Low Complexity MDS Matrices Using GF(2^n) SPB or GPB

Xinggu Chen and Haining Fan

Abstract

While GF(2^n) polynomial bases are widely used in symmetric-key components, e.g. MDS matrices, we show that even low time/space complexities can be achieved by using GF(2^n) shifted polynomial bases (SPB) or generalized polynomial bases (GPB).

Index Terms

Finite field, multiplication, polynomial basis, diffusion matrix, MDS matrix.

I. Introduction

Binary extension fields GF(2^n)s of small sizes play an important role in symmetric-key cryptography. Maximum distance separable (MDS) matrices with special properties are often used to construct linear diffusion layers, for example, the MixColumns operation of AES adopts a circulant MDS matrix over GF(2^8). Much work has been put into building efficient MDS matrices [1] [2]. A detailed survey can be found in, e.g., [3].

The overall performance of a cryptographic system is primarily determined by the efficiency of basic arithmetic operations in the underlying finite field. Compared to the low-cost addition operation, GF(2^n) multiplication has received much attention in recent years [4] [5]. The representation of the field element plays a fundamental role in implementing the multiplication operation. For the purpose of efficient field arithmetic, a number of bases have been proposed in the literature, for example, polynomial, normal, dual, weakly dual, triangular and shifted polynomial bases. Most symmetric-key components use polynomial (or standard/canonical) bases (PB) $M := \{1, x, x^2, \cdots, x^{n-1}\}$ to represent GF(2^n) elements.

In this report, we show that even low time/space complexities can be achieved by using GF(2^n) shifted polynomial bases (SPB) [6] or generalized polynomial bases (GPB) [7]. We list experimental results in the next section and then introduce SPB/GPB and other details.

All the code used to run the search is available from “https://github.com/Singlecxg/SPB”.

Xinggu Chen and Haining Fan are with the Department of Computer Science and Technology, Tsinghua University, Beijing, China. E-mail: cxg15@mails.tsinghua.edu.cn, fhn@tsinghua.edu.cn

II. Comparison of 4×4 MDS matrices over GF(2^8)

We list our MDS matrices in Table I. The original data are listed in the appendix.

For different degree-8 irreduciable polynomials fs, we mainly considered the SPB $x^{-4}M$ in this work. We also tested SPB $x^{-3}M$ and $x^{-5}M$ for some fs, but the d-XOR [3] are not that small. We did not test other SPB. We computed s-XOR [3] for a small number of matrices listed in the appendix by hand. We also tested the type C.1 GPB in [7] ($f = 0x187$ and $R = x^6 + x^5 + 1$).

TABLE I
Comparison of 4×4 MDS matrices over GF(2^8)

f / R	Type	M M^{-1}	d-XOR	s-XOR	T_X Delay	Involutory	Ref.
$0x165$ / 1	Hadamard	$(0x01, 0x02, 0xb0, 0xb2)$	40	38	4	Yes	[1] [3]
$0x14d$ / x^{-4}	Hadamard	$(0x28, 0x08, 0x10, 0x20)$	40	34	4	Yes	Eq. (5)
$0x1c3$ / 1	Hadamard	$(0xe1, 0xe3, 0x01, 0x02)$	42	36	3	Yes	Eq. (11)
$0x1c3$ / x^{-4}	Hadamard	$(0x08, 0x28, 0x10, 0x20)$	42	36	3	Yes	Eq. (3)
$0x187$ $x^6 + x^5 + 1$	Hadamard	$(0x31, 0xf3, 0x61, 0xc2)$	42	35	3	Yes	Eq. (8)
$0x1c3$ / 1	Hadamard	$(0x01, 0x02, 0x04, 0x91)$ $(0x27, 0x4e, 0x9c, 0x79)$	37 141	35 76	3 5	No	[1] [3]
$0x187$ / x^{-4}	Hadamard	$(0x02, 0x08, 0x10, 0x20)$ $(0x05, 0x14, 0x28, 0x50)$	37 71	33 40	3 4	No	Eq. (12)
$0x1c3$ / 1	Hadamard	$(0x04, 0x05, 0x01, 0x02)$ $(0x01, 0x90, 0x91, 0xe1)$	43 43	37 38	3 3	No	Eq. (10)
$0x11d$ / x^{-4}	Hadamard	$(0x80, 0x08, 0x10, 0x20)$ $(0x40, 0x04, 0x08, 0x10)$	39 39	34 34	3 3	No	Eq. (4)
$0x187$ $x^6 + x^5 + 1$	Hadamard	$(0x03, 0x62, 0x61, 0xc2)$ $(0x61, 0xdb, 0xba, 0xf3)$	43 43	36 37	3 3	No	Eq. (7)
$0x11b$ / 1	Circulant	$(0x02, 0x03, 0x01, 0x01)$ $(0x0e, 0x0b, 0x0d, 0x09)$	38 110	36 77	3 5	No	AES [3]
$0x1c3$ / 1	Circulant	$(0x01, 0x01, 0x02, 0x91)$ $(0x55, 0x5a, 0x71, 0x41)$	32 109	31 75	3 4	No	[2] [3]
$0x1c3$ / 1	Circulant	$(0x01, 0x01, 0x02, 0x91)$ $(0x55, 0x5a, 0x71, 0x41)$	32 109	29 69	3 4	No	Eq. (9)
$0x187$ / x^{-4}	Circulant	$(0x40, 0x08, 0x10, 0x10)$ $(0xa9, 0xb7, 0xb2, 0x70)$	32 109	29 68	3 4	No	Eq. (1)
$0x18b$ / x^{-4}	Circulant	$(0x18, 0x08, 0x10, 0x10)$ $(0x12, 0x16, 0x1a, 0x0e)$	36 88	34 60	3 4	No	Eq. (2)
$0x187$ $x^6 + x^5 + 1$	Circulant	$(0x03, 0xf3, 0x61, 0x61)$ $(0xda, 0xaf, 0xf8, 0xa0)$	32 109	29 68	3 4	No	Eq. (6)

III. shifted polynomial basas

We use GF(2^3) PB and SPB multipliers to show advantage of SPB over PB,

A. An example

Let x be a root of $f(u) = u^3+u+1$, which is irreducible on GF(2), and GF(2^3) $:= GF(2)[u]/(f(u))$. Given two GF(2^3) elements $A = a_2x^2 + a_1x + a_0$ and $B = b_2x^2 + b_1x + b_0$ represented in PB $M = \{1, x, x^2\}$, their PB product $C = AB$ in GF(2^3) is defined as

$$\begin{aligned} C &= c_2x^2 + c_1x + c_0 = AB \bmod f(x) \\ &= (b_2a_2)x^4 + (b_2a_1 + b_1a_2)x^3 + (b_2a_0 + b_0a_2 + b_1a_1)x^2 + (b_1a_0 + b_0a_1)x + (b_0a_0) \bmod f(x) \\ &= [b_2a_0 + b_1a_1 + (b_0 + b_2)a_2]x^2 + [b_1a_0 + (b_0 + b_2)a_1 + (b_1 + b_2)a_2]x + b_0a_0 + b_2a_1 + b_1a_2. \end{aligned}$$

Or in the matrix form:

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} b_0 & b_2 & b_1 \\ b_1 & b_0 + b_2 & b_1 + b_2 \\ b_2 & b_1 & b_0 + b_2 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}.$$

The above GF(2^3) PB multiplication operation can be implemented as a bit parallel multiplier. In general, such a parallel $GF(2^n)$ multipliers are typically evaluated according to their space and time complexities. Because a 2-input XOR (respectively AND) gate can be used to realize an addition (respectively multiplication) operation in the ground field GF(2), the space complexity of $GF(2^n)$ parallel multipliers is often measured by the total numbers of 2-input XOR and AND gates used, and the corresponding time complexity is given in terms of the maximum delay faced by a signal due to these gates. Symbols T_A and T_X are often used to represent the delays of one 2-input AND gate and one 2-input XOR gate, respectively.

It is easy to see that we need 3 2-input XOR gate delays, or $3T_X$, to compute

$$c_1 = b_1a_0 + (b_0 + b_2)a_1 + (b_1 + b_2)a_2.$$

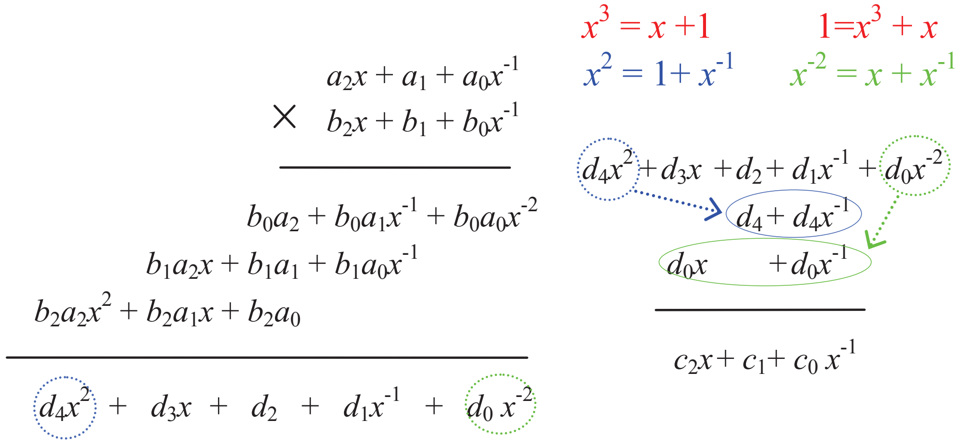
Therefore, the time complexity of this GF(2^3) PB parallel multiplier is $T_A + 3T_X$. In the following, we show that the time complexity of its SPB counterpart is only $T_A + 2T_X$.

We first introduce the SPB representation.

Let x be a root of $f(u)$ and GF(2^n) $:= GF(2)[u]/(f(u))$. A shifted polynomial basis of GF(2^n) over GF(2) is defined as follows [6]:

Definition 1: Let v be an integer, $R = x^{-v}$ and the ordered set $M = \{x^i | 0 \leq i \leq n-1\}$ be a polynomial basis of GF(2^n) over GF(2). The ordered set $R \cdot M := \{x^{i-v} | 0 \leq i \leq n-1\}$ is called a shifted polynomial basis with respect to M.

For the above example, $M = \{1, x, x^2\}$ is a PB of GF(2^3) over GF(2). We define $x^{-1}M = \{x^{-1}, 1, x\} = \{x^2 + 1, 1, x\}$ as an SPB of GF(2^3) over GF(2). To obtain the SPB product $C = c_2x + c_1 + c_0x^{-1}$ of $A = a_2x + a_1 + a_0x^{-1}$ and $B = b_2x + b_1 + b_0x^{-1}$, the SPB reduction operation is performed as follows:


x^3 = x + 1
1 = x^3 + x
x^2 = 1 + x^-1
x^-2 = x + x^-1
a_2x + a_1 + a_0x^-1
× b_2x + b_1 + b_0x^-1
b_0a_2 + b_0a_1x^-1 + b_0a_0x^-2
b_1a_2x + b_1a_1 + b_1a_0x^-1
b_2a_2x^2 + b_2a_1x + b_2a_0
d_4x^2 + d_3x + d_2 + d_1x^-1 + d_0 x^-2
d_4x^2 + d_3x + d_2 + d_1x^-1 + d_0x^-2
d_4 + d_4x^-1
d_0x + d_0x^-1
c_2x + c_1 + c_0 x^-1

And then we have

$$\begin{pmatrix} c_0 \\ c_1 \\ c_2 \end{pmatrix} = \begin{pmatrix} b_0+b_1 & b_0 & b_2 \\ b_2 & b_1 & b_0+b_2 \\ b_0 & b_2 & b_1 \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ a_2 \end{pmatrix}.$$

Therefore, the coordinate formulae of $C = (c_0, c_1, c_2)^T$ are

$$\begin{aligned} c_0 &= [(b_0+b_1)a_0] + [b_0a_1 + b_2a_2], \\ c_1 &= [b_2a_0 + b_1a_1] + [(b_0+b_2)a_2], \\ c_2 &= b_0a_0 + b_2a_1 + b_1a_2. \end{aligned}$$

Terms in square brackets are computed in parallel. Therefore, the time complexity of this GF(2^3) SPB parallel multiplier is $T_A + 2T_X$. While this value is $T_A + 3T_X$ in the above PB multiplier.

