Subquadratic Space Complexity Multiplication over Binary Fields with Dickson Polynomial Representation

M. A. Hasan*and C. Negre†

Abstract

We study Dickson bases for binary field representation. Such representation seems interesting when no optimal normal basis exists for the field. We express the product of two elements as Toeplitz or Hankel matrix vector product. This provides a parallel multiplier which is subquadratic in space and logarithmic in time.

1 Introduction

Finite filed arithmetic is extensively used in cryptography. For public key cryptosystems, the size (i.e. the number of elements) of the field may be quite large, say 2^{2048}. Finite field multiplication over such a large field requires a considerable amount of resources (time or space). For binary extension fields, used in many practical public key cryptosystems, field elements can be represented with respect to a normal basis, where squaring operations are almost free of cost. In order to reduce the cost of multiplication over the extension field, instead of using an arbitrary normal basis, it is desirable to use an optimal normal basis. The latter however does not exist for all extension fields, in which case one may use Dickson bases [1, 6] and develop an efficient field multiplier.

In this paper we consider subquadratic space complexity multipliers using the Dickson basis. To this end, using low weight Dickson polynomials, we formulate the problem of field multiplication as a product of a Toeplitz or Hankel matrix and a vector, and apply subquadratic space complexity algorithm for the product [4], which gives us a subquadratic space complexity field multipliers.

The article is organized as follows. In Section 2 we present some general results on Dickson polynomials. In Section 3 we give the outline of the subquadratic multiplier of matrix vector product of [4]. Then in Section 4 we give a matrix vector product approach in Dickson basis representation. We wind up with complexity comparison and a brief conclusion.

*Department of Electrical and Computer Engineering, University of Waterloo, Canada

†Team Dali/ELIAUS, University of Perpignan, France

2 Dickson Polynomials

Dickson polynomials over finite fields were introduced by L.E. Dickson in [1]. These polynomials have several applications and interesting properties, the main one being a permutation property over finite fields. For a complete explanation on this the reader may refer to [5]. Our interest here concerns the use of Dickson polynomial for finite field representation for efficient binary field multiplication. There are two kinds of Dickson polynomials, and there are several ways to define and construct both of them. We give here the definition of [5] of the first kind Dickson polynomials.

Definition 1 (Dickson Polynomial[5] page 9)**.** *Let R be a ring and $a \in R$. The Dickson polynomial of the first kind $D_n(X,a)$ is defined by*

$$D_n(X,a) = \sum_{i=0}^{\lfloor n/2 \rfloor} \frac{n}{n-i} \left(\begin{array}{c} n-i \\ n \end{array} \right) (-a)^i X^{n-2i}.$$

For $n = 0$, we set $D_0(X,a) = 2$ and for $n = 1$ we have $D_1(X,a) = X$.

In [5] it has been shown that Dickson polynomials can be computed using the following recursive relation

$$\left\{ \begin{array}{rcl} D_0(X,a) & = & 2, \\ D_1(X,a) & = & X, \\ D_n(X,a) & = & XD_{n-1}(X,a) - aD_{n-2}. \end{array} \right. \tag{1}$$

Using these relations we obtain the Dickson polynomials $D_n(X,1)$ in $\mathbb{F}_2[X]$ for $n \leq 20$ given in Table 1.

The following theorem will be extensively used for the construction of subquadratic multiplier in the Dickson basis.

Theorem 1. *We denote $\beta_i = D_i(X,1)$ the n-th Dickson polynomial in $\mathbb{F}_2[X]$. Then for all $i,j \geq 0$ the following equation holds*

$$\beta_i \beta_j = \beta_{i+j} + \beta_{|i-j|}. \tag{2}$$

Proof. This theorem is a consequence of equation (1).

We will show it by induction on i and j. Using Table 1 We can easily check that equation (2) holds for $i,j \leq 1$. We suppose that the equation is true for all $i,j \leq n$ and we prove that the equation is true for $i,j \leq n+1$. We first prove it for $i = n+1$ and $j \leq n$

$$\begin{array}{rcl} \beta_{n+1}\beta_j & = & (X\beta_n + \beta_{n-1})\beta_j \\ & = & X\beta_n\beta_j + \beta_{n-1}\beta_j = X(\beta_{n+j} + \beta_{|n-j|}) + (\beta_{n-1+j} + \beta_{|n-1-j|}), \end{array}$$

by induction hypothesis. Now we have

$$\begin{array}{rcl} \beta_{n+1}\beta_j & = & (X\beta_{n+j} + \beta_{n+j-1}) + (X\beta_{|n-j|} + \beta_{|n-1-j|}) \\ & = & \beta_{n+1+j} + \beta_{|n+1-j|}. \end{array}$$

For the other case $i = n+1$ and $j = n+1$, the product $\beta_n\beta_{n+1}, \beta_{n+1}\beta_{n+1}$ is obtained using similar tricks. □

