Efficient Multiplication Algorithms Over the Finite Fields $GF(q^m)$, Where $q = 3,5$

T. K. Truong, I. S. Hsu, and K. M. Cheung
Communications Systems Research Section

I. S. Reed
Department of Electrical Engineering
University of Southern California

Finite field multiplication is central to coding theory [1]. For this application, there is a need for a multiplication algorithm which can be realized easily on VLSI chips. In this article, a new algorithm is developed which is based on the Babylonian multiplication technique utilizing tables of squares. This new algorithm is applied to the finite fields $GF(q^m)$, where $q = 3$ and 5. It is also shown that this new multiplier can be used to compute complex multiplications defined on the direct sum of two identical copies of such Galois fields.

I. Introduction

Let $GF(q^m)$ be a finite field. Also, let α be a primitive element in $GF(q^m)$. Then, $N = \{\alpha^0, \alpha^1, \alpha^2 \cdots, \alpha^{m-1}\}$ is the standard basis set of the field $GF(q^m)$, and every fixed element $\alpha^j \in GF(q^m)$ can be uniquely expressed as $\alpha^j = b_0\alpha^0 + b_1\alpha^1 + \cdots + b_{m-1}\alpha^{m-1}$, where $b_j \in GF(q)$ for $0 \leqslant j \leqslant m - 1$ is an element in the ground field $GF(q)$. Thus, α^j can be represented as a coordinate vector of form $\alpha^j = [b_0, b_1 \cdots, b_{m-1}]$ in the standard basis.

The most straightforward method to perform a multiplication of two field elements in $GF(q^m)$ is the table lookup method. To illustrate this procedure, let $\beta = [b_0, b_1 \cdots, b_{m-1}]$ and $\gamma = [c_0, c_1, \cdots, c_{m-1}]$ be two elements of the field $GF(q^m)$ in a standard basis representation. Further, let a "log" table be used to find the exponents i and j of $\beta = \alpha^i$ and $\gamma = \alpha^j$. This is accomplished by using elements β and γ as addresses to locate the logarithms i and j of β and γ, respectively. After the addition $k = i + j \bmod (q^m - 1)$ of these exponents, an "antilog" table is used to find the coordinate vector representation for α^k in a standard basis. The element k serves as the address of the field element in the antilog table.

It is reported [2, page 71] that the Babylonians and Egyptians were the first to use tables of squares to efficiently realize a multiplication over the field of integers. In this article, it is shown that such an algorithm can be used to realize a multiplication over the finite fields, $GF(3^m)$ or $GF(5^m)$. The operations needed to realize this multiplier are only two squares and three additions of elements in $GF(q^m)$ where $q = 3$ and 5. The square of any element in the field can be obtained by the table lookup method. The advantage of this new multiplier is that it does not need the antilog procedure required in the conventional table lookup method. Also in this new method, the antilog procedure in the conventional method is replaced by three additions in $GF(q^m)$.

It is well known [3] that a conventional coding system depends crucially on the fast multiplier in the finite fields. $GF(q^m)$. Therefore, the fast multiplication over $GF(q^m)$ for $q = 3$ and 5 can be used for deep space communications in a concatenated coding system. In a coding system, the input sequence is a string of binary digits. In order to use multiplication over $GF(q^m)$ where $q = 3$ and 5, one first needs to convert an input binary sequence to a trinary or quinary sequence, and inversely to reconvert the output trinary or quinary sequence back to a binary sequence. Methods for realizing these radix conversions are given in [4, page 302].

It is shown next that the above new multiplier can be used to perform complex multiplications defined on both the extension field $GF(3^{2m})$ or on the direct sum of two copies of finite fields $GF(q^m)$, where $q = 3$, and 5. The complex multiplication defined on a direct sum can be performed by an efficient method as described in this article.

II. Mathematical Preliminary

Before developing the Babylonian multiplication algorithm over the field $GF(q^m)$, we consider some properties of finite fields that are helpful to the following development. First consider $GF(q^m)$ for $q \neq 2$. Also let $\gamma = \alpha^i \neq 0$ for $0 \leqslant i \leqslant q^m - 1$ be an element in $GF(q^m)$, where α is a primitive element in $GF(q^m)$.

