Secure Multicarrier Filter Bank Based Modem on FPGA

Galia Marinova, Vassil Guliashki, Didier Le Ruyet and Maurice Bellanger

Abstract — **The paper deals with the design and realization of a secure filter bank based (FBB) multicarrier modem on FPGA. The theory and realization of a multicarrier filter bank based modem are presented in brief. Then 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 boards with XC2V1000 circuit from VIRTEX II family and with XC4VSX35 circuit from VIRTEX-4 family.**

Index Terms — **DES, 3DES, AES crypto-processing cores, filter bank based modem, FPGA realization, secure multicarrier modem.**

I. Introduction

Modem-based attacks are occurring with increasing frequency due to the Internet Protocol-based security [8], that most organizations have applied to their Internet Protocol networks. A network security architect at Sun Microsystems stated in [30] 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 this solution has the highest cost in terms of time latency and surface area on FPGA [16], [26]-[29]. Secure encrypting modems work between pairs (or groups) of similarly configured modems which not only restrict access to authorized connections, but encrypt all data transmission to safeguard against eavesdropping (taping) on phone lines.

Encryption standards are established in the United States (see [12]) and four levels of cryptographic security are defined, ranging from Level 1, basic security via integrated security, trough Level 4, the highest level of secure communications. Most encrypting modems operate on Level 2 or Level 3, where the difference is that Level 3 requires users to identify themselves by entering a password or PIN.

There are some realizations of secure modems as crypto-modems for mobile data security, described in [32]. The Palladium Secure Modem [17] 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) [25]. The Secure Terminal STE cryptographic engine is on a removable PC Memory Card [25]. More about different crypto-core algorithms and applications can be found in [5].

Our research concerns the security of a multicarrier filter bank based (FBB) modem which main core is described below. In [22] 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 have consequently performed research in order to develop a flexible IP crypto-core library by studying and adapting some open crypto-core solutions [1], [18], [31] and by developing proprietary IP blocks for DES, 3DES and AES [10], [11], [13] encryption standard implementations. The paper presents the results from this study.

First we present the theory and realization of a FBB multicarrier modem then we describe the specification of the secure multicarrier FBB modem, after that 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 secure multicarrier FBB modem realizations integrating different crypto-cores on FPGA. The study is performed in a specialized environment combining hardware and software tools permitting the design, realization, verification and test of secure modems. Measurement and validation setup using a logic analyzer is integrated. A similar idea can be found in the recently published paper [19].

Manuscript received October 30, 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

(Advance online publication: 19 February 2008)

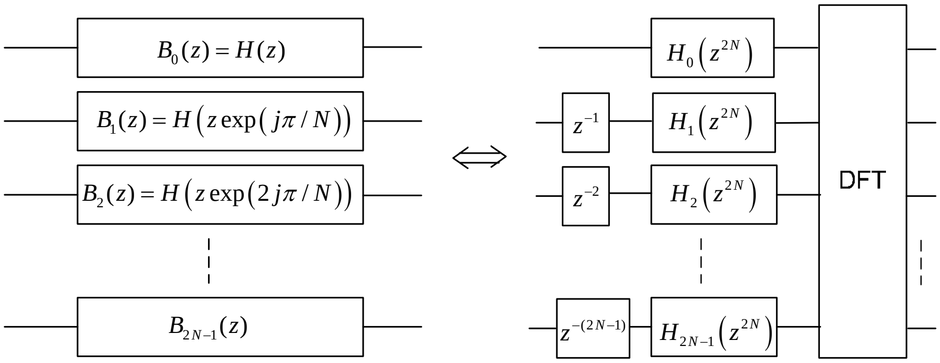


Fig. 1. Block diagram of an analysis filter bank

II. Theory and Realization of a Filter Bank Based Multicarrier Modem

First we present the theory of a FBB multicarrier modem, and then we describe the realization of this core on FPGA.

