New Intellectual Property Blocks for a Secure Modem on FPGA

Galia I. Marinova[1] , Vassil G. Guliashki[2] and Maurice Bellanger[3]

Abstract – **The paper presents new Intellectual Property (IP) blocks realized for completing a Data Base with IPs for secure multicarrier modem design on FPGA. The modems considered are designed on the Filter Banc principle. The new IP blocks described are – equalizer for ADSL and WiFi applications with channel coefficient estimation and crypto-cores based on DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advanced Encryption Standard) algorithms. IPs are developed in VHDL and their realizations are estimated for time and surface area parameters on FPGA from the Virtex-4 Xilinx circuit family.**

Keywords – **multicarrier modem; crypto-processors; DES, AES, 3DES; FPGA; equalizer;**

I. Introduction

The paper presents results from our recent work on creating an environment for design of Filter Banc based multicarrier modems with some emphasis on security functions. We present here new IP blocks developed in VHDL for some DSP functions – equalizer for applications following ADSL and WiFi standards and for security functions – crypto-cores based on DES (Data Encryption Standard), 3DES (Triple DES) and AES (Advanced Encryption Standard) algorithms. We present the structure of the Data Base with IP blocks for Secure multicarrier modem design, completed with the new IP blocks. Then we consider more in details the equalizers and the crypto-core IP blocks specifications, the FPGA based realizations of those blocks and finally we give results for time and surface area estimations of the IPs realized on a concrete FPGA from Xilinx circuit family.

II. Data Base with IP blocks for secure multicarrier modem design

The specification of a multicarrier Filter Banc based modem is presented in [5,8]. Our research during the last three years aimed the development of a Data Base with Intellectual Property (IP) block for the main functions in multicarrier modem specification which permit a flexible approach to design different modem applications following the design methodology described in [7]. The basic multicarrier modem core functions were presented in [6].

In this paper we present our work on completing the Data Base with IPs for equalization and a group of crypto-cores for secure modem designs. Fig. 1 presents the structure of the Data Base with IP blocks for Filter Banc based multicarrier modem design with emphasis on new DSP functions and secure modem crypto-cores.

III. New IP blocks in the Data Base

We describe here the new IPs that we developed, adapted and added in the Data Base for Secure multicarrier modem design on FPGA.

A. New IPs for DSP blocks

The principle of equalization in the multicarrier modem is described in [2]. The equalization is realized in two stages – learning or initialization stage and equalization stage. Two cases are studied – equalization of a multicarrier modem core for ASDL standard where 230 over 256 sub-channels are used for data transmission and equalization for wireless LAN modem application where 115 over 128 sub-channels are used for data transmission.

The transfer function of the transmission multipath channel in both cases is considered as:

$$C(z)=1-0.5z^{-1}+0.3z^{-2}$$

The initial values of the coarse equalizer coefficients are obtained through interpolation with the help of 4 pilot tones uniformly distributed in the transmission bandwidth, which is efficient in keeping synchronization. They are used to track the residual carrier frequency offset that remains after the frequency correction during the training phase.

The simplest form of the fine equalizer with just one coefficient h_i, i=1,115/i=1,230 for each sub-channel is realized. The value of each h_i is updated in a decision directed mode, through least square type of algorithm. The structure is able to track the slow evolutions of the complex sub-channel gain over the duration of the packet.

