RADIX - 7 SIGNED DIGIT ELEMENT FINITE FIELD ARITHMETIC

Michael Naseimo Daikpor[1], Oluwole Adegbenro[2]
Department of Electrical and Electronic Engineering
University of Lagos, Akoka Lagos, Nigeria
[1]E-mail mndaikpor@yahoo.com
[2]wole_adegbenro@yahoo.com

ABSTRACT

In this contribution we present radix – 7 signed digit element finite fields as a gateway to multiple-value logic public key cryptographic systems design. We also construct signed digit Galois Field SGF(7^2). A radix – 7 signed digit element finite field multiplication circuit is implemented using complementary pass-gate derived 7-value. T-gate [1].

Index Terms— *Signed digit:, Element, finite fields, Arithmetic , Multiple-valued logic, diagonal element summation*

1. INTRODUCTION

In most real life applications negative numbers are essential and Signed Digit Number (SDN) system [2] lends itself to parallel system architecture and simplifying high-speed device design. Symmetrical signed digit sets have also been used to develop Multiple-Valued Logic (MVL) systems that fronts: better noise margin, reduced signal lines count, reduced complexity of interconnection, fewer control lines and high device speed

Recently advances in integrated circuit design have also continued to foster development of novel circuits in redundant number system resulting in high-speed conventional and finite field binary arithmetic circuits. Kameyame et al: suggested radices:- 2, 4, 5 SD arithmetic circuits from bi-directional current mode MVL basic building blocks for a wide range of applications (not including) finite field arithmetic circuits). This paper is an overview of radix – 7 signed digit number system in finite field arithmetic and present the design of signed digit element finite field multiplication circuit from yet another MVL systems building block - the complementary pass gate derived 7-valued T – gate. Our choice of radix- 7 is informed by the fact that: i) *Radix – 7* multiple value coded signed digit number system is essentially the symmetrical quaternary signed digit set $\{\bar{3}.\bar{2}.\bar{1}.0.1.2.3\}$. This would simplify conversion procedures if need be. ii) It is also applicable to a infinite set of cryptographic-friendly prime moduli that has 7 as primitive root p. iii) $P = 7$ is itself a finite field.

The rest of this paper is organized as follows: In section II we present the concept of radix – 7 Signed digit element Galois Fields SGF(7^m). Synthesis of signed digit element finite field multiplication MVL circuit is presented in section III. Conclusion is given in section IV.

2. SIGNED – DIGIT - ELEMENT FINITE FIELDS

The kernel to security in cryptographic systems is the intractability of very large integer factors participating in arithmetic operations but a major issue in their hardware implementation is the existence of an efficient Galois field arithmetic. In this section we proceed to show that radix – 7 signed digit arithmetic is also applicable in finite fields. That high-speed signed digit element finite field arithmetic circuits are realize able from 7-valued T-gate radix – 7 SD adders and multipliers circuits.

2.1 Basic properties

Basic properties of finite fields] shows that finite or Galois fields [6,7] are algebraic structures with finite prime number of elements in which the arithmetic operations: addition, subtraction multiplication and division are closed. Usually the field representation defines the element pattern and such representations are chosen to provide efficient field arithmetic operation. Arithmetic in radix – 7 signed digit number system [9] is also very efficient hence, taking the restricted symmetrical radix - 7 SD set {-3,-2.-1,0,1,2,3} as MVL variables recoded rearrangement of the elements of GF(7), basic arithmetic operations of a Signed digit element GF(7) which may be described as in equation (1),

$$\delta_i = \begin{Bmatrix} \bar{1} & ; if\ (\alpha_i \Theta \beta_i) & \bar{a} \\ 1 & ; if\ (\alpha_i \Theta \beta_i) & a \\ 0 & ; if\ otherwise & \end{Bmatrix} \quad \ldots\ldots (1)$$

$$\tau_i = (\alpha_i \Theta \beta_i) - 7\delta_i$$

where: the operator $\Theta \in \{+, -, \times, /\}$ and $a_i, b_i, \tau_i \in \{-3,-2,-1,0,1,2,3\}$ are also closed with additive and multiplicative elements of *0* and *1* respectively. Consequently, we advance the following theorems:

Theorem 1 If the set D = (0,1,2,3,....,p-1) in which p is a prime, form the prime field GF(p) such that addition; subtraction, multiplication and division operations are closed, then, the set D' = (-(p-1)/2, -(p-2)/2, ...,-1,0, 1,2,3,....(p-2),p-1)) also form the Signed digit element prime field (SGF(p)) in which radix - p SD addition; subtraction, multiplication and division operations are closed.

