Results of Galois Field Elements Multipliers Structural Complexity Evaluation

Alexandra Hlukhova

Department of Computer-Aided Design, Lviv Polytechnic National University, S. Bandery Str., 12, Lviv, 79013, UKRAINE, E-mail: aleksandra.glukhova@gmail.com

Abstract – Scalable multiplier for Galois field GF(2m) elements core generator operation is examined. The multiplier uses type 2 Gaussian normal basis for Galois field elements presentation and forms m-bit (m≤998) result by n-bit portions. Generated cores hardware complexity allows their implementation in FPGA for any m and n values. But for big m and n values implementation is impossible because of high structural complexity. The method for such multipliers structural complexity estimation is proposed in this work and results are discussed.

Key words - Galois field GF(2^m), Gaussian normal base of type 2, scalable multiplying, core generator, structural complexity.

I. Introduction

At present the mathematical basis for digital signatures is an elliptic curve. Elliptic curves points processing is based on the Galois field GF(2^m) elements processing. Multiplier hardware implementation for such fields requires large hardware cost. Multipliers can be parallel, serial, and parallel-serial - sectional. This paper analyzes the results of sectional multipliers synthesis by Galois fields GF(2^m) multiplier core generator. The multiplier is processing m-bit elements of the Galois field GF(2^m), elements are represented using Gaussian normal basis of type 2. Sectional multiplier forms the m-bits product by n-bits portions. The hardware complexity of the generated multiplier cores allows their implementation on modern FPGA. But for large values of m and n it is impossible to implement cores due to their high structural complexity. Such multipliers structural complexity estimation method is proposed in this work. The method is based on an analysis of multiplication matrix used for presented in Gaussian normal basis of type 2 Galois Field elements multiplication.

II. The literature review and problem statement

Mathematical Foundations of digital signatures are elliptic curves and Galois field. One Galois field GF(2^m) element alternative representation is a Gaussian normal basis of type 2. For a given base serial multiplier Massey-Omura, parallel multiplier, and parallel-serial multiplier (sectional) are known. Multiplicative matrixes for them were studied in [2]. In [3, 4] the features of sectional multipliers VHDL-description (cores) generation are given and hardware complexity numerical values of generated cores with m = 515, 519, 998 are shown. For large values of m and n it is impossible to implement cores due to their high structural complexity.

Evaluation of the multipliers structural complexity in previous studies is performed in [5].

III. The purpose of work

Purpose of work is to present the results of Gaussian normal basis of type 2 binary Galois fields elements multiplier structural complexity evaluation.

IV. Sectional multiplier implementation

Serial Messi-Omura multiplier (Fig. 1) consists of two operands shift registers (RGA and RGB) and multiplication matrix M [1]. Sectional multiplier contains several multiplication matrices (for example F0, …, F15 on Fig. 2) and pipelined register for multiplication results.

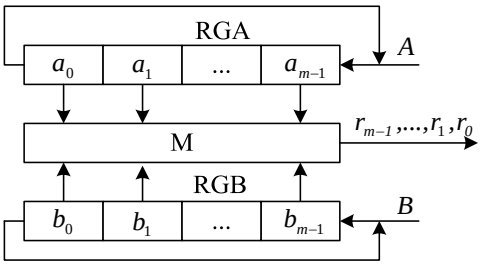

Fig. 1 Serial Messi-Omura multiplier

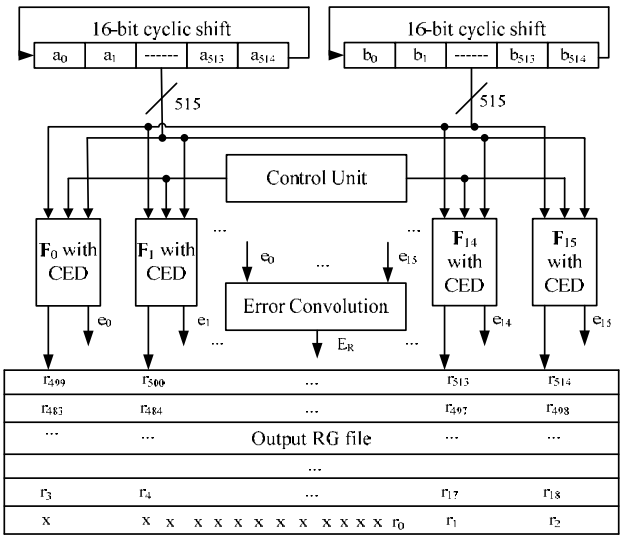

Fig. 2 Sectional multiplier

r0 bit of product R is calculated as $r_0=AMB^T$ (for example on Fig. 3

$$r_0 = a_2b_0 \oplus (a_2 \oplus a_3)b_1 \oplus (a_0 \oplus a_1)b_2 \oplus (a_1 \oplus a_3)b_3$$

in accordance with calculation scheme on Fig. 4).

Multiplier chip topology (Fig. *5*) corresponds to multiplication matrix topology (Fig. 4).

