Highly Regular Architectures for Finite Field Computation Using Redundant Basis

Huapeng Wu[1], M. Anwarul Hasan[2], and Ian F. Blake[3]

[1] Dept of ECE, IIT, Chicago IL 60616
hpwu@ece.iit.edu
This work was done when he worked for his Ph.D degree with the Dept of ECE, University of Waterloo.
[2] Dept of ECE, Univ. of Waterloo, Waterloo, ON N2L 3G1 Canada
ahasan@ece.uwaterloo.ca
Currently, he is with the Motorola Lab on a sabbatical leave from the University of Waterloo.
[3] HP Lab., Mail Stop 3U-4, 1501 Page Mill Road, Palo Alto, CA 94304
ifblake@hpl.hp.com

Abstract. In this article, an extremely simple and highly regular architecture for finite field multiplier using redundant basis is presented, where redundant basis is a new basis taking advantage of the elegant multiplicative structure of the set of primitive n^{th} roots of unity over $\mathbb{F}_2$ that forms a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. The architecture has an important feature of implementation complexity trade-off which enables the multiplier to be implemented in a partial parallel fashion. The squaring operation using the redundant basis is simply a permutation of the coefficients. We also show that with redundant basis the inversion problem is equivalent to solving a set of linear equations with a circulant matrix. The basis appear to be suitable for hardware implementation of elliptic curve cryptosystems.

1 Introduction

Efficient computations in finite field and their architectures are very important to many cryptosystems, *e.g.*, elliptic curve systems. There are mainly three types of bases over finite fields, namely, polynomial basis (PB), normal basis (NB), and dual basis (DB)[12], which are commonly used to represent the field elements. The main advantage of using the normal basis is that the squaring operation in NB is simply a cyclic shift of the coordinates of the element, and thus this basis has found application in computing exponentiations and multiplicative inverses [10,8,1]. However, the computations of exponentiations and inverses require not only squaring but also multiplications. Massey and Omura devised an NB multiplier known as Massey-Omura multiplier [13]. Alternative bit-serial multiplications using the normal basis can be found in [5,2]. The bit-parallel NB multipliers were proposed in [17,9]. PB and DB have been also used for implementing bit-parallel multiplier [14,8,16,6,11,19].

Ç.K. Koç and C. Paar (Eds.): CHES'99, LNCS 1717, pp. 269–279, 1999.

In this article a new basis – redundant basis (RB), is proposed. The redundant basis takes advantage of the elegant multiplicative structure of the set of primitive n^{th} roots of unity over $\mathbb{F}_2$ that forms a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. It is shown that finite field arithmetic operations using the redundant basis have extremely simple and highly regular structures.

Some similar work to ours using polynomial ring basis was proposed recetly [4]. We believe that the polynomial ring basis is a subset of the redundant basis proposed here.

The organization of this paper is as follows: Redundant basis is introduced in Section 2. In Section 3, multiplication operation using RB is discussed and then architectures of bit-serial and bit-parallel multipliers are proposed. Relation between RB and other types of bases is analyzed in Section 4. Squaring and inverse operation using RB are discussed in Section 5 and Section 6, respectively. Finally, a few examples are given in Section 7.

2 Redundant Basis

Definition 1. [12] *Let K be a field of characteristic p and n be a positive integer. The splitting field of $x^n - 1$ over a field K is called the* n^{th} cyclotomic field *over K and denoted by $K^{(n)}$. The roots of $x^n - 1$ in $K^{(n)}$ are called the* n^{th} roots of unity *over K and the set of all these roots is denoted by $E^{(n)}$. Then a generator of the cyclic group $E^{(n)}$ is called a* primitive n^{th} root of unity over K if n is not divisible by p.

Redundant basis uses the set of primitive n^{th} roots of unity over $\mathbb{F}_2$ that forms a basis of $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. Let β be a primitive n^{th} root of unity in $\mathbb{F}_{2^m}$ or some extension field of $\mathbb{F}_{2^m}$, then we have

$$\beta \cdot \beta^i = \begin{cases} \beta^{i+1} & i \neq n-1, \\ 1 = \sum_{j=1}^{n-1} \beta^j & i = n-1. \end{cases}$$

