

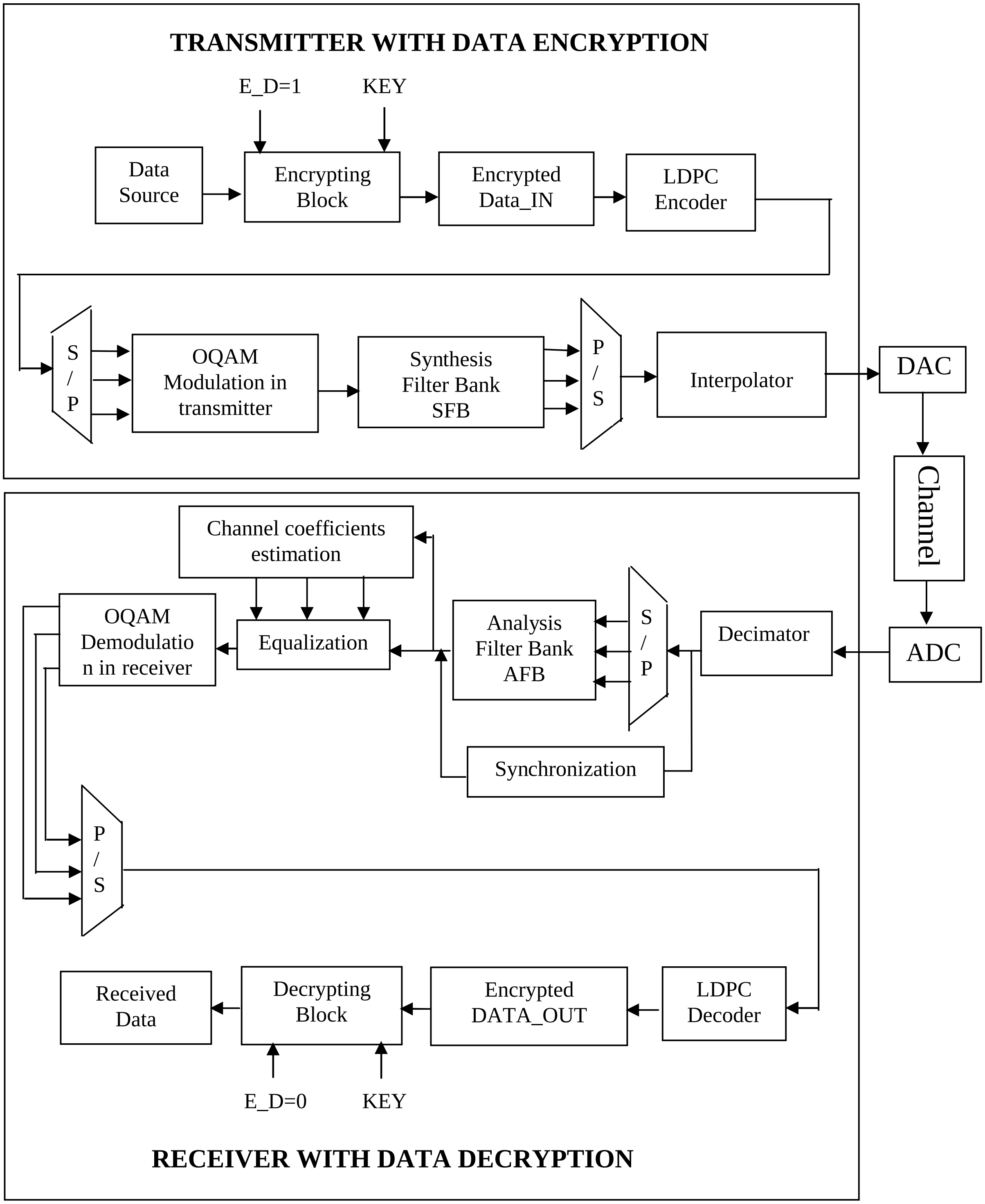

Figure 1. Multicarrier modem with data encryption and decryption.

encryption/decryption IPs.

Fig. 1 presents the specification of a filter bank based multicarrier modem core with data encryption and decryption.

III. Integration of Cryptoprocessing Intellectual Property Blocks in the Multicarrier Modem

We experienced the secure multicarrier modem design by integrating three types of crypto-cores: DES, 3DES and AES crypto-cores.

