Time Complexity of Multipliers for Galois Fields

Mohammed Kadhim Rahma
Valeriy S. Hlukhov

Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, 12 S. Bandery street,
E-mail: muhamed_kadhem@yahoo.com valeriygl@ukr.net

Annotation – Multipliers for binary Galois field GF (2^n) hardware complexity allows to implement in FPGA an operational device with multiple multipliers. But because of large structural complexity for some combinations of large degrees n of field and the multipliers number to make it is practically impossible. One of the possible choices of this problem solving is the move to using Galois fields with the base d, greater than 2. Multipliers for such extended Galois field GF (d^m) with approximately the same number of elements $d^m \approx 2^n$ are estimated in the article in terms of their time complexity to determine the fields in which the multiplier will have the least time complexity.

Key words – time complexity, Galois field, extended field, field characteristic, degree of the field, multiplier.

I. Introduction

Multipliers for binary Galois field GF (2^n) hardware complexity allows to implement in FPGA an operational device with multiple multipliers. But because of the large structural complexity for some combinations of large field order n and the multipliers number to make it is practically impossible. One of the possible choices of this problem solving is the move to Galois fields with the base d≥2 usage. Multipliers for such extended Galois field GF (d^m) with approximately the same number of elements $d^m \approx 2^n$ are estimated in the article to determine the fields in which the multiplier will have the least time complexity. Multiplier based on modified Guild cells are selected for analysis. Modified Guild cells work with d-bit data and have no carry input and output. They are built from programmable combinational logical units (LUTv), each can be programmed to implement l logical functions of v variables in FPGAs. Modern FPGAs have LUTv with v=4 and v=6 inputs. Multiplier time complexity for GF(d^m) is determined in relation to GF(2^n) one. It is shown that the multiplier has less time complexity (less than 1.5 times) compared with GF(2^n) only in GF(3^m) when FPGAs with 6 inputs LUT6 are used.

II. Previous works

The mathematical basis for digital signature processing are elliptic curves and Galois Fields $GF(2^n)$ [1]. Multiplier hardware implementation for these fields is very expensive. Multipliers can be parallel (including based in Guild cells [2]), serial and parallel-serial - sectional. Multipliers are impossible to implement because of their high structural complexity in fields with large degrees n and with large number of sections [3]. Structural complexity evaluation methods and results for one multiplier are given in [4], for multisection multipliers they are given in [5]. Based on software and hardware models structural complexity estimation are described in [6, 7]. Structural complexity reduction methods [8] were developed from its estimation methods.

One of the possible options for solving the problem is transition to Galois fields with base n≥2, first of all with n=3 [9]. Multiplier time characteristics might change after fields change. In this paper multipliers for extended Galois field GF(d^m) with bases d ≥ 2, and approximately the same number of elements $d^m \approx 2^n$ are compared. Time complexity thus is determined relatively to extended binary Galois field GF(2^n). The time complexity is determined as the number of series-connected LUTs, that are part of FPGA [10]. Based on the modified Guild cells multiplier [8] was chosen for analysis.

III. Multiplier for extended Galois fields

Fig. 1 shows the functional scheme of two elements field GF(d^m) multiplier which uses a modified for GF(d^m) Guild cells (Gd). Guild cells detailed circuit is shown in Fig. 2, q_i - field polynomial coefficients, $p = \lceil log_2 d \rceil$ is the number of bits in record of d.

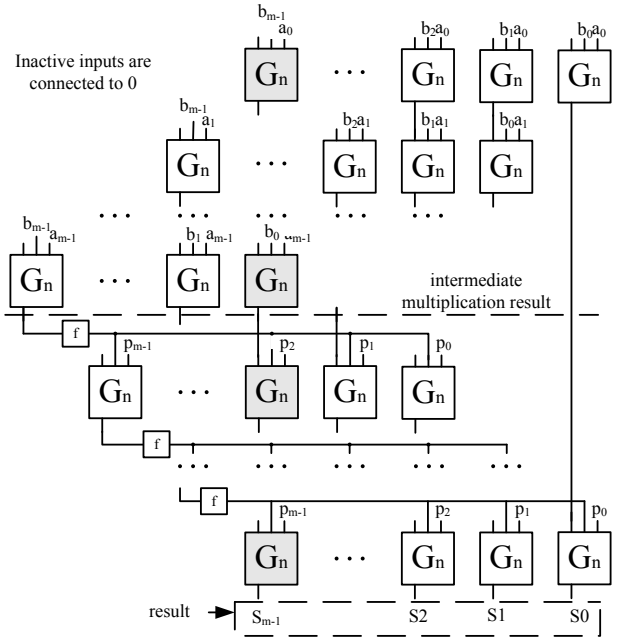

Fig. 1. Multiplier which uses a modified for GF(d^m) Guild cells (Gd)

The biggest delay occurs during formation of the S_{m-1} digit. This largest delay $t_{Mul} = 2mt_G$, where t_G is delay of one Guild cell (Fig. 2). From LUT that has v inputs, you can create LUT that has j inputs (Fig. 3). Then $M_{j,i}$ = (j-v + 1) LUTs with v inputs will be connected serially.

Time complexity $C_{t,d}$ of expanded Galois field GF(d^n) is

$$C_{t,d} = R_{d,2} C_{t,2}; R_{d,2} = \frac{log_2 d}{(3\lceil log_2 d \rceil - v + 1)},$$

$C_{t,2} = 2m$ is time complexity of multiplier for GF(2^m). If $R_{d,2} > 1$ then extended field with base d has less time complexity

compared to the extended binary field. As can be seen (Fig. 4) only fields with d = 3 (among primary bases) have advantage over binary field and only for usage of LUT with 6 inputs.

