Features of multiplication execution of operations in binary and ternary Galois fields

Andrii Kostyk[1], Valerii Hlukhov[2], Ivan Zholubak[3]

[1]Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: andy989gow@gmail.com

[2]Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: valeriygl@ukr.net

[3]Computer Engineering Department, Lviv Polytechnic National University, UKRAINE, Lviv, S. Bandery street 28a, E-mail: IvanZholubak7@ukr.net

Abstract – Consider the proposed method of construction serial ternary multiplier element Galois field GF (3^m). The described method of verification operations on elements of the Galois field GF (2^m) and GF (3^m) use mathematical package Maple.

Key words – Galois field GF(3^m), Galois field GF(2^m), multiplier, mathematical package Maple, digital signature.

I. Introduction

To protect electronic documents from a possible modification, forgery, copying, use digital signature, to guarantee authenticity.

The basis of the checks and obtain a digital signature assigned operations on elements of the Galois field GF (p^q).Software implementation calculations using universal computer tools are not always effective in terms of performance, including, if necessary computations in real time. Therefore actual problem is hardware or software implementation of hardware and computing in finite fields.

Multiplication is the main operation in the processing elements of Galois fields. In [1], [2], [3] describes methods and algorithms for multiplication elements captains Galois fields, but not implemented multiplier. Parallel tubes have high bandwidth and they are best suited to solving problems that require high speed processing and relatively small finite fields [2].

II. Ternary fields

In Ukraine, January 1, 2004 proposed to use the digital signature instead of the usual. Today, the following standards as Ukraine national standard ISO 4145-2002, interstate standard GOST 34.310-95 and international standard IEEE 1363. They described the formation of digital signatures based on Galois field GF (2^m) and elliptic curves. International Standard specifies the maximum Galois field characteristic $m \leq 998$, while international standards only m = 509. Therefore, to develop in this area are beginning to explore the ternary Galois field GF (3^m).

National standard processing involves the use signatures Galois field GF (p^q), where p = 2, but do not exclude the use of fields with p = 3. Each category field GF (2^m) encoded by one bit, and field GF (3^n) - two. To ensure the reliability of digital signatures no less than for binary fields n order field *GF* (3^n) is chosen from the condition n * log3> m; n> 0,6m (m - procedure field GF (2^m)).

To make it convenient to record ternary field in the software implementation was proposed [4] is their representation in Table 1.

TABLE 1.

REPRESENTATION OF TERNARY FIELDS

Coefficient	0	1	2
High bit	0	0	1
Low bit	0	1	0

The remaining combinations are considered invalid with respect to this presentation.

Method bit storage stratification factors has its advantages. During the software implementation of certain tasks in the coefficients can be used in parallel. In the hardware implementation can be built effective schemes for addition and multiplication of elements of the field GF (3^m). Software and hardware implementation method proposed in the bundle bit [3].

III. Implementation of parallel multiplier

To build a binary field GF (2^m) used Hild modified cells, where each cell has a 3-bit input and 1-bit output [6] (Fig. 1).

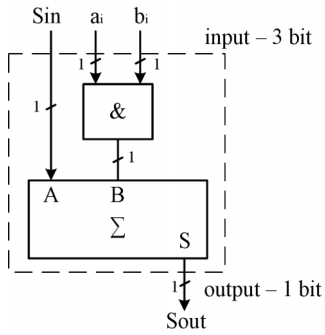

Fig. 1. Hild modified cell for GF (2^m)

To construct the ternary field GF (3^m), used Hild modified cells that are different from the binary field increased number of input and output data. Hild Each cell has a 6-bit input and 2-bit output (Fig. 2). The modification is that the construction does not use cell transfer.

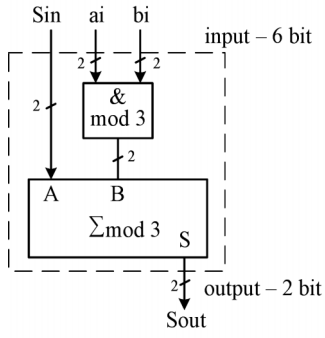

Fig. 2. Hild modified cell for GF (3^m)

Matrix multiplier for direct and reverse field GF (2^3), shown in Fig. 3.

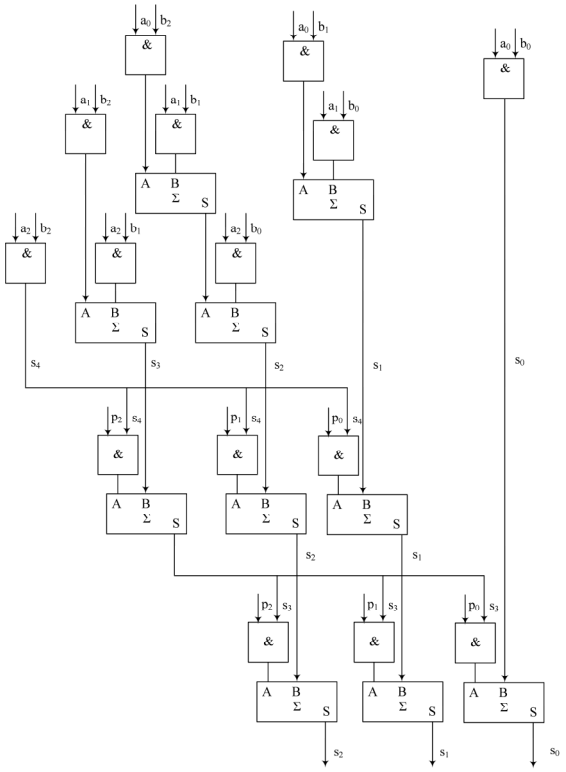

Fig.3 Matrix Multiplier for direct and reverse fields GF(2^3).