- DES crypto-core – The principle of DES algorithm [7, 16] consists in an initial permutation, followed by 16 rounds (iterations) and a final permutation at the end. The DES crypto-core we adapted is from [13]. It uses a 64-bit key and it treats a 64-bit data block. The encryption and the decryption follow the same algorithm, only the key processing steps are inverted. The choice of encryption or decryption mode is done through the signal E_D which is "1" for encryption and "0" for decryption. The DES crypto-core IP treats a 64-bit data block in 16 clock cycles.
- 3DES crypto-core – The 3DES crypto-core is developed on the base of the DES crypto-core. In our case, it supports two independent 64-bit keys. A triple DES encryption operation with 2 independent keys consists of the transformation of a 64-bit data block I into a 64-bit data block O, defined as follows:

$$O = E_{K1}(D_{K2}(E_{K1}(I))),$$

where $E_K(I)$ and $D_K(I)$ represent the DES encryption and decryption of I, using DES key Kn (where n=1,2).

A triple DES decryption operation with 2 independent keys consists in the transformation of a 64-bit data block I into a 64-bit data block O, defined as follows:

$$O = D_{K1}(E_{K2}(D_{K1}(I)))$$

Compared to the DES algorithm, the triple DES algorithm provides a much higher level of security. The 3DES crypto-core IP treats a 64-bit data block into 48 clock cycles.

- AES crypto-core – It implements the Advanced Encrypting Standard [10, 17], based on the cryptographic algorithm, created by Rijndael [8, 9]. In the presented secure modem application the plain text data are encrypted/decrypted in blocks of 128 bits, using 128-bit key size.

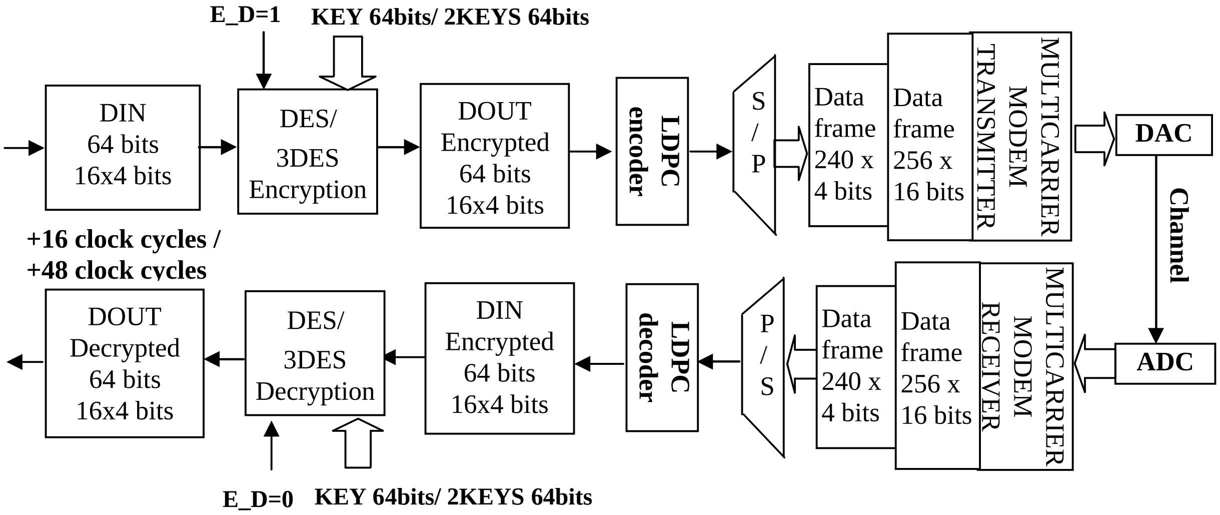

Figure 2. Integration of DES and 3DES crypto-cores in the secure multicarrier modem

