Modified Multiplying Matrix for Galois field GF(2^m) Multiplier Structural Complexity Evaluation

Aleksandra Hlukhova

Department of Information Systems and Networks,
Lviv Polytechnic National University, S. Bandery Str., 12, Lviv,
79013, UKRAINE, E-mail: aleksandra.glukhova@gmail.com

Abstract – Method of structural complexity estimation of modified multiplying matrix with ordered structure is proposed. The method is based on total length of connections inside multiplying matrix calculation. Matrix with ordered structure allows a partition to the same sub-matrix. One sub-matrix can be serially used for multiplication instead of one large unmodified matrix.

Multiplier structural complexity can be reduced more than 100 times.

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. The most difficult multiplier element is its multiplying matrix. Sectional multiplier processes m-bit elements of the Galois field GF(2^m) and forms the m-bits product by n-bits portions. Galois field elements are represented using Gaussian normal basis of type 2. The hardware complexity of the multicore multiplier matrixes 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. The structural complexity estimation method of multiplying matrices is known. Also based on the modified multiplying matrix multiplier is known. In this work modified multiplying matrix structural complexity estimation method is proposed. The method is based on connections length calculation inside multiplication matrix.

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]. Analytical evaluation of structural complexity Galois field multipliers elements proposed in [5]. Multiplier matrix modification was proposed in [7]. Modification consisted in ordering of multipling matrix.

III. The purpose of work

Purpose of work is estimation of modified multiplying matrix structural complexity.

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 and pipelined register for multiplication results.

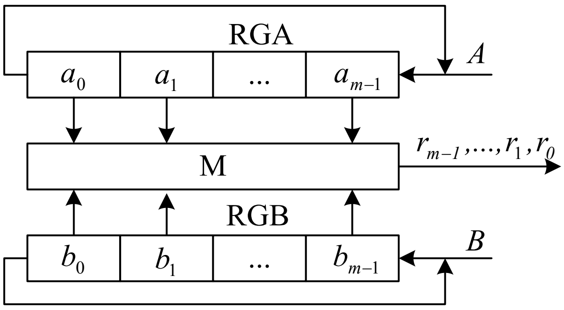

Fig. 1. Serial Messi-Omura multiplier

r0 bit of product R is calculated as r_0=AMB^T (for example on Fig. 2

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

in accordance with calculation scheme on Fig. 3).

Simplified multiplication matrix chip topology (Fig. *4* example for m=3) corresponds to mathematical multiplication matrix topology (Fig. 3). Each point in the Fig. *4* corresponds to one 2AND gate.

Simplified topology of modified multiplying matrix is shown in *Fig. 5*.

We can evaluate multiplier structural complexity as total length L of connections inside rectangle region in *Fig. 4*: b_i connection length is $l_{b_i} = x_{b_i} + 1$, where x_{b_i} is column number of the most right "1" in i row; vertical connection length is equal v_j=m+1, where m is Galois field GF(2^m) order.

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

Fig. 2. 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. 3. Product calculation scheme

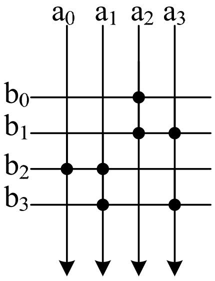

Fig. 4. Multiplying matrix chip topology

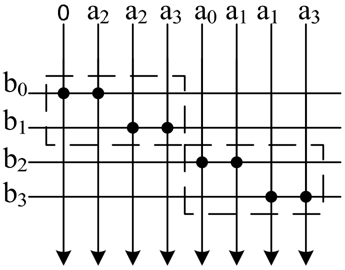

Fig. 5. Modified multiplying matrix chip topology

All vertical connections are the same length equal m+1and their number is 2(m+1). So their total length is

$$L_a = 2(m+1)^2 .$$

Lengths of horizontal connections form an arithmetic progression with step 2. Its sum is

$$L_b = \frac{(m+1)(m+2)}{2} .$$

Finally: $L_m = L_a + L_b$,

$$L_m = 2(m+1)^2 + \frac{(m+1)(m+2)}{2} .$$

Matrix with ordered structure allows a partition to the same sub-matrix *Fig. 5*.

For example, the matrix with m 175 can be divided on 11 matrixes with m=15. So we can use 11 times the matrix with m=15 in steed of one big matrix with m=175.

$$L_{175} = 2(m+1)^2 + \frac{(m+1)(m+2)}{2} =$$

$$= 2(175+1)^2 + \frac{(175+1)(175+2)}{2} = 46552 ;$$

$$L_{15} = 2(m+1)^2 + \frac{(m+1)(m+2)}{2} =$$

$$= 2(15+1)^2 + \frac{(15+1)(15+2)}{2} = 392 .$$

After that we can reduce structural complicity in k times where

$$k = \frac{L_{175}}{L_{15}} = 119 .$$

Conclusion

Method of structural complexity estimation of modified multiplying matrix with ordered structure is proposed. The method is based on total length of connections inside multiplying matrix calculation. Matrix with ordered structure allows a partition to the same sub-matrix. One sub-matrix can be serially used for multiplication instead of one large unmodified matrix.

Multiplier structural complexity can be reduced more than 100 times.

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.

[6] Hlukhova O. V., Ignatovich A. O., Lozinsky A. Y., Yaremchuk R. I. Analitichna otsinka strukturnoi skladnosti pomnozhuvachiv elementiv poliv Galois // ACIT'5. "Suchasni kompyuterni informatsiyni tehnologii." TNEU. – Ternopol. 22-23 Travnia 2015. – C. 169-171.

[7] V. S. Hlukhov, R. Elias. Zmenshennya strukturnoi skladnosti bagatosektsiynih pomnozhuvachiv elementiv poliv Galois. Elektrotehnichni ta komp`yuterni Systemy. – Odessa – 2015. Vydavnytstvo Nauka i tehnika. – № 19 (95). – S. 222 – 226.