Set of Symmetric Block Ciphering Soft-Cores

Viktor Melnyk

Abstract - **The possibilities of IP-technologies for information protection are discussed. An analysis of modern information protection Soft-Cores that support symmetric block ciphers is done. Forty-six variations of the DES and Triple DES Soft-Core are proposed. The developed DES and Triple DES Soft-Cores support all of the discussed functional possibilities. This allows achieving a high performance, a low equipment volume for their realization and an effective usage of them at a wide spectrum of the application fields.**

Keywords - **information protection, symmetric block cipher, Soft-Core, DES, Triple DES.**

I. Introduction

Modern computer systems allow the user to protect the data that are processed. Some ways of protection are user identification, distribution of the access to the information, provision of the integrity, confidentiality of the information, its protection from modification and destruction [1]. Some of these ways of protection are traditionally realized with the help of the cryptographic algorithms of the data transformation as a programmable module for the universal processors. However, such a realization with the advantage of flexibility of the program module usage and modification has a disadvantage, too: the problem of how to provide the module integrity, and the low data rate. The support of the program module integrity, which is responsible for the cryptographic transformation, is necessary to avoid the key-data distortion and, even more, the program module distortion. The low datarate of the program modules is caused by the discrepancy of the command set of the universal processors with the common operations used in cryptographic algorithms.

One of the possible ways to solve these problems is to use specialized VLSI circuits for data protection. The execution of the cryptographic algorithm with the specialized VLSI circuits allows avoiding the visibility of the algorithm and the key-data integrity. Free access to the content of a VLSI circuit is not possible.

Several approaches are used to solve the task of data protection. One of them is use of symmetric block ciphers. Very popular symmetric block cipher is DES (Data Encryption Standard), which has been used as a national standard of data protection in USA [2]. Also it is used as a built-up algorithm in other standards, i.e. ATM encryption, protocol SSL, standards ANSI.

Main effort of developers is concentrated today at this direction, that raised a creation a host of multimode DES processors. On the other hand, availability of a high-level programmable logical devices gives the possibility to create a processors oriented for a work in one preferred mode. Such a narrow specialization allows optimizing their structure very well to obtain a high performance and a competitive gate count.

II. Approach to the Design of the Data Protection Soft-Cores

The high level of integration, high reliability and a wide spectrum of the functional possibilities in the different modes characterize modern VLSI circuits of the data protection. Soft-Cores are designed with a hardware description language like Verilog [3] or VHDL [4]. This leads to the approach that the customer can buy such Soft-Cores from other companies and include them in his own design. The customer is able to complete the core with additional functional blocks to obtain a data protection system built as a system-on-a-chip [5]. Such an approach is called "core-technology" [6, 7].

The use of a Soft-Core can be:

- a model of a datapath and a control system with a simplified interface – such an approach allows the designer of a data protection system to use pre-designed components or to develop his own specific interface logic and thus to match the requirements;
- a complete description with a very specific interface – such an approach makes it possible to get a running data protection system very quickly, but this system can’t be adapted to match complex requirements.

Flexibility in a selection of a data processing mode allows using a VLSI circuit of a symmetric-key encryption in the data protection systems effectively. However, data protection systems use only a few modes. So, on the one hand, unused modes waste silicon, and such a realization makes it on the other hand impossible to achieve a high data rate. The alternative of the development of a symmetric-key VLSI circuit is specialized datapath/control architecture for the specific data protection requirements.

III. Variations of the DES Soft-Cores

A development progress of the symmetric block ciphers theory, availability of computer engineering / techniques and cheapen of VLSI manufacturing are causing a wide range of use the symmetric block cipher processors in specialized data protection systems and in devices designed for universal computer systems, i.e. personal computers that work in global or local networks. The symmetric block cipher processors realize a cryptographic functions, including cryptographic algorithms, keys generation, and it is placed in cryptographic

Viktor Melnyk – Intron ltd., Lviv, Ukraine
E-mail: intron@mail.lviv.ua

environment. For such processors a set of cryptographic algorithms and their work modes must be clearly determined.

For the symmetric block ciphering processors the following characteristics are used:

- symmetric block cipher;
- modes of symmetric block cipher work;
- data / control interface specification;
- data interface specification for connection with the universal computer;
- keys internal memory size.

Beside the listed above characteristics an additional characteristics are used. Presence of them depends on the certain block cipher, which is realized, i.e.:

- data blocks width;
- data loading sequence;
- architecture of the operational units.

Next to determining the symmetric block cipher functionality the characteristics, or parameters, make possible choosing the processor that corresponds with needed requirements in gate count and performance [8].