B. Three reduction methods

Montgomery first introduced his reduction algorithm in the integer framework [8]. Brent and Zimmermann pointed out that Montgomery's N-*residue* is just the remainder of Hensel's division [9]. Fan et al. showed that the polynomial N-*residue* is just the generalized remainder of a modulo f defined in the following generalized division algorithm [10]:

Theorem 1: Let F be a field, and $f, a, R \in F[u]$ be polynomials with $deg(f) > 0$. Let R^{-1} be the multiplicative inverse of R module f. Then there exist unique polynomials q and r in $F[u]$ with $0 \leq \deg(r) < deg(f)$ such that $a = f \cdot q + R^{-1} \cdot r$. Here, r is called the generalized remainder of a modulo f, and it is equal to $(aR \bmod f)$.

While the classical reduction scheme cancels the most significant half and the original Montgomery reduction the least significant half, the SPB multiplication performs the reduction operation from both ends. This is a typical application of the balancing principle of algorithm design. The following Fig. 1 illustrates the merit of SPB.

Because of the above symmetric reduction operations, the gate delay of an SPB multiplier is reduced. In 2013, SPB was generalized to GPB [7]:

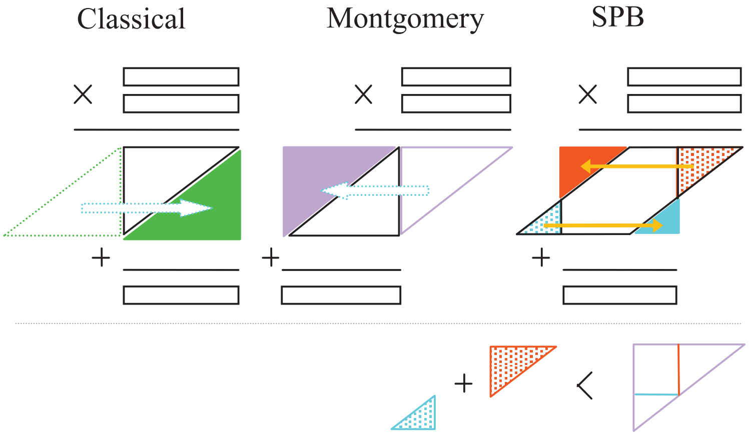


Fig. 1. Three modular reduction algorithms

Definition 2: Let $R \in GF(2^n)^*$ and the ordered set $M = \{x^i | 0 \leq i \leq n-1\}$ be a polynomial basis of GF(2^n) over GF(2). The ordered set $R \cdot M := \{Rx^i | 0 \leq i \leq n-1\}$ is called a Generalized Polynomial Basis with respect to M.

Both $N\text{-}residue$ and SPB/GPB can be traced technically back to the above generalized remainder in Theorem 1.

Finally, we list in Table II gate delays of some multipliers based on the irreducible trinomial $u^n + u^k + 1$, where $2 < 2k < n$. The AND and XOR gate complexities of these multipliers are the same, namely, n^2 and $(n^2 - 1)$ respectively. For irreducible pentanomials, complexity results can be found in [7].

TABLE II
COMPARISONS OF GATE DELAYS FOR $(u^n + u^k + 1)$-BASED MULTIPLIERS $(2 < 2k < n)$

Multiplier	Gate delay
PB Mastrovito [11] [12] [13]	$T_A + \lceil \log_2 4n \rceil T_X$
PB mod reduction [14] [15]	$T_A + \lceil \log_2 (4n-4) \rceil T_X$
PB Montgomery [16]	$\leq T_A + \lceil \log_2 (4n-8) \rceil T_X$
PB Mastrovito [17]	$T_A + \lceil \log_2 (2n+2k-3) \rceil T_X$
SPB Mastrovito [6]	$T_A + \lceil \log_2 2n \rceil T_X$
SPB binary XOR tree [18]	$T_A + \lceil \log_2 (2n-k) \rceil T_X$

IV. 4×4 MDS MATRICES ON GF(2^8)

A. *Complexities of AES's 4×4 circulant MDS matrices*

Let x be a root of $f(u) = u^8 + u^4 + u^3 + u + 1$, and GF$(2^8) := GF(2)[u]/(f(u))$. The AES MixColumns() computes the following matrix product

$$\begin{pmatrix} s'_{0,0} & s'_{0,1} & s'_{0,2} & s'_{0,3} \\ s'_{1,0} & s'_{1,1} & s'_{1,2} & s'_{1,3} \\ s'_{2,0} & s'_{2,1} & s'_{2,2} & s'_{2,3} \\ s'_{3,0} & s'_{3,1} & s'_{3,2} & s'_{3,3} \end{pmatrix} := \begin{pmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{pmatrix} \begin{pmatrix} s_{0,0} & s_{0,1} & s_{0,2} & s_{0,3} \\ s_{1,0} & s_{1,1} & s_{1,2} & s_{1,3} \\ s_{2,0} & s_{2,1} & s_{2,2} & s_{2,3} \\ s_{3,0} & s_{3,1} & s_{3,2} & s_{3,3} \end{pmatrix},$$

where 2 is $x \in GF(2^8)$ and 3 is $1 + x \in GF(2^8)$.

The inverse matrix of the above circulant MDS matrix is

$$\begin{pmatrix} 0x0e & 0x0b & 0x0d & 0x09 \\ 0x09 & 0x0e & 0x0b & 0x0d \\ 0x0d & 0x09 & 0x0e & 0x0b \\ 0x0b & 0x0d & 0x09 & 0x0e \end{pmatrix},$$

where $0x0e$ is $x + x^2 + X^3 \in GF(2^8)$, etc.

In the literature, the complexity of the AES MixColumns() is often measured by the inner product $(0x02, 0x03, 0x01, 0x01)(A, B, C, D)^T$, where $A = \sum_{j=0}^{7} a_i x^j, B = \sum_{j=0}^{7} b_i x^j, C = \sum_{j=0}^{7} c_i x^j$ and $D = \sum_{j=0}^{7} d_i x^j \in GF(2^8)$. The result of this inner product is

$$\begin{aligned} & (0x02, 0x03, 0x01, 0x01)(A, B, C, D)^T \\ = \quad & 1(d_0 + a_7 + b_0 + b_7 + c_0) \\ + \quad & x(d_1 + a_0 + a_7 + b_0 + b_1 + b_7 + c_1) \\ + \quad & x^2(d_2 + a_1 + b_1 + b_2 + c_2) \\ + \quad & x^3(d_3 + a_2 + a_7 + b_2 + b_3 + b_7 + c_3) \\ + \quad & x^4(d_4 + a_3 + a_7 + b_3 + b_4 + b_7 + c_4) \\ + \quad & x^5(d_5 + a_4 + b_4 + b_5 + c_5) \\ + \quad & x^6(d_6 + a_5 + b_5 + b_6 + c_6) \\ + \quad & x^7(d_7 + a_6 + b_6 + b_7 + c_7). \end{aligned}$$

A direct implementation of this inner product requires d-XOR=38 XOR gates. Therefore, the MixColumn requires $38 * 4 = 152$ XOR gates. Because coefficients of x, x^3 and x^4 are summations of 7 terms, the XOR gate delay of the MixColumn is $\lceil \log_2 7 \rceil = 3$, or $3T_X$.

The result of the inner product of the inverse matrix is

$$
\begin{aligned}
& (0x0e, 0x0b, 0x0d, 0x09)(A, B, C, D)^T \\
= \;& 1(d_0 + d_5 + a_5 + a_6 + a_7 + b_0 + b_5 + b_7 + c_0 + c_5 + c_6) \\
+ \;& x(d_1 + d_5 + d_6 + a_0 + a_5 + b_0 + b_1 + b_5 + b_6 + b_7 + c_1 + c_5 + c_7) \\
+ \;& x^2(d_2 + d_6 + d_7 + a_0 + a_1 + a_6 + b_1 + b_2 + b_6 + b_7 + c_0 + c_2 + c_6) \\
+ \;& x^3(d_0 + d_3 + d_5 + d_7 + a_0 + a_1 + a_2 + a_5 + a_6 + b_0 + b_2 + b_3 + b_5 + c_0 + c_1 + c_3 + c_5 + c_6 + c_7) \\
+ \;& x^4(d_1 + d_4 + d_5 + d_6 + a_1 + a_2 + a_3 + a_5 + b_1 + b_3 + b_4 + b_5 + b_6 + b_7 + c_1 + c_2 + c_4 + c_5 + c_7) \\
+ \;& x^5(d_2 + d_5 + d_6 + d_7 + a_2 + a_3 + a_4 + a_6 + b_2 + b_4 + b_5 + b_6 + b_7 + c_2 + c_3 + c_5 + c_6) \\
+ \;& x^6(d_3 + d_6 + d_7 + a_3 + a_4 + a_5 + a_7 + b_3 + b_5 + b_6 + b_7 + c_3 + c_4 + c_6 + c_7) \\
+ \;& x^7(d_4 + d_7 + a_4 + a_5 + a_6 + b_4 + b_6 + b_7 + c_4 + c_5 + c_7).
\end{aligned}
$$

A direct implementation of this inner product requires d-XOR=110 XOR gates. Therefore, the inverse MixColumn requires $110 * 4 = 440$ XOR gates. Because coefficients of x^3 and x^4 are summations of 19 terms, the XOR gate delay of the inverse MixColumn is $\lceil \log_2 19 \rceil T_X = 5T_X$.

B. *Complexities of* 4×4 *circulant MDS matrices using SPB on GF*(2^8)

We found some MDS circulant matrices with less XOR gates using SPB, for example, the following M for $f(u) = u^8 + u^7 + u^2 + u + 1$ $(0x187)$ and SPB $x^{-4}M := \{x^{i-4} | 0 \leq i \leq 7\}$.

$$
\begin{pmatrix}
0x40 & 0x08 & 0x10 & 0x10 \\
0x10 & 0x40 & 0x08 & 0x10 \\
0x10 & 0x10 & 0x40 & 0x08 \\
0x08 & 0x10 & 0x10 & 0x40
\end{pmatrix}, \tag{1}
$$

where $0x08$ is $x^{-1} \in GF(2^8)$.