We can evaluate multiplier structural complexity as total conventional length L of connections inside square region in *Fig. 5*: b_i connection length is $l_{b_b} = x_{b_i} + 1$, where x_{b_i} is column number of the most right "1" in i row; vertical connection length is equal $v_j=m+d_j+1$, where d_j is number difference of row with "1".

$$r_0 = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Fig. 3. Product calculation

$$\begin{bmatrix} a_0 & a_1 & a_2 & a_3 \end{bmatrix} \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix}$$

Fig. 4. Product calculation scheme

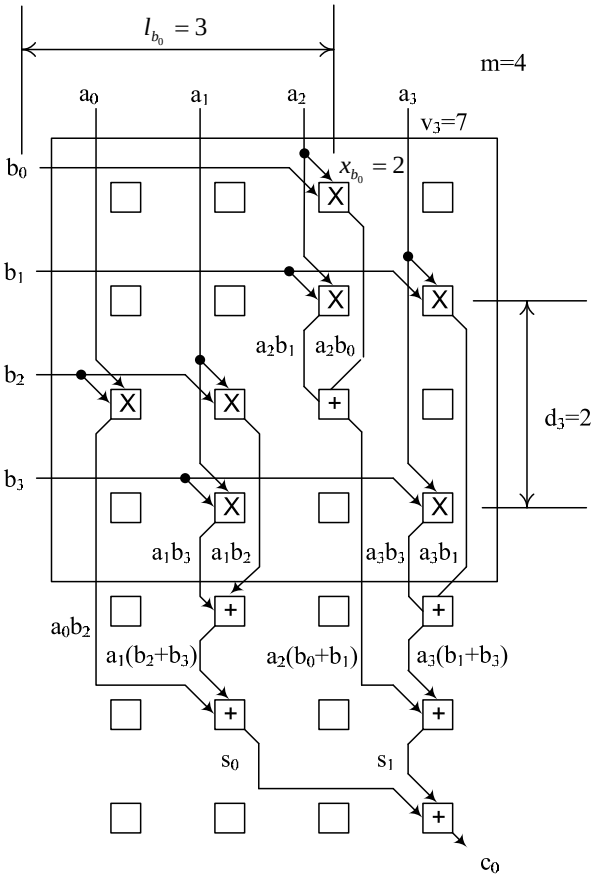

Fig. 5. Multiplier chip topology

Finally: $L = \sum_{i=0}^{m-1} (l_{b_i} + v_i)$.

V. Implementation results for FPGA

The program has been developed to evaluate the structural complexity of multipliers [5]. The input data for the program is the description of the multiplicative matrix. The result of calculation is the total length of the links in the rectangular area in *Fig. 5*. The results of calculations are shown in table 1, table 12, table 13.

TABLE 1

VIRTEX 6VLX130T (M=515)

m=515, n=	1	8	16	32
Slice number (%)	688 (3%)	1771 (8%)	2307 (11%)	7018 (35%)
Implementation time, minutes		5	304	**Not routed**
Structural complexity, interconnections length	265139	2121112	4242224	8484448

TABLE 2

VIRTEX 6VLX130T (M=519)

m=519, n=	1	8	16	32
Slice number (%)	675 (3%)	2248	3240	6,112
Structural complexity, interconnections length	268456	2147648	4295296	8590592

TABLE 3

SPARTAN XC6SLX150T (M=998)

m=998, n=	2	4	8
Slice number (%)	1,323 (5%)	1,896 (8%)	3,253 (14%)
Implementation time, minutes	1	20	133 **Not routed**
Structural complexity, interconnections length	559624	1119248	2238496

Conclusion

The results of structural complexity evaluation method for presented in Gaussian normal basis of type 2 binary Galois fields elements multiplier was proposed. The method is based on multiplier topology study and its connection conventional length L calculation. Special program was designed to calculate L for binary Galois fields GF(2^m) with big order m.

References

[1] Elias Rodrigue. Design of an Elliptic Curve Cryptography Using A Finite Field Multiplier in GF(2^{521}). Proceedings of the Lviv Polytechnic National University "Computer Systems and Networks" - Lviv, 2009. - № 658. - Pp. 144 - 149.

[2] V. Hlukhov. Matrices operations in Galois fields features. Proceedings of the Lviv Polytechnic National University "Computer systems design. Theory and Practice" - Lviv, 2006. - № 564. - Pp. 35-39.

[3] Hlukhov V., Elias R. Sectional multiplier for optimal normal basis of type 2 Galois field GF(2^m) elements core generator // Proceedings of the Lviv Polytechnic National University "Computer Science and Information Technology" - Lviv, 2012. - № 732. - Pp. 78 - 84.

[4] V. Hlukhov, R. Elias, A. Melnyk. Features of the FPGA-based Galois field GF(2^m) elements sectional multipliers with extra large exponent. // "Computer-Integrated Technologies: education, science and industry" - Lutsk National Technical University. № 12, 2013. Pp. 103 – 106.

[5] V. Hlukhov, A. Hlukhova. Galois field elements multipliers structural complexity evaluation. Proceedings of the 6-th International Conference ACSN-2013. September 16-18, 2013. Lviv, Ukraine. Pp. 18-19.