Let's take a look at the parameters of DES and Triple DES [9] processors. These parameters are:

1. Symmetric block cipher C:

$$C \in \{C_1, C_2\}, \tag{1}$$

where $C_1 \in \{DES\}$, $C_2 \in \{TripleDES\}$;

2. Mode of work M [10, 11]:

$$M \in \{M_1, M_2, M_3, M_4\}, \tag{2}$$

where $M_1 \in \{ECB\}$; $M_2 \in \{CBC\}$; $M_3 \in \{CFB\}$; $M_4 \in \{OFB\}$;

3. Enciphering operation E:

$$E \in \{E_1, E_2, E_3\}, \tag{3}$$

where $E_1 \in \{encryption\}$; $E_2 \in \{decryption\}$; $E_3 \in \{encryption, decryption\}$;

4. Data blocks size D (only for CFB and OFB modes):

$$D \in \{1, 2, ..., 64\}; \tag{4}$$

5. Operational unit (that realizes a symmetric block cipher) architecture A:

$$A \in \{A_1, A_2\}, \tag{5}$$

where $A_1 \in \{iterative\}$, $A_2 \in \{pipelined\}$.

A total number of the DES and Triple DES processors variations can be calculated from the following equation:

$$N_T = \sum_i C_i \left(\left(\sum_{i=1}^{2} M_i \cdot D_{64} \right) + \left(\sum_{i=3}^{4} M_i \cdot \sum_{i=1}^{64} D_i \right) \right) \cdot \sum_i E_i \cdot \sum_i A_i . \tag{6}$$

After the calculations we obtain N_T = 1536.

On the base of analysis the structure features of the symmetric block ciphers and their modes of work the expedient variations of DES and Triple DES processors have been determined [12]. Their qualitative and quantitative composition can be defined from the following equation:

$$N_X = \sum_i C_i \left(A_1 \sum_i E_i \left(D_{64} \sum_i M_i + D_1 \sum_{i=3}^{4} M_i \right) \right) +$$

$$+ A_2 \left(\sum_i E_i \cdot M_1 \cdot D_{64} + E_2 \left((M_2 + M_3) D_{64} + M_3 \cdot D_1 \right) \right) - N_R , \tag{7}$$

where

$$N_R = \sum_i C_i \left(M_4 \sum_{i=1}^{2} E_i (D_1 + D_{64}) \right). \tag{8}$$

The number N_R determines a number of redundant processor variations. A feature of the mode OFB, in which encryption and decryption operate with the same algorithm, causes this redundancy. Thus one processor can provide all three enciphering operations.

After the calculations we obtain N_R = 8, N_X = 46.

IV. Available symmetric block ciphering Soft-Cores

Some modern available on the market symmetric block ciphering (DES and Triple DES) Soft-Cores are shown in the table I. The cores (table I) are characterized by a specialized interface; they support data blocks of 64 bits, have a very specialized functionality and support the ECB mode only. As has been said before the ECB mode has a low reliability, which is due to the lack of feedback. To develop a Soft-Core that supports the other modes – CBC, CFB and OFB – is an important task.

Table I

Modern available symmetric block ciphering Soft-Cores

Producer	FPGA Library	Speed grade	Algorithm	Frequency, MHz	Performance, Mbit/s	Gate count
Alatek	EPF6016	-2	DES	39	156	623LC
	V150	-6	DES	100	400	281Slices
CAST	Virtex V150	-6	DES	101	404	255Slices
	EPF10K30A	-1	DES	73	292	570 LC
Ocean Logic	Virtex E	–	DES	138	552	239Slices
	Virtex E	–	3DES	126	168	799Slices
Helion	Virtex E	-5	DES	58	232	855CLB
	Virtex II	--8	DES	90	360	888CLB

TABLE II

THE RESULTS OF SYNTHESIS AND EVALUATION OF THE DES AND TRIPLE DES SOFT-CORES

FPGA Library	Speed Grade	Algorithm	Mode	Data bus width, bit	Frequency, MHz	Performance[1], Mbit/s	Gate count
EP20K160	-01X	DES	ECB	64	92	5936	5449 LEs
EP20K60	-01X	DES	ECB	64	87	330,2	591 LEs
EP20K200	-01X	DES	CBC	64	46	E: 240,9 D: 4096	7235 LEs
EP20K60	-01X	DES	CBC	64	74	278,58	110 3LEs
EP20K200	-01X	DES	CFB	64	69.4	E: 261,27 D: 4441	7404 LEs
XCV1000	-4	DES	CFB	1	89,1	E: 4,68 D: 89,1	2541 Slices
EP20K60	-01X	DES	CFB	64	90,9	342,21	815 LEs
XCV1000	-4	DES	CFB	1	74	4.35	913 Slices
EP20K60	-01X	DES	OFB	64	86,2	324,51	823 LEs
XCV1000	-4	DES	OFB	1	55	3,23	908 Slices
EP20K60	-01X	3DES	ECB	64	75	85.7	1027 LEs
EP20K600	-01X	3DES	ECB	64	51.28	3281.92	19693 LEs
EP20K60	-01X	3DES	CBC	64	73.529	84.03	1669 LEs
EP20K600	-01X	3DES	CBC	64	52	E: 65.25 D: 3328	20678 LEs
XCV1000	-4	3DES	CFB	64	56	67,6	1228 Slices
XCV1000	-4	3DES	CFB	1	55	66,4	1139 Slices
XCV1000	-4	3DES	CFB	64	87	E: 105 D: 5568	10548 Slices
XCV1000	-4	3DES	CFB	1	55	E: 66,4 D: 3520	9763 Slices
XCV1000	-4	3DES	OFB	64	57	68,8	1194 Slices
XCV1000	-4	3DES	OFB	1	56	1,05	1130 Slices