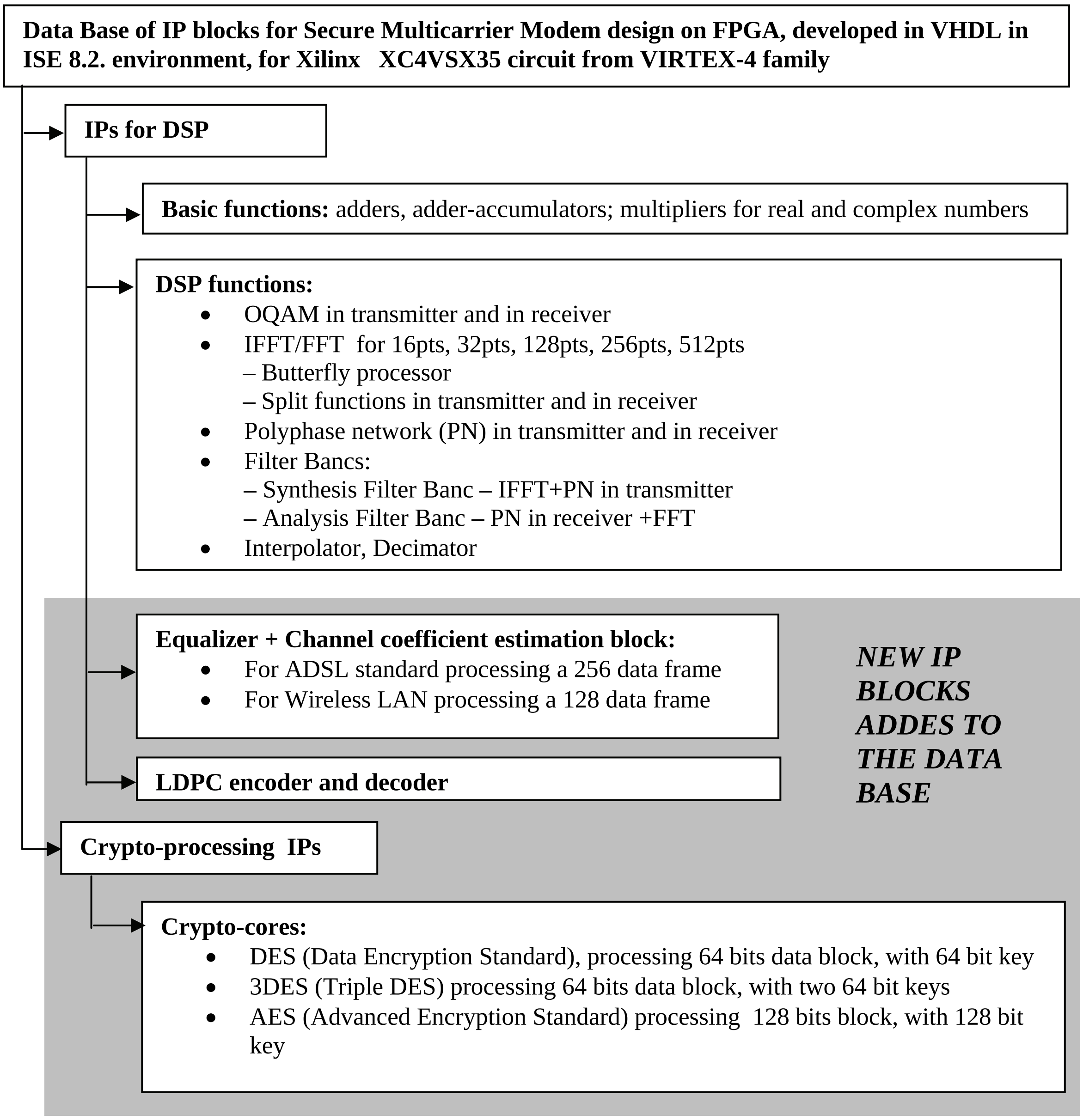
The input data at the modem transmitter is a known sequence of random data d(i), $i=1,10^5$; $d(i)\in\{+1,-1\}$, the data coming out from the analysis Filter Banc in the modem receiver are x(i), $i=1,10^5$ and the output error for sub-channel i, with sub-channel equalizer, at time n is:

$$e(n)=d_i(n)-(c_i+h_i)x_i(n)$$

[1] Galia I. Marinova is with the Faculty of Telecommunications, Technical University – Sofia, 8, bul. "Kliment Ohridski", Sofia 1000, Bulgaria, e-mail: gim@tu-sofia.bg

[2] Vassil G. Guliashki is with the Institute for Information Technologies – BAS, "Acad. G. Bonchev" Str., bl. 29A, Sofia 1113, Bulgaria, e-mail: vggul@yahoo.com

[3] Maurice Bellanger is with CNAM-Paris, 2, Rue Conte, Paris 75003, France, e-mail: bellang@cnam.fr



Data Base of IP blocks for Secure Multicarrier Modem design on FPGA, developed in VHDL in ISE 8.2. environment, for Xilinx XC4VSX35 circuit from VIRTEX-4 family

IPs for DSP

Basic functions: adders, adder-accumulators; multipliers for real and complex numbers