The result of the inner product is

$$
\begin{aligned}
& (0x40, 0x08, 0x10, 0x10)(A, B, C, D)^T \\
= \;& 1(a_6 + a_7 + b_0 + b_1 + c_0 + d_0) \\
+ \;& x(a_6 + b_0 + b_2 + c_1 + d_1) \\
+ \;& x^2(a_0 + a_6 + b_3 + c_2 + d_2) \\
+ \;& x^3(a_1 + a_7 + b_4 + c_3 + d_3) \\
+ \;& x^4(a_2 + b_5 + c_4 + d_4) \\
+ \;& x^5(a_3 + b_6 + c_5 + d_5) \\
+ \;& x^6(a_4 + b_0 + b_7 + c_6 + d_6) \\
+ \;& x^7(a_5 + a_6 + b_0 + c_7 + d_7).
\end{aligned}
$$

A direct implementation of this inner product requires d-XOR=32 XOR gates. It can be reduced to s-XOR=29 after common subexpression elimination:

```
     a6 + a7 + b0 + b1 + c0 + d0
     a6 +      b0 + b2 + c1 + d1
a0 + a6 +           b3 + c2 + d2
a1 +      a7 +      b4 + c3 + d3
a2 +                b5 + c4 + d4
a3 +                b6 + c5 + d5
a4 +           b0 + b7 + c6 + d6
a5 + a6 + a7 + b0 +      c7 + d7

A=a6+b0, B=A+a7                    32 XORs

     B + b1 +      c0 + d0
     A + b2 +      c1 + d1
a0 + a6+ b3 +      c2 + d2
a1 + a7+ b4 +      c3 + d3
a2 +     b5 +      c4 + d4
a3 +     b6 +      c5 + d5
a4 +     b0 + b7 + c6 + d6
a5 + B +           c7 + d7         29 XORs
```

Because the longest coefficient is a summation of 7 terms (We add a 0 in B=A+a7=(a6+b0)+(a7+0).), the XOR gate delay of the matrix is $\lceil \log_2 6 \rceil T_X = 3T_X$.

The inverse of the above matrix is

$$\begin{pmatrix} 0xa9 & 0xb7 & 0xb2 & 0x70 \\ 0x70 & 0xa9 & 0xb7 & 0xb2 \\ 0xb2 & 0x70 & 0xa9 & 0xb7 \\ 0xb7 & 0xb2 & 0x70 & 0xa9 \end{pmatrix},$$

where $0x70$ is $x^2 + x + 1 \in GF(2^8)$.

This inverse needs 109 XOR gates, which can be reduced to s-XOR=68, and $4T_X$ delays.

We also found the other MDS Circulant matrix with a total of 94 XOR gates for $f(u) = u^8 + u^7 + u^3 + u + 1$ $(0x18b)$ and $x^{-4}M := \{x^{i-4} | 0 \leq i \leq 7\}$.

$$\begin{pmatrix} 0x18 & 0x08 & 0x10 & 0x10 \\ 0x10 & 0x18 & 0x08 & 0x10 \\ 0x10 & 0x10 & 0x18 & 0x08 \\ 0x08 & 0x10 & 0x10 & 0x18 \end{pmatrix}, \qquad (2)$$

where $0x08$ is $x^{-1} \in GF(2^8)$.

The result of the inner product is:

$$\begin{aligned}
& (0x18, 0x08, 0x10, 0x10)(A, B, C, D)^T \\
= \; & 1(a_1 + b_0 + b_1 + c_0 + d_0) \\
+ \; & x(a_1 + a_2 + b_2 + c_1 + d_1) \\
+ \; & x^2(a_0 + a_2 + a_3 + b_0 + b_3 + c_2 + d_2) \\
+ \; & x^3(a_3 + a_4 + b_4 + c_3 + d_3) \\
+ \; & x^4(a_4 + a_5 + b_5 + c_4 + d_4) \\
+ \; & x^5(a_5 + a_6 + b_6 + c_5 + d_5) \\
+ \; & x^6(a_0 + a_6 + a_7 + b_0 + b_7 + c_6 + d_6) \\
+ \; & x^7(a_0 + a_7 + b_0 + c_7 + d_7).
\end{aligned}$$

A direct implementation of this inner product requires 36 XOR gates. It will be reduced to 34 after common subexpression elimination:

```
     a1 +                           b0 + b1 + c0 + d0
     a1 + a2 +                           b2 + c1 + d1
a0 +      a2 + a3 +                +b0 + b3 + c2 + d2
               a3 + a4 +                 b4 + c3 + d3
                    a4 + a5 +            b5 + c4 + d4
                         a5 + a6+        b6 + c5 + d5
a0 +                          a6+a7+b0 + b7 + c6 + d6
a0 +                             a7+b0 +      c7 + d7     36 XORs

A=a0+b0

     a1 +                           b0 + b1 + c0 + d0
     a1 + a2 +                           b2 + c1 + d1
A +      a2 + a3 +                     + b3 + c2 + d2
               a3 + a4 +                 b4 + c3 + d3
                    a4 + a5 +            b5 + c4 + d4
                         a5 + a6+        b6 + c5 + d5
A +                          a6+a7     + b7 + c6 + d6
A +                             a7     +      c7 + d7     34 XORs
```

The XOR gate delay of the matrix is $\lceil \log_2 7 \rceil T_X = 3T_X$.

The inverse of the above matrix is

$$\begin{pmatrix} 0x12 & 0x16 & 0x1a & 0x0e \\ 0x0e & 0x12 & 0x16 & 0x1a \\ 0x1a & 0x0e & 0x12 & 0x16 \\ 0x16 & 0x1a & 0x0e & 0x12 \end{pmatrix},$$

where $0x12$ is $1 + x^{-3} \in GF(2^8)$.

The result of the inner product:

$$\begin{aligned}
& (0x12, 0x16, 0x1a, 0x0e)(A, B, C, D)^T \\
= \ & 1(a_0 + a_1 + a_2 + a_3 + b_3 + c_2 + c_3 + d_1 + d_3) \\
+ \ & x(a_0 + a_4 + b_3 + b_4 + c_0 + c_2 + c_4 + d_1 + d_2 + d_3 + d_4) \\
+ \ & x^2(a_0 + a_1 + a_5 + b_4 + b_5 + c_1 + c_3 + c_5 + d_0 + d_2 + d_3 + d_4 + d_5) \\
+ \ & x^3(a_3 + a_6 + b_3 + b_5 + b_6 + c_3 + c_4 + c_6 + d_4 + d_5 + d_6) \\
+ \ & x^4(a_0 + a_4 + a_7 + b_0 + b_4 + b_6 + b_7 + c_0 + c_4 + c_5 + c_7 + d_0 + d_5 + d_6 + d_7) \\
+ \ & x^5(a_1 + a_5 + b_0 + b_1 + b_5 + b_7 + c_1 + c_5 + c_6 + d_0 + d_1 + d_6 + d_7) \\
+ \ & x^6(a_2 + a_6 + b_1 + b_2 + b_6 + c_0 + c_2 + c_6 + c_7 + d_0 + d_1 + d_2 + d_7) \\
+ \ & x^7(a_0 + a_1 + a_2 + a_7 + b_2 + b_7 + c_1 + c_2 + c_7 + d_0 + d_2).
\end{aligned}$$

Similarly, the inverse needs 88 XOR gates, which can be reduced to 60:

```
         b3+                        a3+a2+a1+a0+      c2+c3+               d1+   d3
         b3+b4+                  a4+         a0+c0+   c2+   c4+            d1+d2+d3+d4
            b4+b5+            a5+         a1+a0+   c1+   c3+   c5+      d0+   d2+d3+d4+d5
         b3+   b5+b6+      a6+      a3+                  c3+c4+   c6+               d4+d5+d6
b0+         b4+   b6+b7+a7+      a4+         a0+c0+         c4+c5+   c7+d0+            d5+d6+d7
b0+b1+         b5+   b7+      a5+         a1+      c1+         c5+c6+   d0+d1+            d6+d7
   b1+b2+         b6+      a6+         a2+      c0+   c2+         c6+c7+d0+d1+d2+            d7
      b2+            b7+a7+            a2+a1+a0+   c1+c2+            c7+d0+   d2

A=a7+a0, B=a0+d3, C=c1+a1, D=c2+a2, G=a3+c3, H=a4+c4, I=a6+c6, E=c7+d0, F=d0+a5,
J=b4+d4, K=b5+d5, L=b6+d6, M=b7+d7, N=b0+c5, O=b2+d2, P=b1+d1, Q=b3+d1,
Z=D+E,   Y=M+N,   X=J+B,   W=H+c0,  V=C+F,   U=X+d2,  T=Z+O

                                     G+ D+a1+                               Q+    B
             U+                   W+                  c2+                   Q
             U+ K+                                       c3+   c5+       V
         b3+    K+ L+       I+       G+                     c4+                     d4
 Y+         b4+    L+    A+       W+                                  E+               d5
 Y+ P+         b5+                                                c6+    V+               d6
    P+ T+         b6+       I+                  c0+                                          d7
       T+            b7+ A+                         C
```

Because the longest coefficient (x^4) is a summation of 15 terms, the XOR gate delay of the matrix is $\lceil \log_2 15 \rceil \, T_X = 4T_X$.

Therefore, the matrix and its inverse needs $34 + 60 = 94$ XOR gates in total and $3 + 4 = 7T_X$ delays in total.

C. *Complexities of* 4×4 *Hadamard MDS matrices using SPB/GPB on GF*(2^8)

We found an involutory Hadamard matrix with less XOR gates and delays using $f(u) = u^8 + u^7 + u^6 + u + 1$ and SPB with $R = x^{-4}$.

$$\begin{pmatrix} 0x08 & 0x28 & 0x10 & 0x20 \\ 0x28 & 0x08 & 0x20 & 0x10 \\ 0x10 & 0x20 & 0x08 & 0x28 \\ 0x20 & 0x10 & 0x28 & 0x08 \end{pmatrix}, \tag{3}$$

where $0x10$ is $1 \in GF(2^8)$.

The result of the inner product is:

$$\begin{aligned}
& (0x08, 0x28, 0x10, 0x20)(A, B, C, D)^T \\
= \;& 1(a_0 + a_1 + b_0 + b_1 + b_7 + c_0 + d_7) \\
+ \;& x(a_2 + b_0 + b_2 + b_7 + c_1 + d_0 + d_7) \\
+ \;& x^2(a_3 + b_1 + b_3 + c_2 + d_1) \\
+ \;& x^3(a_4 + b_2 + b_4 + c_3 + d_2) \\
+ \;& x^4(a_5 + b_3 + b_5 + c_4 + d_3) \\
+ \;& x^5(a_0 + a_6 + b_0 + b_4 + b_6 + c_5 + d_4) \\
+ \;& x^6(a_0 + a_7 + b_0 + b_5 + c_6 + d_5 + d_7) \\
+ \;& x^7(a_0 + b_0 + b_6 + b_7 + c_7 + d_6 + d_7).
\end{aligned}$$

A direct implementation of this inner product requires 42 XOR gates. It can be reduced to 36 after common subexpression elimination:

```
a0 + a1 + b0 + b1+                b7 + c0 +      d7
     a2 + b0 +    b2+             b7 + c1 + d0 + d7
     a3 +      b1+   b3+               c2 + d1
     a4 +         b2+   b4+            c3 + d2
     a5 +            b3+   b5+         c4 + d3
a0 + a6 + b0 +          b4+   b6+      c5 + d4
a0 + a7 + b0 +             b5+         c6 + d5 + d7
a0 +      b0 +                b6+ b7 + c7 + d6 + d7   42 XORs

A=a0+b0, B=b7+d7, C=A+b6

A +     a1 +     b1+             B + c0
        a2 + b0 +   b2+          B + c1 + d0
        a3 +     b1+   b3+           c2 + d1
        a4 +        b2+   b4+        c3 + d2
        a5 +           b3+   b5+     c4 + d3
    C + a6 +              b4+        c5 + d4
A +     a7 +                 b5+     c6 + d5 + d7
    C +                          B + c7 + d6          36 XORs
```

The XOR gate delay of the matrix is $\lceil \log_2 7 \rceil T_X = 3T_X$.

We even found an involutory Hadamard matrix with only 35 s-XORs and $3T_X$ delays using $f(u) = u^8 + u^7 + u^2 + u + 1$ and GPB with $R = x^6 + x^5 + 1$, See Eq. (8).