Table 1: Dickson polynomials

β_1	X
β_2	X^2
β_3	$X^3 + X$
β_4	X^4
β_5	$X^5 + X^3 + X$
β_6	$X^6 + X^2$
β_7	$X^7 + X^5 + X$
β_8	X^8
β_9	$X^9 + X^7 + X^5 + X$
β_{10}	$X^{10} + X^6 + X^2$
β_{11}	$X^{11} + X^9 + X^5 + X^3 + X$
β_{12}	$X^{12} + X^4$
β_{13}	$X^{13} + X^{11} + X^9 + X^3 + X$
β_{14}	$X^{14} + X^{10} + X^2$
β_{15}	$X^{15} + X^{13} + X^9 + X$
β_{16}	X^{16}
β_{17}	$X^{17} + X^{15} + X^{13} + X^9 + X$
β_{18}	$X^{18} + X^{14} + X^{10} + X^2$

Polynomial and finite field representation using Dickson polynomials.

A consequence of equation (1) is that each β_i or $i \geq 1$ has degree i. As a result each polynomial $A = \sum_{i=0}^{n} A_i X^i \in \mathbb{F}_2[X]$ can be expressed as

$$A = a_0 + \sum_{i=1}^{n} a_i \beta_i.$$

Such expression can be obtained using Algorithm 2.

For example for $A = 1 + X^2 + X^5$ the execution of the previous algorithm gives

	$R \leftarrow 1 + X^2 + X^5$
begin for	
$i = 5$	$R \leftarrow R + \beta_5 = 1 + X + X^2 + X^3, a_5 \leftarrow 1$
$i = 4$	$a_4 \leftarrow 0$
$i = 3$	$R \leftarrow R + \beta_3 = 1 + X^2, a_3 \leftarrow 1$
$i = 2$	$R \leftarrow R + \beta_2 = 1, a_2 \leftarrow 1$
$i = 1$	$a_1 \leftarrow 0$
end for	
	$a_0 \leftarrow 1$
$A = 1 + \beta_2 + \beta_3 + \beta_5$	

Since each polynomial can be written in term of Dickson polynomials, we can use Dickson polynomials for basis representation of binary fields.

Algorithm 1 Conversion of polynomial from regular polynomial to Dickson polynomial

```
Require: A polynomial $A(X) \in \mathbb{F}_2[X]$ of degree $n$.
  $R \leftarrow A$
  for $i = n$ to 1 do
    if $R_i = 1$ then
      $a_i \leftarrow 1$
      $R \leftarrow R + \beta_i$
    else
      $a_i \leftarrow 0$
    end if
  end for
  $a_0 \leftarrow R$
Ensure: Return $(a_0, \ldots, a_n)$
```

Theorem 2. *Let P be an irreducible polynomial of degree n in $\mathbb{F}_2[X]$. The system $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$ forms a basis of $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ over $\mathbb{F}_2$.*

Proof. To show that $\mathcal{B}$ is a basis we have to show that each element $A \in \mathbb{F}_{2^n}$ can be expressed as

$$A = \sum_{i=1}^{n} a_i\beta_i \text{ with } a_i \in \{0, 1\},$$

and this expression is unique.

Let us first show that for each $A \in \mathbb{F}_{2^n}$ an expression in $\mathcal{B}$ exists. The polynomial P is an irreducible polynomial in $\mathbb{F}_2[X]$ and using Algorithm 2 it can be expressed as

$$P = 1 + \sum_{i=1}^{n-1} p_i\beta_i + \beta_n.$$

Let $A \in \mathbb{F}[X]/(P)$ which is a polynomial of degree less than n and can also be written as $A = a_0 + \sum_{i=0}^{n-1} a_i\beta_i$ with Algorithm 2. To get required expression of A in $\mathcal{B}$ we need to express the coefficient a_0 in $\mathcal{B}$. To do this, we use the expression of P in $\mathcal{B}$. Since $1 = \sum_{i=1}^{n-1} p_i\beta_i + \beta_n \mod P$ we can replace a_0 by $\sum_{i=1}^{n-1} a_0p_i\beta_i + a_0\beta_n$. We finally obtain

$$A = \sum_{i=1}^{n-1} (a_i + a_0p_i)\beta_i + a_0\beta_n.$$

Now we show that such expression is unique. If we have a second different expression $A = \sum_{i=1}^{n} a_i'\beta_i$, then by adding the two we get

$$\sum_{i=1}^{n} (a_i + a_i')\beta_i = 0. \tag{3}$$

Let d the maximal subscript such that $a_d \neq a'_d$. We rewrite $\beta_d = X^d + \beta'_d$ where $\deg \beta'_d < d$ and then using (3) we obtain

$$\sum_{i=1}^{d-1}(a_i + a'_i)\beta_i + (a_d + a'_d)\beta'_d + (a_d + a'_d)X^d = 0.$$

Now $\deg(\sum_{i=1}^{d-1}(a_i+a'_i)\beta_i+(a_d+a'_d)\beta'_d) \leq d-1$, and thus we must have $(a_d+a'_d)X^d = 0$, this contradicts the fact that $a_d \neq a'_d$. □

3 Asymptotic Complexities of Toeplitz Matrix Vector Product

In this section we recall some basics matrix-vector multiplication and their corresponding space and time complexities [4]. A Toeplitz matrix is defined as

Definition 2. *An $n \times n$ Toeplitz matrix is a matrix $[t_{i,j}]_{0 \leq i,j \leq n-1}$ such that $t_{i,j} = t_{i-1,j-1}$ for $1 \geq i, j$.*

If $2|n$ we can use a *two way approach* presented in Table 2, to compute a matrix vector product $T \cdot V$ where T is an $n \times n$ Toeplitz matrix. If $3|n$ we can use the *three way* approach which is also presented in Table 2.