Definition: If the polynomial $x^2 - \gamma = 0$ is solvable in $GF(q^m)$, then γ is called a quadratic residue in $GF(q^m)$; otherwise γ is known as a quadratic nonresidue in $GF(q^m)$.

For $\gamma \neq 0$, let

$$\left(\frac{\gamma}{q^m}\right) = \gamma^{\frac{q^m-1}{2}} \qquad (1)$$

It is seen in the next theorem that the symbol (γ/q^m) is a generalization of the Jacobi symbol to Galois fields [9]. First it is not difficult to see that $(\gamma^{(q^m-1)/2}) = \pm 1$. Thus, from (1), $(\gamma/q^m) = \pm 1$, where "1" is the unit element of $GF(q^m)$. A more specific result is provided in the following theorem:

Theorem 1: Let $q > 2$. If $(\gamma/q^m) = 1$, then γ is a quadratic residue in $GF(q^m)$. If $(\gamma/q^m) = -1$, then γ is a nonresidue in $GF(q^m)$.

Proof: See [5].

The following theorem is to be found in [5].

Theorem 2: Let $GF(q^m)$ be a finite field where $q > 2$. Then

$$\left(\frac{-1}{q^m}\right) = (-1)^{\frac{q^m-1}{2}} = \begin{cases} 1, \text{ for } q \equiv 1 \bmod 4 \\ 1, \text{ for } q \equiv 3 \bmod 4 \text{ and } m \equiv 0 \bmod 2 \\ 1, \text{ for } q \equiv 3 \bmod 4 \text{ and } m \equiv 1 \bmod 2 \end{cases} \qquad (2)$$

Proof: See Appendix.

The following theorem is well known and a proof can be found in [5].

Theorem 3: Let $GF(q^m)$ be a finite field, where $q^m - 1 = q_1^{e_1} q_2^{e_2} \cdots q_r^{e_r}$, $(q_i, q_j) = 1$, for $i \neq j$. Then α is a primitive element in $GF(q^m)$ if and only if $\alpha^{(q^m-1)/q_i} \not\equiv 1 \bmod q$ for $1 \leqslant i \leqslant r$.

III. Multiplication Over $GF(q^m)$ where $q = 3$ and 5

In this section, a fast method is developed to perform a multiplication on $GF(q^m)$ where $q = 3$ and 5 which uses tables of square roots. This new technique, called the Babylonian multiplication algorithm over the field $GF(q^m)$ for two elements β and γ is obtained as follows:

$$\delta = \beta\gamma = \sum_{i=0}^{m-1} d_i \alpha^{q^i} \equiv \frac{(\beta+\gamma)^2 + (\beta-\gamma)^2}{4} \bmod q \qquad (3)$$

For $q = 3$, (3) becomes

$$\delta \equiv [(\beta+\gamma)^2 + (\beta-\gamma)^2] \bmod 3 \qquad (4a)$$

For $q = 5$, (3) becomes

$$\delta \equiv - [(\beta+\gamma)^2 + (\beta-\gamma)^2] \bmod 5 \qquad (4b)$$

It is easy to see that the operations needed to compute (4a) or (4b) require only two squares and three additions of elements in the field. The square of any element needed in (4a) and (4b) is found by the table lookup method.

IV. Complex Multiplication Over the Finite Field $GF(3^{2m})$, where m is odd

Consider $q = 3$ and m is odd, i.e., $m = 2n + 1$. By Theorem 2, the negative unit element -1 is a quadratic nonresidue in $GF(3^m)$, where $m = 2n + 1$. Thus, the polynomial $p(x) = x^2 + 1$ is irreducible in $GF(3^m)$ for $m \equiv 1 \bmod 2$. Hence a root, say i, of the quadratic polynomial equation,

$$p(x) = x^2 + 1 = 0 \tag{5}$$

exists and can be found in the extension field $GF(3^{2m})$. $GF(3^{2m})$ is composed of the set $GF(3^{2m}) = \{a + ib \mid a, b \in GF(3^m)\}$where i is a root of (5), satisfying