A. Theory of a FBB multicarrier modem

The principle of OFDM-OQAM multicarrier modulation system [20] is to divide the transmission into N independent transmissions using N sub-channels. In OFDM-OQAM the Discrete Fourier Transform (DFT) is replaced by a filter bank. A DFT can be seen as a special kind of filter bank where the frequency response of the filter is a sinc (sine cardinal function). Consequently, the frequency separation is only possible for perfect frequency synchronization. In order to improve the frequency separation, it is possible to perform a filtering using a filter bank composed of a DFT and a polyphase filter. We wish to build a filter bank of $2N$ filter in the frequency range [0, f_s], where f_s is the sampling frequency. If $H(z)$ is the z-transfer function of the prototype filter a frequency shift of $\frac{m}{2N}f_s$ corresponds to a variable change from z to $z\exp(j2\pi\frac{m}{2N})$.

Using the polyphase decomposition of $H(z)$ of length $2KN$, we have:

$$H(z) = \sum_{i=0}^{2KN-1} h_i z^{-i} = \sum_{l=0}^{2N-1} z^{-l} H_l(z^{2N}) \tag{1}$$

with $$H_l(z^{2N}) = \sum_{k=0}^{K-1} h_{2kN+l}(z^{-2N})^k \tag{2}$$

The sequence of $2KN$ filter coefficients is decomposed into $2N$ interleaved sequences of K coefficients. Consequently, we can write the transfer function of the m-th filter as:

$$B_m(z) = H(z\exp(j2\pi\frac{m}{2N}))$$
$$= \sum_{l=0}^{2N-1} z^{-l}\exp(-j2\pi\frac{ml}{2N})H_l(z^{2N}) \tag{3}$$

Then we have:

$$\begin{bmatrix} B_0(z) \\ B_1(z) \\ \vdots \\ B_{2N-1}(z) \end{bmatrix} = \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & W & \dots & W^{2N-1} \\ & \vdots & & \vdots \\ 1 & W^{(2N-1)} & \dots & W^{(2N-1)(2N-1)} \end{bmatrix} \begin{bmatrix} H_0(z^{2N}) \\ z^{-1}H_1(z^{2N}) \\ \vdots \\ z^{-(2N-1)}H_{2N-1}(z^{2N}) \end{bmatrix} \tag{4}$$

where $W = e^{-j\frac{2\pi}{N}}$

The corresponding block diagram of an analysis filter bank is given on Fig. 1.

A filter bank based multicarrier modem [6], [7] employs two filter banks: a synthesis filter bank (SFB) at the transmitter side and an analysis filter bank (AFB) at the receiver. The structure of the synthesis filter is composed of an Inverse Discrete Fourier Transform (IDFT) and a polyphase filter. In OFDM-OQAM, the N sub-channels are spaced by the symbol rate $1/T$, where $T = 2N/f_s$. The prototype filter for the synthesis and analysis filter banks must be half-Nyquist which means that the square of its frequency response must satisfy the Nyquist criterion. The prototype filter is a low-pass filter whose transition band is centred on the frequency $f_s/4N$ and the maximum transition bandwidth is $f_s/2N$. Consequently, two neighbouring sub-channels overlap and interference between sub-channels exist as shown in Table I.

Since the sub-channels significantly overlap in the frequency domain only with their neighbours, it is necessary to use a specific signalling in order to guaranty the separation of the different data. Using alternatively real and imaginary parts of the complex symbols at neighbour sub-channels leads to the elimination of inter-channel interference.

Table I. Typical bidimensional impulse response of the association of a synthesis and an analysis filter banks

Frame Sub-channel	n'–1	n'	n'+1
m–1	–0.25j	0.32	0.25
m	0.5	1	0.5
m+1	0.25j	0.32	–0.25j

The OQAM modulation [14], [15] consists in multiplication and delay of symbols by half symbol period T/2, alternatively by sine and by cosine, which makes them orthogonal. The symbols are transmitted alternatively: first time the signals in phase at the odd sub-channels and the signals on quadrature on the even sub-channels. As a consequence, the neighbour sub-channels are always orthogonal. At the next frame places are inverted and the signals in phase are on the even sub-channels and the signals in quadrature are on the odd sub-channels. Consequently, two consecutive frames are also orthogonal. Then the even and the odd frames can be transmitted simultaneously with a delay of half a period.

