Implementation of extended Galois field operational unit with help of multiprocessor computers

Andrii Kostyk[1], Valerii Hlukhov[2]

1. Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: andy989gow@gmail.com

2. Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: valeriygl@ukr.net

The features of implementation of operational units for performing operations over elements of extended binary Galois fields are considered. It is shown that implementation using a multiprocessor computers allows obtain research results in a shorter period of time and improves performance at each step of the synthesis and implementation in the Xilinx ISE Design Suite.

Keywords – binary Galois fields GF(2^m), Xilinx ISE Design Suite, LUT (Lookup Table), Guild cell, performance.

Introduction

The paper discusses the features of implementation of operational units for performing operations over elements of extended binary Galois fields in modern field programmable gate arrays (FPGAs). Galois fields are used for based in elliptic curves electronic digital signatures, ensuring their reliability and protection from unauthorized persons (intruders) [1], [2]. For reliable protection of information their hardware implementation on the FPGA is increasingly used. The paper shows that implementation of operational units for operations over elements of a extended binary Galois field using a multiprocessor computers allows one to obtain the results of research much faster in comparison with a dual-processor computers.

Operations over elements of extended Galois Field

To build the multiplier for extended binary Galois field GF(2^m), modified Guild cells are used ([3]). A modified Guild cell consists of an adder and a multiplier. Total number of Guild Cells in multiplier is near m^2.

For the synthesis and implementation of a 239-bit arithmetic unit over elements of the Galois binary field GF (2^m), m = 239, the Xilinx ISE and FPGA Spartan 6 are used. A multi-core computer is used to speed up processes such as Synthesis, Map and Place & Route. The results of synthesis and implementation are compared for 2 core mobile processor Intel Core i3-3120M and a 12 core processor Intel Xeon E5-2600 v4 (Table 1).

Table 1

Comparison of execution time of the synthesis and implementation in the Xilinx ISE Design Suite, sec

Xilinx ISE Design Suite (Stages)	Intel Core i3-3120M	Intel Xeon E5-2600 v4
Synthesize – XST– Check Syntax	57	30,2
Synthesize – XST– Generate RTL	0,6	0,4
Synthesize – XST – Generate Technology Schematic	0,4	0,4
Synthesize – XST	124,5	73,42
Implement Design – Translate	38,81	28,8
Implement Design – Map	22,89	16,22
Summary	244,2	149,44

Fig. 1 shows the workload of 12 core Intel Xeon E5-2600 v4 processor during the implementation design in this study.

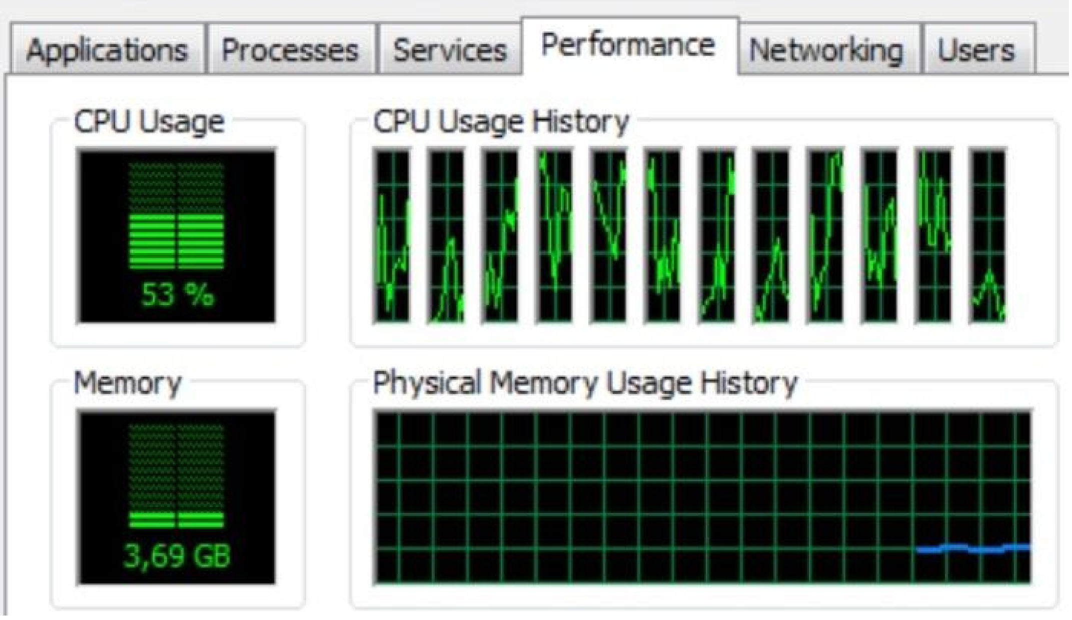

Fig. 1. Implement Design – Translate.

The results of the study show a significant improvement in performance at each step of the synthesis and implementation when multicore computer are used.

Conclusion

In this paper discusses implementation of operational units for performing operations over elements of extended binary Galois fields in modern FPGAs. Comparison of different computers execution time of synthesis and implementation in the Xilinx ISE Design Suite are performed. A significant improvement in research performance was achieved thanks to a 12 core Intel Xeon E5-2600 v4 processor compared with 2 core mobile processor Intel Core i3-3120M .

References

[1] IEEE 1363-2000: Standard Specifications For Public Key Cryptography. 2000. The Institute of Electrical and Electronics Engineers, Inc.

[2] DSTU 4145-2002 (2002), Information Technology. Cryptographic Techniques. Digital Signatures Based on Elliptic Curves. Generation and Verification [Informatsiyni tekhnolohiyi. Kryptohrafichnyy zakhyst informatsiyi. Tsyfrovyy pidpys, shcho gruntuyet'sya na eliptychnykh kryvykh. Formuvannya ta pereviryannya], *Derzhavnyy komitet Ukrayiny z pytan' tekhnichnoho rehulyuvannya ta spozhyvchoyi polityky*, Kiyv, Ukraine, 2003 (In Ukrainian).

[3] V.S. Hlukhov, A.T. Kostyk, M.M. Shniak, Osoblyvosti vykonannia operatsii mnozhennia elementiv poliv Halua GF(2m) ta GF(3m) // Visnyk Natsionalnoho universytetu "Lvivska politekhnika"//Kompiuterni nauky ta informatsiini tekhnolohii. – Lviv, 2016. – № 843 – S. 19-27.