Research Hardware Complexity of Multipliers of Extended Galois Field GF(d^m)

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 – The paper analyzes the hardware costs of multipliers of extended Galois fields GF(d^m). There are compared realised on modern FPGA Galois fields multipliers hardware cost to select Galois field GF(d^m) with approximately the same number of elements and the lowest multiplier hardware complexity. Totally the hardware cost increases while basics of the field increase. Local minimums for odd d correspond to d = 2^i-1 and the global minimum for analisys based on Guild cell with realization like single unit corresponds to the value d = 3 and based on Guild cell with its multiplier and adder separate realization – the value d=7.

Key words – Galois fields GF(d^m), multiplier, modified Guild cell, LUT.

I. Introduction

Operations on Galois fields GF(2^n) with a lot of elements that are represented in the polynomial basis are using in modern data protection. Processing elements such fields is highly hardware, structural and time complexity. Therefore, determining the possibility of reducing hardware complexity using Galois field GF(d^m) with base d > 2 (d – simple number) and about the same number of elements ($d^m \approx 2^n$) is an urgent task.

II. Analysis of the literature

In modern data protection are using Galois fields GF(2^n), code of elements of such fields [1, 2] presented in polynomial or normal basis.

Mathematical foundations of digital signature processing are elliptic curves [3]. Processing of elliptic curve points based on the performance of sequences of operations in the Galois fields GF(2^n). Multipliers for these fields are highly hardware [4] structural [5, 6] and time complexity.

There are many devices for processing elements of the Galois fields GF(d^m) in the literature, which are used in a variety of cryptographic transformations. Is known matrix multiplier, which consists of Hild cells, to perform multiplication of binary numbers. Also is known multiplier based on modified Hild cells to perform multiplication of elements of the Galois field GF(d^m). The article discusses the hardware cost of matrix multiplier of Galois fields GF(d^m) when d <4, but does not address the cost of the hardware multipliers for Galois field GF(d^m) with higher fundamentals d> 4, which is the subject of this work.

III. Implementation on FPGA

Multiplier for Galois fields GF(d^m) can be implemented based on modified Guild cells (GC). Modified GC for Galois fields GF(d^m) shall be 3p inputs and p outputs $p = \lceil \log_2 m \rceil$ (Fig. 1). When using the modern FPGA logic cells which are based on programmable 6-input combinational circuit (LUT), implementation on FPGA of Guild cells in the general case when not specified the structure of GC, and takes only the number of inputs and outputs, requires $q_1 = (2^{3p-5} - 1) \cdot p$ LUT.

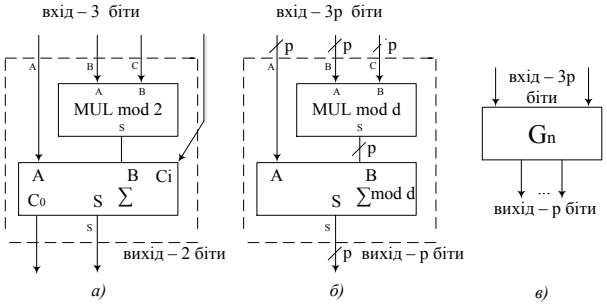

Fig. 1. a) Guild cell, b) modified Guild cell processing elements of Galuis field GF(d^m), c) symbol for the modified Guild cell of field GF(d^m)

Estimate the number of LUT in Guild Cells can in two options:

1) Consider Guild cells as "black box" - a fully integral part, which has negligible internal structure of the cells and take on attantion only the number of inputs and outputs;

2) Specification of internal structure (Guild cells consists of two "black boxes": multiplier and adder).

Hardware costs is conveniently assessed in comparison to the cost of multiplier for binary Galois field GF(2^n).

For the first version of the hardware cost factor where - coefficients of complexity and number of COG, and, and - the number of LUT in COG and COG for the number of Galois field GF (dm) and GF (2n), respectively.

For the first version coefficient of the hardware cost - $k_{mul} = k_g * k_k$, $k_g = k_{gd} / k_{g2}$, $k_k = \frac{k_{kd}}{k_{k2}}$ - coefficients of complexity and number of GC, k_{gd} and k_{gd}, k_{kd} and k_{kd} - the number of LUT in GC and number of GC in Galois fields GF(d^m) and GF (2^n), respectively.

For binary Galois fields GF(2^n) $k_{g2} = 1$, for others $k_{gd} = (2^{p-5} - 1) * k$, where $p = 3 * \lceil \log_2 d \rceil$, and k $= \lceil \log_2 d \rceil$. It follows that $k_{gd} = (2^{3*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil$. So:

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

In the binary fields GF(2^n) to implement multiplier need $k_{k2} = 2n^2 - 2n + 1$ Guild cells, and in the Galois fields with basis d GF(d^m) - $k_{kd} = 2m^2 - 2m + 1$ (Fig. 2) and additional $(m-1) * (2^{3*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil$ LUT for finding negative value of bits a_i. These hardware costs could in this case be neglected because they are small

compared with the costs for implementation of most Guild cells. So:

$$k_k \approx \frac{2m^2 - 2m + 1}{2n^2 - 2n + 1} \quad (2)$$

$$k_{mul} \approx \frac{(2^{3*\lceil \log_2 d \rceil - 5} - 1) * \lceil \log_2 d \rceil (2m^2 - 2m + 1)}{2n^2 - 2n + 1} \quad (3)$$