$$i^2 \equiv -1 \bmod 3 \tag{6}$$

By the above, in order that $x^2 + 1 = 0$ not be solvable in $GF(3^m)$, it is necessary that $m = 2n + 1$. Thus, in $GF(3^{2m})$, the "imaginary" element i in (5) plays a similar role over the finite field $GF(3^m)$ that $\sqrt{-1} = i$ plays over the field of rational numbers. For example, suppose $a + ib$ and $c + id$ are elements of $GF((3^m)^2)$ where $m \equiv 1 \bmod 2$. Then, by (5),

$$(a + ib) + (c + id) = (a + c) + i(b + d) \tag{7}$$

and

$$(a + ib)(c + id) = (ac - bd) + i(bc + ad) \tag{8}$$

These are the exact analogies of what one might expect if $a + ib$ and $c + id$ were complex numbers. The operations needed to compute (8) require only four multiplications and two additions in $GF(3^m)$.

V. Complex Multiplication Defined Over the Direct Sum of Two Copies of *GF*(q^m)

Let $GF(q^m)$ be a finite field. Further, let (-1) denote the negative of the real integer one and let i be the solution of equation $x^2 = -1$. Finally, define the set $Z_{q^m}[i] = \{a + ib \mid a, b \in GF(q^m)\}$ of q^{2m} elements in such a manner that addition is given by $(a + ib) + (c + id) = (a + c) + i(c + d)$ and multiplication is given by $(a + ib)(c + id) = (ac - bd) + i(bc + ad)$, where $ac - bd$ and $bc + ad$ are elements in $GF(q^m)$.

Theorem 4. If -1 is a quadratic residue in $GF(q^m)$, then the set $Z_{q^m}[i]$ is a commutative ring and is not a field.

Proof: It is not difficult to show that any arbitrary elements such as u, v, and w of $Z_{q^m}[i]$ satisfy the six postulates of a ring [6, page 1]. Thus $Z_{q^m}[i]$ is a commutative ring.

To prove that $Z_{q^m}[i]$ is not a finite field, it is necessary to show that its nonzero elements do not form a group under multiplication [7, page 126]. To show this, assume there exists an inverse element w^{-1} of an arbitrary element $w = \alpha + i\beta \in Z_{q^m}[i]$ such that $ww^{-1} = 1$. Then,

$$w^{-1} = \frac{1}{\alpha + i\beta} = \frac{\alpha - i\beta}{\alpha^2\left(1 + \left(\frac{\beta}{\alpha}\right)^2\right)} \tag{9}$$

Since -1 is a quadratic residue in $GF(q^m)$, there exist two solutions $\pm s$ of $x^2 + 1 = 0$ in $GF(q^m)$. Let $w = \alpha + i\beta$ have the property that $s = \beta/\alpha$. Then the denominator of Eq. (9) is equal to zero. This implies that no inverse w^{-1} of w exists in $Z_{q^m}[i]$. Thus, $Z_{q^m}[i]$ is not a field.

Now suppose that $\pm x$ are the solutions of $x^2 + 1 = 0$ in $GF(q^m)$. If $a + ib \in Z_{q^m}[i]$, then let ϕ be the mapping

$$\phi: a + ib \to ((a + sb), (a - sb)) = (\gamma, \bar{\gamma}) \tag{10}$$

where $\gamma = (a + sb)$, $\bar{\gamma} = (a - sb)$ and $\gamma, \bar{\gamma} \in GF(q^m)$. With the same procedure that was used in the proof of Theorem 1 in [8], it can be shown that the mapping in (10) is an isomorphic mapping. Also, it can be demonstrated that the set $S_{q^m} = \{(\alpha, \bar{\alpha}) \in GF(q^m)\}$is the direct sum of two copies of $GF(q^m)$, and that S_{q^m} is isomorphic to the ring $Z_{q^m}[i]$.