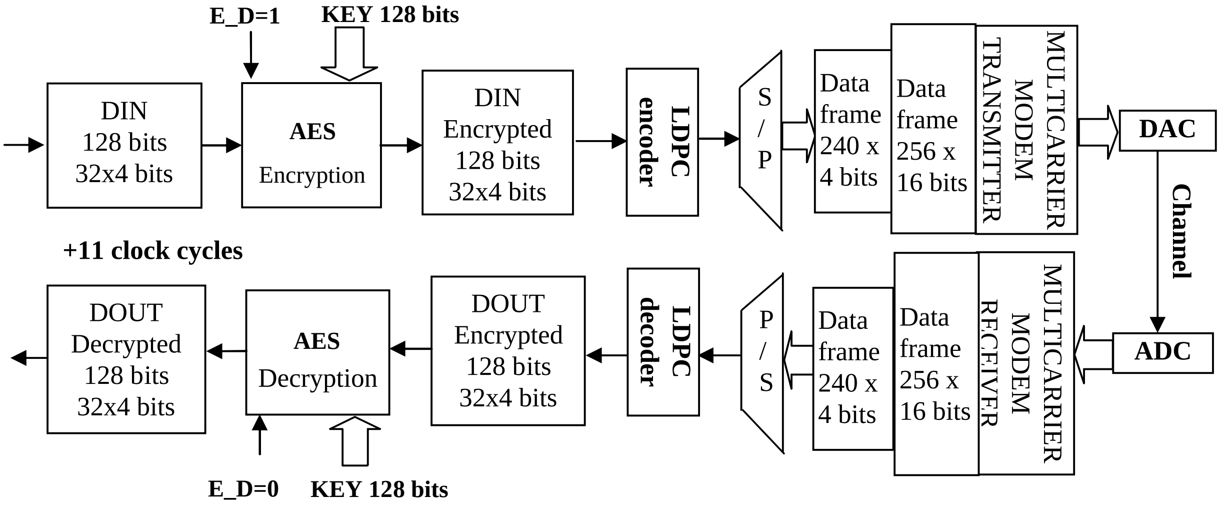

Figure 3. Integration of AES crypto-core in the secure multicarrier modem

The AES algorithm consists of a complex non-linear function, which is iterated multiple times (rounds) starting from the incoming plain text data block. There is an initial pre-processing round at the start of every encryption. The number of rounds required depends on the selected key size – in our case with 128-bit key size 10 rounds are necessary, or together with the initial pre-processing round 11 rounds in total. Each round requires an unique 128-bit round key schedule. The necessary schedules are generated by means of a key expansion algorithm using the supplied initial 128-bit key. Eleven key schedules are necessary for this key size. They can be generated in real time, when they are required by the encryption algorithm. They might also be generated off-line and they might be stored in an internal RAM. We realized the last possibility in this application by means of AES cores, which cover both encryption/decryption functions and key expansion for 128-bit key size. The cores implement all the building blocks of AES algorithm individually and they are easily integrated in the created VHDL code. The AES crypto-core IP treats a 128 bits data block into 11 clock cycles. In AES decryption algorithm the basic transformations used in AES encryption algorithm are inverted. The sequence of these transformations differs in the straightforward AES decryption algorithm, from that one of the AES encryption algorithm. However, by means of a change in the key schedule an equivalent AES decryption algorithm, having the same order of transformations as the encryption algorithm, is obtained. This decryption algorithm has a more efficient structure than that one of the straightforward AES decryption algorithm. In our application we implemented the equivalent AES decryption algorithm. The selection of encryption or decryption mode is done through the signal E_D, which is "1" for encryption and "0" for decryption.

Fig. 2 presents the data organization in a secure multicarrier modem integrating DES or 3DES crypto-cores. Fig. 3 presents the data organization in a secure multicarrier modem integrating an AES crypto-core. The data frame that is treated in the multicarrier modem core has 256 data and they are coded on 16 bits in two's compliment. 240 sub-channels over 256 available sub-channels in the modem are used for data transmission and 4bits are transmitted by sub-channel. It determines the data organization in the three cases of crypto-processing cores integration. A frame with 240x4-bit encrypted data is formed at the entry of the multicarrier modem transmitter and at the output of the multicarrier modem receiver.

IV. Efficiency estimation of secure modem solutions

The secure multicarrier modem realizations using three different types of crypto-cores are designed in VHDL language and they are simulated in ISE 8.2 environment. Then they are realized on Xilinx development board with XC4VSX35 circuit from the VIRTEX-4 family from [27]. The clock frequency of the FPGA used is 500 MHz.