Theorem 2. If a finite field of characteristic p, for a non-negative integer of n, has p^n elements, for which a unique finite field of order p^n exist then a signed digit element finite field of characteristic p, for a non- negative integer

1-4244-1236-6/07/$25.00 © 2007 IEEE

n, has p^n signed digit elements for which a unique field of order p^n exist.

That is, if the field GF(p) exist then field SGF(p) exist and if field $GF(p^n)$ exist then SGF(p^n) exist. Also the elements of SGF(p) representable, either in polynomial or in normal basis form are MVL variables and thus can be stored as MVL strings. We illustrate further the existence of signed digit element Galois fields by constructing SGF(p^n).

2.2 Constructing signed digit element finite field SGF(7^m)

Definitions: Let x be a single independent restricted radix *r* SDN variable such that $x \in \{\overline{(a-1)}, \overline{(a-2)}, \ldots, \bar{2}, \bar{1}, 0, 1, 2, \ldots (a-2), (a-1)\}$ with $a \geq \left\lceil \frac{r-1}{2} \right\rceil$ and l_i - some coefficients in the restricted radix **r** signed digit number system field. Then we define:

i) A degree ***m*** signed digit polynomial Q(x) as:

$$Q(x) = \sum_{i=0}^{m-1} l_i x^i \text{ provided}$$

$x \in \{\overline{(a-1)}, \ldots, \bar{2}, \bar{1}, 0, 1, 2, \ldots, (a-1)\}$,

l_i – a restricted radix - **r** SDN system string

ii) A primitive SD Polynomial is the least SD Polynomial of primitive element α of the extension field SGF(p^m) and

$\alpha \in \{\overline{(a-1)}, \ldots, \bar{2}, \bar{1}, 0, 1, 2, \ldots, (a-1)\}$.

If ***a***. is an element of SGF(p^m) and α is a root in SGF(p^m) then any a_i can be represented as $\{\overline{\alpha^{p^2}} \ldots \overline{\alpha^2}.\overline{\alpha}.\bar{1}.0.1.\alpha.\alpha^2 \ldots \alpha^{p^2}\}$. Reducing these elements by a reduction modulo Polynomial enable us to represent elements of SGF (p^m) in Polynomial basis.

iii) A SD irreducible Polynomial of degree ***m*** is any non-constant SD Polynomial that cannot be factored.

Thus taking a *p(x)* as an irreducible (monic) signed digit polynomial [5] of degree ***m*** over $\mathbf{F}_7$ such that

$$p(x) = x^m + \sum_{i=1}^{m} a^{m-i} x^{m-i} : \; a_i \in \{\bar{3}.\bar{2}.\bar{1}.0.1.2.3\}$$

for i= 0,1,2,...,m-1) ..... (2)

Then we refer to the universal set of such polynomials *p(x)* of degree less than ***m*** over $\mathbf{F}_7$ as a signed digit element finite field $\mathbf{F}_7^m$, designated with SGF(7^m) and can be represented as

$SGF(7^m) = \{a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \ldots\ldots\ldots + a_2 x^2 + a_1 x^1 + a_0$

$a_i, x \in \{-3.\bar{3}.\bar{2}.\bar{1}.0.1.2.3\}\}$ .....(3).

Similar to positive element fields, the field elements of SGF(7^m) are denoted by symmetrical quaternary signed digit strings of length ***m*** so that SGF(7^m) can be alternatively represented as

$SGF(7^m) = \{(a_{m-1}a_{m-2}a_{m-3}\ldots\ldots a_1 a_0): \; a_i \in \{\bar{3}.\bar{2}.\bar{1}.0.1.2.3\}\}$ .....(4)

That is a SGF(7^m), m>0 contains 7^m elements each of which can be uniquely represented with a degree up to *m-1* signed digit polynomial *p(x)* in the form:

$p(x) = a_{m-1} x^{m-1} + a_{m-2} x^{m-2} + \ldots\ldots\ldots + a_2 x^2 + a_1 x^1 + a_0$ $a_i, x^i \in \{\bar{3}.\bar{2}.\bar{1}.0.1.2.3\}$

To construct a signed digit element finite field is to find monic irreducible signed digit polynomials $q(x) \in$ SGF(7^m) of degree $m \geq 1$ with coefficients in SGF(7^m). That is, we followed the brute force method out lined in [7]. List out all SD monic Polynomials of degree m in SGF(7^m)[x] with constant terms and for each one of the listed substitute $x \in \{\bar{3}.\bar{2}.\bar{1}.0.1.2.3\}$. The reducible Polynomials evaluates to zero, otherwise the Polynomial is irreducible. We found *21, 112 and 57580* radix 7 signed digit monic irreducible polynomials corresponding to *degrees 2, 3* and *7* and constructed the corresponding finite fields for degree 2 and 3.