And we found a non-involutory Hadamard matrix and its inverse matrix with a total of $34 + 34 = 68$ XOR gates and $3T_X$ using $f(u) = u^8 + u^4 + u^3 + u^2 + 1$ and SPB $R = x^{-4}$.

$$\begin{pmatrix} 0x80 & 0x08 & 0x10 & 0x20 \\ 0x08 & 0x80 & 0x20 & 0x10 \\ 0x10 & 0x20 & 0x80 & 0x08 \\ 0x20 & 0x10 & 0x08 & 0x80 \end{pmatrix}, \tag{4}$$

where $0x10$ is $1 \in GF(2^8)$.

The result of the inner product is

$$\begin{aligned}
& (0x80, 0x08, 0x10, 0x20)(A, B, C, D)^T \\
= \;& 1(a_5 + b_1 + c_0 + d_7) \\
+ \;& x(a_6 + b_0 + b_2 + c_1 + d_0) \\
+ \;& x^2(a_5 + a_7 + b_0 + b_3 + c_2 + d_1 + d_7) \\
+ \;& x^3(a_0 + a_5 + a_6 + b_0 + b_4 + c_3 + d_2 + d_7) \\
+ \;& x^4(a_1 + a_5 + a_6 + a_7 + b_5 + c_4 + d_3 + d_7) \\
+ \;& x^5(a_2 + a_6 + b_7 + b_6 + c_5 + d_4) \\
+ \;& x^6(a_3 + a_7 + b_7 + c_6 + d_5) \\
+ \;& x^7(a_4 + b_0 + c_7 + d_6).
\end{aligned}$$

A direct implementation of this inner product requires 39 XOR gates. It can be reduced to 34 after common subexpression elimination:

```
     a5 +                b1 + c0 +      d7
          a6 +      b0 + b2 + c1 + d0
     a5 +      a7 + b0 + b3 + c2 + d1 + d7
a0 + a5 + a6 +      b0 + b4 + c3 + d2 + d7
a1 + a5 + a6 + a7 +      b5 + c4 + d3 + d7
a2 +      a6 + a7 +      b6 + c5 + d4
a3 +           a7 +      b7 + c6 + d5
a4 +                b0 +      c7 + d6        39 XORs

A=a5+d7, B=a6+b0, C=a6+a7

     A +              b1 +      c0
         B +          b2 +      c1 + d0
     A +         a7 + b0 + b3 + c2 + d1
a0 + A + B +          b4 +      c3 + d2
a1 + A +     C +      b5 +      c4 + d3
a2 +         C +      b6 +      c5 + d4
a3 +             a7 + b7 +      c6 + d5
a4 +                  b0 +      c7 + d6      34 XORs
```

The XOR gate delay of the matrix is $\lceil \log_2 8 \rceil T_X = 3T_X$.

The inverse of the above matrix is

$$\begin{pmatrix} 0x40 & 0x04 & 0x08 & 0x10 \\ 0x04 & 0x40 & 0x10 & 0x08 \\ 0x08 & 0x10 & 0x40 & 0x04 \\ 0x10 & 0x08 & 0x04 & 0x40 \end{pmatrix},$$

where $0x04$ is $x^{-2} \in GF(2^8)$.

```
                  a6+   b0+   b2+                  c1+d0
                     a7+b0+b1+   b3+            c0+   c2+d1
a0+               a6+   b0+b1+      b4+         c0+      c3+d2
```

```
a1+            a6+a7+   b1+         b5+      c0+         c4+d3
   a2+         a6+a7+                  b6+                  c5+d4
      a3+         a7+                     b7+                  c6+d5
         a4+         b0+                                          c7+d6
            a5+         b1+                  c0+                        d7

                  (a6 + b0) + b2 + c1 + d0
             a7 + b0 + (b1 + c0) + b3 + c2 + d1
          a0 + (a6 + b0) + (b1 + c0) + b4 + c3 + d2
          a1 + (a6 + a7) + (b1 + c0) + b5 + c4 + d3
               a2 + (a6 + a7) + b6 + c5 + d4
                  a3 + a7 + b7 + c6 + d5
                    a4 + b0 + c7 + d6
                    a5 + (b1 + c0) + d7
```

The inverse needs $3T_X$ delays and 39 XOR gates, which can be reduced to 34.

D. Some Matrix Pairs

Finally, we note that products of the following matrix pairs, which are represented in SPB with $R = x^{-4}$, are 4×4 identity matrix I_4 over the polynomial ring GF(2)$[x]$:

circulant: AES's (0x20, 0x30, 0x10, 0x10) and (0xe0, 0xb0, 0xd0, 0x90), (0x18, 0x08, 0x10, 0x10) and (0x12, 0x16, 0x1a, 0x0e);

Hadamard: (0x28, 0x08, 0x10, 0x20) and (0x28, 0x08, 0x10, 0x20), (0x08, 0x28, 0x10, 0x20) and (0x08, 0x28, 0x10, 0x20), (0x18, 0x08, 0x10, 0x20) and (0x06, 0x02, 0x04, 0x08), (0x30, 0x08, 0x10, 0x20) and (0xc0, 0x20, 0x40, 0x80) etc.

V. Conclusion

他山之石，可以攻玉。

Stones from other hills may serve to polish the jade of this one.

References

[1] S. M. Sim, K. Khoo, F. Oggier, and T. Peyrin, "Lightweight mds involution matrices," in *Fast Software Encryption*, G. Leander, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2015, pp. 471–493.

[2] M. Liu and S. M. Sim, "Lightweight mds generalized circulant matrices," in *Fast Software Encryption*, T. Peyrin, Ed. Berlin, Heidelberg: Springer Berlin Heidelberg, 2016, pp. 101–120.

[3] J. Jean, T. Peyrin, S. Sim, and J. Tourteaux, "Optimizing implementations of lightweight building blocks," *IACR Transactions on Symmetric Cryptology*, vol. 4, pp. 130–168, 2017.

[4] G. L. Mullen and D. Panario, *Handbook of Finite Fields*. CRC Press, 2013.

[5] H. Fan and M. A. Hasan, "A survey of some recent bit-parallel $GF(2^n)$ multipliers," *Finite Fields and Their Applications*, vol. 32, pp. 5–43, March 2015.

[6] H. Fan and Y. Dai, "Fast bit-parallel $GF(2^n)$ multiplier for all trinomials," *IEEE Transactions on Computers*, vol. 54, no. 4, pp. 485–490, 2005.

[7] A. Cilardo, "Fast parallel $GF(2^m)$ polynomial multiplication for all degrees," *IEEE Transactions on Computers*, vol. 62, no. 5, pp. 929–943, 2013.

[8] P. L. Montgomery, “Modular multiplication without trial division,” *Mathematics of Computation*, vol. 44, no. 170, pp. 519–521, 1985.

[9] R. P. Brent and P. Zimmermann, *Modern Computer Arithmetic*. Cambridge Univ. Press, 2010.

[10] H. Fan, J. Sun, M. Gu, and K. Lam, “Obtaining more Karatsuba-like formulae over the binary field,” *IET Information Security*, vol. 6, no. 1, pp. 14–19, 2012.

[11] E. Mastrovito, “VLSI designs for multiplication over finite fields $GF(2^m)$,” *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, pp. 297–309, 1988.

[12] B. Sunar and Ç. K. Koç, “Mastrovito multiplier for all trinomials,” *IEEE Transactions on Computers*, pp. 522–527, 1999.

[13] T. Zhang and K. K. Parhi, “Systematic design of original and modified Mastrovito multipliers for general irreducible polynomials,” *IEEE Transactions on Computers*, vol. 50, no. 7, pp. 734–748, 2001.

[14] H. Wu, “Bit-parallel finite field multiplier and squarer using polynomial basis,” *IEEE Transactions on Computers*, vol. 51, no. 7, pp. 750–758, 2002.

[15] A. Reyhani-Masoleh and M. A. Hasan, “Low complexity bit parallel architectures for polynomial basis multiplication over $GF(2^m)$,” *IEEE Transactions on Computers*, vol. 53, no. 8, pp. 945–959, Aug. 2004.

[16] H. Wu, “Montgomery multiplier and squarer for a class of finite fields,” *IEEE Transactions on Computers*, vol. 51, no. 5, pp. 521–529, 2002.

[17] N. Petra, D. D. Caro, and A. G. Strollo, “A novel architecture for Galois fields $GF(2^m)$ multipliers based on Mastrovito scheme,” *IEEE Transactions on Computers*, vol. 56, no. 11, pp. 1470–1483, 2007.

[18] H. Fan and M. A. Hasan, “Fast bit parallel-shifted polynomial basis multipliers in $GF(2^n)$,” *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 53, no. 12, pp. 2606–2615, 2006.

Appendix A
Some M and M^{-1} with a total of T_X less than 8

Complexities of M and M^{-1} are listed as :

M, d-XOR of M, T_X of M, M^{-1}, d-XOR of M^{-1}, T_X of M^{-1}, Total d-XOR, Total T_x,

where “d-XOR of M”, e.g., 172 and 312 in the first line, is the number of XOR gates used to computed the matrix-vector product, not the inner-product.

Only matrices with a total of $7T_X$ or less are listed.

A. Circulant Matrices, SPB, $R = x^{-4}$

1) GF$(2^8)/0x11b$:

```
(4c 08 10 10) 172 3  (20 07 40 85) 312 4  484 7
(20 a4 10 10) 192 3  (f0 18 10 26) 300 4  492 7
(40 13 10 10) 180 3  (08 3b 4e 26) 336 4  516 7
(40 02 10 10) 160 3  (68 6d 84 26) 408 4  568 7
(20 9d 10 10) 196 3  (5e 63 10 50) 376 4  572 7
(20 03 10 10) 160 3  (43 68 62 01) 420 4  580 7
(16 08 10 10) 160 3  (ae 2c 12 ea) 432 4  592 7
(20 36 10 10) 172 3  (04 31 74 96) 420 4  592 7
```

2) GF$(2^8)/0x11d$:

```
(40 88 10 10) 168 3  (84 10 12 44) 260 4  428 7
(20 86 10 10) 184 3  (4d 14 20 24) 272 4  456 7
(30 04 10 10) 164 3  (1d 44 40 cc) 312 4  476 7
(30 11 10 10) 208 3  (04 3a 87 8a) 336 4  544 7
(04 32 10 10) 188 3  (2a 04 4f 72) 372 4  560 7
(40 22 10 10) 180 3  (11 ec 40 5a) 396 4  576 7
(19 08 10 10) 180 3  (28 11 e8 b2) 400 4  580 7
(5d 08 10 10) 180 3  (c9 41 19 8e) 408 4  588 7
```

3) $GF(2^8)/0x12b$*:*

```
(d6 08 10 10) 180 3  (d4 03 02 10) 300 4  480 7
(20 84 10 10) 172 3  (5e 80 4b 44) 384 4  556 7
(6b 08 10 10) 176 3  (7b 4d eb 20) 412 4  588 7
(b0 08 10 10) 180 3  (2f 80 46 c3) 408 4  588 7
(40 6b 10 10) 188 3  (82 cf 20 6c) 404 4  592 7
```

4) $GF(2^8)/0x12d$*:*

```
(04 28 10 10) 168 3  (5a 2a 18 1d) 360 4  528 7
(40 28 10 10) 168 3  (ab 10 fc 04) 364 4  532 7
(80 04 10 10) 156 3  (40 de 5d 53) 436 4  592 7
(2d 02 10 10) 180 3  (b4 1d f9 84) 412 4  592 7
```