DSP functions:
- OQAM in transmitter and in receiver
- IFFT/FFT for 16pts, 32pts, 128pts, 256pts, 512pts
  – Butterfly processor
  – Split functions in transmitter and in receiver
- Polyphase network (PN) in transmitter and in receiver
- Filter Bancs:
  – Synthesis Filter Banc – IFFT+PN in transmitter
  – Analysis Filter Banc – PN in receiver +FFT
- Interpolator, Decimator

Equalizer + Channel coefficient estimation block:
- For ADSL standard processing a 256 data frame
- For Wireless LAN processing a 128 data frame

LDPC encoder and decoder

NEW IP BLOCKS ADDES TO THE DATA BASE

Crypto-processing IPs

Crypto-cores:
- DES (Data Encryption Standard), processing 64 bits data block, with 64 bit key
- 3DES (Triple DES) processing 64 bits data block, with two 64 bit keys
- AES (Advanced Encryption Standard) processing 128 bits block, with 128 bit key

Fig. 1. Data Base with IP blocks for Secure modem design

These output errors serve to update the equalizer coefficients - h_i, i=1,115/230 and to compute in real time the SNR in the corresponding sub-channel. The benefit of the fine spectral analysis of the radio-channel performed by the AFB is that a single complex coefficient can be sufficient for each equalizer, since the distortion in the sub-channels can be approximated reasonably close by a flat gain. If the radio channels are severely distorted, more coefficients might be needed to cope with the residual timing offset and to reduce the interference level. Four-bit symbols are transmitted by sub-channel.

The IP-oriented specification of the equalizer in the multicarrier modem is presented on Fig. 2.

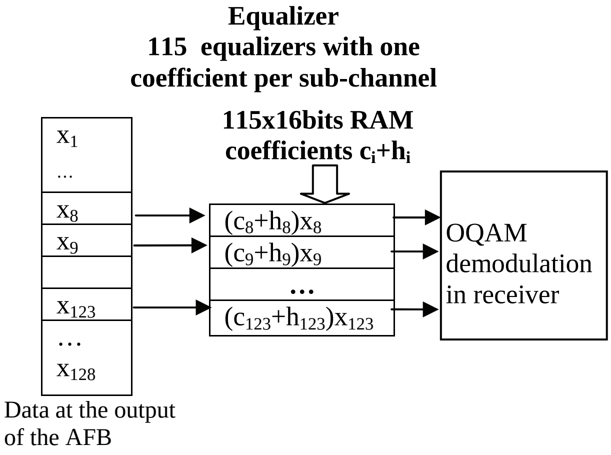

Equalizer
115 equalizers with one coefficient per sub-channel
115x16bits RAM coefficients c_i+h_i
x_1
…
x_8
x_9
x_{123}
…
x_{128}
Data at the output of the AFB
$(c_8+h_8)x_8$
$(c_9+h_9)x_9$
…
$(c_{123}+h_{123})x_{123}$
OQAM demodulation in receiver

Fig. 2. IP-oriented specification of the equalizer block

The equalizer IPs are integrated in the multicarrier modem cores and they are realized on FPGA from XILINX family - VIRTEX-4 , the circuit XC4VSX35 with frequency f=400MHz and surface area of 10^7gates.The ISE development system from [10] is used for the synthesis and the programming of the FPGA.

The equalization IP block for ADSL application is realized with fully serial architecture using one real multiplier. It treats a 256 data frame. The equalizer IP realizes 115 serial complex multiplications.

The architecture of the modem for wireless LAN uses 4 parallel multipliers and it treats a 128 data frame. The equalizer IP realizes 230 complex multiplications parallelized on 4 real number multipliers.

Table I presents time estimation of the modem core including equalizer IP in two applications and Table II presents the surface area taken by the equalizer IP blocks on the FPGA.

Table I. TIME ESTIMATION OF THE EQUALIZER IP BLOCKS

IP block	Time per frame	
	Modem for ADSL Fully serial architecture with one multiplier Frame of 256 data	Modem for wireless LAN Architecture with 4 parallel multipliers Frame of 128 data
Equalizer	3.6µs	0.6µs

Table II. SURFACE AREA ESTIMATION OF THE EQUALIZER IP BLOCKS

Equalizer IP block	BRAM	TBUF	MULT	Number of Slices
Modem for ADSL	6%	1%	1%	4%
Modem for wireless LAN	10%	1%	4%	6%

The LDPC encoder and decoders we used are described in [11].