3 SIGNED DIGIT ELEMENT FINITE FIELD MULTIPLICATION CIRCUIT

We now present the synthesis of a radix 7 SD element finite field multiplication circuit. To enhance device speed, we simultaneously generate and accumulate all partial products to formed an intermediate product and reduce this by some modulo. Hence the design of a radix 7 SD element finite field multiplication unit is essentially the implementation of parallel radix 7 SD addition and multiplier modules. Consequently, let a(t) and b(t) be two radix – 7 signed digit finite field elements in the polynomial basis representation and w(t) be some monic irreducible polynomial, such that

$a(t) = a_{k-1}t^{k-1} + a_{k-2}t^{k-2} + \ldots\ldots + a_1 t + a_0$

$b(t) = b_{r-1}t^{r-1} + b_{r-2}t^{r-2} + \ldots\ldots + b_1 t + b_0$

$w(t) = t^h + w_{h-1}t^{h-1} + w_{h-2}t^{h-2} + \ldots\ldots\ldots + w_1 t + w_0$

where : a(t), b(t) and w(t) $\in$ SGF(7^m)

3.1 Signed digit element finite field addition

$$a(t) + b(t) = c(t) = \sum_{i=0}^{n-1} c_i t^i \; . \quad \ldots(5)$$

where $c_i = a_i + b_i - 7\delta_i$ is implemented using 7-value T-gates as a radix-7 SD full adder and has a speed of 0.9μsec. Thus adding coefficient component-wise in

restricted radix 7 SDN system arithmetic without the carry, performs addition operation of two radix 7 signed digit finite field elements. A signed digit element finite field parallel addition circuit is simply a row of ***n*** radix 7 SD full adders with unutilized carry-ins and carry-outs.

3.2 Signed digit element finite field multiplication

A signed digit finite field elements multiplication operation involves the multiplication of polynomial basis represented multiplier *a(t)* and multiplicand *b(t)* in restricted radix – 7 signed digit number system component wise with ignored product digit carry ρ^{0}_{nm} and computing the residue modulo some given irreducible polynomial w(t). Thus in designing a signed digit field elements multiplication architecture we employed a `parallel multiply/add/subtract coefficient method . The multiplication of a(t) and b(t) is expressed as

$$a(t) * b(t) = a(t) . b(t) \bmod w(t)$$

$$[\sum_{i=0}^{k-1} a_i\, b(t)] \bmod w(t) \quad \ldots\ldots(6)$$

$$= (a_{k-1}t^{k-1}(b_1t^1 + b_{1-1}t^{r-1} + \ldots b_1t + b_0) + a_{k-2}t^{k-2}(b_1t^1 + b_{1-1}t^{r-1} + \ldots b_1t + b_0)$$

$$+ \ldots\ldots\ldots + a_1t(b_1t^1 + b_{1-1}t^{r-1} + \ldots b_1t + b_0) + a_0(b_1t^1 + b_{1-1}t^{r-1} + \ldots b_1t + b_0)) \bmod w(t) \ldots$$

$$= \{\sum_{n=0}^{k-1} a_n t^{k-n}(b_{r-1}t^{r-1} + b_{r-2}t^{r-2} + \ldots + b_1t + b_0) \bmod w(t)\} \bmod w(t) \quad \ldots(7)$$

let $d_i = a_{k-n}b_{r-m} - 7\rho^{0}_{h}$ then

$$a(t) * b(t) = \{\sum_{i=0}^{k\,r-1} d_i t^{i}\} \bmod w(t)\} \bmod w(t)$$

$$= \{\sum_{i=0}^{k\,r-1}(\sum_{n=0,m=0}^{n=k-1,m=r-1} a_{k-n}b_{r-m} - 7p^{0}_{nm}) \bmod w(t)\} \bmod w(t) \quad \ldots\ldots(8)$$

where $\rho^{0}_{nm} = \rho^{0}_{ij}$ is a product carry. The term $a_{k-n}.b_{r-m} - 7p^{0}_{nm}$ represents multiplication operation of two restricted radix – 7 SD. It is also hardware implemented (using 7-value T-gates) with a speed of 0.6 μsec . Equation (8) appears complicated but a second look at equation (6) shows that operation in bracket can be performed simply by writing the coefficients of the multiplicand b(t) in rows that terminate with a corresponding coefficients of the multipliers a(t) as in equation (9).