Table 2: Subquadratic Toeplitz matrix vector product

Matrix decomposition	
Two way	Three way
$T = \begin{bmatrix} T_1 & T_0 \\ T_2 & T_1 \end{bmatrix} \begin{bmatrix} V_0 \\ V_1 \end{bmatrix}$	$T = \begin{bmatrix} T_2 & T_1 & T_0 \\ T_3 & T_2 & T_1 \\ T_4 & T_3 & T_2 \end{bmatrix} \begin{bmatrix} V_0 \\ V_1 \\ V_2 \end{bmatrix}$
Recursive formulas	
$T \cdot V = \begin{bmatrix} P_0 + P_2 \\ P_1 + P_2 \end{bmatrix}$ where $P_0 = (T_0 + T_1)V_1,$ $P_1 = (T_1 + T_2)V_0,$ $P_2 = T_1(V_0 + V_1),$	$T \cdot V = \begin{bmatrix} P_0 + P_3 + P_4 \\ P_1 + P_3 + P_5 \\ P_2 + P_4 + P_5 \end{bmatrix}$ where $P_0 = (T_0 + T_1 + T_2)V_2,$ $P_1 = (T_0 + T_1 + T_3)V_1,$ $P_2 = (T_2 + T_3 + T_4)V_0,$ $P_3 = T_1(V_1 + V_2,)$ $P_4 = T_2(V_0 + V_2),$ $P_5 = T_3(V_0 + V_1),$

If n is a power of 2 or a power of 3 the formulas of Table 2 can be used recursively to perform $T \cdot V$. Using these recursive processes through parallel computation, the resulting multipliers [4] have the complexity given in Table 3.

Table 3: Asymptotic complexity

	Two-way split method	Three-way split method
# AND	$n^{\log_2(3)}$	$n^{\log_3(6)}$
# XOR	$5.5n^{\log_2(3)} - 6n + 0.5$	$\frac{24}{5}n^{\log_3(6)} - 5n + \frac{1}{5}$
Delay	$T_A + 2\log_2(n)T_X$	$T_A + 3\log_3(n)T_X$

The above subquadratic approach can also be used when H is an Hankel matrix. We recall the definition of an Hankel matrix.

Definition 3 (Hankel matrix). *Let $H = [h_{i,j}]_{0\leq i,j\leq n-1}$ be an $n \times n$ matrix. We say that H is Hankel if*

$$h_{i,j} = h_{i-1,j+1} \text{ for } 1 \leq i \text{ and } j < n-1 \tag{4}$$

Moreover we say that H is an essentially Hankel matrix, if H satisfies (4) unless for $i = n-1$ and for $0 \leq j \leq n-1$ where $h_{n-1,j} = 0$.

Let H be an Hankel matrix. The matrix H' with the same rows as H in the reverse order

$$H' = [h_{n-1-i,j}]_{0\leq i,j\leq n-1}$$

is a Toeplitz matrix. Consequently to perform $W = H \cdot V$, we compute $W' = H' \cdot V$ using the subquadratic of Table 3 method and then reverse the order of the coefficients of W' to get W.

4 Field multiplication using low weight Dickson polynomials

In this section we consider multiplication of two elements of the binary field $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ where the polynomial P is a low weight Dickson polynomial. In particular we consider two and three-term Dickson polynomials P, i.e., Dickson binomials and trinomials. Like low weight conventional polynomials the use of low weight Dickson polynomials is expected to yield lower space complexity multipliers.

4.1 Irreducible Dickson binomials

In this subsection we will focus on finite field $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ where P is two terms irreducible polynomial of the form $P = \beta_n + 1$ where β_n is the n-th Dickson polynomial. The elements of $\mathbb{F}_{2^n}$ are expressed in the Dickson basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$.

The following theorem shows that the product of two elements A and B in $\mathbb{F}_{2^n}$ can be computed as a matrix-vector product $M_A \cdot B$ where M_A is a sum of a Toeplitz matrix and an essentially Hankel matrix.