5) $GF(2^8)/0x139$*:*

```
(40 09 10 10) 168 3  (62 88 30 72) 324 4  492 7
(19 04 10 10) 168 3  (9c 18 22 8c) 324 4  492 7
(20 26 10 10) 188 3  (40 d2 1c 19) 324 4  512 7
(c8 08 10 10) 188 3  (09 70 96 04) 324 4  512 7
(40 8c 10 10) 184 3  (96 29 50 52) 336 4  520 7
(62 04 10 10) 184 3  (94 14 11 d2) 336 4  520 7
(20 4b 10 10) 176 3  (3c 53 10 12) 356 4  532 7
(9d 08 10 10) 176 3  (90 10 ad 78) 356 4  532 7
(40 12 10 10) 164 3  (31 86 03 79) 380 4  544 7
(90 04 10 10) 164 3  (05 b9 c2 21) 380 4  544 7
(20 95 10 10) 196 3  (90 33 af 10) 364 4  560 7
(6b 08 10 10) 196 3  (10 d3 a1 12) 364 4  560 7
(06 31 10 10) 212 3  (10 ce 54 01) 360 4  572 7
(c0 21 10 10) 212 3  (10 e6 54 39) 360 4  572 7
(44 04 10 10) 168 3  (79 c2 32 8d) 408 4  576 7
(40 08 10 10) 132 3  (57 90 c5 40) 444 4  576 7
(40 44 10 10) 168 3  (5b 98 86 05) 408 4  576 7
(20 04 10 10) 132 3  (04 7f 12 ed) 444 4  576 7
```

6) $GF(2^8)/0x13f$*:*

```
(c0 02 10 10) 184 3  (20 6b 42 cc) 396 4  580 7
```

7) $GF(2^8)/0x14d$*:*

```
(14 02 10 10) 176 3  (18 a0 86 0d) 304 4  480 7
(ae 12 10 10) 216 3  (08 40 06 2d) 280 4  496 7
(30 18 10 10) 184 3  (0d d2 10 86) 312 4  496 7
(c0 02 10 10) 208 3  (10 18 2c 8e) 304 4  512 7
(59 28 10 10) 200 3  (58 a0 68 14) 336 4  536 7
(20 21 10 10) 188 3  (24 eb 92 10) 352 4  540 7
(50 01 10 10) 188 3  (e0 09 21 02) 356 4  544 7
(20 52 10 10) 172 3  (51 8d 40 ca) 376 4  548 7
(ae 08 10 10) 180 3  (01 48 ba 69) 372 4  552 7
(40 84 10 10) 192 3  (41 d0 10 56) 364 4  556 7
(20 72 10 10) 200 3  (8a 12 a5 a2) 360 4  560 7
(b2 18 10 10) 208 3  (c0 10 97 85) 352 4  560 7
(24 12 10 10) 196 3  (59 92 b4 82) 372 4  568 7
(12 18 10 10) 188 3  (50 92 4d e6) 380 4  568 7
(40 29 10 10) 188 3  (34 45 72 09) 380 4  568 7
(20 4d 10 10) 164 3  (81 3a 20 b6) 404 4  568 7
(90 08 10 10) 180 3  (19 dd 3c 40) 392 4  572 7
```

```
(12 0c 10 10) 204 3  (85 ed 47 08) 376 4  580 7
(9a 04 10 10) 188 3  (22 8d b2 58) 396 4  584 7
(14 45 10 10) 204 3  (47 04 aa 23) 380 4  584 7
(20 a2 10 10) 168 3  (59 e0 be 57) 416 4  584 7
(30 45 10 10) 208 3  (26 ba 4a 20) 380 4  588 7
(80 a2 10 10) 196 3  (12 ae e8 49) 392 4  588 7
(a0 01 10 10) 192 3  (53 5a 50 c5) 396 4  588 7
(1a a6 10 10) 216 3  (86 87 12 70) 376 4  592 7
(79 08 10 10) 192 3  (8a 56 4a 12) 400 4  592 7
```

8) $GF(2^8)/0x15f$:

```
(20 16 10 10) 188 3  (10 14 bb 85) 364 4  552 7
```

9) $GF(2^8)/0x163$:

```
(20 30 10 10) 152 3  (e0 b0 d0 90) 352 4  504 7
(43 02 10 10) 208 3  (19 12 10 b1) 328 4  536 7
(18 48 10 10) 184 3  (0a d0 24 b1) 368 4  552 7
(30 18 10 10) 176 3  (20 47 06 ff) 384 4  560 7
(03 04 10 10) 172 3  (f8 04 c5 a3) 396 4  568 7
(50 24 10 10) 200 3  (c3 9c 06 a1) 384 4  584 7
(60 48 10 10) 200 3  (69 b0 10 57) 384 4  584 7
(03 08 10 10) 156 3  (98 32 0c 69) 432 4  588 7
```

10) $GF(2^8)/0x177$:

```
(20 50 10 10) 172 3  (51 bd 77 18) 404 4  576 7
```

11) $GF(2^8)/0x17b$:

```
(08 12 10 10) 180 3  (46 30 50 58) 364 4  544 7
(20 60 10 10) 176 3  (f5 17 f6 10) 380 4  556 7
```

12) $GF(2^8)/0x187$:

```
(0d 08 10 10) 180 3  (c7 d8 24 10) 308 4  488 7
(18 08 10 10) 144 3  (12 16 1a 0e) 344 4  488 7
(20 90 10 10) 164 3  (2c 01 d9 10) 324 4  488 7
(e9 08 10 10) 208 3  (8d c7 0c 02) 304 4  512 7
(97 18 10 10) 204 3  (9d 14 04 c7) 316 4  520 7
(09 08 10 10) 152 3  (40 d2 b7 a2) 384 4  536 7
(02 0a 10 10) 172 3  (20 a2 68 ca) 364 4  536 7
(24 04 10 10) 172 3  (49 12 44 17) 372 4  544 7
(40 a7 10 10) 176 3  (14 56 32 02) 372 4  548 7
(60 80 10 10) 168 3  (22 96 cd 20) 384 4  552 7
(02 08 10 10) 136 3  (0b 18 ef 2a) 420 4  556 7
(50 02 10 10) 168 3  (47 60 05 5a) 388 4  556 7
(1a 18 10 10) 204 3  (0c 21 05 a8) 352 4  556 7
(08 cf 10 10) 196 3  (1c 6c 09 06) 364 4  560 7
(09 24 10 10) 196 3  (08 48 03 f2) 364 4  560 7
(40 08 10 10) 128 3  (a9 b7 b2 70) 436 4  564 7
(c7 0a 10 10) 188 3  (b7 02 0a 9c) 376 4  564 7
(0a 28 10 10) 192 3  (08 91 0f d3) 376 4  568 7
(d0 04 10 10) 192 3  (30 68 a5 a8) 376 4  568 7
(60 09 10 10) 180 3  (09 c7 42 b6) 388 4  568 7
(15 08 10 10) 176 3  (04 33 26 c3) 392 4  568 7
(40 c0 10 10) 160 3  (c7 b2 64 13) 412 4  572 7
(14 06 10 10) 196 3  (d7 52 cb 30) 380 4  576 7
```

```
(80 c0 10 10) 172 3  (0d bf 04 b2) 404 4  576 7
(60 04 10 10) 156 3  (ac 95 10 4b) 420 4  576 7
(07 02 10 10) 172 3  (a4 17 11 89) 404 4  576 7
(20 0e 10 10) 160 3  (18 e8 8e d0) 416 4  576 7
(14 28 10 10) 188 3  (39 c0 0c 51) 392 4  580 7
(30 14 10 10) 176 3  (b4 09 8c 0e) 408 4  584 7
(40 14 10 10) 160 3  (60 82 ce 37) 424 4  584 7
(d7 18 10 10) 208 3  (01 ac 87 34) 380 4  588 7
(09 0a 10 10) 188 3  (d5 67 18 d7) 400 4  588 7
(18 48 10 10) 196 3  (6d 27 20 11) 392 4  588 7
(40 1c 10 10) 172 3  (08 6e a5 94) 420 4  592 7
(40 16 10 10) 196 3  (43 17 50 c5) 396 4  592 7
```

13) GF$(2^8)/0x18b$*:*

```
(18 08 10 10) 144 3  (12 16 1a 0e) 352 4  496 7
(cd 08 10 10) 172 3  (e0 c8 20 95) 348 4  520 7
(20 9b 10 10) 188 3  (3d 38 08 83) 352 4  540 7
(06 31 10 10) 212 3  (a0 21 14 48) 344 4  556 7
(30 24 10 10) 188 3  (23 b5 18 60) 368 4  556 7
(90 08 10 10) 172 3  (e7 7a 1a 10) 384 4  556 7
(20 cb 10 10) 176 3  (02 88 23 90) 380 4  556 7
(0b 02 10 10) 184 3  (1d 42 28 64) 380 4  564 7
(11 08 10 10) 168 3  (40 90 ef 56) 400 4  568 7
(c0 08 10 10) 152 3  (42 ab 71 03) 416 4  568 7
(40 06 10 10) 168 3  (62 61 71 08) 404 4  572 7
(60 18 10 10) 172 3  (3a ba 10 bd) 400 4  572 7
(20 03 10 10) 168 3  (11 90 ac d9) 404 4  572 7
(30 09 10 10) 196 3  (a2 42 0d 06) 384 4  580 7
(0c 12 10 10) 192 3  (30 ad 98 b1) 392 4  584 7
(e0 08 10 10) 188 3  (a1 db 2c 0a) 396 4  584 7
(30 cd 10 10) 196 3  (18 dd d4 56) 388 4  584 7
(40 02 10 10) 164 3  (94 4e 50 34) 428 4  592 7
```

14) GF$(2^8)/0x19f$*:*

```
(40 a8 10 10) 188 3  (9f 32 80 4c) 372 4  560 7
(50 df 10 10) 200 3  (80 48 ac df) 360 4  560 7
(04 18 10 10) 168 3  (7d 08 cc 42) 404 4  572 7
(40 09 10 10) 196 3  (f5 10 a1 d9) 380 4  576 7
(20 11 10 10) 184 3  (bf 04 e7 42) 396 4  580 7
(01 08 10 10) 160 3  (61 bc 04 97) 424 4  584 7
(40 32 10 10) 212 3  (05 02 fd 61) 380 4  592 7
```

15) GF$(2^8)/0x1cf$*:*

```
(80 12 10 10) 192 3  (11 63 30 ef) 340 4  532 7
(80 e1 10 10) 220 3  (79 30 10 15) 332 4  552 7
(4f 04 10 10) 200 3  (4e 80 40 9d) 392 4  592 7
```

16) GF$(2^8)/0x1d7$*:*

```
(06 08 10 10) 180 3  (c7 05 33 80) 392 4  572 7
(20 c0 10 10) 180 3  (02 4f 97 11) 392 4  572 7
(e7 08 10 10) 192 3  (08 37 ab 28) 400 4  592 7
(20 19 10 10) 192 3  (28 7d 0f 20) 400 4  592 7
```

B. Hadamard Matrices, SPB, $R = x^{-4}$

1) GF$(2^8)/0x11b$*:*

```
(18 08 10 20) 156 3  (06 02 04 08) 220 4  376 7
(30 08 10 20) 164 3  (c0 20 40 80) 228 4  392 7
(40 88 10 20) 180 3  (3b 52 48 90) 388 4  568 7
(26 08 10 20) 176 3  (af 42 84 13) 400 4  576 7
(08 44 10 20) 180 3  (90 a4 3b 76) 412 4  592 7
```

2) $GF(2^8)/0x11d$:

```
(80 08 10 20) 156 3  (40 04 08 10) 156 3  312 6
(64 08 10 20) 180 3  (c8 10 20 40) 196 4  376 7
(40 c8 10 20) 196 4  (20 64 08 10) 180 3  376 7
(30 08 10 20) 164 3  (c0 20 40 80) 228 4  392 7
(08 18 10 20) 164 3  (02 06 04 08) 236 4  400 7
(1d 08 10 20) 168 3  (0e 32 64 c8) 356 4  524 7
```