The inverse mapping ϕ^{-1} which maps $(\alpha, \bar{\alpha}) \in S_{q^m}$ into $Z_{q^m}[i]$ is defined by

$$\phi^{-1}: (\gamma, \bar{\gamma}) \to a + ib \tag{11}$$

To find a and b in (11), note that (10) implies

$$a + sb \equiv \gamma \bmod q \tag{12a}$$

$$a - sb \equiv \bar{\gamma} \bmod q \tag{12b}$$

Summing (12a) and (12b) yields

$$2a \equiv (\gamma + \bar{\gamma}) \bmod q \tag{12c}$$

Subtracting (12b) from (12a) yields

$$2sb \equiv (\gamma - \bar{\gamma}) \bmod q \tag{12d}$$

Since the quantities 2 and $2s$ are two nonzero elements in $GF(q^m)$, the inverse elements of these two elements exist in $GF(q^m)$. Thus,

$$a \equiv 2^{-1}(\gamma + \bar{\gamma}) \bmod q \tag{13a}$$

and

$$b \equiv (2s)^{-1}(\gamma - \bar{\gamma}) \bmod q \tag{13b}$$

Consider in the next section complex multiplications over the special finite rings $Z_{q^m}[i]$, where $q = 3$ and 5.

A. Complex Multiplication Over the Ring Z_{3^m} [i] Where m is Even

Consider the finite field $GF(3^m)$ where m is even, i.e., $m = 2n$. By Theorem 2, one obtains $(-1/3^m) = 1$. Thus, -1 is a quadratic residue in $GF(3^m)$. Hence elements $\pm s$ exist in $GF(3^m)$ which are solutions of $p(x) = x^2 + 1 = 0$. To find these roots, note from (1) that

$$\left(\frac{-1}{3}\right) = (-1)^{\frac{(3-1)}{2}} = -1$$

Thus, -1 is a quadratic nonresidue modulo 3, and $x^2 + 1 = 0$ is not solvable in the ground field $GF(3)$. A root, say s, of the quadratic polynomial equation, $p(x) = x^2 + 1 = 0$ exists and can be found in the extension field $GF(3^m)$. To show this, let α be a primitive element in $GF(3^m)$, where $m \equiv 0 \bmod 2$. Then

$$\alpha^{3^m-1} \equiv 1 \bmod 3 \tag{14}$$

Since $4 \mid 3^m - 1$ for $m \equiv 0 \bmod 2$, Eq. (14) becomes

$$\alpha^{\frac{3^m-1}{2}} = \left(\pm\alpha^{\frac{3^m-1}{4}}\right)^2 \equiv -1 \bmod 3 \tag{15}$$

or $s^2 + 1 = 0 \bmod 3$ where $s = \pm\alpha^{(3^m-1)/4} \epsilon\, GF(3^m)$. Evidently, $(s, -s)$ are the roots of the polynomial $p(x) = x^2 + 1 = 0$ over the Galois field $GF(3^m)$ where $m \equiv 0 \bmod 2$.

Let $s = \pm\alpha^{(3^m-1)/4}$. Also let the set $Z_{3^m}[i] = \{a + ib \mid a, b \;\epsilon\; GF(3^m)\}$ be a ring of 3^{2m} elements where $i^2 = -1$. Assume the mapping and its inverse mapping are defined by

$$\phi: (a + ib) \rightarrow ((\alpha + sb), (\alpha - sb)) \tag{16a}$$

and

$$\phi^{-1}: (\gamma, \bar{\gamma}) \rightarrow (\alpha + ib) \tag{16b}$$

where a and b are computed by

$$\alpha \equiv 2^{-1}(\gamma + \bar{\gamma}) \equiv 2(\gamma + \bar{\gamma}) \bmod 3 \tag{17a}$$

$$b \equiv (2s)^{-1}(\gamma - \bar{\gamma}) \bmod 3 \tag{17b}$$

Then, by Theorem 1 in [8] the ring $Z_{3^m}[i]$ is isomorphic to the direct sum of two copies of $GF(3^m)$ which is defined by

$$S_{3^m} = \{(\gamma, \bar{\gamma}) \mid \gamma, \bar{\gamma} \;\epsilon\; GF(3^m)\} \tag{18}$$

where $(\gamma, \bar{\gamma}) + (\beta, \bar{\beta}) = (\gamma + \beta, \bar{\gamma} + \bar{\beta})$ and $(\gamma, \bar{\gamma})(\beta, \bar{\beta}) = (\gamma\beta, \bar{\gamma}\bar{\beta})$.

