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_kadhim@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 fields 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 $GF(d^n)$ with approximately the same number of elements $d^n \approx 2^n$ 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 fields 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 $GF(d^n)$ with approximately the same number of elements $d^n \approx 2^n$ 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.

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 $n \geq 2$, first of all with $n = 3$ [9]. Multiplier time characteristics might change after fields change. In this paper multipliers for extended Galois field $GF(d^n)$ with bases $d \geq 2$, and approximately the same number of elements $d^n \approx 2^n$ 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 $GF(d^n)$ multiplier which uses a modified for $GF(d^n)$ Guild cells (Gd). Guild cells detailed circuit is shown in Fig. 2, $q_i$ - field polynomial coefficients, $p = \left\lceil \log_2 d \right\rceil$ - the number of bits in record of $d$.

![Fig. 1. Multiplier which uses a modified for $GF(d^n)$ Guild cells (Gd)](image)

The biggest delay occurs during formation of the $S_{m-1}$ digit. This largest delay $t_{\text{total}} = 2mt_G$, 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 $M_{ij} = (j-v+1)$ LUTs with $v$ inputs will be connected serially.

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

$$C_{r,d} = R_{d,2} C_{d,2}, R_{d,2} = \frac{\log_2 d}{\left\lceil 3 \log_2 d \right\rceil - \left\lceil \log_2 d \right\rceil - 1}, \quad C_{d,2} = 2m$$

is time complexity of multiplier for $GF(2^n)$. 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.

\[
\begin{align*}
\text{Fig. 2. Original a) and modified for GF}(d^m) \text{ Guild cell} \\
\end{align*}
\]

\[
\begin{align*}
\text{Fig. 3. LUT with } j+1 \text{ inputs} \\
\end{align*}
\]

\[
\begin{align*}
\text{Fig. 4. Relative time complexity} \\
\end{align*}
\]

### 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\((d^n)\) 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


[8] Hlukhov V.S., Elias R. Umenshenie strukturoyi skladnosti pomnozhuvachiv poliv Halua (GF\((2m)\) GF\((3m)\)) when FPGA with 6-input LUT are used, its multiplier time complexity is in 1.5 times less than Galois field GF\((2m)\) one.