By adding the element '1' to the set of primitive n^{th} roots of unity, we have[1] $\langle 1, \beta, \beta^2, \ldots, \beta^{n-1} \rangle \triangleq I_1$, which can be used as a basis in $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ and it is referred to as a redundant basis. Note that the base elements are in the cyclotomic field $\mathbb{F}_2{}^{(n)}$ and they may not belong to the field $\mathbb{F}_{2^m}$. Clearly, any field $\mathbb{F}_{2^m}$ has a redundant basis if there is a cyclotomic field over $\mathbb{F}_2$ that contains $\mathbb{F}_{2^m}$ as a subfield. Thus one redundant basis can be the set of $(2^m - 1)$st roots of unity. To efficiently represent the field elements, the redundant basis should be chosen such that its size is as small as possible. Now the question is: Given $\mathbb{F}_{2^m}$, what is the smallest cyclotomic field $\mathbb{F}_2{}^{(n)}$ that contains $\mathbb{F}_{2^m}$ as a subfield? An algorithm for computing such an n is given below.

Algorithm 1 Computing the smallest cyclotomic field $\mathbb{F}_2{}^{(n)}$ that includes $\mathbb{F}_{2^m}$ as a subfield

[1] We denote a set by $\{\cdots\}$ and an orderly set by $\langle\cdots\rangle$.

1. Find all the factors d_i of $2^m - 1$ that are greater than m and list them in an increasing order: $d_1, d_2, \ldots, d_k = 2^m - 1$;
2. DO WHILE($i \leqslant k$)
   IF $m \mid \phi(d_i)$ AND $j = m$ is the smallest integer such that $2^j = 1 \bmod d_i$, THEN $t \leftarrow d_i$, and BREAK; ELSE $i \leftarrow i + 1$.
3. Let $n \leftarrow t$ and let h be the largest positive integer such that $t > hm$.
   IF $h > 1$ THEN
   FOR $i = 2$ TO h DO
   a) Find all the factors d_i of $2^{im} - 1$ that are greater than im and list them in an increasing order: $d_1, d_2, \ldots, d_{k_i} = 2^{im} - 1$;
   b) DO WHILE($i \leqslant k_i$)
   IF $im \mid \phi(d_i)$ AND $j = im$ is the smallest integer such that $2^j = 1 \bmod d_i$, THEN $n \leftarrow \min\{n, d_i\}$, and BREAK; ELSE $i \leftarrow i + 1$.

□

Since the $(2^m - 1)^{\text{st}}$ cyclotomic field has a degree of $\phi(2^m - 1)$ and contains the field $\mathbb{F}_{2^m}$ as a subfield, we have that m divides $\phi(2^m - 1)$, where ϕ is the Euler Phi function.

3 Redundant Basis Multiplier

3.1 Multiplication Operation

Consider the redundant basis in $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$: $I_1 = \langle 1, \beta, \beta^2, \ldots, \beta^{n-1} \rangle$. Let field element $A \in \mathbb{F}_{2^m}$ and be represented with I_1:

$$A = a_0 + a_1\beta + a_2\beta^2 \cdots + a_{n-1}\beta^{n-1}, \tag{1}$$

where $a_i \in \mathbb{F}_2, i = 0, 1, \ldots, n-1$. Note that $n \geq m+1$ and the set of coefficients $\{a_i\}$ is not unique.

Now let us look at multiplication operation under the redundant basis I_1. Let $B \in \mathbb{F}_{2^m}$ be given as $B = b_0 + b_1\beta + b_2\beta^2 + \cdots + b_{n-1}\beta^{n-1}$. Then we have

$$\begin{aligned} \beta \cdot B &= b_0\beta + b_1\beta^2 + b_2\beta^3 + \cdots + b_{n-2}\beta^{n-1} + b_{n-1}\beta^n \\ &= b_{n-1} + b_0\beta + b_1\beta^2 + b_2\beta^3 + \cdots + b_{n-2}\beta^{n-1}. \end{aligned}$$

Obviously, the coordinates of βB is a cyclic shift of those of B, with respect to I_1. From

$$\begin{aligned} \beta^n \cdot B &= b_0\beta^n - b_1\beta^{n+1} + b_2\beta^{n+2} - \cdots - b_{n-2}\beta^{2n-2} + b_{n-1}\beta^{n-1} + b_{n-2}\beta + \cdots - b_{n-1}\beta^n \\ &= b_{n-1} + b_{n-2}\beta^2 + \cdots - b_{n-1}\beta^{n-1} + b_0\beta^n - b_1\beta^{n+1} + \cdots + b_{n-2}\beta^{2n-2} \\ &\quad - \sum_{j=0}^{n-1} b_{n-1-j}\beta^j, \end{aligned} \tag{2}$$

where $(j-i) = (j-i) \bmod n$ denotes that $j-i$ is to be reduced modulo n, we have

$$A \cdot B = \sum_{i=0}^{n-1} a_i(\beta^i \cdot B) = \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-1} b_{(j-i)}\beta^j = \sum_{j=0}^{n-1} \Big(\sum_{i=0}^{n-1} a_i b_{(j-i)} \Big) \beta^j.$$