From (16) and (17), the arithmetic needed to compute the mapping ϕ and its inverse ϕ^{-1} require three multiplications, one multiplication by 2 and four additions in $GF(3^m)$. The operations needed to perform a complex multiplication in S_{3^m} in (18) require only two multiplications in $GF(3^m)$.

Example 1: Let $GF(3^2)$ be a finite field and α be a primitive element in $GF(3^2)$. Also let $A = \alpha^3 + i\alpha$ and $B = \alpha^4 + i\alpha^5$, where $\alpha^3, \alpha, \alpha^4, \alpha^8 \;\epsilon\; GF(3^2)$. Calculate the product of A and B by using a complex multiplication over the direct sum of two copies of $GF(3^2)$.

Since $b(x) = x^2 + x + 2$ is a primitive irreducible polynomial over $GF(3)$, then the nonzero elements of $GF(3^2)$ are as follows: α, $\alpha^2 = -\alpha - 2$, $\alpha^3 = -\alpha + 2$, $\alpha^4 = 2$, $\alpha^5 = 2\alpha$, $\alpha^6 = -2\alpha - 1$, $\alpha^7 = \alpha + 1$, and $\alpha^8 = 1$. From (15), $s = \pm\alpha^{(3^2-1)/4} = \pm\alpha^2$ are the solutions of $p(x) = x^2 + 1 = 0$, where $\pm\alpha^2 \;\epsilon\; GF(3^2)$. From (16a) and (16b), one obtains

$$A = \alpha^3 + i\alpha \rightarrow (\alpha^3 + \alpha^2\alpha, \alpha^3 - \alpha^2\alpha) = (\alpha^7, 0)$$

and

$$B = \alpha^4 + i\alpha^5 \rightarrow (\alpha^4 + \alpha^2\alpha^5, \alpha^4 - \alpha^2\alpha^5) = (\alpha, \alpha^2)$$

The multiplication over $Z_{3^m}[i]$ is $(\alpha^7, 0)(\alpha, \alpha^2) = (1,0)$. From (17a) and (17b), one obtains $a \equiv 2(1 + 0) \bmod 3 = \alpha^4$ and $b \equiv (2\alpha^2)^{-1}(1 - 0) \bmod 3 = \alpha^2$. Hence $AB = a + ib = \alpha^4 + i\alpha^2$. This result can be verified readily by a direct computation.

B. Complex Multiplication Over the Ring Z_{5^m}[i]

Consider the finite field $GF(5^m)$. By Theorem 2, one obtains $(-1/5^m) = 1$. Thus, -1 is a quadratic residue in $GF(5^m)$. Hence elements $\pm s$ exist as the roots of $p(x) = x^2 + 1 = 0$ in $GF(5^m)$. To find the roots, it is not difficult to show that -1 is a quadratic residue modulo 5 and $x^2 + 1 = 0$ is solvable in the ground field $GF(5)$. Since $(\pm 2)^2 + 1 \equiv 0 \bmod 5$, then elements $s = \pm 2$ exist as the roots of $p(x) = x^2 + 1 = 0$ in $GF(5)$.