3) $GF(2^8)/0x12b$:

```
(08 28 10 20) 176 3  (08 28 10 20) 176 3  352 6
(40 50 10 20) 188 3  (10 14 04 08) 204 4  392 7
(18 08 10 20) 156 3  (06 02 04 08) 244 4  400 7
(30 08 10 20) 164 3  (c0 20 40 80) 244 4  408 7
(30 40 10 20) 176 3  (03 04 01 02) 316 4  492 7
(6b 08 10 20) 188 3  (78 03 06 0c) 336 4  524 7
(30 04 10 20) 188 3  (7d 40 2b 56) 344 4  532 7
```

4) $GF(2^8)/0x12d$:

```
(40 50 10 20) 188 4  (10 14 04 08) 172 3  360 7
(14 04 10 20) 172 3  (05 01 04 08) 236 4  408 7
(30 08 10 20) 164 3  (c0 20 40 80) 244 4  408 7
(08 18 10 20) 164 3  (02 06 04 08) 244 4  408 7
(30 04 10 20) 176 3  (77 40 2d 5a) 320 4  496 7
(2d 04 10 20) 176 3  (c0 03 0c 18) 360 4  536 7
(30 02 10 20) 192 3  (f1 80 b4 45) 396 4  588 7
```

5) $GF(2^8)/0x139$:

```
(08 18 10 20) 164 3  (02 06 04 08) 228 4  392 7
(30 08 10 20) 164 3  (c0 20 40 80) 228 4  392 7
```

6) $GF(2^8)/0x13f$:

```
(18 08 10 20) 180 3  (06 02 04 08) 244 4  424 7
(30 08 10 20) 188 3  (c0 20 40 80) 268 4  456 7
```

7) $GF(2^8)/0x14d$:

```
(24 04 10 20) 184 3  (24 04 10 20) 184 3  368 6
(40 50 10 20) 172 4  (10 14 04 08) 172 3  344 7
(08 18 10 20) 164 3  (02 06 04 08) 244 4  408 7
(14 04 10 20) 172 3  (05 01 04 08) 236 4  408 7
(30 08 10 20) 164 3  (c0 20 40 80) 244 4  408 7
(80 90 10 20) 220 4  (20 24 04 08) 196 3  416 7
(14 12 10 20) 196 3  (a0 90 80 4d) 308 4  504 7
(30 04 10 20) 176 3  (d7 40 4d 9a) 336 4  512 7
(04 a4 10 20) 192 3  (a4 e0 0a 14) 324 4  516 7
(04 12 10 20) 180 3  (b4 10 4a 94) 344 4  524 7
```

8) $GF(2^8)/0x15f$:

```
(18 08 10 20) 180 3  (06 02 04 08) 260 4  440 7
(30 08 10 20) 188 3  (c0 20 40 80) 276 4  464 7
```

9) $GF(2^8)/0x163$:

```
(40 50 10 20) 172 3  (10 14 04 08) 188 4  360 7
(18 08 10 20) 156 3  (06 02 04 08) 220 4  376 7
(30 08 10 20) 164 3  (c0 20 40 80) 236 4  400 7
```

10) $GF(2^8)/0x165$:

```
(40 50 10 20) 172 3 (10 14 04 08) 172 4 344 7
(08 18 10 20) 164 3 (02 06 04 08) 244 4 408 7
(30 08 10 20) 164 3 (c0 20 40 80) 244 4 408 7
```

11) $GF(2^8)/0x177$:

```
(18 08 10 20) 180 3  (06 02 04 08) 268 4  448 7
(30 08 10 20) 188 3  (c0 20 40 80) 276 4  464 7
```

12) $GF(2^8)/0x17b$:

```
(18 08 10 20) 180 3  (06 02 04 08) 268 4  448 7
(30 08 10 20) 188 3  (c0 20 40 80) 276 4  464 7
```

13) $GF(2^8)/0x187$:

```
(28 08 10 20) 168 3  (28 08 10 20) 168 3  336 6
(40 50 10 20) 172 3  (10 14 04 08) 172 3  344 6
(30 08 10 20) 156 3  (c0 20 40 80) 204 4  360 7
(18 08 10 20) 156 3  (06 02 04 08) 212 4  368 7
(04 14 10 20) 172 3  (01 05 04 08) 228 4  400 7
(12 02 10 20) 180 3  (c7 c3 04 08) 236 4  416 7
(30 40 10 20) 164 3  (03 04 01 02) 260 4  424 7
(02 08 10 20) 148 3  (05 14 28 50) 284 4  432 7
(40 04 10 20) 148 3  (28 c1 0a 14) 304 4  452 7
(80 07 10 20) 188 3  (07 09 30 60) 264 4  452 7
(40 c7 10 20) 172 3  (c0 ce 30 60) 320 4  492 7
(a0 08 10 20) 164 3  (1b 60 c0 07) 332 4  496 7
(1c 08 10 20) 176 3  (15 0e 1c 38) 336 4  512 7
(0e 04 10 20) 180 3  (1b 0a 28 50) 340 4  520 7
(50 14 10 20) 196 3  (22 cb 0a 14) 344 4  540 7
(0e 18 10 20) 196 3  (15 24 38 70) 356 4  552 7
(12 18 10 20) 188 3  (2d 3c 28 50) 388 4  576 7
```

14) $GF(2^8)/0x18b$:

```
(08 28 10 20) 176 3  (08 28 10 20) 176 3  352 6
(30 08 10 20) 156 3  (c0 20 40 80) 220 4  376 7
(18 08 10 20) 156 3  (06 02 04 08) 220 4  376 7
(cd 08 10 20) 184 3  (a3 04 08 10) 216 4  400 7
(30 04 10 20) 172 3  (16 40 8b 9d) 300 4  472 7
(0b 04 10 20) 184 3  (a0 03 0c 18) 292 4  476 7
(cb 08 10 20) 188 3  (b3 0b 16 2c) 368 4  556 7
(c0 08 10 20) 164 3  (53 90 ab dd) 404 4  568 7
(06 08 10 20) 164 3  (ec 62 c4 03) 412 4  576 7
(16 18 10 20) 196 3  (28 a6 c4 03) 380 4  576 7
(0c 08 10 20) 160 3  (67 c3 0d 1a) 432 4  592 7
```

15) $GF(2^8)/0x19f$:

```
(40 50 10 20) 196 3  (10 14 04 08) 196 4  392 7
(18 08 10 20) 180 3  (06 02 04 08) 252 4  432 7
(30 08 10 20) 180 3  (c0 20 40 80) 260 4  440 7
(30 40 10 20) 188 3  (03 04 01 02) 292 4  480 7
```

16) $GF(2^8)/0x1c3$:

```
(08 28 10 20) 168 3  (08 28 10 20) 168 3  336 6
(40 50 10 20) 172 3  (10 14 04 08) 172 3  344 6
(18 08 10 20) 156 3  (06 02 04 08) 204 4  360 7
(30 08 10 20) 156 3  (c0 20 40 80) 212 4  368 7
(80 90 10 20) 180 3  (20 24 04 08) 204 4  384 7
(14 04 10 20) 172 3  (05 01 04 08) 220 4  392 7
(40 02 10 20) 160 3  (45 10 80 c3) 236 4  396 7
(80 08 10 20) 148 3  (83 14 28 50) 284 4  432 7
(06 04 10 20) 172 3  (90 e0 06 0c) 276 4  448 7
(0a 08 10 20) 164 3  (73 03 06 0c) 332 4  496 7
(03 01 10 20) 204 3  (48 38 06 0c) 300 4  504 7
(70 08 10 20) 176 3  (93 38 70 e0) 336 4  512 7
(40 14 10 20) 172 3  (06 d8 e0 03) 348 4  520 7
(80 03 10 20) 184 3  (50 d8 0a 14) 336 4  520 7
(50 04 10 20) 172 3  (e6 38 e0 03) 364 4  536 7
(e0 18 10 20) 196 3  (93 24 38 70) 348 4  544 7
(40 e0 10 20) 180 3  (70 a8 1c 38) 372 4  552 7
(1a 04 10 20) 204 3  (16 a0 c5 49) 360 4  564 7
(90 18 10 20) 188 3  (ab 3c 28 50) 396 4  584 7
(60 03 10 20) 196 3  (24 a8 0e 1c) 396 4  592 7
```

17) $GF(2^8)/0x1cf$:

```
(40 50 10 20) 196 3  (10 14 04 08) 196 4  392 7
(18 08 10 20) 180 3  (06 02 04 08) 252 4  432 7
(30 08 10 20) 180 3  (c0 20 40 80) 252 4  432 7
(80 90 10 20) 204 3  (20 24 04 08) 236 4  440 7
```

18) $GF(2^8)/0x1d7$:

```
(28 08 10 20) 192 3  (28 08 10 20) 192 3  384 6
(18 08 10 20) 180 3  (06 02 04 08) 268 4  448 7
(30 08 10 20) 180 3  (c0 20 40 80) 268 4  448 7
```

C. Circulant Matrices, PB, $R = 1$

1) $GF(2^8)/0x11b$:

```
(42 8d 01 01) 172 3 &  (02 57 04 b7) 312 4 & 484 7
(02 c1 01 01) 192 3 &  (0f 8c 01 21) 300 4 & 492 7
(04 9d 01 01) 180 3 &  (8d 12 aa 21) 336 4 & 516 7
(04 e8 01 01) 160 3 &  (8b 34 c3 21) 408 4 & 568 7
(02 3b 01 01) 196 3 &  (ab 9a 01 05) 376 4 & 572 7
(02 9c 01 01) 160 3 &  (98 8b ee 74) 420 4 & 580 7
(22 8d 01 01) 160 3 &  (a4 44 e9 6b) 432 4 & 592 7
(02 20 01 01) 172 3 &  (cb 77 cc 2a) 420 4 & 592 7
```

2) $GF(2^8)/0x1c3$:

```
(a8 e1 01 01) 164 3 &  (01 2b 10 e7) 324 4 & 488 7
```

```
(02 03 01 01) 144 3 &  (0e 0b 0d 09) 344 4 & 488 7
(02 16 01 01) 180 3 &  (01 e5 3b 24) 308 4 & 488 7
(02 cb 01 01) 208 3 &  (08 06 24 bf) 304 4 & 512 7
(03 b4 01 01) 204 3 &  (24 04 05 be) 316 4 & 520 7
(08 0a 01 01) 172 3 &  (e1 40 72 32) 364 4 & 536 7
(02 12 01 01) 152 3 &  (40 55 31 91) 384 4 & 536 7
(04 e5 01 01) 172 3 &  (1d 95 09 83) 372 4 & 544 7
(54 91 01 01) 176 3 &  (08 e8 9c 05) 372 4 & 548 7
(70 a9 01 01) 168 3 &  (e9 a4 2e e1) 384 4 & 552 7
(03 0b 01 01) 204 3 &  (4a 14 f1 06) 352 4 & 556 7
(08 90 01 01) 168 3 &  (9a 14 70 8d) 388 4 & 556 7
(02 08 01 01) 136 3 &  (eb c7 03 1a) 420 4 & 556 7
(12 e5 01 01) 196 3 &  (02 93 18 d0) 364 4 & 560 7
(02 26 01 01) 196 3 &  (07 76 12 0c) 364 4 & 560 7
(0a 24 01 01) 188 3 &  (ae 0a 08 55) 376 4 & 564 7
(02 91 01 01) 128 3 &  (71 41 55 5a) 436 4 & 564 7
(02 15 01 01) 176 3 &  (20 ed f8 04) 392 4 & 568 7
(0a e3 01 01) 192 3 &  (02 b8 1e 21) 376 4 & 568 7
(12 70 01 01) 180 3 &  (45 99 24 12) 388 4 & 568 7
(04 39 01 01) 192 3 &  (4a 5c 72 e0) 376 4 & 568 7
(38 91 01 01) 160 3 &  (19 74 41 24) 412 4 & 572 7
(0e e1 01 01) 160 3 &  (39 a7 db 03) 416 4 & 576 7
(04 70 01 01) 156 3 &  (8b 01 bc 4e) 420 4 & 576 7
(05 0c 01 01) 196 3 &  (25 98 22 e0) 380 4 & 576 7
(08 1c 01 01) 172 3 &  (bb 11 1d 4c) 404 4 & 576 7
(38 a9 01 01) 172 3 &  (41 04 57 16) 404 4 & 576 7
(05 e3 01 01) 188 3 &  (f2 38 06 80) 392 4 & 580 7
(05 e0 01 01) 176 3 &  (0e af 12 4d) 408 4 & 584 7
(05 91 01 01) 160 3 &  (fc 36 a1 70) 424 4 & 584 7
(03 25 01 01) 208 3 &  (e4 b5 4e 10) 380 4 & 588 7
(03 93 01 01) 196 3 &  (66 fd e1 11) 392 4 & 588 7
(0a 12 01 01) 188 3 &  (25 03 6c 2d) 400 4 & 588 7
(0d 91 01 01) 196 3 &  (2c 90 1d 89) 396 4 & 592 7
(07 91 01 01) 172 3 &  (ac 5c 7e 02) 420 4 & 592 7
```