Theorem 3. *Let n be an integer such that $\beta_n + 1$ is irreducible and let $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(\beta_n + 1)$. Let $A = \sum_{i=1}^{n} a_i\beta_i$ and $B = \sum_{i=1}^{n} b_i\beta_i$ be two elements of $\mathbb{F}_{2^n}$ expressed in $\mathcal{B}$. The coefficients in $\mathcal{B}$ of the product $A \times B$ can be computed as*

$$\begin{bmatrix} a_n & a_{n-1}+a_1 & \cdots & a_2+a_{n-2} & a_1+a_{n-1} \\ a_1 & a_n & \cdots & a_3+a_{n-3} & a_2+a_{n-2} \\ \vdots & & & & \vdots \\ a_{n-2} & \cdots & \cdots & a_n & a_{n-1}+a_1 \\ a_{n-1} & \cdots & \cdots & a_1 & a_n \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}$$
$$+ \begin{bmatrix} a_2 & a_3 & \cdots & a_{n-1} & 0 & a_{n-1} \\ a_3 & a_4 & \cdots & 0 & a_{n-1} & a_{n-2} \\ \vdots & & & & \vdots & \\ 0 & a_{n-1} & & & a_2 & a_1 \\ 0 & & & & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}.$$

Proof. If we multiply the two elements A and B we get the following:

$$AB = \left(\sum_{i=1}^{n} a_i\beta_i\right) \times \left(\sum_{i=1}^{n} b_i\beta_i\right) = \sum_{i,j=1}^{n} a_i b_i \beta_i \beta_j. \tag{5}$$

Then from Theorem 1 we have $\beta_i\beta_j = \beta_{i+j} + \beta_{|i-j|}$, we can rewrite (5) as

$$AB = \underbrace{\left(\sum_{i,j=1}^{n} a_i b_j \beta_{i+j}\right)}_{S_1} + \underbrace{\left(\sum_{i,j=1}^{n} a_i b_j \beta_{|i-j|}\right)}_{S_2}$$

Now we express this former expression of AB as a sum of Toeplitz or Hankel matrix vector product.

Let us begin with S_1. We remark that S_1 has a similar expression as product of two polynomials of the same degree. In other words, S_1 can be computed as $Z_A \cdot B$ where

$$Z_A = \begin{array}{cl} \begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ a_1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ a_{n-1} & \cdots & \cdots & a_1 & 0 \\ a_n & \cdots & \cdots & a_2 & a_1 \\ 0 & a_n & \cdots & a_3 & a_1 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_n \end{bmatrix} & \begin{array}{l} \leftarrow \beta_1 \\ \leftarrow \beta_2 \\ \vdots \\ \leftarrow \beta_n \\ \leftarrow \beta_{n+1} \\ \leftarrow \beta_{n+2} \\ \vdots \\ \leftarrow \beta_{2n} \end{array} \end{array}$$

We reduce the matrix Z_A modulo $P = \beta_n + 1$ to get non-zero coefficients only on rows corresponding to $\beta_1, \ldots, \beta_n$. We use the fact that β_{n+i} for $i \geq 0$ satisfies

$$\beta_{n+i} = \beta_i\beta_n + \beta_{n-i} = \beta_i + \beta_{n-i}.$$

This equation is a simple consequence of equation (2) and that $\beta_n = 1 \mod P$. This implies that the rows corresponding to β_{n+i} are reduced into two rows one corresponding to β_i and the other to β_{n-i}. After performing this reduction and removing zero rows we get

$$S_1 = Z_A \cdot B = \underbrace{\begin{bmatrix} a_n & a_{n-1} & \cdots & a_2 & a_1 \\ a_1 & a_n & \cdots & a_3 & a_2 \\ \vdots & & & & \vdots \\ a_{n-1} & \cdots & \cdots & a_1 & a_n \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}}_{S_{1,1}}$$

$$+ \underbrace{\begin{bmatrix} 0 & 0 & \cdots & a_n & a_{n-1} \\ \vdots & & & & \vdots \\ 0 & a_n & \cdots & a_3 & a_1 \\ a_n & a_{n-1} & \cdots & a_2 & a_1 \\ 0 & \cdots & \cdots & 0 & 0 \end{bmatrix} \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}}_{S_{1,2}}$$

Finally, we get an expression of S_1 as matrix vector product where the matrix is a sum of a Toeplitz and an essentially Hankel matrix.

Now we do the same for S_2. We split S_2 into two sums

$$\begin{aligned} S_2 &= \left(\textstyle\sum_{i,j=1}^{n} a_i b_j \beta_{|i-j|}\right) \\ &= \underbrace{\left(\sum_{k=1}^{n}\sum_{j=1}^{n-k} a_{j+k} b_j \beta_k\right)}_{S_{2,1}} + \underbrace{\left(\sum_{k=1}^{n}\sum_{j=k}^{n} a_{j-k} b_j \beta_k\right)}_{S_{2,2}}. \end{aligned} \tag{6}$$

We express $S_{2,1}$ and $S_{2,2}$ as matrix vector products

$$S_{2,1} = \begin{bmatrix} a_2 & a_3 & \cdots & a_{n-1} & a_n & 0 \\ a_3 & a_4 & \cdots & a_n & 0 & 0 \\ \vdots & & & & \vdots & \\ a_n & & & & 0 & 0 \\ 0 & & & & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}, \tag{7}$$

$$S_{2,2} = \begin{bmatrix} 0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & 0 & a_1 & \cdots & a_{n-2} \\ \vdots & & & & \vdots \\ 0 & 0 & & & a_1 \\ 0 & & & & 0 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}. \tag{8}$$