Suppose that the complex input symbols are

$$c_{m,n} = c^R_{m,n} + jc^I_{m,n} \qquad (5)$$

where $c^R_{m,n}$ and $c^I_{m,n}$ are respectively the real and imaginary part of the m-th symbol. The transmitted symbol $a_{m,n'}$ at sub-channel m-th and at frame n'-th is given by

$$a_{m,n'} = \begin{cases} c^R_{m,\frac{n}{2}} & \text{if } m \text{ is even and } n \text{ is even} \\ c^I_{m,\frac{n-1}{2}} & \text{if } m \text{ is even and } n \text{ is odd} \\ c^I_{m,\frac{n}{2}} & \text{if } m \text{ is odd and } n \text{ is even} \\ c^R_{m,\frac{n-1}{2}} & \text{if } m \text{ is odd and } n \text{ is odd} \end{cases} \qquad (6)$$

With the OQAM principle, the orthogonality is kept for the neighbouring sub-channels m–1 and m+1. Therefore interference comes from the sub-channels m–2 and m+2. It can be shown that the integration of OQAM modulation with filter banks result in a robust multicarrier modulation system which doesn’t need very precise synchronization at the reception. Another advantage of this system compared to OFDM is the increased transmission rate because it doesn’t need a guard interval. The main difficulties in achieving high data rate on the wireless channels are known to be the frequency selectivity and the fading due to the existence of multiple paths. Multicarrier technique can significantly alleviate the impacts of frequency selective fading and is attractive for the next generation of wireless systems.

The OFDM-OQAM mapping is illustrated in Table II.

Table II. OFDM-OQAM Mapping

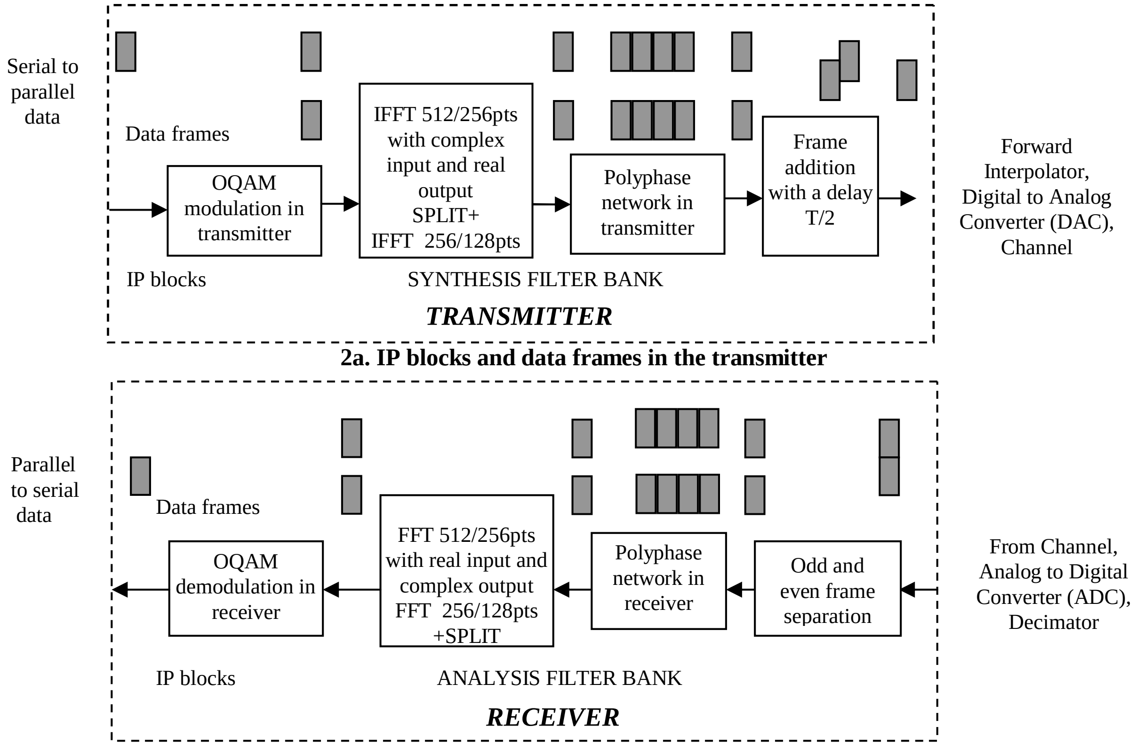
Frame / Sub-channel	$n' = 0$	$n' = 1$	$n' = 2$	$n' = 3$
$m = 0$	$c^R_{0,0}$	$c^I_{0,0}$	$c^R_{0,1}$	$c^I_{0,1}$
$m = 1$	$c^I_{1,0}$	$c^R_{1,0}$	$c^I_{1,1}$	$c^R_{1,1}$
$m = 2$	$c^R_{2,0}$	$c^I_{2,0}$	$c^R_{2,1}$	$c^I_{2,1}$
$m = 3$	$c^I_{3,0}$	$c^R_{3,0}$	$c^I_{3,1}$	$c^R_{3,1}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
$m = N$–1	$c^I_{N-1,0}$	$c^R_{N-1,0}$	$c^I_{N-1,1}$	$c^R_{N-1,1}$