Detailed estimations of time and surface area parameters of the multicarrier modem core IP blocks, like OQAM modulation/demodulation, blocks, FFT/IFFT, polyphase network, equalizer, can be found in [14]. The three types of crypto-cores integrated to the multicarrier modem for ensuring its security formed three different secure modem architectures and implementations. All three crypto-cores treat serially a number of data blocks in order to form the 240x4bits data frame at the entry of the transmitter or in order to treat the 240x4bits data frame at the output of the multicarrier modem receiver. A serial crypto-processing of data blocks is adopted in order to improve surface area efficiency. The architectures and the implementations were estimated in order to find the time latency and the surface area on the FPGA, added by each one crypto-core. Table I presents the estimation of time efficiency in clock cycles for the three crypto-cores. In the case of AES

Table I. Estimation of time efficiency in clock cycles for the three crypto-cores

Crypto-cores	Number of bits per block	Clock cycles per encrypted data block	Number of encrypted data blocks per frame with 240x4-bit data	Number of clock cycles per frame with 240x4-bit data
DES	64 bits	16	15	240
3DES	64 bits	48	15	720
AES	128 bits	11	8	89

Table II. Time and frequency parameters of the secure modem core

IP block		**Time per frame**		
OQAM modulation in transmitter/ OQAM demodulation in receiver		10ns		
SFB/ AFB	**IFFT/FFT**	18μs		
	Polyphase network	15μs		
Equalizer		3.6μs		
Multicarrier modem core		36.61μs		
Frequency per frame		27.31kHz per frame		
Crypto-processing core		**DES**	**3DES**	**AES**
		480ns	1.44μs	178ns
Frequency per frame 256x16bits		26.96 kHz	26.28 kHz	27.18 kHz
Frequency per data 16 bits		6.9 MHz	6.73 MHz	6.96 MHz

crypto-block one clock cycle is added at the end of encryption/decryption processing.

Table II presents results related to time efficiency of the three architectures of the secure modem with DES, 3DES and AES crypto-cores. The frequency per 256-bits data frame and the frequency for 16-bits data of the secure modem are estimated and they are compared to the non secure modem core frequency. The AES crypto-core insures the best time efficiency parameters. Table III presents data for the surface area added to the multicarrier modem core by the three different types of crypto-cores – DES, 3DES and AES. The estimation is made for a XC4VSX35 circuit from the Xilinx VIRTEX-4 family

Table III. Surface area of the modem crypto-cores on XC4VSX35 circuit

Crypto-processing IP	GCLK	LUT	Number of Slices Flip-Flops	Number of Slices
DES	1%	4%	1%	4%
3DES	1%	5%	1%	5%
AES	1%	4%	1%	10%

V. Conclusion

The paper presents results from a research on secure multicarrier modem solutions. The IP core library for the multicarrier modem core is completed with three types of crypto-processing cores – DES, 3DES and AES, which permit flexible design of secure multicarrier modems on FPGA. The estimations of time latency and surface area efficiency demonstrate that the deteriorations of multicarrier modem performance due to the studied crypto-cores is negligible. All three solutions are feasible on FPGA. The best one in time efficiency is the AES crypto-core solution and it allows increased data throughput.

This experience can be used later for the design of other secure modems with different parameters for example according to the 802.11 wireless communication standard (WiFi).

References

[1] AES (Rijndael) IP-cores for encryption/decryption and key expansion, ErSt Electronic GmbH, Switzerland, April 2006, http://www.opencores.org

[2] Alliance core, "X_DES cryptoprocessor", Xilinx Corporation, February 9, 2001.

[3] Alliance core, "X_3 DES triple DES cryptoprocessor", Xilinx Corporation, February 9, 2001.

[4] Alliance core, "XF_DES data encryption standard engine core", Xilinx Corporation, September 16, 1999.

[5] Anderson R., Bond M., Clulow J., and Skorobogatov S., “Cryptographic processors – a survey” , Proceedings of IEEE, Vol. 94 No.2, February 2006, pp. 357-370.

[6] Collier M. D., "Enterprise telecom security solutions", Secure Logix, available at: http://www.securelogix.com, 2004.