So now we have each of S_1 and S_2 in the required form. We can add $S_{1,1}$ to $S_{2,2}$

and $S_{1,2}$ to $S_{2,1}$ to get the following expression of $S_1 + S_2 = A \times B$.

$$\begin{array}{rcl}
A \times B & = & (S_{1,1} + S_{2,2}) + (S_{1,2} + S_{2,1}) \\
& = & \left(\begin{bmatrix}
a_n & a_{n-1} + a_1 & \cdots & a_2 + a_{n-2} & a_1 + a_{n-1} \\
a_1 & a_n & \cdots & a_3 + a_{n-3} & a_2 + a_{n-2} \\
\vdots & & & & \vdots \\
a_{n-2} & \cdots & \cdots & a_n & a_{n-1} + a_1 \\
a_{n-1} & \cdots & \cdots & a_1 & a_n
\end{bmatrix} \right. \\
& & + \left. \begin{bmatrix}
a_2 & a_3 & \cdots & a_{n-1} & 0 & a_{n-1} \\
a_3 & a_4 & \cdots & 0 & a_{n-1} & a_{n-2} \\
\vdots & & & & \vdots & \\
0 & a_{n-1} & & & a_2 & a_1 \\
0 & & & & 0 & 0
\end{bmatrix} \right) \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix}
\end{array}$$

This ends the proof. □

Example 1. *Let us consider the field $\mathbb{F}_{2^9}$. It is defined as $\mathbb{F}_{2^9} = \mathbb{F}_2[X]/(\beta_9+1)$. The Dickson basis of $\mathbb{F}_{2^9}$ is $\mathcal{B} = \{\beta_1, \ldots, \beta_9\}$. The multiplication of two elements A and B can be computed as a matrix vector product. As stated in Theorem 3 the matrix can be decomposed as the sum of a Toeplitz T_A matrix and an essentially Hankel matrix H_A. The Toeplitz matrix T_A is*

$$T_A = \begin{bmatrix}
a_9 & a_8+a_1 & a_7+a_2 & a_6+a_3 & a_4+a_5 & a_5+a_4 & a_6+a_3 & a_2+a_7 & a_1+a_8 \\
a_1 & a_9 & a_8+a_1 & a_7+a_2 & a_6+a_3 & a_4+a_5 & a_5+a_4 & a_6+a_3 & a_2+a_7 \\
a_2 & a_1 & a_9 & a_8+a_1 & a_7+a_2 & a_6+a_3 & a_4+a_5 & a_5+a_4 & a_6+a_3 \\
a_3 & a_2 & a_1 & a_9 & a_8+a_1 & a_7+a_2 & a_6+a_3 & a_4+a_5 & a_5+a_4 \\
a_4 & a_3 & a_2 & a_1 & a_9 & a_8+a_1 & a_7+a_2 & a_6+a_3 & a_4+a_5 \\
a_5 & a_4 & a_3 & a_2 & a_1 & a_9 & a_8+a_1 & a_7+a_2 & a_6+a_3 \\
a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_9 & a_8+a_1 & a_7+a_2 \\
a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_9 & a_8+a_1 \\
a_8 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 & a_9
\end{bmatrix}$$

and the essentially Hankel matrix H_A is

$$H_A = \begin{bmatrix}
a_2 & a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & 0 & a_8 \\
a_3 & a_4 & a_5 & a_6 & a_7 & a_8 & 0 & a_8 & a_7 \\
a_4 & a_5 & a_6 & a_7 & a_8 & 0 & a_8 & a_7 & a_6 \\
a_5 & a_6 & a_7 & a_8 & 0 & a_8 & a_7 & a_6 & a_5 \\
a_6 & a_7 & a_8 & 0 & a_8 & a_7 & a_6 & a_5 & a_4 \\
a_7 & a_8 & 0 & a_8 & a_7 & a_6 & a_5 & a_4 & a_3 \\
a_8 & 0 & a_8 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 \\
0 & a_8 & a_7 & a_6 & a_5 & a_4 & a_3 & a_2 & a_1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}$$

4.2 Dickson trinomials

Now we assume that the field $\mathbb{F}_{2^n}$ is defined by a three-term irreducible Dickson trinomial P

$$P = 1 + \beta_k + \beta_n, \text{ with } k \leq n/2.$$

The elements in $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ are expressed in the Dickson basis $\mathcal{B} = \{\beta_1, \ldots, \beta_n\}$. Our aim is to express the product of two elements A, and B of $\mathbb{F}_{2^n}$ as Toeplitz or Hankel matrix vector product. We first have

$$C = AB = \underbrace{\left(\sum_{i,j=1}^{n} a_i b_j \beta_{i+j}\right)}_{S_1} + \underbrace{\left(\sum_{i,j=1}^{n} a_i b_j \beta_{|i-j|}\right)}_{S_2}$$