B. Multicarrier filter bank based modem core

On the above theoretical principle a multicarrier FBB modem core has been designed. Fig. 2 presents the IP blocks and data frames in this core. Corresponding to the ADSL or WiFi modem application the size of the input data frame is 256 or 128. This scales the size of the IFFT and the FFT IPs used in the core.

Realization of ADSL modem configuration on XC2V1000

A multicarrier filter FBB modem core for ADSL with a fully serial realization on FPGA was examined. The results from this research are presented in paper [21].


Serial to parallel data
Data frames
OQAM modulation in transmitter
IFFT 512/256pts with complex input and real output SPLIT+ IFFT 256/128pts
Polyphase network in transmitter
Frame addition with a delay T/2
Forward Interpolator, Digital to Analog Converter (DAC), Channel
IP blocks
SYNTHESIS FILTER BANK
TRANSMITTER
Parallel to serial data
Data frames
OQAM demodulation in receiver
FFT 512/256pts with real input and complex output FFT 256/128pts +SPLIT
Polyphase network in receiver
Odd and even frame separation
From Channel, Analog to Digital Converter (ADC), Decimator
IP blocks
ANALYSIS FILTER BANK
RECEIVER

2a. IP blocks and data frames in the transmitter

2b. IP blocks and data frames in the receiver

Fig. 2. IP blocks and data frames in the filter bank multicarrier modem core

Table III. Bidimensional impulse response

Frame /Time Data /Frequency	6	7	8	9	10
1	-0.0008	0.0005	-0.0003	0.0004	-0.0008
2	-0.107-j0.0007	0.0015-j0.2508	0.3187+j0.002	-0.0015+j0.2498	-0.1059-j0.0006
3	-0.0015	0.5041	1.0012	0.4982	-0.0015
4	-0.1069-j0.0006	0.0015+j0.251	0 .3187+j0.0019	0.0015-j0.25	-0.1058-j0.0006
5	-0.0004	0.0002	-0.0001	0.0002	-0.0004

The IP core is implemented on FPGA with 10^6 gates XC2V1000 from the VIRTEX II family of XILINX and the time and surface area estimations corresponding to this FPGA are 134μs processing time for a frame and frequency of 7.46kHz per frame.

In order to estimate the accuracy of the ADSL application of the multicarrier FBB modem realized on XC2V1000 FPGA two verifications have been performed.

- *Impulse response verification*

To obtain the impulse response, 8 initial frames (becoming 16 after the OQAM modulation in the transmitter) are treated in the transmitter, and then in the receiver.

All frames contain zeros, except the fifth frame whose third data value is 1. For this experience the theoretical OQAM response corresponds to data in Table I with m=3, n'=8.

Table III presents the bidimensional impulse response of the filter bank multicarrier modem simulated in ISE environment.

