Hardware complexity of multipliers of extended Galois field in FPGA

Ivan Zholubak[1], Valeriy Hlukhov[2]

1. Social Communication and Information Science Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: IvanZholubak7@ukr.net

2. Security of Information Technologies Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 12, E-mail: valeriygl@ukr.net

***Abstract* – In this paper, the implamantation of matrix multiplier of the Galois fields with basics 2, 3, 7, 13 and the analysis of the implementation of multipliers with a higher basis on the FPGA Xilinx Virtex-7 is considered. It is shown that the smallest hardware costs will be in multiplier of Galois fields with a base 3, 29% less than in binary fields. For the implementation of the Guild cells with a large foundation, the core generator of the modified Guild cells was implemented..**

Keywords: Galois fields GF(d^m), multiplier, modified Guild cell, LUT, nucleus generator.

I. Introduction

At present, cryptographic methods for protecting information based on the use of FPGA and cryptographic protocols built on multiplication operations in Galois fields GF(n^m) have become acute. Matrix multipliers of Galois fields GF(n^m) are characterized by high hardware costs, and therefore it is expedient to find the best method for their implementation. The paper compares the hardware costs of multiplier fields of Galois GF(n^m) based on their practical implementation in FPGA.

II. Analysis of the literature

In [4], in order to reduce the hardware complexity of the multiplier of the Galois field elements, the main element of which is the multiplicative matrix, an approach is proposed, which is to replace the multiplication matrix with the size mxm on the mixer and the ordered modified smaller multiplier matrix. Due to this, the reduction of structural and hardware complexity will increase the time complexity of multiplication [5]. To determine the possibility of implementing a multiplier on FPGA, the problem of a more accurate evaluation of it, taking into account the features of the FPGA topology, appears. The aim of the work is to estimate the hardware cost of creating a multiplier matrix [6] of the multiplier of the Galois field elements in a polynomial basis in order to select the field in which the hardware costs will be the smallest. During the execution of this work, on the basis of the proposed multiplier model in [1] and [2], its implementation was carried out and the theoretically verified the values of the hardware complexity obtained in [1] and [2].

III. Implementation on FPGA

To perform a multiplication operation in Galois fields, you can apply a matrix multiplier. It has a number of advantages and disadvantages. Among the disadvantages is a large hardware and structural complexity, among the advantages – high performance hardware implementation multiplier.

Matrix multipliers perform a multiplication operation in a non-traditional way through successive shifts and additions, but in parallel. The scheme of the operation of multiplication corresponds to the usual "multiplication by column". In the matrix of the elements of the multiplier, there is a bitwise multiplication of discharges and the summation of intermediate results. For the multiplication and summing up of intermediate results, Modified Guld cells (MGC) are used.

Modified GC for Galois GF(d^m) fields have 3p inputs and p outputs, each bit. Modified KG can be considered in 2 variants:

1) to consider Guild cell as a "black box" – a completely integral element in which the internal structure is insignificant, and only the number of inputs and outputs is taken into account;

2) with clarification of the internal structure (Guld cell consists of a multiplier and adder);

In the first variant, the number of LUT, used to implement a single modified GC – $k_{gd} = (2^{p-5} - 1) * k$, where $p = 3 * \lceil \log_2 d \rceil$, and k $= \lceil \log_2 d \rceil$. Hence it follows. So:

$$k_g = (2^{3*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil \qquad (1)$$

To implement a multiplier in the Galois fields with the base d GF (d^m) you need – $k_{kd} = 2m^2 - 2m + 1$ modified GC and additionally $(m-1) * (2^{3*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil$ LUT to find the coefficient, which must be multiplied by an irreducible polynomial. These hardware costs for the implementation of the element f, which forms this coefficient, can be neglected in this case, since they are small in comparison with the utilities for the implementation of the Guild cells himself.

Hardware costs, when sold, modified by the GC for the second option, ie as a set of multipliers and adder are calculated by the formula:

$k_{gd} = (2^{2*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2$. So:

$$k_g = (2^{2*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil * 2 \qquad (2)$$

In the Galois fields GF(d^m) multiplier implementation requires – $2m^2 - 2m + 1$ GC. The costs for the implementation of the element f are neglected, because they are small, in comparison with the expenses for the implementation of the multiplier itself.

In fig. 1 shows the internal structure of modified GC in the implementation as a) "black box" and b) with refinement of the internal structure of the multiplier GF (3^4).

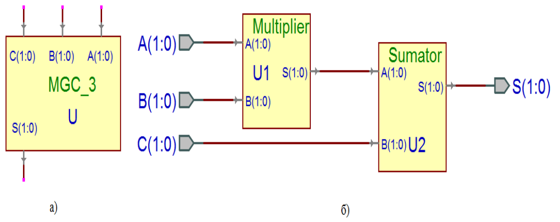

Fig. 1. Implementation of modified GC for Galois fields GF (3^4): a) "black box"; b) with clarification of the internal structure

In the first version, one function is formed which depends on 6 variables, which performs multiplication by module 3 and addition by module 3, in the second one – 2 functions that depend on 4 variables, the first of which performs multiplication by module 3, and the second is the addition for module 3.