Similar to the previous subsection, here we express S_1 and S_2 as matrix vector product separately. Specifically

1. The sum S_1 is expressed as $Z_A \cdot B$ where Z_A is

$$Z_A = \begin{array}{c} \left[\begin{array}{ccccc} 0 & 0 & \cdots & 0 & 0 \\ a_1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ a_{n-1} & \cdots & \cdots & a_1 & 0 \\ a_n & \cdots & \cdots & a_2 & a_1 \\ 0 & a_n & \cdots & a_3 & a_1 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_n \end{array}\right] \end{array} \begin{array}{l} \leftarrow \beta_1 \\ \leftarrow \beta_2 \\ \vdots \\ \leftarrow \beta_n \\ \leftarrow \beta_{n+1} \\ \leftarrow \beta_{n+2} \\ \vdots \\ \leftarrow \beta_{2n} \end{array}$$

2. For S_2 we get the same expression to (6)

$$S_2 = \underbrace{\left(\sum_{k=1}^{n} \sum_{j=1}^{n-k} a_{j+k} b_j \beta_k\right)}_{S_{2,1}} + \underbrace{\left(\sum_{k=1}^{n} \sum_{j=k}^{n} a_{j-k} b_j \beta_k\right)}_{S_{2,2}}. \qquad (9)$$

where

$$S_2 = \left(\left[\begin{array}{cccccc} a_2 & a_3 & \cdots & a_{n-1} & a_n & 0 \\ a_3 & a_4 & \cdots & a_n & 0 & 0 \\ \vdots & & & & \vdots & \\ a_n & & & & 0 & 0 \\ 0 & & & & 0 & 0 \end{array}\right] \cdot + \left[\begin{array}{ccccc} 0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & 0 & a_1 & \cdots & a_{n-2} \\ \vdots & & & & \vdots \\ 0 & 0 & & & a_1 \\ 0 & & & & 0 \\ \vdots & & & & 0 \\ 0 & & & & 0 \end{array}\right] \right) \cdot \left[\begin{array}{c} b_1 \\ \vdots \\ b_n \end{array}\right] \qquad (10)$$

Now we replace S_1 and S_2 by their corresponding expressions given above in $AB = S_1 + S_2$. We get

$$\begin{aligned} AB \;=\; & \left(\begin{bmatrix} 0 & 0 & \cdots & 0 & 0 \\ a_1 & 0 & \cdots & 0 & 0 \\ \vdots & & & & \vdots \\ a_{n-1} & \cdots & \cdots & a_1 & 0 \\ a_n & \cdots & \cdots & a_2 & a_1 \\ 0 & a_n & \cdots & a_3 & a_1 \\ \vdots & & & & \vdots \\ 0 & 0 & \cdots & 0 & a_n \end{bmatrix} + \begin{bmatrix} 0 & a_1 & a_2 & \cdots & a_{n-1} \\ 0 & 0 & a_1 & \cdots & a_{n-2} \\ \vdots & & & & \vdots \\ 0 & & & & 0 \\ 0 & & & & 0 \\ 0 & & & & 0 \\ \vdots & & & & \vdots \\ 0 & & & & 0 \end{bmatrix} \right) \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \\ & + \begin{bmatrix} a_2 & a_3 & \cdots & a_{n-1} & a_n & 0 \\ a_3 & a_4 & \cdots & a_n & 0 & 0 \\ \vdots & & & & \vdots & \\ a_n & & & & 0 & 0 \\ 0 & & & & 0 & 0 \\ \vdots & & & & & \\ 0 & & & & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} b_1 \\ \vdots \\ b_n \end{bmatrix} \end{aligned} \tag{11}$$

In (11) the addition of two $2n \times n$ Toeplitz matrices results in one single $2n \times n$ Toeplitz matrix. The latter can be horizontally split into the middle to obtain two $n \times n$ Toeplitz matrices, say T_{up} and T_{down}, which can be then multiplied separately with vector $(b_1, \ldots, b_n)$ with a total cost of two $n \times n$ Toeplitz matrix vector products.

The other $2n \times n$ Hankel matrix in (11) has all zero in the lower n rows, contributing nothing to the cost of the matrix vector multiplication. Thus, the total computational cost of (11) is no more than three $n \times n$ Toeplitz or Hankel matrix-vector products.

Remark 1. *Among the above three matrices, two of them are triangular. One can attempt to reduce the cost of matrix vector product by using this triangular structure. For example, in the two way split strategy, we can perform $T \cdot V$ as*

$$T \cdot V = \begin{bmatrix} T_0 & T_1 \\ 0 & T_0 \end{bmatrix} \cdot \begin{bmatrix} V_0 \\ V_1 \end{bmatrix} = \begin{bmatrix} T_0V_0 + T_1V_1 \\ T_0V_1 \end{bmatrix}$$

Such an approach seems to be interesting since the recursive formula needs less computation than in Table 2. However our analysis shows that asymptotically the gain is negligible and the resulting dominant term remains the same as in Table 3.