[1] E – encryption; D – decryption

V. SYNTHESIS AND EVALUATION OF THE PROPOSED SOFT-CORES

With the use of the proposed DES Soft-Core structures author has synthesized these processors on FPGA. Also the specialization for enciphering operation is used. Functional and timing simulations have been done with the help of simulators: Active-HDL from Aldec, and ModelSim from Mentor Graphics, Inc. Logical synthesis has been done with the help of Synplify from Synplicity Inc., for FPGA synthesis the Quartus II from Altera and the Xininx Design Manager from Xilinx were used.

The results of synthesis and evaluation of the DES and Triple DES Soft-Cores, which operate for encryption and decryption, are shown in Table II.

Evidently, the technical characteristics of the Soft-Cores are high. Comparing the proposed Soft-Cores with the available on the market Soft-Cores we can say the following:

- in contrast to available on the market Soft-Cores the proposed Soft-Cores support all modes defined for DES algorithm;
- some proposed Soft-Cores could be used for sequential data processing (as they support 1-bit data blocks) without additional hardware;
- high performance is achieved owing to use the pipelined architecture of the operational unit of realization the DES cipher.

This allows an effective usage of them at a wide spectrum of the application fields including the symmetric block ciphering subsystems embedded to the high-performance data protection systems.

VI. CONCLUSIONS

In this paper the Soft-Cores for information protection have been analyzed. The analysis of the technical characteristics of existing Soft-Cores shows a high amount of specialization. Flexible designs, fast realization and high design quality require parameterizable models and libraries of Soft-Cores for information protection systems. Using them has the following advantages:

- the development process is dramatically simplified and rapid;

- a high level of integration is achieved and errors are virtually impossible;
- the customer can choose the cores which match his requirements.

The characteristics of the existing DES Soft-Cores are considered. Their disadvantage in general is their limited functionality – an absence of the cores that work in CFB and OFB modes. In the paper 43 variations of the DES Soft-Cores' architecture are shown. These cores have a wide functionality – all modes are supported – which allows using them in a wide spectrum of the application fields.

The Soft-Cores have been synthesised and evaluated on Altera's and Xilinx's FPGAs, high-level technical characteristics have been obtained. A high performance and a low equipment volume for their realization allow an effective usage of them at a wide spectrum of the application fields, including the embedded high-performance symmetric block ciphering subsystems. In contrast to available on the market Soft-Cores the proposed Soft-Cores support all modes defined for DES algorithm. Some proposed Soft-Cores could be used for sequential data processing (as they support 1-bit data blocks) without additional hardware. High performance is achieved owing to use the pipelined architecture of the operational unit of realization the DES cipher.

REFERENCES

[1] H. Feistel, "Cryptography and computer privacy", Scientific American, Vol.228, N5, May 1993, pp. 15-23.

[2] FIPS 46, "Data Encryption Standard", Federal Information Processing Standard (FIPS), Publication 46, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

[3] IEEE, Standard Verilog Hardware Description Language Reference Manual. Standard 1364-1995, New York, NY: IEEE, 1995.

[4] IEEE, Standard VHDL Language Reference Manual. Standard 1076-1993, New York, NY: IEEE, 1993.

[5] M. Keating, P. Bricaud "Reuse Methodology Manual for System-On-a-Chip Design", Kluwer Academic Publishers, 1999, pp.224.

[6] P. Lapsey and J. Bier "DSP Cores Bring New Level of Integration" //Microprocessor report, August 1994.

[7] DSP Design Tools and Methodologies, Berkeley Design Technology, Inc. (Fremont, California), 1995.

[8] Коркішко Т.А., Мельник А.О. Вимоги до продуктивності процесорів шифрування симетричними блоковими алгоритмами // Вісник національного університету «Львівська політехніка» №437 "Комп'ютерні системи і мережі". – Львів, 2001. – С. 83 – 89.

[9] American Bankers Association, Tripple Data Encryption Algorithm Modes of Operation, ANSI X9.52-1998, Washington, D.C., 1998.

[10] FIPS 81, "Operational modes of DES", Federal Information Processing Standard (FIPS), Publication 81, National Bureau of Standards, U.S. Department of Commerce, Washington D.C.

[11] Menezes A., Oorshot P., Vanstone S. Handbook of applied cryptography. – N.Y.: CRC Press Inc., 1996. – 816 p.

[12] Байсіг Ю., Коркішко Т., Мельник В., Мельник А. Порівняльний аналіз варіантів структурної організації процесора захисту інформації за алгоритмом DES // Матеріали міжнародної науково-технічної конференції "Сучасні проблеми в комп'ютерних науках в Україні" (CCU'2000). Славське, 2000. – С. 100 – 109.