If we define $AB = C = \sum_{j=0}^{n-1} c_j \beta^j$, then it follows

$$c_j = \sum_{i=0}^{n-1} a_i b_{(j-i)}, \qquad j = 0, 1, \ldots, n-1. \tag{2}$$

3.2 Bit-Serial Multiplier Architecture

Figure 1 shows the multiplier structure to realize multiplication using redundant basis. The coordinates of B with respect to the redundant basis I_1 are loaded into a register of length n bits whose contents can be shifted cyclically. The binary tree of $n-1$ adders in $\mathbb{F}_2$ takes n terms of $a_i b_k$ as its inputs and generates a c_j term as output every clock cycle. All c_j's, $j = 0, 1, \ldots, n-1$, which are represented using I_1, are computed and obtained in n clock cycles. It can be seen that n AND gates, $n-1$ XOR gates and n 1-bit registers are required for constructing the multiplier. The clock period should not be less than $T_A + \lceil \log_2 n \rceil T_X$, where T_A and T_X denote the time delays of an AND gate and an XOR gate, respectively.

Table 1 shows the complexity of the bit-serial multipliers using redundant basis and normal basis when there is a type I optimal normal basis. While Table 2 shows comparison of the complexities between RB multiplier and NB multiplier when there is a type II optimal normal basis or no optimal basis.

Table 1. Comparison of bit-serial multipliers using type I ONB and RB (here $n = m+1$).

Multiplier	#AND	#XOR	#1-bit reg.	# clk cycles	Basis
Massey-Omura [13]	$2m-1$	$2m-2$	$2m$	m	normal
Feng [5]	$2m-1$	$3m-2$	$3m-2$	m	normal
Agnew *et al* [2]	m	$2m-1$	$3m$	m	normal
presented here	$m+1$	m	$m+1$	$m+1$	redundant

It can be seen that the bit-serial redundant basis multiplier has lower complexity only when there is a type I optimal basis. When there is a type II optimal NB or no optimal basis, then the redundant basis multiplier will have a long time delay. In this case, partially parallel architecture can be employed and it is discussed in the next section.

Table 2. Comparison of bit-serial multipliers using NB and RB (where $n = km + 1$).

Multipliers	#AND	#XOR	#1-bit reg.	# clk cycles	basis
Massey-Omura [13]	C_N	$C_N - 1$	$2m$	m	normal
Feng [5]	$2m - 2$	$C_N + m - 1$	$3m - 2$	m	normal
Agnew *et al* [2]	m	C_N	$3m$	m	normal
presented here	$km + 1$	km	$km + 1$	$km + 1$	redundant

In the example presented in [5], a technique of reusing partial sum was used to reduce the complexity. Thus the number of XOR gates should be not greater than $C_N + m - 1$ if a non-optimal normal basis is used.

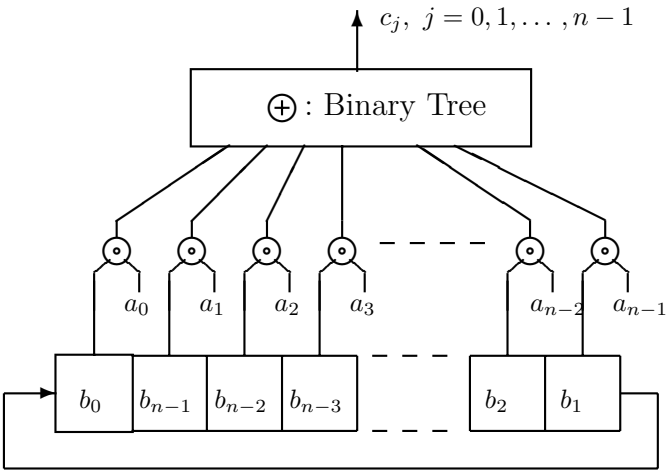

Fig. 1. Bit serial multiplier using the redundant basis.

