CIPHER TWOFISH IMPLEMENTATION ON FPGA BOARD

Peter Cíbik
Bachelor Degree Programme (3.), FEEC BUT
E-mail: xcibik00@vutbr.cz

Supervised by: David Smékal
E-mail: smekal@phd.feec.vutbr.cz

Abstract: This paper deals with nowadays hot topic, which is data security and secure communication. It describes solution which uses Twofish cipher to ensure confidentiality of data. The cipher Is implemented in VHDL language and used on FPGA chip because of execution speed. The teoretical introduction explains need for secure the communication and data. In the next parts Twofish cipher and implementation are being discussed.

Keywords: Encryption, block cipher, Twofish, FPGA, VHDL, Netcope

1 INTRODUCTION

We are living in a period, where technology is used on daily basis. The amount of digital data and communication rise every day. The problem is, attackers have accordingly moved to cyberspace. Because of amount of data, transfer speed and threat of data leakage, we need fast and secure solution.
This paper describes solution which merges these problems and solve it. The main goal is to implement Twofish cipher in VHDL language and use it on FPGA board to encrypt / decrypt data. Field Programable Gate Array (FPGA) ensures the speed and Twofish cipher confidentiality of data.
Because of implementation on Network Interface Card (NIC) with FPGA, this solution can be used to secure point-to-point communication through the internet, or to secure huge amount of data moving through network interface to data storage.

2 TWOFISH

Cipher well known as a one of the candidates to Advanced Encryption Standard program of NIST institute. It is a symetric blok cipher and uses 128 bits block size, which means it uses the same key to encryption and decryption while it encrypts / decrypts whole blocks of data. We can see the scheme of this process on Figure 1. Key size can be up to 256 bits.
The main structure is based on pseudo-Feistel network with main one-way function F, which uses keys derived from main key in each round and in whitening part. It is still consider as a secure cipher with good parameters and it is good choice for our solution [1].

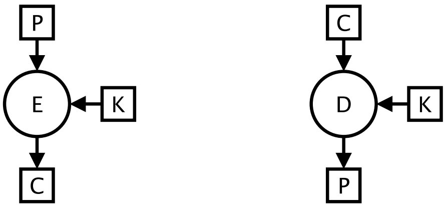
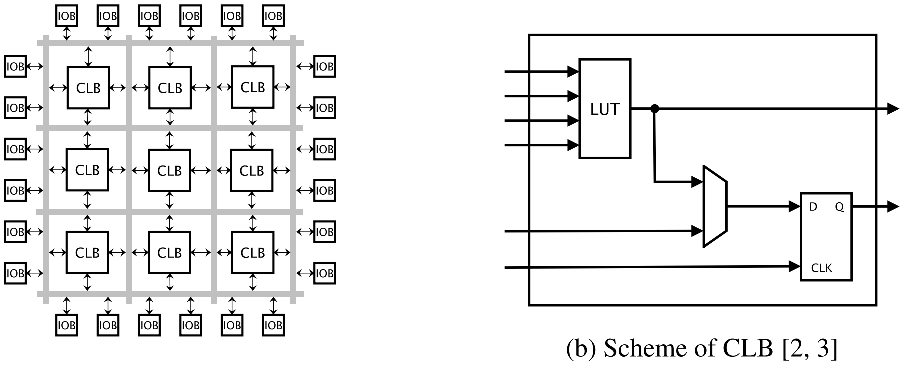


Figure 1: Scheme of symetric encryption (E) and decription (D), K– key, P– block of plaintext, C– blok of ciphertext

3 TECHNOLOGIES

- **VHDL** – One of the most popular Hardware Description Languages, which describes logic circuits. It can be used for programming of FPGAs [2].
- **FPGA** – Field Programable Gate Array is programable logical circuit consisting of three basic elements shown on the Figure 2a. Input and Output Block, Configurable Logic Block, shown on the Figure 2b, and programable horizontal and vertical interconection. All elements respectively interconection and inputs / outputs are programable. It uses Look-Up Tables (LUT) to compute, so it is really fast.



(a) Basic elements [3]

(b) Scheme of CLB [2, 3]

Figure 2: FPGA scheme

4 IMPLEMENTATION AND RESULTS

In implementation, the cipher with key size of 128 bits is used and also the block size is 128 bits. For 128 bits key length the 16 round pseudo-Feistel network structure is used. Cipher is based on its documentation Twofish: A 128-Bit Block Cipher [1]. Xilinx Vivado Design suite (XVDs) was used as a development environment for VHDL language.

Firstly after the documentation studying, cipher was divided to logically separated parts based on their functionality. Each part was implemented as a separate component like bit adder, matrix multiplication atc. Hierarchically higher based components include base ones. Gradually we have two main components. One for encryption and one for decryption data. On Figure 3 we can see main component of this structure, component F, which is the main function of pseudo-Feistel network.