B. *New crypto-processing IP cores*

In previous work [9] we gave results from the integration of commercial DES and 3DES crypto-cores in a secure multicarrier modem design. But in order to improve the flexibility of our environment we developed proprietary crypto-cores and/or adapted existing open cores of the encryption/decryption blocs. We developed three types of crypto-cores: DES, 3DES and AES crypto-cores.

- DES crypto-core – The principle of DES algorithm 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 [4]. 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, based on the cryptographic algorithm, created by Rijndael [1, 3]. In the presented secure modem application the plain text data are encrypted/decrypted in blocks of 128 bits, using 128-bit key size. 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 can also be generated off-line and can 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 are easily integrated in the created VHDL code. The AES crypto-core IP treats a 128-bit 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.

Table III gives time parameters for the crypto-cores realized and Table IV presents data for the surface area taken 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. TIME PARAMETERS OF THE CRYPTO-CORES

IP block	**Time per frame**		
Crypto-processing core	**DES**	**3DES**	**AES**
	480ns	1.44μs	178ns

Table IV. 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%

IV. CONCLUSION

The Data Base with Intellectual Property Blocks that we presented here is a part of an environment which permits to design Filter Banc based multicarrier modems for different applications: for example applications following ADSL or WiFi standards. The emphasis of the new blocks we developed is on crypto-cores DES, 3DES and AES that allow the design of different secure modem couples performing encryption in transmitters and decryption in receivers with previous key exchange. We also added equalizer blocks for two applications and LDPC encoding/decoding IPs blocks. A future work is foreseen on more precise modem synchronization algorithms and IP blocks, as well as further optimization of the Filter Banc based modem designs and realizations. The new IPs complete the Data Base and create an useful environment for teaching and self-education in the area of Filter Banc – based mulcarrier modem design and Secure modem design.

ACKNOWLEDGEMENT

The research work described in this paper is partly supported by NATO grant: CLG 981551/2005.

The authors thank Milen Vassilev Simeonov for his work on DES core design and testing during his final project work.

REFERENCES

[1] AES (Rijndael) IP-Cores for Encryption/Decryption and Key Expansion, ErSt Electronic GmbH, Switzerland, April 2006, http://www.opencores.org

[2] Bellanger M., Increasing the data throughoutput of wireless LAN with OFDM/OQAM, March, CNAM-Paris, 2006

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

[4] Lagger A., “Implementation of DES Algorithm Using FPGA Technology”, 2003, available at: http://lsmwww.epfl.ch/Education/reports/lagger_report_2003.pdf

[5] Marinova G., C. Fernandes, M. Bellanger, "Specification of multicarrier modem aimed to intellectual property and FPGA implementation", Proceedings of the *International Conference on Basic Technologies for E-business'2002*, 15-18 09.2002, Albena, Bulgaria, pp. 203-210.

[6] Marinova G. and C. Fernandes, "Data base of IP blocks developed in VHDL for multicarrier modem realization on FPGA", *MELECON 2004* Proceedings, Volume I, *The 12th IEEE Mediterranean Electrotechnical Conference*, May 12-15, 2004, IEEE Catalog Number 04CH37521, Dubrovnik, Croatia, pp. 217-220.

[7] Marinova G. and C. Fernandes, "Study on the realization with FPGA of a multicarrier modem", Proceedings of the *2004 International TICSP Workshop on Spectral Methods and Multirate Signal Processing, SMMSP2004*, Vienna, Austria, September 11-12,2004, Edited by Jaako Astola, Karen Egiazarian and Tapio Saramaki, TICSP Series 25, pp. 115-122.

[8] Marinova G., V. Guliashki, D. Le Ruyet, M. Bellanger, Multicarrier modem core on FPGA, *MELECON’2006*, Proceedings of *IEEE Mediterranean Electrotechnical Conference*, May 16-19, Benalmadena (Malaga), Spain, Volume 1. pp. 66-69.

[9] 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.

[10] www.xilinx.com

[11] 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.