IV. Mathematical check

To verify proper operations of elements of the field GF (3^2) and GF (2^3), the mathematical package Maple. This package allows you to ask Galois field in digital forms, polynomial basis and perform mathematical operations on elements of the field [11]. Example program to verify proper operations in GF (2^3) and GF (3^2) Galois fields are listed in Table 2.

TABLE 2.

CHECKING THE CORRECT EXECUTION OF OPERATIONS IN GF (2^3) AND GF (3^2)

>G3:=GF(3,2,2+x+x^2):	>G2:=GF(2,3,1+x+x^3):
> Primitive(G3) mod 3;	> Primitive(G2) mod 2;
true	true
> b:=convert("5", decimal, hex);	>b:=convert("5", decimal, hex);
b:=5	b:=5
> c:=G3[input](b);	> c:=G2[input](b);
c:=(x + 2) mod 3	c:=(x^2 + 1) mod 2
> d:=convert("6", decimal, hex);	>d:=convert("6", decimal, hex);
d:=6	b:=6
> e:=G3[input](d);	> e:=G2[input](d);
e:=2 x mod 3	e:= (x^2 + x) mod 2
> f:=G3[`*`](e,c);	> f:=G2[`*`](e,c);
f:= (2x + 2) mod 3	f:= (x + 1) mod 2
> g:=G3[output](f);	> g:=G2[output](f);
g:= 8	g:= 3
> convert(g, hex);	> convert(g, hex);
8	3

The program is set golf binary and ternary Galois fields, elements of which are served in polynomial basis. For GF (2^3) primitive polynomial x3 + x + 1 for GF (3^2) - x2 + x + 2. By using the Primitive (G3) mod p, checked whether the primitive polynomial modulo p. Operand b and d are represented in decimal code, checked the correctness of multiplication. The table program in the field GF (2^3) multiplication is performed in decimal notation 5_{10} x 6_{10} result is 3_{10} (check: in binary code 5_{10} = 101_2, 6_{10} = 110_2, 3_{10} = 011_3 , that result in a binary field GF(2^3) 101_2 x 110_2 = 011_2), in the field GF(3^2) also performed in decimal notation GF(3^2) 5_{10} x 6_{10} result is 8_{10} check: in ternary code 5_{10} = 12_3, 6_{10} = 20_3, 8_{10} = 22_3 , that result in a ternary field GF(3^2) 12_3 x 20_3 = 22_3). Implementation of multiplications of elements of Galois fields in mathematical package Maple, to verify the correctness basic operation in binary and ternary fields at their hardware implementation on FPGA..

V. Modified cells Hild implementation on FPGA

Hild modified cells are planned to realized on FPGA combinational elements (LUT). Modern FPGA LUT Spartan6 with 6 inputs and one output. Hild number of cells to build a parallel multiplier is kq^2, for the field GF (2^m) each cell Hild has a 3-bit input and 1-bit output. Accordingly, the number of LUT $N_2 = km^2$. For the field GF (3^n) each cell Hild has a 6-bit input and 2-bit output. Accordingly, the number of LUT $N_3 = 2kn^2$.

Then the ratio of hardware expenses is:

$$s = N_2/N_3 = km^2/2kn^2 = m^2/2*(0{,}6m)^2 = 1{,}4 > 1.$$

That is, modern element base hardware cost of the parallel multiplier for Galois field elements ternary less than to implement it in a binary field [5].

Conclusion

Considered the construction of a parallel multiplier based on modified cells Hild. Proved its advantages over similar items multiplier binary Galois field GF (2^m). Showing schematic implementation Hild cell. The possibility of checking the correct execution of operations in binary and ternary Galois fields in mathematical package Maple.

References

[1] V. S. Hlukhov, R. M. Elias, A. O. Melnyk, “Osoblyvosti realizatsii na PLIS sektsiinykh pomnozhuvachiv elementiv poliv Halua GF(2m) z nadvelykym stepenem”, Kompiuterno-intehrovani tekhnolohii, Lutsk № 12., 103 – 106 st., 2013.

[2] Steininger A., Serra M., Reconfigurable Hardware Implementation of Polynomial Arithmetic over the Finite Field GF(3), Wien, December, 30, pp. 88, 2006.

[3] Merchan J. G. Arithmetic Architectures for Finite Fields GF(p^m) with Cryptographic Applications. Bochum, pp. 221, May, 2004.

[4] Deschamps J.P., Imana J.L, Gustavo D., Hardware Implementation of Finite-Field Arithmetic. 2009 The McGraw-Hill Companies, Inc.

[5] T. Berko, V. Hlukhov, “Perevirka prystroiv dlia obrobky tsyfrovykh pidpysiv, shcho gruntuiutsia na eliptychnykh kryvykh”, Naukovo-sotsialnyi zhurnal «Tekhnichni novyny», orhan Ukrainskoho inzhenernoho tovarystva u Lvovi, 1, 53-57 st., 26, 2007.

[6] Hlukhov V.S., Kostyk A.T., Vykorystannia suchasnykh PLIS dlia opratsiuvannia elementiv poliv Halua (pq). Tezy dlia 9-toi nauk. konf. KhUPS.,178 st., kviten 2013.