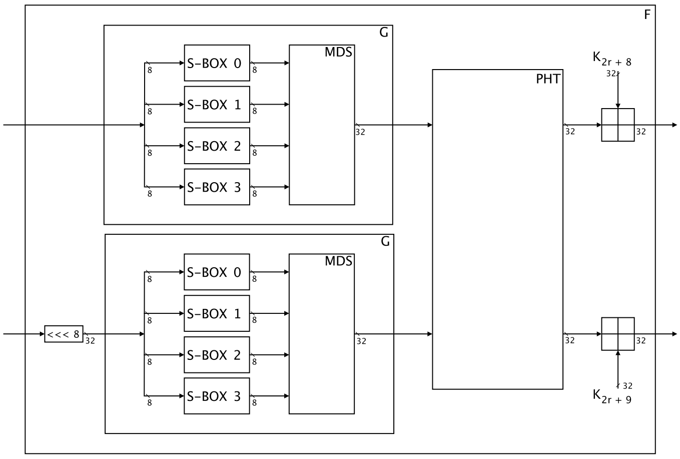
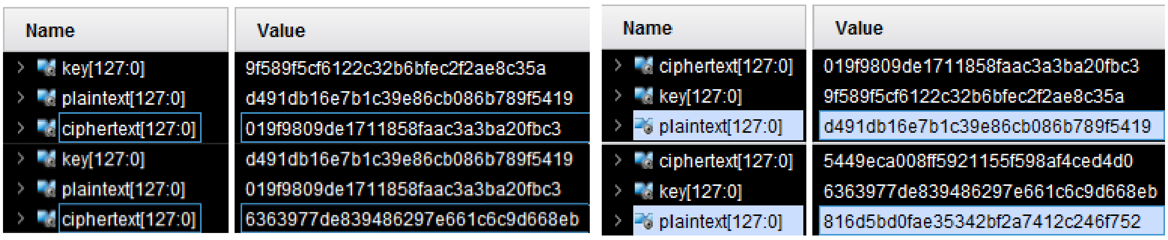


Figure 3: Scheme of component F [1]

4.1 Simulation

To verify the results and correct behaviour of components, simulation was executed on Artix-7 AC701 FPGA chip via XVDs. The behaviour and data-flow correspond with design and Twofish documentation [1]. The verification of results, which we can see on Figure 4a and 4b, of encryption and decryption with test vectors also from Twofish documentation [1] was correct. Now we have correctly working components design ready for the implementation.



Name	Value
key[127:0]	9f589f5cf6122c32b6bfec2f2ae8c35a
plaintext[127:0]	d491db16e7b1c39e86cb086b789f5419
ciphertext[127:0]	019f9809de1711858faac3a3ba20fbc3
key[127:0]	d491db16e7b1c39e86cb086b789f5419
plaintext[127:0]	019f9809de1711858faac3a3ba20fbc3
ciphertext[127:0]	6363977de839486297e661c6c9d668eb

(a) Results of encryption

Name	Value
ciphertext[127:0]	019f9809de1711858faac3a3ba20fbc3
key[127:0]	9f589f5cf6122c32b6bfec2f2ae8c35a
plaintext[127:0]	d491db16e7b1c39e86cb086b789f5419
ciphertext[127:0]	5449eca008ff5921155f598af4ced4d0
key[127:0]	6363977de839486297e661c6c9d668eb
plaintext[127:0]	816d5bd0fae35342bf2a7412c246f752

(b) Results of decryption

Figure 4: Simulation example results

4.2 Synthesis

The next step of implementation on hardware is synthesis, which is process of translating VHDL design description, maping into targeted technology and constructing a gate level netlist. Synthesis was performed on Xilinx Virtex-7 HT FPGA chip using XVDs. Synthesis was successful, without any complication. In Table 1 we can see used resources on FPGA chip with encryption design.

Table 1: Used resources on Xilinx Virtex-7 HT FPGA

Site type	Used	Available	Util %
LUTs	28229	433200	6.52
Bonded IOB	384	850	45.18

5 CONCLUSION

The purpouse of this paper was implemented Twofish cipher on FPGA platform by VHDL language. Simulation step, which used test vectors, verify functionality and results of components and whole design. Synthesis step performed functionality verification on specific FPGA chip. The next step will be optimization of used resources and optimization to the card interface and Netcope Development Kit. Final step will be implementation on the real hardware NIC card NFB-100G2Q with FPGA chip Xilinx Virtex-7 HT. Expected operating frequency is 60 MHz (speed approximately 7.5 Gbps).

REFERENCES

[1] SCHNEIER, Bruce, John KELSEY, Doug WHITING, David WAGNER, Chris HALL a Niels FERGUSON. *Twofish: A 128-Bit Block Cipher* [online]. 1998 [cit. 2017-10-14]. Available: https://www.schneier.com/academic/paperfiles/paper-twofish-paper.pdf

[2] PINKER, Jiří a Martin POUPA. *Číslicové systémy a jazyk VHDL*. Praha: BEN - technická literatura, 2006. ISBN 80-7300-198-5.

[3] Programovatelná logika II: FPGA. *Abclinuxu* [online]. [cit. 2017-11-02]. Available: http://www.abclinuxu.cz/blog/digital_design/2013/1/programovatelna-logika-ii-fpga