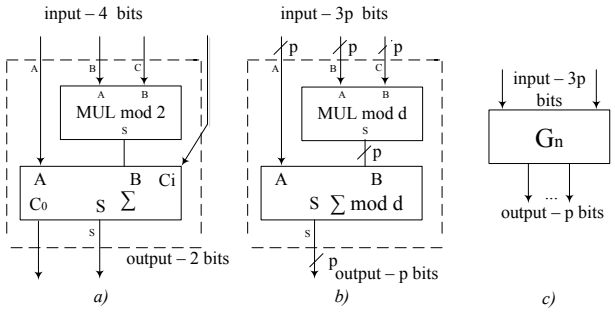

Fig. 2. Original a) and modified for GF(d^m) Guild cell

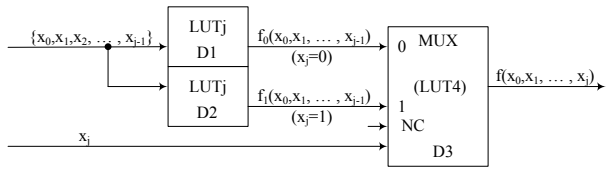

Fig. 3. LUT with j+1 inputs

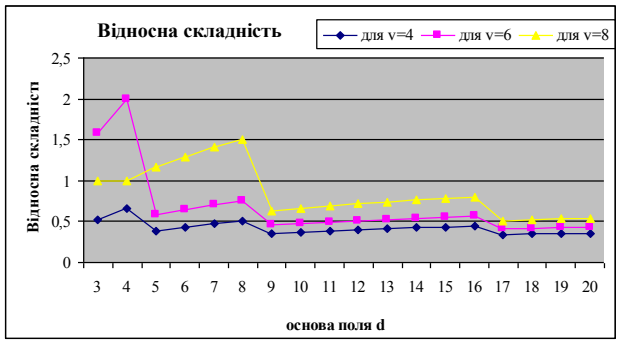

Fig. 4. Relative time complexity

Conclusion

In an article the extended Galois field in which multiplier time complexity in its implementation on modern FPGA is the smallest and is less then extended binary field one is determined for the set of extended Galois field GF(d^m) with approximately same number of elements. It is GF(3^m) when FPGA with 6-input LUT are used, its multiplier time complexity is in 1.5 times less than Galois field GF(2^m) one.

References

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

[2] H.H. Guild. Fully iterative fast array for binary multiplication and addition. Electronics Letters, Volume 5, Issue 12, 12 June 1969, page 263 (In English).

[3] V.S. Hlukhov, R.M.Elias, A.O.Mel'nyk. Osoblyvosti realizatsiyi na PLIS sektsiynykh pomnozhuvachiv elementiv poliv Halua GF(2m) z nadvelykym stepenem [Features of the FPGA-based Galois Field GF(2m) Elements Sectional Multipliers with Extra Large Exponent]. Komp"yuterno-intehrovani tekhnolohiyi: osvita, nauka, vyrobnytstvo - naukovyy zhurnal, Luts'kyy natsional'nyy tekhnichnyy universytet. Luts'k, Ukraine, 2013, vol. 12, pp. 103 – 106 (In Ukrainian).

[4] Hlukhov V. S., Hlukhova O. V. Rezul'taty otsinky strukturnoyi skladnosti pomnozhuvachiv elementiv poliv Halua [Structural Complexity of Galois Field Elements Multipliers Evaluation Results]. Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi". Lviv, Ukraine, 2013, vol. 773, pp. 27-32 (In Ukrainian).

[5] Hlukhov V. S., Trishch H. M. Otsinka strukturnoyi skladnosti bahatosektsiynykh pomnozhuvachiv elementiv poliv Halua [Evaluation of structural complexity multisection multiplier for Galois field elements]. Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi". Lviv, Ukraine, 2014, vol. 806, pp. 27-33 (In Ukrainian).

[6] Sholohon O. Z. Obchyslennya strukturnoyi skladnosti pomnozhuvachiv u polinomial'nomu bazysi elementiv poliv Halua GF(2m) [Structural Complexity of Galois Field GF(2m) Elements Multipliers in Polynomial Basis Calculation]. Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi". Lviv, Ukraine, 2014, vol. 806, pp. 284-289 (In Ukrainian).

[7] Sholohon Yu. Z. Otsinyuvannya strukturnoyi skladnosti pomnozhuvachiv poliv Halua na osnovi elementarnykh peretvoryuvachiv [Based on Elementary Transducers Structural Complexity of Galois Field Multipliers Evaluation]. Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi". Lviv, Ukraine, 2014, vol. 806, pp. 290-295 (In Ukrainian).

[8] Hlukhov V.S., Elias R. Umenshenie strukturnoy slozhnosti mnogosektsionnyih umnozhiteley elementov poley Galua [Galois Fields Elements Multisection Multipliers Structural Complexity Reduction]. Elektrotehnicheskie i kompyuternyie sistemyi. - 2015. - № 19(95) - pp. 222-226 (In Russian).

[9] M. Zholubak, A. T. Kostyk, V. S. Hlukhov. Osoblyvosti opratsyuvannya elementiv triykovykh poliv Halua na suchasniy elementniy bazieskye y komp'yuternыe systemы [Features of processing Binary Galois fields elements on modern hardware base]. Visnyk Natsional'noho universytetu "L'vivs'ka politekhnika" "Komp"yuterni systemy ta merezhi". Lviv, Ukraine, 2015, vol. 830, pp. 27-33 (In Ukrainian).

[10] Spartan-6 Family Overview. DS160 (v2.0) October 25, 2011. © 2009–2011 Xilinx, Inc. (In English