3.3 Bit-Parallel Multiplier Architecture

A parallel version of the multiplier using a redundant basis is shown in Figure 2. On the left side of the figure inputs $\{a_i\}$ and $\{b_i\}$ are fed into n blocks (Block B). The detailed structure of Block B is shown on the right side of the figure. It can be seen that n^2 AND gates and $n(n-1)$ XOR gates are required. The time delay is $T_A + \lceil \log_2 n \rceil T_X$.

Trade-off with complexities or partial-parallel architecture The proposed bit-parallel architecture can be easily made for trade-offs between size and time complexities: If t Block B's are used to construct a multiplier and thus in one clock cycle t c_j's are computed and output, then one multiplication operation can be completed in $\left\lceil \frac{n}{t} \right\rceil$ clock cycles. This feature has great significance for hardware implementation since it might be difficult to implement a full-scale bit-parallel multiplier in hardware if the field is very large.

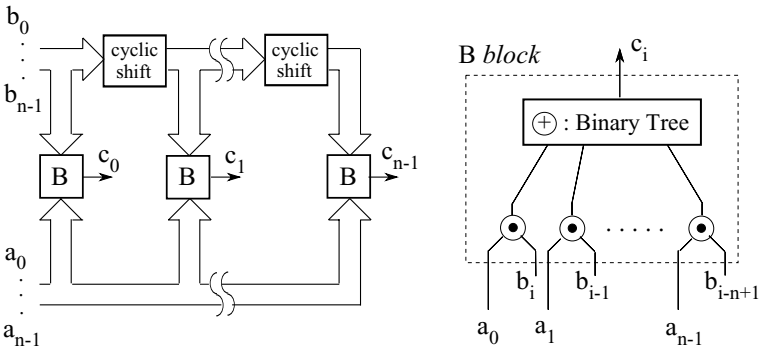

Fig. 2. Parallelization of the bit-serial multiplier using the redundant basis.

Table 3 adn Table 4 show the comparisons between bit-parallel redundant basis multipliers and bit-parallel normal basis multipliers.

Table 3. Comparison of bit-parallel multipliers using type I ONB and RB, here $n = m + 1$.

Multipliers	#AND	#XOR	Time delay	Partial-parallel Arch.
Hasan et al [9]	m^2	$m^2 - 1$	$T_A + (1 + \lceil \log_2 m \rceil)T_X$	not avail.
Koc and Sunar [11]	m^2	$m^2 - 1$	$T_A + (2 + \lceil \log_2 m \rceil)T_X$	not avail.
New proposal	$(m+1)^2$	$m(m+1)$	$T_A + \lceil \log_2(m+1) \rceil T_X$	available

Table 4. Comparison of bit-parallel multipliers using type II ONB and RB (where $n = 2m + 1$).

Multipliers	#AND	#XOR	Time delay	Partial-parallel Arch.
Massey-Omura	$2m^2 - m$	$2m^2 - m$	$T_A + \lceil \log_2(2m-1) \rceil T_X$	available
New proposal	m^2	$2m^2 - m$	$T_A + (1 + \lceil \log_2 m \rceil)T_X$	available

3.4 Complexity

Clearly the complexity of the RB multipliers in $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ depends on the size n of the cyclotomic field $\mathbb{F}^{(n)}$. There seems no easy way to give a general relation between n and m. In Table 1, we have computed values of n for certain small values of m using Algorithm 1.

Table 5. Smallest cyclotomic field $\mathbb{F}^{(n)}$ that includes $\mathbb{F}_{2^m}$ as a subfield.

m	2	3	4	5	6	7	8	9	10	11	12	13	14	15	18	19
n	3	7	5	11	9	29	17	19	11	23	13	53	29	31	19	37

For a subset of redundant basis, which can be derived from certain normal basis (optimal normal basis), the complexity can be easily solved which is discussed in the next section. Also, for the field in which there exists an equally spaced polynomial (ESP), a small value of n can be found.

4 Relation/Conversion between Redundant Basis and Other Bases

4.1 Redundant Basis and Normal Basis

Some redundant bases can be easily introduced by the normal basis generated with Gauss period, which also reveals the relation/conversion between the redundant basis and the normal basis.