$$\left.\begin{array}{l|l} b_{r-1}\ b_{r-2}\ b_{r-3}\ldots\ b_1\ b_0 & a_{k-1} \\ b_{r-1}\ b_{r-2}\ b_{r-3}\ldots\ldots b_1\ b_0 & a_{k-2} \\ \ldots\ldots\ldots\ldots\ldots\ldots & \ldots \\ b_{r-1}\ b_{r-2}\ b_{r-3}\ldots\ldots b_1\ b_0 & a_1 \\ b_{r-1}\ b_{r-2}\ b_{r-3}\ldots\ldots b_1\ b_0 & a_0 \end{array}\right\} \quad (9)$$

Next multiplier-coefficient-column elements a_{k-z}, (z =1,2,…k) radix - 7 signed digit-wise multiply corresponding multiplicand-coefficient-row elements $\{b_{r-v}\}_z$, v = (r,(r-1),(r-2),…,2,1) to produce the partial product-coefficient matrix of equation (10). Intermediate

$$\left.\begin{array}{llll} a_{k-1}b_{r-1} & a_{k-1}b_{r-2} & \ldots a_{k-1}.b_1 & a_{k-1}b_0 \\ a_{k-2}b_{r-1} & a_{k-2}b_{r-2} & \ldots a_{k-2}b_1 & a_{k-2}b_0 \\ \ldots\ldots\ldots\ldots & & & \\ a_1b_{r-1} & a_1b_{r-2} & \ldots\ldots a_1.b_1 & a_1b_0 \\ a_0\ b_{r-1} & a_0b_{r-2} & \ldots\ldots a_0.b_1 & a_0b_0 \end{array}\right\} \quad (10)$$

- product coefficients $p_{k\ r-i}$, are obtained by carry-free radix 7-signed digit summation of the diagonal elements from the left. These are finally reduced modulo w(t) to obtain the product of *a(t) * b(t)* multiplication operation. The multiplier coefficient-column element positioning may start with the junior coefficient a_0 and end with the senior, a_{k-1}. In this case, the summation of diagonal elements starts from the right. However, in either case the same number of diagonal elements and the same diagonal elements adds up to form any particular intermediate-product coefficient $p_{k\ r-i}$, i.e:

$$p_{k\ r-i} = (\sum_{i=0}(a_{k-n}.b_{r-m} - 7p^{0}_{nm})) \quad \ldots\ldots(11)$$

where *n = 0,1,2….k-1 and m=0,1,2…r-1*

For the reduction operation; while some employ direct division by the reduction modulo w(t), others (since in field arithmetic, addition and subtraction operations are similar), suggested an add-shift interleaved subtraction [3,8] strategy . In our algorithm of parallel radix 7 signed digit multiplication of operand coefficients and simultaneous formation of intermediate- product coefficients by diagonal elements summation, the reduction phase is accomplished by repeatedly component-wise radix - 7 signed digit subtraction operation of the reduction modulo w(t), from the intermediate product coefficients since only a very small and negligible time is expended in the first phase. The subtraction starts with the highest power term of the independent variable *t*, of the intermediate product $IP(t)$ polynomial with gradual sliding of the reduction polynomial $w(t)$, to the right until $IP(t) < w(t)$. Using the radix 7 SD adders and multiplier units as basic building blocks we realize a radix 7 SD finite field multiplication circuit that performs the field multiplication operation a(t) * b(t) modulo w(t) where;

$a(t) = a_3t^3 + a_2t^2 + a_1t + a_0$,

$b(t) = b_3t^3 + b_2t^2 + b_1t + b_0$ and

$w(t) = t^5 + w_4t^4 + w_3t^3 + wt^2 + w_1t + w_0$

The circuit acquired a very high operational speed when multiplier-coefficient-column elements were simultaneously multiplied by corresponding multiplicand-coefficient-row elements with simultaneous accumulation of partial products to form the intermediate product coefficients. The 'slide and repeated subtraction' modulo reduction technique is carried out in a parallel radix – 7 SD field element addition circuit which is simply a $n = k + r$ number of radix –7 SD adders in a row with sum outputs feed back into the third input. The circuit speed T, may be estimated using the expression $T = t_{mr} + t_{SD}((k-1)+u))$; where u is the number of subtractions and t_{mr} = t_{SD} = radix – 7 SD full adder/ multiplier signal delay period. Thus taking a(t), b(t) and w(t) in their polynomial coefficient form of representation as: a = {2,-3 , -2, 2,–1, 3}, b = {-1,2,-3,3,2,1} and the monic irreducible polynomial as w = {1, -3,-3, 3,-1, 2, 1,-3} over SGF(7^8) in which SGF(7^2) is a sub field then, the following polynomial arithmetic operations were successfully carried out using the above outlined.