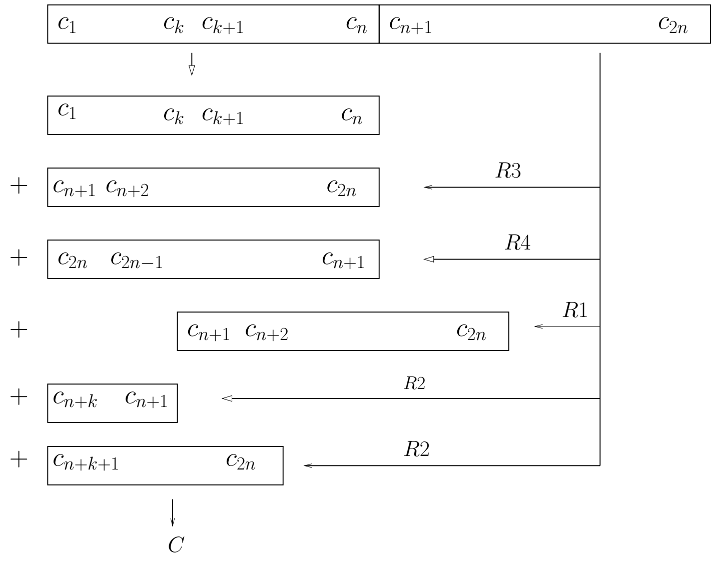
The reduction.

The resulting expression of C in (11) is an unreduced form of $A \times B$, since it has non zero coefficients c_i on rows $i = n + 1, \ldots, 2n$. It must be reduced modulo $P = \beta_n + \beta_k + 1$, to get an expression of C in $\mathcal{B}$. We have

$$\begin{aligned} \beta_i &= \beta_n\beta_{i-n} + \beta_{2n-i} \\ &= (\beta_k + 1)\beta_{i-n} + \beta_{2n-i} \\ &= \underbrace{\beta_{i-n+k}}_{(R1)} + \underbrace{\beta_{|i-n-k|}}_{(R2)} + \underbrace{\beta_{i-n}}_{(R3)} + \underbrace{\beta_{2n-i}}_{(R4)} \end{aligned}$$

In Figure 1 we give the reduction process obtained by replacing in $C = \sum_{i=1}^{2n} c_i\beta_i$ each β_i for $i > n$ by the expression given above.

Figure 1: Dickson Trinomial Reduction Process


c_1 c_k c_{k+1} c_n c_{n+1} c_{2n}
c_1 c_k c_{k+1} c_n
+ c_{n+1} c_{n+2} c_{2n}
$R3$
+ c_{2n} c_{2n-1} c_{n+1}
$R4$
+ c_{n+1} c_{n+2} c_{2n}
$R1$
+ c_{n+k} c_{n+1}
$R2$
+ c_{n+k+1} c_{2n}
$R2$
C

The process depicted in Figure 1 must be performed two times to get C expressed in the Dickson basis $\mathcal{B}$, since $k \leq n/2$. The full reducing part requires $8n$ XOR gates and is performed in time $6T_X$.

5 Complexity and Comparison

In this section we provide the corresponding complexity of each of our multipliers presented in the previous section. The complexity are easily deduced from complexity given in Table 2.

In a recent paper Mullin *et al.* [6] pointed out that there were some links between the Dickson basis and the normal basis. In practice, a Dickson basis is interesting when no optimal normal basis exists for the considered field. This is the case for NIST recommended binary fields $\mathbb{F}_{2^{163}}$ and $\mathbb{F}_{2^{283}}$.

In Table 5 we give fields which can be constructed with a Dickson binomial. In Table 6 we give irreducible Dickson trinomials of low degree. We can remark that NIST fields can be constructed with Dickson trinomials, and thus we obtain a subquadratic multiplier in each of these cases.

We also note that recently a type II optimal normal basis has been proposed in [2] using the FFT technique, which normally outperforms other sub-quadratic complexity multipliers for very large values of n. Hardware architectures of *bit-serial* type multipliers using the Dickson basis have been presented in [7].

Table 4: Complexity of Dickson Multiplier

Method	b	Space		Time
		# AND	# XOR	
Dick. Bin.	2	$2n^{\log_2(3)}$	$11n^{\log_2(3)} - 11n$	$(2\log_2(n) + 1)T_X + T_A$
	3	$2n^{\log_3(6)}$	$48/5n^{\log_3(6)} - 11n + 3/5$	$(3\log_3(n) + 1)T_X + T_A$
Dick. Tri.	2	$2n^{\log_2(3)}$	$11n^{\log_2(3)} - 4n + 1$	$(2\log_2(n) + 6)T_X + T_A$
	3	$2n^{\log_3(6)}$	$48/5n^{\log_3(6)} - 2n + 1/5$	$(3\log_3(n) + 6)T_X + T_A$
ONB I [3]	2	$n^{\log_2(3)} + n$	$5.5n^{\log_2(3)} - 4n - 0.5$	$(2\log_2(n) + 1)T_X + T_A$
	3	$n^{\log_3(6)} + n$	$24/5n^{\log_3(6)} - 3n - 4/5$	$(3\log_3(n) + 1)T_X + T_A$
ONB II [3]	2	$2n^{\log_2(3)}$	$11n^{\log_2(3)} - 12n + 1$	$(2\log_2(n) + 1)T_X + T_A$
	3	$2n^{\log_3(6)}$	$48/5n^{\log_3(6)} - 10n - 2/5$	$(3\log_3(n) + 1)T_X + T_A$