Let the set $Z_{5^m}[i] = \{a + ib \mid a, b \;\epsilon\; GF(5^m)\}$ be a ring of 5^{2m} elements, where $i^2 = -1$. Also let $s = \pm 2$. Assume the mapping and its inverse mapping are defined by

$$\Phi: (\alpha + ib) \rightarrow ((a + 2b), (a - 2b)) = (\beta, \bar{\beta}) \tag{19a}$$

$$\Phi^{-1}: (\beta, \bar{\beta}) \rightarrow (a + ib) \tag{19b}$$

where a and b are computed by

$$a \equiv 2^{-1}(\gamma - \bar{\gamma}) \equiv -2(\gamma + \bar{\gamma}) \bmod 5 \qquad (20a)$$

and

$$b \equiv 2^{2}(\gamma - \bar{\gamma}) \bmod 5 \qquad (20b)$$

Then the ring $Z_{5^m}[i]$ is isomorphic to the direct sum of two copies of $GF(5^m)$ which is defined by

$$S_{5^m} = \{(\gamma, \bar{\gamma}) \mid \gamma, \bar{\gamma} \in GF(5^m)\} \qquad (21)$$

where $(\gamma, \bar{\gamma}) + (\beta, \bar{\beta}) = (\gamma + \beta, \bar{\gamma} + \bar{\beta})$ and $(\gamma, \bar{\gamma})\,(\beta, \bar{\beta}) = (\gamma\beta, \bar{\gamma}\bar{\beta})$.

By (19) and (20), the arithmetic needed to compute the mapping Φ and its inverse Φ^{-1} requires three multiplications by powers of two and four additions in $GF(5^m)$. By (21), the arithmetic needed to compute a complex multiplication over S_{5^m} requires only two multiplications in $GF(5^m)$.

Example 2: Let $GF(5^2)$ be a finite field and α be a primitive element in $GF(5^2)$. Also let $A = (\alpha^{12} + i\alpha)$ and $B = (\alpha^{10} + i\alpha^2)$, where α^{12}, α, α^{10}, and $\alpha^2 \in GF(5^2)$. Calculate the product of A and B by using a complex multiplication over the direct sum of two copies of $GF(5^2)$.

Since $b(x) = x^2 + 2x + 3$ is a primitive irreducible polynomial over $GF(5)$, then the nonzero elements of $GF(5^2)$ are as follows: α, $\alpha^2 = -2\alpha + 2$, $\alpha^3 = \alpha + 1$, $\alpha^4 = -\alpha + 2$, $\alpha^5 = -\alpha - 2$, $\alpha^6 = -2$, $\alpha^7 = -2\alpha$, $\alpha^8 = -\alpha + 1$, $\alpha^9 = 3\alpha - 2$, $\alpha^{10} = 2\alpha + 1$, $\alpha^{11} = 2\alpha - 1$, $\alpha^{12} = -1$, $\alpha^{13} = -\alpha$, $\alpha^{14} = 2\alpha - 2$, $\alpha^{15} = -\alpha - 1$, $\alpha^{16} = \alpha - 2$, $\alpha^{17} = \alpha + 2$, $\alpha^{18} = 2$, $\alpha^{19} = 2\alpha$, $\alpha^{20} = \alpha - 1$, $\alpha^{21} = -3\alpha + 2$, $\alpha^{22} = -2\alpha - 1$, $\alpha^{23} = -2\alpha + 1$, and $\alpha^{24} = 1$.

In $GF(5^2)$, $s = \pm 2$ are the solutions of $x^2 + 1 = 0$. From (19a), one obtains

$$A = (\alpha^{12} + i\alpha) \rightarrow (\alpha^{12} + 2\alpha, \alpha^{12} - 2\alpha) = (\alpha^{11}, \alpha^{22})$$

and

$$B = (\alpha^{10} + i\alpha^2) \rightarrow (\alpha^{10} + 2\alpha^2, \alpha^{10} - 2\alpha^2) = (\alpha^7, \alpha^{17})$$

The multiplication over $Z_{5^2}[i]$ is

$$(\alpha^{11}, \alpha^{22})(\alpha^7, \alpha^{17}) = (\alpha^{18}, \alpha^{15})$$

From (20a) and (20b), one obtains

$$a \equiv -2(\alpha^{18} + \alpha^{15}) \bmod 5 = \alpha^{14}$$

and

$$b \equiv 2^2(\alpha^{18} - \alpha^{15}) \bmod 5 = \alpha^4$$

Hence $AB = a + ib = \alpha^{14} + i\alpha^4$. This result can be verified readily by a direct computation.