- *Mean square error (MSE) estimation in a FBS-BFA loop with an ideal channel*

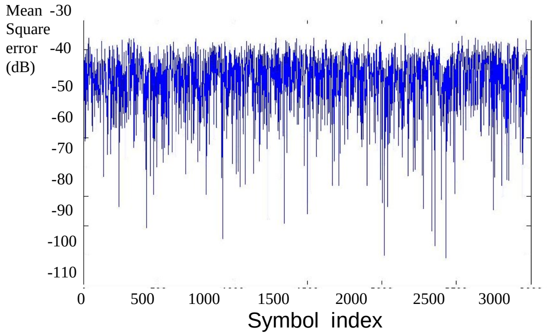


Fig. 3. MSE estimation in a FBS-BFA loop with an ideal channel

A bipodal random sequence is generated at the transmitter input. This sequence is compared with the sequence at the output of the receiver and the measured MSE is presented on Fig. 3. The average value of the MSE obtained is –50dB (theoretical worst case value –45dB). After hardware implementation a degradation of 3dB is measured.

Realization of ADSL and WiFi modem configurations on XC4VSX35

Two configurations for ADSL and WiFi applications of the multicarrier modem core were realized on XILINX VIRTEX 4 XC4VSX35 / 500MHz circuit. The time characteristics for these realizations of the filter bank multicarrier modem core are presented in Table IV. The results show that the circuits from the VIRTEX 4 family make both ADSL and WiFi standards achievable for the multicarrier FBB modem core from Fig. 2.

Table IV. Time characteristics of the modem core realization on XILINX VIRTEX 4 XC4VSX35 / 500MHz circuit

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
OQAM modulation in transmitter	10ns	3ns
FT/IFFT	18μs	1.5μs
SFB/AFB	15μs	2.5μs
Equalizer	3.6μs	0.6μs
Modem core	36.61μs	4.603μs
Frequency per frame	27.31kHz per frame	217.3kHz per frame
Frequency per symbol	6.3MHz per symbol	25MHz per symbol

III. Specification of the secure Filter Bank Based 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 [33] are available in proprietary VHDL realizations.

Fig. 4 presents the specification of a filter bank based multicarrier modem core with data encryption and decryption.

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 encryption/decryption IPs.