6 Conclusion

In this paper we have presented new parallel multipliers based on Dickson basis representation of binary fields. The multiplier for an irreducible Dickson binomial has a complexity similar to subquadratic multiplier for ONB II. For an irreducible Dickson trinomial, the multiplier has a slightly more space complexity, but can be used for fields with degree less than 300.

References

[1] L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group. *Ann. of Math.*, 11:161–183, 1883.

[2] P. Giorgi, C. Negre and T. Plantard. Subquadratic Binary Field Multiplier in Double Polynomial System. In proceedings of *SECRYPT*, 2007.

[3] H. Fan and M. A. Hasan. A new approach to sub-quadratic space complexity parallel multipliers for extended binary fields. *IEEE Trans. Computers*, 56(2):224–233, 2007.

[4] H. Fan and M. A. Hasan. Subquadratic computational complexity schemes for extended binary field multiplication using optimal normal bases. *IEEE Trans. Computers*, 56(10):1436-1437,2007.

[5] R. Lild, G. L. Mullen, and G. Turnwald. *Dickson Polynomials*, volume 65. Pitman Monograph and Survey in Pure and Applied Mathematics, 1993.

[6] R. C. Mullin and A. Mahalanobis. Dickson bases and finite fields. Technical report, University of Waterloo, Ontario, 2005.

[7] B. Ansari and M. Anwar Hasan Revisiting Finite Field Multiplication Using Dickson Bases Technical report, University of Waterloo, Ontario, 2007.

A Binomials and trinomials for field definition

In Table 5 we give the degree $n \in [160, 300]$ of field $\mathbb{F}_{2^n} = \mathbb{F}_2[X]/(P)$ where P satisfies

$$P \times (X + 1) = \beta_{n+1} + 1,$$

β_{n+1} is a Dickson polynomial. For such field, binomial subquadratic multiplier can be used to perform the multiplication.

Table 5: Degrees of fields which admit a binomial subquadratic multiplier

n	$167, 173, 198, 196, 190, 198, 238, 252, 262, 268, 270$

Table 6: Irreducible Dickson trinomials $\beta_n + \beta_k + 1$

n	k
163	43, 67, 97, 100, 128, 155
165	66, 78, 114, 132
167	68, 88
170	5, 11, 25, 55, 61, 71, 125, 155, 157
171	144
172	95
173	40, 82, 85
175	26, 158
176	79, 89
178	65, 73
179	85
181	35, 115, 134
183	138
184	151
187	28, 32, 95, 115, 128, 163
188	73
189	54
191	14, 74, 106, 124, 146
193	188
194	25, 55
197	88, 107, 110, 155, 170
199	86
200	7, 17, 31, 77
201	84
202	7, 187
203	5, 107, 113
205	43, 53, 109, 169, 179, 193
207	18, 180
208	7, 125
211	19, 85, 95
212	73
215	22, 64, 98, 122, 166
218	113, 127, 133, 137
219	120, 156
220	167
221	14, 46, 71, 145, 200, 209
223	82, 190
224	101
225	36, 72, 144
226	121, 205
227	125, 145
229	50
231	30, 114, 156
235	13, 17, 32, 37, 88, 103, 112, 128, 173
237	42
239	124, 164, 220
241	16, 160, 176, 200
242	85, 223
244	121, 169
245	37, 43, 52, 61, 116, 172, 187
247	22, 50, 110, 245
248	65, 137
250	25, 85, 125, 155, 175, 181, 185, 209, 217, 245
251	119, 145, 211
253	7, 10, 23, 115, 142, 158, 170, 205
255	174, 186
256	91, 209
259	5, 20
259	160
260	97
261	234
263	20, 98, 178
265	112
268	25
269	34, 49, 125, 140, 146, 190, 254
271	46
272	7, 235, 245
273	240
274	65, 101, 181, 205, 269
275	44, 59, 88, 176, 227
277	70, 95, 98, 118, 125, 130, 175
279	90, 234
280	17, 103, 173, 197
283	37, 80, 145, 155, 157, 215, 95
285	42, 132
285	246
289	40, 280
290	41, 53, 79, 85, 113, 125, 163, 185
291	24, 25
292	133, 265
293	17, 55, 82, 100, 140, 227, 233, 262, 275, 278
295	46, 62, 154, 254
296	65, 221
298	35, 97
299	119, 145