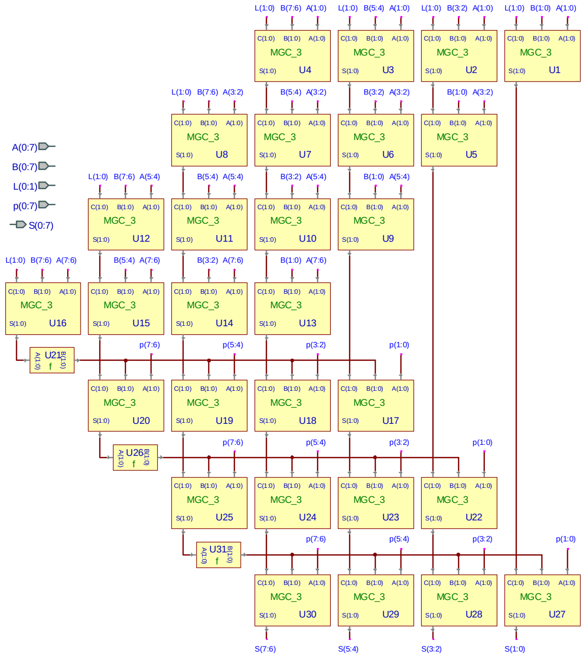

Fig. 2. Scheme of Galois multiplier GF (3^4)

The value of hardware costs for the implementation of memory modulators GF(2^{15}), GF(3^9), GF(7^5), GF(13^4), all having schemes similar to Fig. 2, is shown in the graph of Fig. 3 and table 1.

From graphic fig. 3 shows that the smallest hardware cost has a multiplier for the elements of the GF field (3^9).

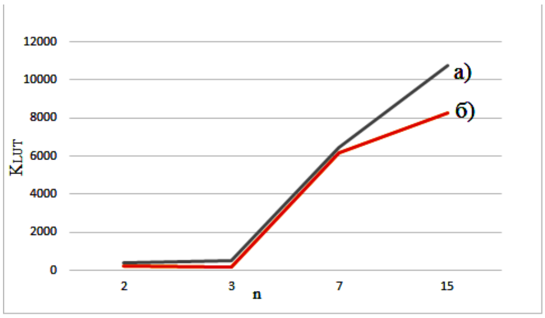

Fig. 3. Graph of hardware costs of multipliers of fields of Galois GF (2^{15}), GF (3^9), GF (7^5), GF (13^4): a) with refinement of the internal structure; b) "black box"

TABLE 1

HARDWARE COSTS OF LUT AND SLICE IN THE IMPLEMENTATION OF MULTIPLIERS FIELDS OF GALOIS FIELDS

The field for which the multiplier is constructed	The number of modified Guild cells	Number of elements in the box compared to GF (13^4)	The amount of used LUT in the multiplier when presenting the modified Guild cells as a "black box"	The amount of SLICE used in the multiplier when presenting the modified Guild cells as a "black box"	The amount of used LUT in the multiplier when the modified Guld cells is represented as a multiplier and adder	The amount of SLICE spent in the multiplier when a modified Guild cell is presented as a multiplier and adder
GF(2^{15})	435	101,3 %	207	144	195	131
GF(3^9)	153	96,5 %	148	75	381	144
GF(7^5)	45	95,4 %	6192	2423	276	135
GF(13^4)	28	100 %	8250	3758	2508	1128

From the table, we see that the smallest hardware costs will be in fields with a base of 3 GF(3^9).

Conclusion

A comparison of the hardware costs of multipliers of Galois fields with bases 2, 3, 7, 13 on the FPGA Xilinx Virtex-7. As a result of the comparison of the results of implementation of the multipliers, it can be seen that the smallest hardware costs will be in the Galois multipliers with the base 3, 29% less than the binary fields that coincide (does not match) with the previously obtained theoretical results.

References

[1] I. M. Zholubak, A. T. Kostik, V. S. Hlukhov. Osoblivosti opracuvanna elementiv triykovih poliv Galua na suchasniy elementniy bazy// Visnik Nacionalnoho universitetu “Lvivska politehnika” “Komputerni systemy ta merezhi”. – Lviv: – 2015. – Vip. 830. – p. 27 – 33.

[2] I. M. Zholubak, V. S. Hlukhov. Viznachenna rozshirenoho pola Galua GF(d^m) z naymenshoyou aparatnoyou skladnistu pomnozhuvacha // Visnik Nacionalnoho universitetu “Lvivska politehnika” “Informaciyni systemy ta merezhi”. – Lviv: – 2016. – Vip. 835. – p. 50 – 58.

[3] I. M. Zholubak, V. S. Hlukhov. Aparatni vitraty pomnozhuvachiv poliv Galua GF(d^m) z velikoyou osnovoyou // Visnik Nacionalnoho universitetu “Lvivska politehnika” “Computerni nauky ta informaciyni tehnologiyi”. – Lviv: – 2017.

[4] Hlukhov V. S., Elias P. M. Zmenshenna structurnoyi skladnosty bagatosekciynih pomnozhuvachiv elementiv poliv Galua // Electrotehnichni ta computerni systemy.– 2015.– № 19 (95).– p. 222–226.

[5] Cherkaskiy M. V., Tkachuk T. I. Harakteristiky skladnosty pristroyiv mnozhenna // Radioelectronni ta komputerni systemy. – 2012. – No. 5. – 142 – 147 p.