D. Hadamard Matrices, PB, $R = 1$

1) $GF(2^8)/0x14d$*:*

```
(51 53 01 02) 184 3 &  (51 53 01 02) 184 3 & 368 6
(04 05 01 02) 172 4 &  (01 52 53 a6) 172 3 & 344 7
(a6 a7 01 02) 164 3 &  (8f dc 53 a6) 244 4 & 408 7
(52 53 01 02) 172 3 &  (b2 e1 53 a6) 236 4 & 408 7
(03 a6 01 02) 164 3 &  (0c 02 04 08) 244 4 & 408 7
(08 09 01 02) 220 4 &  (02 51 53 a6) 196 3 & 416 7
(52 8e 01 02) 196 3 &  (0a 09 08 10) 308 4 & 504 7
(03 53 01 02) 176 3 &  (30 04 10 20) 336 4 & 512 7
(53 59 01 02) 192 3 &  (59 0e 29 52) 324 4 & 516 7
(53 8e 01 02) 180 3 &  (58 01 2d 5a) 344 4 & 524 7
```

2) $GF(2^8)/0x165$*:*

```
(04 05 01 02) 172 3 &  (01 58 59 b2) 172 4 & 344 7
(b2 b3 01 02) 164 3 &  (9e c7 59 b2) 244 4 & 408 7
(03 b2 01 02) 164 3 &  (0c 02 04 08) 244 4 & 408 7
```

3) $GF(2^8)/0x1c3$*:*

```
(e1 e3 01 02) 168 3 &  (e1 e3 01 02) 168 3 & 336 6
```

```
(04 05 01 02) 172 3 &  (01 90 91 e1) 172 3 & 344 6
(e0 e1 01 02) 156 3 &  (38 a9 91 e1) 204 4 & 360 7
(03 e1 01 02) 156 3 &  (0c 02 04 08) 212 4 & 368 7
(08 09 01 02) 180 3 &  (02 93 91 e1) 204 4 & 384 7
(90 91 01 02) 172 3 &  (24 b5 91 e1) 220 4 & 392 7
(04 a9 01 02) 160 3 &  (20 01 08 10) 236 4 & 396 7
(08 e1 01 02) 148 3 &  (14 90 e3 05) 284 4 & 432 7
(38 91 01 02) 172 3 &  (09 0e 38 70) 276 4 & 448 7
(48 e1 01 02) 164 3 &  (1b 1c 38 70) 332 4 & 496 7
(1c b5 01 02) 204 3 &  (e5 e2 38 70) 300 4 & 504 7
(07 e1 01 02) 176 3 &  (15 e2 07 0e) 336 4 & 512 7
(04 90 01 02) 172 3 &  (38 ec 0e 1c) 348 4 & 520 7
(08 1c 01 02) 184 3 &  (05 ec 48 90) 336 4 & 520 7
(05 91 01 02) 172 3 &  (36 e2 0e 1c) 364 4 & 536 7
(0e e0 01 02) 196 3 &  (15 93 e2 07) 348 4 & 544 7
(04 0e 01 02) 180 3 &  (07 eb 71 e2) 372 4 & 552 7
(49 91 01 02) 204 3 &  (39 0a 28 50) 360 4 & 564 7
(09 e0 01 02) 188 3 &  (f7 73 e3 05) 396 4 & 584 7
(06 1c 01 02) 196 3 &  (93 eb d9 71) 396 4 & 592 7
```

E. Circulant Matrices, GPB, $f = 0x187$, $R = x^6 + x^5 + 1$

```
(a4 f3 61 61) 180 3 &  (f 97 78 61) 308 4 & 488 7
(92 f3 61 61) 144 3 &  (3c 86 cf 14) 344 4 & 488 7
(c2 67 61 61) 164 3 &  (8b ed 7a 61) 324 4 & 488 7
(d9 f3 61 61) 208 3 &  (a2 f 49 5d) 304 4 & 512 7
(6d 92 61 61) 204 3 &  (c3 db ba f) 316 4 & 520 7
(1e f3 61 61) 152 3 &  (3 39 af 99) 384 4 & 536 7
(5d ae 61 61) 172 3 &  (c2 99 32 ab) 364 4 & 536 7
(78 ba 61 61) 172 3 &  (1d 3c b9 6b) 372 4 & 544 7
(3 ce 61 61) 176 3 &  (db 85 fe 5d) 372 4 & 548 7
(c1 6 61 61) 168 3 &  (9f 80 a1 c2) 384 4 & 552 7
(5d f3 61 61) 136 3 &  (43 92 3e 6c) 420 4 & 556 7
(62 5d 61 61) 168 3 &  (9 c1 57 cc) 388 4 & 556 7
(cf 92 61 61) 204 3 &  (49 2f 57 37) 352 4 & 556 7
(f3 fc 61 61) 196 3 &  (28 88 1e e7) 364 4 & 560 7
(1e 78 61 61) 196 3 &  (f3 f0 b0 fb) 364 4 & 560 7
(3 f3 61 61) 128 3 &  (da af f8 a0) 436 4 & 564 7
(f ae 61 61) 188 3 &  (af 5d ae 2e) 376 4 & 564 7
(ae 31 61 61) 192 3 &  (f3 8a f9 d4) 376 4 & 568 7
(64 ba 61 61) 192 3 &  (a3 32 93 37) 376 4 & 568 7
(c1 1e 61 61) 180 3 &  (1e f 5e 42) 388 4 & 568 7
(36 f3 61 61) 176 3 &  (ba 13 25 b5) 392 4 & 568 7
(3 5 61 61) 160 3 &  (f f8 7b d1) 412 4 & 572 7
(db e7 61 61) 196 3 &  (6e 3f 46 a3) 380 4 & 576 7
(6 5 61 61) 172 3 &  (a4 5c ba f8) 404 4 & 576 7
(c1 ba 61 61) 156 3 &  (8d 30 61 40) 420 4 & 576 7
(a 5d 61 61) 172 3 &  (7e 6b 8c 18) 404 4 & 576 7
(c2 14 61 61) 160 3 &  (92 34 12 64) 416 4 & 576 7
(db 31 61 61) 188 3 &  (bd 5 49 8f) 392 4 & 580 7
(a3 db 61 61) 176 3 &  (1f 1e 4f 14) 408 4 & 584 7
(3 db 61 61) 160 3 &  (c1 5b 11 a9) 424 4 & 584 7
(6e 92 61 61) 208 3 &  (ed 8d c 19) 380 4 & 588 7
(1e ae 61 61) 188 3 &  (33 cb 92 6e) 400 4 & 588 7
(92 f0 61 61) 196 3 &  (65 c8 c2 8c) 392 4 & 588 7
(3 28 61 61) 172 3 &  (f3 d5 93 dd) 420 4 & 592 7
(3 86 61 61) 196 3 &  (b3 6b 62 52) 396 4 & 592 7
```

F. Hadamard Matrices, GPB, $f = 0x187$, $R = x^6 + x^5 + 1$

```
(31 f3 61 c2) 168 3 & (31 f3 61 c2) 168 3 & 336 6
(3 62 61 c2) 172 3 & (61 db ba f3) 172 3 & 344 6
(a3 f3 61 c2) 156 3 & (5 c2 3 6) 204 4 & 360 7
(92 f3 61 c2) 156 3 & (e7 5d ba f3) 212 4 & 368 7
(ba db 61 c2) 172 3 & (ed 57 ba f3) 228 4 & 400 7
(3c 5d 61 c2) 180 3 & (f b5 ba f3) 236 4 & 416 7
(a3 3 61 c2) 164 3 & (b0 ba ed 5d) 260 4 & 424 7
(5d f3 61 c2) 148 3 & (57 db 31 62) 284 4 & 432 7
(3 ba 61 c2) 148 3 & (31 e8 ae db) 304 4 & 452 7
(6 a 61 c2) 188 3 & (a 1e a3 c1) 264 4 & 452 7
(3 f 61 c2) 172 3 & (5 11 a3 c1) 320 4 & 492 7
(c4 f3 61 c2) 164 3 & (22 c1 5 a) 332 4 & 496 7
(28 f3 61 c2) 176 3 & (36 14 28 50) 336 4 & 512 7
(14 ba 61 c2) 180 3 & (22 ae 31 62) 340 4 & 520 7
(62 db 61 c2) 196 3 & (9f 46 ae db) 344 4 & 540 7
(14 92 61 c2) 196 3 & (36 78 50 a0) 356 4 & 552 7
(3c 92 61 c2) 188 3 & (66 ea 31 62) 388 4 & 576 7
```

APPENDIX B
SOME BETTER MATRICES

A. $f = 0x14d$ SPB($R = x^{-4}$) Hadamard Involutory (28 8 10 20) 40-6=34

```
(28 8 10 20):

   a1+               a7+   b1+c0+                         d7
      a2+               b0+   b2+c1+d0
a0+a1+   a3+         a7+b0+      b3+c2+d1+                d7
      a2+   a4+      a7+            b4+c3+d2+             d7
         a3+   a5+                     b5+c4+d3
a0+         a4+   a6+   b0+               b6+c5+d4
               a5+                           b7+c6+d5+    d7
a0+               a6+   b0+                        c7+d6          40 XORs

    Y+                     b1+c0
      a2+               b0+   b2+c1+d0
 A+ Y+   a3+                     b3+c2+d1
      a2+   a4+       B+            b4+c3+d2
         a3+   a5+                     b5+c4+d3
            a4+    Z+                     b6+c5+d4
               a5+                           b7+c6+d5+    d7
                   Z+                              c7+d6

A=a0+b0  B=a7+d7        Z=A+a6  Y=B+a1                             34 XORs
```

(5)