VI. Implementation of Complex Multiplications

Let $GF(q^m)$ be a finite field. $GF(q^m)$ can be generated by any irreducible polynomial of degree m over $GF(q)$ [3]. However, for mathematical convenience it is more desirable to generate $GF(q^m)$ using a primitive irreducible polynomial.

An algorithm to find a primitive irreducible polynomial of degree m over $GF(q)$ is given as follows:

(1) Construct an irreducible polynomial $g(x)$ of degree m over $GF(q)$ via the method proposed in [3]. The existence of such a polynomial is guaranteed, and there are

$$\frac{1}{m} \sum_{i=d, d \mid m} \mu(d) q^{\frac{m}{d}}$$

such polynomials, where $\mu(d)$ is the Moebius function.

(2) Generate the field $GF(q^m)$ using $g(x)$.

(3) Find a primitive element β in $GF(q^m)$ using Theorem 3.

(4) Construct a primitive irreducible polynomial $b(x)$ via the following formula:

$$b(x) = (x - \beta)(x - \beta^q) \cdots (x - \beta^{q^{m-1}})$$

The primitive irreducible polynomial $b(x)$ so obtained can be used to generate the field $GF(q^m)$.

Let the set $Z_{q^m}[i] = \{a + ib \mid a, b \in GF(q^m)\}$ be a set of q^{2m} elements where $i^2 = -1$. It is shown in the above sections that if $(-1/q^m) = -1$, $Z_{q^m}[i]$ is a field. Also if $(-1/q^m) = +1$, $Z_{q^m}[i]$ is a ring. Let $\gamma = a + ib$ and $\beta = c + id$ be two elements in $Z_{q^m}[i]$. Let $\delta = x + iy$ denote the product of γ and β. A complex multiplication of γ and β is defined to be $\delta = \gamma\beta = (a + ib)\,(c + id) = x + iy$ where $x = ac - bd$ and $y = ad + bc$.

It was shown in the above sections that complex multiplications over the ring $Z_{q^m}[i]$ can be more efficiently done in the transform domain $S_{q^m} = \{(\gamma, \bar{\gamma}) \mid \gamma, \bar{\gamma} \in GF(q^m)\}$. The flowchart of an algorithm for the multiplication over the ring

$Z_{q^m}[i]$ is given in Fig. 1. This algorithm has been verified by a software simulation.

VII. Conclusion

In this article, the Babylonian multiplication algorithm using tables of squares is applied to special finite fields and complex rings. The above new multiplication algorithm has been verified both by examples and simulation programs. The computationally architectural designs for the Babylonian multiplication over the finite field or ring are both simple and regular and suitable for a VLSI realization. Finally, this new multiplication algorithm can be applied to the development of coding systems based on the fields $GF(3^{2m})$ and $GF(5^{2m})$.

References

[1] R. Lidl and H. Neiderreiter, *Finite Fields*, Reading, MA: Addison-Wesley, 1983.

[2] D. Smeltzer, *Man and Numbers*. New York: Collier Books, 1962.

[3] E. R. Berlekamp, *Algebraic Coding Theory*, New York: McGraw-Hill Book Company, 1968.

[4] D. E. Knuth, *The Art of Computer Programming*, vol. 2, Reading, MA: Addison-Wesley, 1976.

[5] J. P. Wang, *Golomb's Conjecture in Finite Fields*, Master thesis. Department of Mathematics, Beijing University, China, 1984.

[6] N. H. McCoy, *Rings and Ideals*, Wisconsin: George Banta Company, Inc., 1984.

[7] I. N. Herstein, *Topics in Algebra*, Massachusetts: Xerox College Publishing, 1975.

[8] T. K. Truong, J. J. Chang, I. S. Hsu, D. Y. Pei, and I. S. Reed, "Techniques for Computing the Discrete Fourier Transform Using the Quadratic Residue Fermat Number Systems," *IEEE Trans. on Computers*, vol. C-35, no. 11, pp. 1008–1012, November 1986.

[9] L. K. Hua, *Introduction to Number Theory*, Berlin, Heidelberg, and New York: Springer-Verlag, 1982.