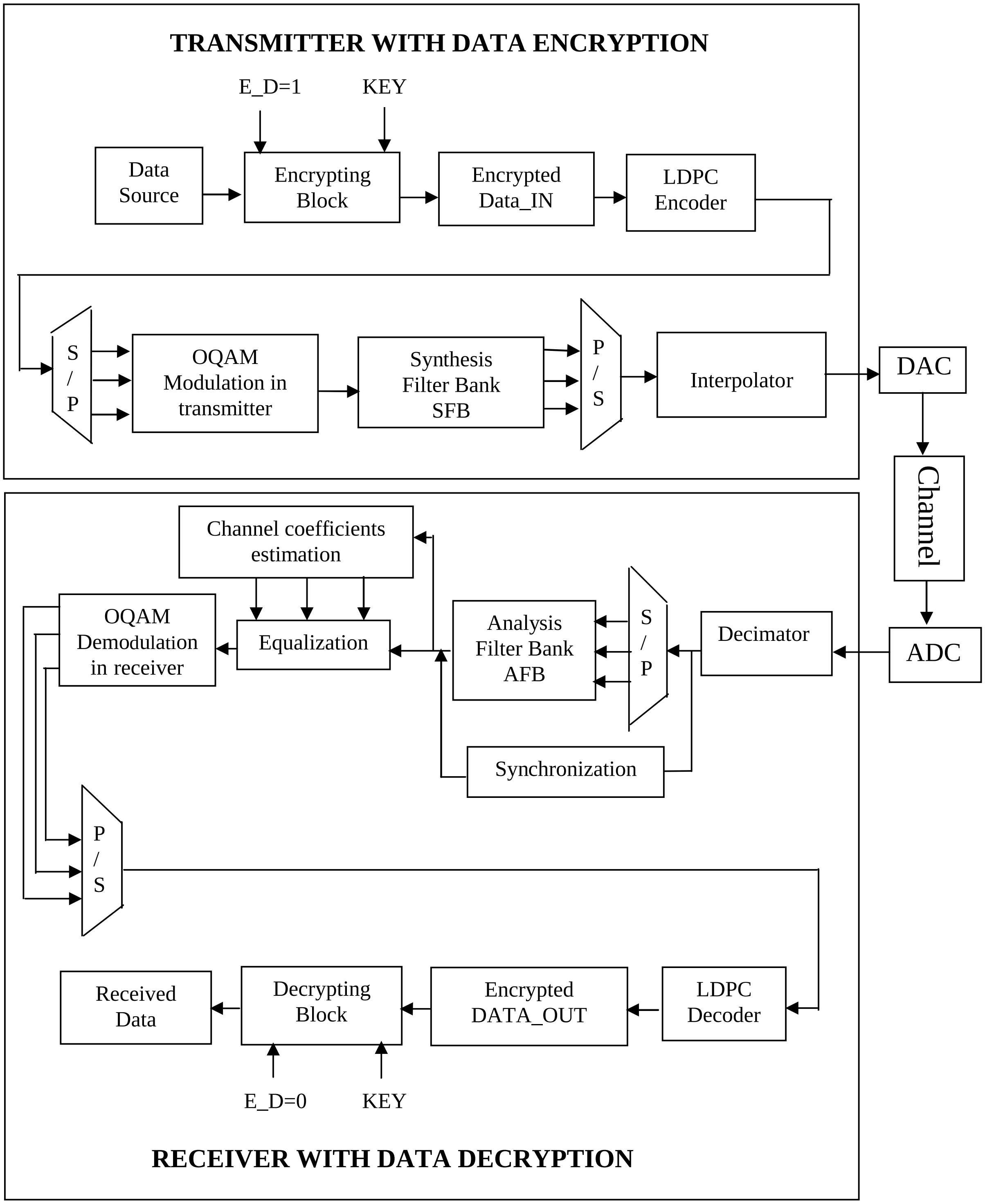


Fig. 4. Multicarrier modem with data encryption and decryption

IV. 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 [9], [23] 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 [18]. 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

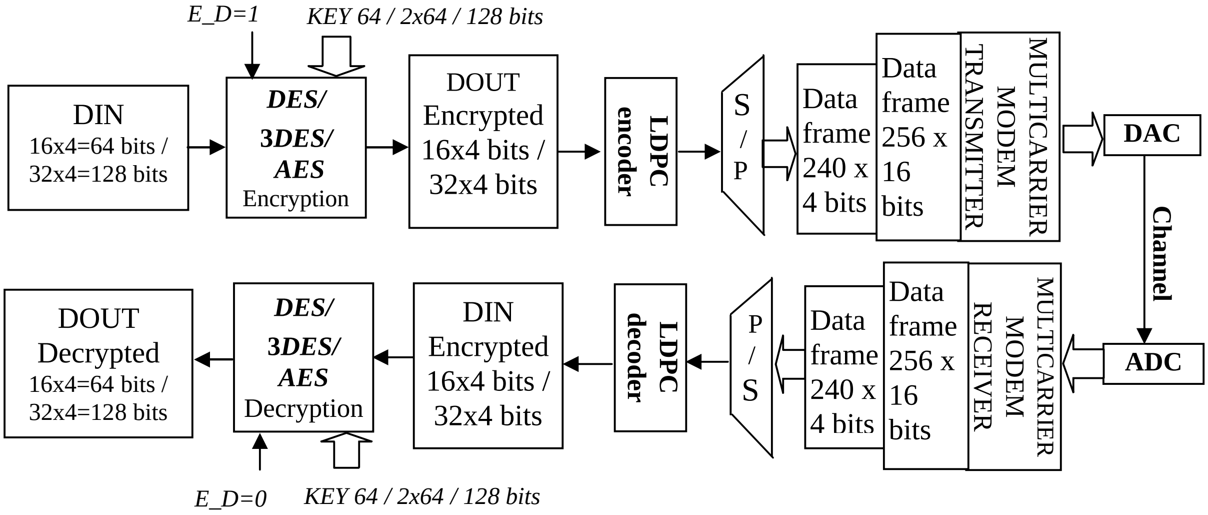


Fig. 5. Integration of DES, 3DES and AES crypto-cores in the secure filter bank based multicarrier modem