Gauss period, normal basis and redundant basis The Gauss period (GP) was discovered by Gauss and is defined as follows: Let $m, k \geqslant 1$ be integers such that $r = mk + 1$ is a prime, and let q be a prime power with $\gcd(q, r) = 1$. Let $\mathcal{K}$ be the unique subgroup of order k of the multiplicative group of $\mathbb{Z}_r = \mathbb{Z}/r\mathbb{Z}$, then for any primitive rth root β of unity in $\mathbb{F}_{q^{mk}}$, the elements

$$\alpha = \sum_{\gamma \in \mathcal{K}} \beta^{\gamma} \tag{3}$$

is called a *Gauss period of type* (m, k) over $\mathbb{F}_q$. It can be checked that $\alpha \in \mathbb{F}_{q^m}$.

Gauss periods have been used to construct normal bases with low complexity [15,3]. A Gauss period of type (m, k) over $\mathbb{F}_2$ naturally introduces a normal basis $I_2 = \langle \alpha, \alpha^2, \ldots, \alpha^{2^{m-1}} \rangle$ in $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$ if and only if $\gcd(e, m) = 1$, where e is the index of 2 modulo r. Furthermore, such a normal basis has complexity at most $mk' - 1$ with $k' = k$ if k even and $k+1$ otherwise [3,18,7]. Clearly, Gauss periods of type $(m, 1)$ and $(m, 2)$ generate optimal normal bases with complexity $2m-1$, which are usually called type-I and type-II optimal normal bases (ONB), respectively [15].

On the other hand, a redundant basis in this case can be given as $I_1 = \langle 1, \beta, \beta^2, \beta^3, \ldots, \beta^{mk} \rangle$. Consider two sets of km elements in $\mathbb{F}_{2^{km}}$: $S_1 = \{\beta^{2^i \gamma^j}, i = 0, 1, \ldots, m-1; j = 0, 1, \ldots, k-1\}$ and $S_2 = \{\beta, \beta^2, \ldots, \beta^{km}\}$. For any element $\beta^{2^i \gamma^j} \in S_1$, we have $\beta^{2^i \gamma^j} = \beta^{2^i \gamma^j \bmod (mk+1)} \in S_2$, and thus, $S_1 \subseteq S_2$. Let $G = \mathbb{F}^*_{km+1}$ then $G = \langle 2, \gamma \rangle$. For any integer $l \in \{1, 2, \ldots, km\}$, there exist integers $i \in \{0, 1, \ldots, m-1\}$ and $j \in \{0, 1, \ldots, k-1\}$, such that $l = 2^i \gamma^j \bmod (km + 1)$. Therefore, $S_2 \subseteq S_1 \Rightarrow S_2 = S_1$.

Since $I_2 = \langle \alpha, \alpha^2, \ldots, \alpha^{2^{m-1}} \rangle = \langle \sum_{i=0}^{k-1} \beta^{\gamma^i}, \sum_{i=0}^{k-1} \beta^{2\gamma^i}, \ldots, \sum_{i=0}^{k-1} \beta^{2^{m-1}\gamma^i} \rangle$ and each element in I_2 is a sum of k elements in S_1, it can be seen that elements in $S_1 (= S_2)$ can serve as a basis in $\mathbb{F}_{2^m}$ and which is a permutation of $\langle \beta, \beta^2, \ldots, \beta^{mk} \rangle \triangleq I_3$. Obviously, the redundant basis can be obtained by adding element '1' to the basis I_3.

Conversion between normal basis and redundant basis Now let us look at the conversion from the normal basis $I_2 = \langle \alpha, \alpha^2, \ldots, \alpha^{2^{m-1}} \rangle$ to the redundant basis I_1. As we have seen before, the conversion between redundant basis I_1 and the basis consisting of elements from S_1 is simple. If $A = (a'_0, a'_1, \ldots, a'_{m-1})$ with the normal basis, then with the basis from S_1,

$$A = (a''_{0,0}, a''_{0,1}, \ldots, a''_{0,k-1}, \ldots, a''_{m-1,k-1}),$$

where $a''_{i,j} = a'_i$ for $j = 0, 1, \ldots, k-1$ and $i = 0, 1, \ldots, m-1$.