i) $a + b$ = {2,-3 , -2, 2,–1, 3} + {-1,2,-3,3,2,1} = {1,-1,2,-2,1,-3}

ii) $a - b$ = {2,-3 , -2, 2,–1, 3} - {-1,2,-3,3,2,1} = {3,2,1,-1,-3,-1}

iii) $a * b$= {2,-3 , -2, 2,–1, 3} * {-1,2,-3,3,2,1}/{1, -3,-3, 3,-1, 2, 1,-3)= {-3,2,2,2-3,2,3}

iv) {2,-3,0,2,-1,0,3)$^{-1}$ modulo {1, -3,-3, 3,-1, 2, 1,-3) = {1,-2,2,-1,2,1-2,-1}

3.4 Observations : SGF(p) when p is prime > 7

A. In our examination of radix –7 SDN system. the applicability of the primitive root $p = 7$ to certain prime modulo in the set: $q = 7^l \pm 6l$. $l \in$ {0.1.2.....n-1} and $n \in$ {2,3,4,...}. For example: 13.37.61.109.157.....373.....222993....81893. ....119953.....: generated very great interest. Field arithmetic in these fields requires the consideration of intra element carries. For example. $F_{61} = F12\bar{2}$ where the elements in radix – 7 SD coding are {0.1.2.3. $1\bar{3}.1\bar{2}.1\bar{1}.10.11.12.13.2\bar{3}.2\bar{2}.2\bar{1}.20.21.22.....12\bar{3}$ } the following arithmetic operations elicits the above peculiarity.

i) $23 + 22 = 23 + 22 \bmod 12\bar{2} = 1\bar{2}\,\bar{1}$

ii) $23 * 22 = 23 * 22 \bmod 12\bar{2} = 1\bar{3}0$

iii) $23^{-1} = 23^{-1} \bmod 12\bar{2} = 11$

B. For practical applications such as in the area of cryptography requiring input operands of very long word lengths, the method of folded operand multiplication [4] can be adopted

3. CONCLUSION

We have shown that extending radix 7 SD arithmetic to finite fields can bring about efficient signed digit Element finite fields arithmetic. We have used this concept to construct SGF (7^2) and proposed parallel-signed digit element finite field multiplication architecture. This contribution may find application in signed digit code theory as well as in the design of fast and more compact very high radix MVL cryptographic systems.

4. References

[1].Oluwole Adegbenro and Michael Naseimo Daikpor;"Design of 7-valued Complementary Pass gate derived T-gate". Proceedings of the International Engineering Conference, Faculty of Engineering, University of Lagos, May 2005, Vol. 1 pp 146 – 158. Lagos Nigeria.

[2]. Israel Koren " Digital Computer Arithmetic ECE 666 Part 2, Unconventional Number System" . University of Massachusetts, Dept of Electrical of Computer Engineering, MA. spring 2004 pp. 1 - 30, MA USA

[3]. Israel Koren; "Digital Computer Arithmetic ECE 666 part 6c, High-speed Multiplication III"; University of Massachsetts, Dept of Electrical & Computer engineering, Spring 2004.pp1-9, MA ; USA.

[4.] Daikpor; Michael Naseimo and Oluwole Adgbenro ;"A new approach to big integer multiplication using folded operand method". Proceedings of National Conference and Exhibition in Telecommunications and Broadcasting., University of Lagos August 2006, Vol. 1, pp 90 – 97. Lagos, Nigeria.

[5]." Irreducible Polynomial" Wikipedia, the free encyclopediia

[6] "Finite field Arithmetic"; Wikipedia, the free Encyclopedia.

[7]. "Introduction to finite fields;" Galois % 2002\galois % 2005 htm pp 1 – 9 . A Matache sum Oct. 20th ,1996 finite field Wikipedia, the free Encyclopedia.

[8]. Johann Grobschadl;" A low-power bit-serial multiplier for finite fields GF(2^m)".Proceedings of the 34th IEEE Symposium on circuits and systems (ISCAS 2001), vol. IV, pp. 37 – 40.