[7] De Canniere C., Biryukov A., and Preneel B., “An introduction to block cipher cryptoanalysis”, Proceedings of IEEE, Vol. 94 No.2, February 2006, pp. 346-357.

[8] Daemen J. and Rijmen V., AES Proposal: Rijndael, “AES algorithm submission”, September 3, 1999, available at: http://www.nist.gov/CryptoToolkit

[9] Daemen J. and Rijmen V., “The block cipher Rijndael”, Smart Card research and Applications, LNCS 1820, Springer-Verlag, pp. 288-296.

[10] Federal Information Processing Standards Publication 197 (FPSP 197), “Announcing the Advanced Encryption Standard (AES)”, November 26, 2001, available at: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[11] IEEE Power Engineering Society, *IEEE Guide for Electric Power Substation Physical and Electronic Security*, IEEE Standard 1402-2000, New York, NY, April 4, 2000.

[12] Kasten Chase Applied Research Limited, "RASP secure access: palladium secure modem", User's Guide, July 2001, available at: http://www.kastenchase.com

[13] Lagger A., “Implementation of DES algorithm using FPGA technology”, 2003, available at: http://lsmwww.epfl.ch/Education/reports/lagger_report_2003.pdf

[14] Marinova G., Guliashki V., LeRuyet D., Bellanger M., "Multicarrier modem core on FPGA", in Proceedings of the 13-th IEEE Mediterranean Electrotechnical Conference MELECON’2006, *Circuits and Systems for Signal and Image Processing, Information and Communication Technologies and Power Sources and Systems*, edited by Francisco Sandoval, Carlos Camacho and Antonio Puerta; Benalmagena (Malaga), Spain, May 16-19, 2006, pp. 66-69.

[15] Marinova G., Guliashki V., “Security solutions for modem communications”, Proceedings of National Conference with international participation *ELECTRONIKA’*2006, Sofia, Bulgaria, June 1-2. 2006, pp. 287-292.

[16] Mazzeo A., “Special issue on cryptography and security”, Proceedings of IEEE, Vol. 94 No.2, February 2006, pp. 343-346.

[17] National Institute of Standards and Technology Special Publication 800-21 (NIST SP 800-21), “Guideline for implementing cryptography in the Federal Government”, available at: http://csrc.nist.gov/publications/

[18] National Security Agency (NSA), "Secure telephone unit - third generation (STU III) / secure terminal equipment (STE)", USA, July 2005, available at: http://www.fas.org/irp/program/security/_work/stu3.html

[19] National Security Telecommunications Advisory Committee Information Assurance Task Force, "Electric power risk assessment", March 1997, available at http://www.ncs.gov/n5_hp/Reports/EPRA/electric.html

[20] Oman P., "Low cost authentication devices for secure modem and network connections", Application Guide, Volume VII, AG2001-10, Schweitzer Engineering Laboratories, SEL 2001, USA, available at: http://www.selinc.com

[21] Oman P., E. Schweitzer, and D. Frincke "Concerns about intrusions into remotely accessible IEDs, controllers, and SCADA systems", in *Proceedings of the 27-th Annual Western Protective Relay Conference*, Paper No. 4, (October 23-25, Spokane, WA), 2000, available at: http://www.selinc.com

[22] Oman P., E. Schweitzer, and J. Roberts, "Safeguarding IEDs, substations, and SCADA systems against electronic intrusions", in *Proceedings of the 2001 Western Power Delivery Automation Conference*, Paper No. 1, (April 9-12, Spokane, WA), 2001, available at: http://www.selinc.com

[23] Ranger, Steve, "Sun Sacs employees for modem security breaches", Network Week, CPMnet, TechWeb, March 18, 1998.

[24] Sandi Habinc, GRAES – Advanced Encryption Standard (AES) IP Core User’s Manual, Gaisler Research, 2006.

[25] Sectra Communications AB, "SECTRA receives crypto-modem from the Swedish defense to increase mobile data security", Linköping, Sweden, May 2001.

[26] Yang Sun, M. Karkooti and J. R. Cavallaro, “High throughput, parallel, scalable LDPC encoder/decoder architecture for OFDM systems”. Fifth IEEE Dallas Circuits and Systems Workshop (DCAS-06) , Dallas, Oct 2006, pp 39-42.

[27] http://www.xilinx.com