"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:

$$O = E_{K1}(D_{K2}(E_{K1}(I))), \quad \textbf{(7)}$$

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:

$$O = D_{K1}(E_{K2}(D_{K1}(I))) \quad \textbf{(8)}$$

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 [13], [24], based on the cryptographic algorithm, created by Rijndael [10], [11]. 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 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-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.

Fig. 5 presents the data organization in a secure multicarrier modem integrating DES, 3DES or AES crypto-cores. 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 4 bits 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.

V. 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

Table V. 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 VI. 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 256x16 bits		26.96 kHz	26.28 kHz	27.18 kHz
Frequency per data 16 bits		6.9 MHz	6.73 MHz	6.96 MHz

from the VIRTEX-4 family from [34]. As previously, 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 [21]. 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 240x4-bit data frame at the entry of the transmitter or in order to treat the 240x4-bit 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 V presents the estimation of time efficiency in clock cycles for the three crypto-cores. In the case of AES crypto-block one clock cycle is added at the end of encryption/decryption processing.

Table VI 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-bit data frame and the frequency for 16-bit 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 VII 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 VII. 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%

VI. Conclusion

In this paper we have described a complete secure multicarrier filter bank based modem. The IP block library containing the multicarrier filter bank based 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] Bellanger M., G. Bonnerot and M. Coudreuse, "Digital filtering by polyphase network : application to sample rate alteration and filter banks", *IEEE Trans. on Acoustics*, Speech and Signal Processing, vol. 24, no. 2, April 1976, pp. 109-114.

[7] Bellanger M., "Specification and design of a prototype filter for filter bank based multicarrier transmission*", Proceedings of IEEE ICCASP*, Salt Lake City, vol. 4, May 07-11, 2001, pp. 2417-2420.

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

[9] 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.

[10] Daemen J. and Rijmen V., AES Proposal: Rijndael, "AES algorithm submission", September 3, 1999. Available: http://www.nist.gov/CryptoToolkit

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

[12] Federal Information Processing Standards Publication 140-2 (FIPS PUB 140-2), "Security requirements for cryptographic modules", May 25, 2001, Change Notices (12.03.2002). Available: http://fips201ep.cio.gov/documents/fips1402.pdf

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

[14] Hirosaki B., "An Orthogonally Multiplexed QAM System Using the DFT", *IEEE Trans. on Communications*, vol. 29, no. 7, July 1981, pp. 982-989.

[15] Hirosaki B., S.Hasegawa and A.Sabato, "Advanced groupband data modem using orthogonally multiplexed QAM technique", *IEEE Trans. on Communications*, Vol. Com-34, No6, July 1986, pp. 587-592.

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

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

[18] Lagger A., "Implementation of DES algorithm using FPGA technology", 2003. Available: http://lsmwww.epfl.ch/Education/reports/lagger_report_2003.pdf

[19] Lashkarian N., E. Hemphill, H. Tarn, H. Parekh, and C. Dick, "Reconfigurable Digital Front-End Hardware for Wireless Base-Station Transmitters: Analysis, Design and FPGA Implementation", *IEEE Transactions on Circuits and Systems – I: Regular Papers*, vol. 54, No 8, August 2007, pp. 1666-1677.

[20] Le Floch, M. Alard, and C. Berrou, "Coded orthogonal frequency division multiplex," *Proceedings of the IEEE*, vol. 83, June 1995, pp. 982-996.

[21] Marinova G., Guliashki V., Le Ruyet 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.

[22] 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.

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

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

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

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

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

[28] 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: http://www.selinc.com

[29] 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: http://www.selinc.com

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

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

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

[33] 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.

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