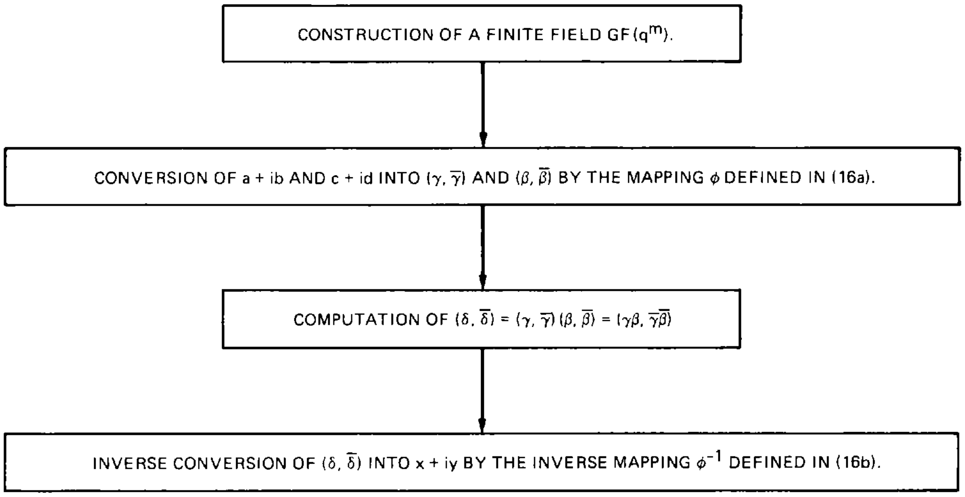
CONSTRUCTION OF A FINITE FIELD GF(q^m).
CONVERSION OF $a + ib$ AND $c + id$ INTO $(\gamma, \overline{\gamma})$ AND $(\beta, \overline{\beta})$ BY THE MAPPING ϕ DEFINED IN (16a).
COMPUTATION OF $(\delta, \overline{\delta}) = (\gamma, \overline{\gamma})(\beta, \overline{\beta}) = (\gamma\beta, \overline{\gamma\beta})$
INVERSE CONVERSION OF $(\delta, \overline{\delta})$ INTO $x + iy$ BY THE INVERSE MAPPING ϕ^{-1} DEFINED IN (16b).

Fig. 1. A flowchart of implementing a complex multiplication over the ring $Z_{q^m}[i]$

Appendix
Proof of Theorem 2

First, one has

$$\frac{q^m - 1}{2} = \frac{(q - 1)}{2}\,(q^{m-1} + q^{m-2} + \cdots + q + 1)$$

$$\equiv \begin{cases} 0 \bmod 2 \text{ for } q \equiv 1 \bmod 4 \\ q^{m-1} + q^{m-2} + \cdots + q + 1 \bmod 2 \\ \text{for } q \equiv 3 \bmod 4 \end{cases} \qquad \text{(A-1)}$$

Thus, if $q \equiv 1 \bmod 4$, then (2) becomes

$$\left(\frac{-1}{q^m}\right) \equiv (-1)^{0 \bmod 2} = 1$$

If $q \equiv 3 \bmod 4$, then $q + 1 \equiv 0 \bmod 4$. Then (2) becomes

$$\frac{q^m - 1}{2} = q^{m-2}(q + 1) + \cdots + (q + 1) \bmod 2,$$

$$\text{for } m \equiv 0 \bmod 2$$

and

$$\frac{q^m - 1}{2} = q^{m-2}(q + 1) + \cdots + q(q + 1) + 1 \bmod 2,$$

$$\text{for } m \equiv 1 \bmod 2$$

From (3), one has

$$\left(\frac{-1}{q^m}\right) = (-1)^{\frac{q^m - 1}{2}} = \begin{cases} 1 \text{ for } q \equiv 3 \bmod 4 \text{ and } m \equiv 0 \bmod 2 \\ -1 \text{ for } q \equiv 3 \bmod 4 \text{ and } m \equiv 1 \bmod 2 \end{cases}$$