4.2 Redundant Basis and Polynomial Basis

Given a basis I in $\mathbb{F}_{2^m}$, the general case of basis conversion between I and the redundant basis I_1 may not be trivial. If I is a normal basis generated with the Gauss period of type (m, k), then how to obtain I_1 has been discussed in the last section. If $I = \langle 1, \alpha, \ldots, \alpha^{m-1} \rangle$ is the polynomial basis, and if we know that the order of element α is ord(α), then the redundant basis I_1 can be obtained using the following algorithm:

Algorithm 2 Computing the redundant basis from a polynomial basis $\langle 1, \alpha, \ldots, \alpha^{m-1} \rangle$

1. *Compute n using Algorithm 1;*
2. *Compute the order of the irreducible polynomial ord(α);*
3. *Let $t = ord(\alpha)/n$, then the redundant basis is given by* $\langle 1, \alpha^t, \alpha^{2t}, \ldots, \alpha^{(n-1)t} \rangle$.

□

It can be shown that for the field that there exists an ESP, the value of n is always between $m+1$ and $2m$.

5 Squaring Operation Using Redundant Basis

Let $\langle 1, \beta, \beta^2, \ldots, \beta^{n-1} \rangle$ be a redundant basis for $\mathbb{F}_{2^m}$ over $\mathbb{F}_2$. For a field element represented in the redundant basis:

$$A = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1}$$

its square is given by

$$A^2 = a_0 + a_1\beta^2 + \cdots + a_{n-1}\beta^{2(n-1)}.$$

Since $\beta^n = 1$, we have that $a_j\beta^{2j} = a_j\beta^{2j-n}$ if $2j > n-1$. It can be seen that a squaring operation using the redundant basis is equivalent to a permutation of the element coefficients.

6 Inversion with Redundant Basis

The problem of inversion in redundant basis is as follows: Given a field element

$$A = a_0 + a_1\beta + \cdots + a_{n-1}\beta^{n-1} \in \mathbb{F}_{2^m},$$

find

$$B = b_0 + b_1\beta + \cdots + b_{n-1}\beta^{n-1} \in \mathbb{F}_{2^m}$$

which is the inverse of A. Clearly, the methods proposed by Itoh and Tsujii [10] and by Agnew *et al* [1] can be used. With their methods, about $\frac{3}{2}\log(m-1)$ multiplications on average and $(m-1)$ squaring operations are required. Since squaring operation in the redundant basis is a permutation of lines and free, while the multiplication can be efficiently implemented in hardware, it is expected that with this method inversion using the redundant basis can be as good as using normal basis.

Another method for inversion is to solve a set of linear equations. From $AB = 1$, we have

$$\begin{aligned} 1 &= \sum_{i=0}^{n-1} a_i\beta^i \sum_{j=0}^{n-1} b_j\beta^j \\ &= \sum_{j=0}^{n-1} b_j \sum_{i=0}^{n-1} a_i\beta^{i+j} \\ &= \sum_{j=0}^{n-1} b_j \sum_{i=0}^{n-1} a_i\beta^{(i+j)} \\ &= \sum_{j=0}^{n-1} \Big(\sum_{i=0}^{n-1} a_{(j-i)} b_i \Big) \beta^j, \end{aligned}$$

where $(x) \triangleq x \bmod (n)$, or,

$$\begin{bmatrix} a_0 & a_{n-1} & a_{n-2} & \cdots & a_1 \\ a_1 & a_0 & a_{n-1} & \cdots & a_2 \\ a_2 & a_1 & a_0 & \cdots & a_3 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_{n-1} & a_{n-2} & a_{n-3} & \cdots & a_0 \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ \vdots \\ b_{n-1} \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \tag{4}$$

The circulant matrix is always singular and the equations allow many solutions, all of which is a representation of the inverse B in the redundant basis. Note that the circulant matrix is a special case of Toplitz matrix and any algorithm for solving Toplitz system can also be used to solve (4).

7 Examples

Example 1. For the field $\mathbb{F}_{2^{10}}$*, we can compute the smallest cyclotomic field that includes it as a subfield is* $\mathbb{F}^{(11)}$*. Highly regular architectures for bit-serial and bit-parallel multipliers using redundant basis can be built as discussed in Section 3. Clearly, a bit-serial multiplier requires* 11 *AND gates,* 10 *XOR gates, and* 11 *1-bit registers. It takes* 11 *clock cycles to accomplish a multiplication operation. The complexities for a fully bit-parallel multiplier are:* 121 *AND gates,* 110 *XOR gates and a propagation delay of* $T_A + \lceil \log_2(m+1) \rceil T_X$*.*