And $d^m \approx 2^n$. Then $m \approx log_d\, 2^n = \frac{n}{log_2 d}$,

$$k_k \approx \frac{\frac{2n^2}{(\log_2 d)^2} - \frac{2n}{\log_2 d} + 1}{2n^2 - 2n + 1} \approx \log_2^{-1} d,$$

$$k_{mul} \approx \frac{(2^{3*\lceil \log_2 d \rceil - 5} - 1)(\log_2 d)}{\log_2 d} \approx 2^{3*\lceil \log_2 d \rceil - 5}$$

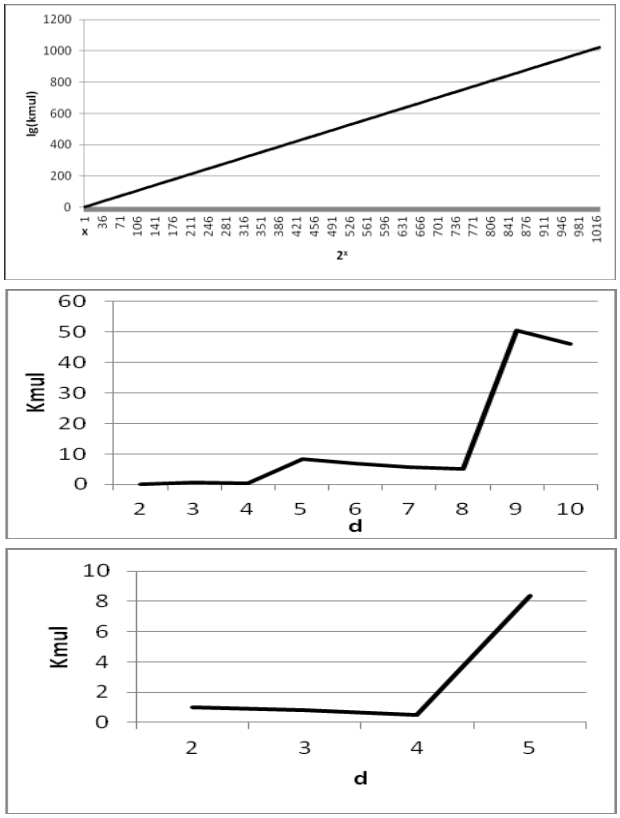

Fig. 2. The cost relation of hardware of multiplier's elements of the Galois fields GF(d^m) and GF(2^n) for: 1) range from 1 to 2^{342}, 2) range from 1 to 10, 3) range of 1 to 5

For small n k_{mul} need to rely on more precision formuls (1, 2, 3).

Pochatokovu plot graph of kmul shown in Fig. 2. In Fig. 2 can see that increasing the basics of field hardware costs are soaring.

Starting area of graph k_{mul} shown in Fig. 2. In Fig. 2 can see that increasing the basis of field hardware costs are increasing.

Conclusion

In some local areas with increasing d hardware costs are reducing. Local minimum of unpaired d correspond d = 2i-1. This global minimum in presenting Guild cells as "black box" correspond value d = 3, when presenting like set of multiplier and adder - the value of d = 7.

References

[1] Alexander Kushnerov, Troichnaya cifrovaya tehnica. Perspectivi I sovremennost //Universitet imeny Ben-Huriona, Beyer-ShevaБеер, Izrail. - 2005. – C.1-7.

[2] Oded Goldrich, Foundations of Cryptography, Volume 1: Basic Tools //Cambridge University Press, - 2014 – C.7-10.

[3] DSTY 4145-2002. Informaciyni tehnologiyi. Kriptografichniy zahist informaciyi. Cifroviy pidpis, shcho gruntuyetsa na eliptichnih krivih. Formuvanna ta pereviryanna //Derzhavniy komitet Ukrainy z pitan tehnichnoho rehuluvanna ta spozhivchoyi politiky. - 2002. – C.5-7.

[4] Hlukhov O.V., Lozinskiy A. Y., Yaremkevich R.I., Ihnatovich A.O// Analitichna ocinka structurnoyi skladnosty pomnozhuvachiv elementiv poliv Halua // ACIT'2015. – Ternopil: THEУ, 2015. – 1-5 c.

[5] Hlukhov V. S., Elias R. M., Melnik A. O. Osoblivosty realizaciyi na PLIS sekciynih pomnozhuvachiv elementiv poliv Halua GF(2^m) z nadvelikym stepenem // "Komputerno-intehrovany tehnologiyi: osvita, nauka, vyrobnictvo" – naukoviy zhurnal, Luckiy nacionalniy tehnichniy universitet. – Luck: 2013. - № 12. - C. 103 – 106.

[6] Hlukhov V. S., Hlukhova O. V. Resultaty ocinuvanna strukturnoyi skladnosty pomnozhuvachiv elementiv poliv Halua // Visnik Nacionalnoho Universitetu "Lvivska Politehnika "Komputerny systemy ta merezhy". – Lviv: - 2013. – Vip. 773. - C. 27 - 32.