Example 2. From Algorithm 1, we find the smallest cyclotomic field that includes $\mathbb{F}_{2^6}$ *as a subfield is* $\mathbb{F}^{(9)}$*. Let the redundant basis in* $\mathbb{F}_{2^6}$ *over* $\mathbb{F}_2$ *be given by* $\langle 1, \beta, \beta^2, \ldots, \beta^8 \rangle$*, where* β *is a primitve* 9^{th} *root of unity in* $\mathbb{F}_{2^6}$*. In fact,* β *is a root of irreducible polynomial* $x^6 + x^3 + 1$*. The complexities of the bit-serial redundant basis multiplier are* 9 *AND gate,* 8 *XOR gate,* 9 *1-bit registers and* 9 *clock cycles for performing a multiplication operation.*

Example 3. It can be computed that the redundant basis in $\mathbb{F}_{2^8}$ *has* 17 *elements* ($m = 8$ *and* $n = 17$*). Then the redundant basis multipliers can be built and their complexities can be decided.*

8 Summary

In this paper, we have presented redundant bases and their applications to the construction of multipliers. It has shown the new constructions are advantageous over other normal basis constructions when bit-parallel or partial-parallel structures are required. The comparisons have been made between redundant basis and normal basis, since the squaring operation using redundant basis is also a simple cyclic shift of lines. The inversion using the new basis has also been discussed. It can be shown that the polynomial ring basis proposed in [4] is a subset of the redundant basis.

References

1. Agnew, G.B., Beth, R., Mullin, R.C., Vanstone, S.A.: Arithmetic operations in GF(2^m). J. Cryptology **6** (1993) 3-13
2. Agnew, G.B., Mullin, R.C., Onyszchuk, I., Vanstone, S.A.: An implementation for a fast public key cryptosystem. J. Cryptology **3** (1991) 63-79
3. Ash, D.W., Blake, I.F., Vanstone, S.A.: Low complexity normal bases. Disc. Appl. Math. **25** (1989) 191-210
4. Drolet, G.: A New Representation of Elements of Finite Fields GF(2^m) Yielding Small Complexity Arithmetic Circuits. IEEE Trans. Comput. **47** (1998)
5. Feng, M.: A VLSI architecture for fast inversion in GF(2^m). IEEE Trans. Comput. **38** (1989) 1383-1386

6. Fenn, S.T.J., Benaissa, M., Taylor, D.: GF(2^m) multiplication and division over the dual basis. IEEE Trans. Comput. **45** (1996) 319-327
7. Gao, S., Vanstone, S.A.: On orders of optimal normal basis generators. Math. Comp. **64** (1995) 1227-1233
8. Hasan, M.A., Wang, M., Bhargava, V.K.: Modular construction of low complexity parallel multipliers for a class of finite fields GF(2^m). IEEE Trans. Comput. **41** (1992) 962-971
9. Hasan, M.A., Wang, M., Bhargava, V.K.: A modified Massey-Omura parallel multiplier for a class of finite fields. IEEE Trans. Comput. **42** (1993) 1278-1280
10. Itoh, T., Tsujii, S.: A fast algorithm for computing multiplicative inverse in GF(2^m) using normal bases. Inform. and Comput. **78** (1988) 171-177
11. Koc, C.K., Sunar, B.: Low-complexity bit-parallel canonical and normal multipliers for a class of finite fields. IEEE Trans. Comput. **47** (1998) 353-356
12. Lidl, R., Niederreiter, H.: Finite Fields. Addison-Wesley Publishing Company, 1983, Reading, MA
13. Massey, J.L., Omura, J.K.: Computational method and apparatus for finite field arithmetic. U.S. Patent No.4587627, 1984.
14. Mastrovito, E.D.: VLSI Architectures for Computations in Galois Fields. Ph.D Thesis, Linköping University, 1991, Linköping, Sweden
15. Mullin, R., Onyszchuk, I., Vanstone, S.A., Wilson, R.: Optimal normal bases in GF(p^n). Disc. Appl. Math. **22** (1988) 149-161
16. Paar, C.: Efficient VLSI Architectures for Bit-Parallel Computation in Galois Fields. Ph.D Thesis, VDI-Verlag, Düsseldorf, 1994
17. Wang, C.C., et al: VLSI architectures for computing multiplications and inverses in GF(2^m). IEEE Trans. Comput. **34** (1985) 709-717
18. Wassermann, A.: Konstruktion von Normalbasen. Bayreuther Mathematische Schriften **31** (1990) 155-164
19. Wu, H., Hasan, M.A.: Low complexity bit-parallel multipliers for a class of finite fields. IEEE Trans. Comput. **47** (1998) 883-887