B. $f = 0x187$ GPB($R = x^6 + x^5 + 1$) Circulant (03 f3 61 61) 128 3 (da af f8 a0) 436 4

```
#(03 f3 61 61) 128 3
                  a6+a7+b0+b1+                 c0+d0
                  a6+   b0+   b2+              c1+d1
a0+               a6+            b3+           c2+d2
   a1+               a7+            b4+        c3+d3
      a2+                              b5+     c4+d4
         a3+                              b6+   c5+d5
            a4+         b0+                  b7+c6+d6
```

```
               a5+a6+a7+b0+                     c7+d7

                         B+b1+                  c0+d0
                         A+   b2+               c1+d1
a0+               a6+            b3+            c2+d2
   a1+               a7+            b4+         c3+d3
      a2+                              b5+      c4+d4
         a3+                              b6+   c5+d5
            a4+         b0+                  b7+c6+d6
               a5+       B+                     c7+d7
A=a6+b0  B=A+a7                                              29 XORs


#(da af f8 a0) 436 4
         a3+a4+a5+a6+   b0+         b4+b5+b6+         c2+c3+   c5+c6+   d0+               d6
a0+      a3+         a7+b0+b1+      b4+      b7+c0+   c2+   c4+c5+   c7+d0+d1+            d6+d7
   a1+   a3+   a5+a6+      b1+b2+   b4+   b6+      c1+c2+               d0+d1+d2+         d6+d7
      a2+   a4+a6+   a7+      b2+b3+   b5+   b7+c0+   c2+c3+               d1+d2+d3+         d7
         a3+   a5+   a7+b0+      b3+b4+   b6+   c0+c1+   c3+c4+               d2+d3+d4
a0+         a4+   a6+      b1+      b4+b5+   b7+   c1+c2+   c4+c5+               d3+d4+d5
   a1+         a5+   a7+      b2+      b5+b6+   c0+   c2+c3+   c5+c6+               d4+d5+d6
      a2+a3+a4+a5+               b3+b4+b5+   b7+   c1+c2+   c4+c5+   c7+               d5+   d7

             B+   T+a6+                                        E+ Q+    Z
 K+                     D+b0+                              c4+ E+    O+ Z+ G
    U+              a6+      b1+                c1+   S+                Z
       W+                       b2+          P+       S+ V
          X+      T+               b3+                   V+                  d2   +d4
 K+          B+                       b4+    P+    H+                           d3+d4+ Y
    U+                  D+               b5+                      Q+               d4+ Y+d6
       W+ X+   a5+                                                   O+                Y+   d7

A=a3+b4  B=a4+b5  C=a5+b6  D=a7+c0  E=c2+c5  F=d0+d6  G=d1+d7  H=c1+c4 I=c2+d2 J=c3+d3
K=a0+b1  L=a1+b2  M=a2+b3  O=b7+c7  P=a6+b7  Q=c3+c6

Z=A+F    Y=E+d5   X=A+H    W=B+M    V=D+J    U=L+C    S=I+G                         68 XORs
         T=C+b0
```

(6)

C. $f = 0x187$ *GPB($R = x^6 + x^5 + 1$) Hadamard (3 62 61 c2) (61 db ba f3)*

```
(3 62 61 c2):
                  a6+a7+b0+               b6+b7+c0+   d7
                  a6+      b1+            b6+   c1+d0+d7
a0+               a6+   b0+   b2+         b6+   c2+d1+d7
   a1+               a7+   b1+   b3+         b7+c3+d2
      a2+                     b2+   b4+         c4+d3
         a3+                     b3+   b5+      c5+d4
            a4+                     b4+   b6+   c6+d5
               a5+a6+a7+               b5+b6+   c7+d6+d7        43 XORs

                         Z+                   B+c0
                   A+      b1+                  c1+d0
a0+                      Z+   b2+               c2+d1
   a1+                     b1+   b3+          B+c3+d2
      a2+                     b2+   b4+         c4+d3
         a3+                     b3+   b5+      c5+d4
            a4+                     b4+   b6+   c6+d5
```

```
               a5+ A+a7+               b5+b6+   c7+d6
A=a6+d7  B=a7+b7  C=b0+b6  Z=A+C                                36 XORs
```

```
(61 db ba f3):
a0+                     b0+b1+b2+                  c1+c2+               d0+d1
   a1+                  b0+      b3+            c0+c1+   c3+            d0+d2
      a2+                     b2+   b4+                     c4+            d3
         a3+                     b3+   b5+                     c5+         d4
            a4+                     b4+   b6+                     c6+      d5
               a5+      b0+            b5+   b7+c0+                  c7+   d6
                  a6+      b1+            b6+      c1+                  d0+d7
                     a7+b0+b1+               b7+c0+c1+                  d0       43 XORs

a0+                     b0+b1+b2+                   A+c2+                  d1
   a1+                           b3+             B+ A+   c3+               d2
      a2+                     b2+   b4+                     c4+            d3
         a3+                     b3+   b5+                     c5+         d4
            a4+                     b4+   b6+                     c6+      d5
               a5+                     b5+   b7+ B+                  c7+   d6
                  a6+       Z+            b6+                              d7
                     a7+    Z+               b7+ B

A=c2+d0  B=b0+c0      Z=b1+A                                                     37 XORs
```

The first coefficient also includes "Z=b1+A", bur it has 8 terms. We do not reuse it.
The last one has 7+1=8 terms("Z=b1+A" adds a 0 and includes 4 terms.). We do not reuse "b7+B".
Otherwise the delay will be 4T_X.

(7)

D. $f = 0x187$ *GPB(*$R = x^6 + x^5 + 1$*) Hadamard Involutory (31 f3 61 c2) 42-7=35*

```
(31 f3 61 c2):
a0+a1+               a7+b0+b1+c0+                         d7
      a2+            a7+b0+   b2+c1+                   d0+d7
   a1+   a3+         a7+         b3+c2+                d1+d7
      a2+   a4+                     b4+c3+             d2
         a3+   a5+                     b5+c4+          d3
            a4+   a6+                     b6+c5+       d4
a0+            a5+   a7+b0+                  b7+c6+    d5
a0+               a6+a7+b0+                        c7+ d6+d7   42 XORs


 Z+a1+                     b1+c0
      a2+               b0+   b2+c1+                   d0+ A
   a1+   a3+                     b3+c2+                d1+ A
      a2+   a4+                     b4+c3+             d2
         a3+   a5+                     b5+c4+          d3
            a4+   a6+                     b6+c5+       d4
 B+            a5+                           b7+c6+    d5
 Z+               a6+                              c7+ d6

A=a7+d7  B=a0+b0  Z=A+B                                        35 XORs
```

(8)

E. $f = 0x1c3$ *PB(*$R = 1$*) Circulant (2 91 1 1) 128 3 (71 41 55 5a) 436 4 564 7*

```
(2 91 1 1):
```

```
                     c7 + d0 + d1 + d2 + a0 + b0
                        c7 + d3 + a1 + b1 + c0
                          d4 + a2 + b2 + c1
                          d5 + a3 + b3 + c2
                        d6 + c3 + d0 + a4 + b4
                        d7 + c4 + d1 + a5 + b5
                        c5 + c7 + d1 + a6 + b6
                     c6 + c7 + d0 + d1 + a7 + b7


                      B+      d2+               a0+b0
c0+                  c7+         d3+            a1+b1
   c1+                              d4+         a2+b2
      c2+                              d5+      a3+b3
         c3+            d0+               d6+   a4+b4
            c4+            d1+               d7+a5+b5
               c5+    A+                        a6+b6
                  c6+ B+                        a7+b7

A=c7+d1   B=A+d0    32-3=29 XORs

(71 41 55 5a):
 a0 + a2 + b0 + b2 + b3 + b5 + b6 + c0 + c2 + c3 + c4 + d2 + d3 + d4 + d5
 a1 + a2 + a3 + b1 + b2 + b4 + b5 + b7 + c1 + c2 + c5 + d0 + d2 + d6
 a2 + a3 + a4 + b2 + b3 + b5 + b6 + c0 + c2 + c3 + c6 + d1 + d3 + d7
 a3 + a4 + a5 + b3 + b4 + b6 + b7 + c1 + c3 + c4 + c7 + d0 + d2 + d4
 a0 + a4 + a5 + a6 + b4 + b5 + b7 + c0 + c2 + c4 + c5 + d0 + d1 + d3 + d5
 a0 + a1 + a5 + a6 + a7 + b5 + b6 + c1 + c3 + c5 + c6 + d1 + d2 + d4 + d6
 a0 + a1 + a6 + a7 + b0 + b2 + b3 + b5 + b7 + c0 + c3 + c6 + c7 + d0 + d4 + d7
 a1 + a7 + b1 + b2 + b4 + b5 + c1 + c2 + c3 + c7 + d1 + d2 + d3 + d4
4Tx

 a0+   a2+               b0+   b2+b3+   b5+b6+   c0+   c2+c3+c4+               d2+d3+d4+d5
    a1+a2+a3+               b1+b2+   b4+b5+   b7+   c1+c2+      c5+      d0+   d2+         d6
       a2+a3+a4+               b2+b3+   b5+b6+   c0+   c2+c3+      c6+      d1+   d3+         d7
          a3+a4+a5+               b3+b4+   b6+b7+   c1+   c3+c4+      c7+d0+   d2+   d4
 a0+         a4+a5+a6+               b4+b5+   b7+c0+   c2+   c4+c5+      d0+d1+   d3+   d5
 a0+a1+         a5+a6+a7+               b5+b6+      c1+   c3+   c5+c6+      d1+d2+   d4+   d6
 a0+a1+            a6+a7+b0+   b2+b3+   b5+   b7+c0+      c3+      c6+c7+d0+         d4+      d7
    a1+               a7+   b1+b2+   b4+b5+         c1+c2+c3+         c7+   d1+d2+d3+d4


 a0+   a2+               b0+                                 c4+               d2+ W+ Y+ I
    a1+ O+                   V+ T+                     c2+      c5+                        d6
        O+   a4+                            F+            c3+       Q+             W+         J
          a3+                         X+             C+                c7+ E+          Y
                                      X+ U+                                E+d1+    D+    I
                a5+    Z+                U+b6+       C+             Q+                     d6
                    G+ Z+b0+    T+b3+                              c6+c7+                     J
                       Z+    V+                                       c7+   d1+    W


A=b2+b5  B=c3+d4  C=c1+d2  D=c2+d3  E=b7+d0  F=b3+b6  G=a0+a6  H=a1+a7  I=c0+d5  J=c0+d7
K=b5+c5  L=c4+b4  M=b1+b4  O=a2+a3  P=a4+a5  Q=c6+d1
Z=H+B  Y=B+F X=P+L W=A+D  V=M+C  U=G+K  T=A+E    69 XORs
```

(9)

F. $f = 0x1c3$ PB($R = 1$) Hadamard NON-INVOLUTORY (4 5 1 2) (1 90 91 e1) 37+38=75

```
(4 5 1 2):
                   d6 + d7 + c6 + c7 + d0 + a0 + b7
                     d6 + c6 + d1 + a1 + b0 + b7
                   d7 + c7 + d0 + d2 + a2 + b1 + c0
                        d1 + d3 + a3 + b2 + c1
                        d2 + d4 + a4 + b3 + c2
                        c3 + d3 + d5 + a5 + b4
                d7 + c4 + c6 + c7 + d4 + a6 + b5 + b7
                d6 + d7 + c5 + c6 + d5 + a7 + b6 + b7


 C+               d6+                           a0+                     A
   d1+            d6+                           a1+b0+                  A
 C+   d2+               c0+                     a2+   b1
   d1+   d3+               c1+                  a3+      b2
      d2+   d4+               c2+               a4+         b3
         d3+   d5+               c3+            a5+            b4
            d4+                     c4+       B+a6+               b5+   A
               d5+d6+d7+               c5+      a7+                  b6+A

A=c6+b7  B=c7+d7  C=B+d0       43-6=37 XORs

(1 90 91 e1):
c0+c1+c2+               d0+d1+                  a0+   b1+b2
         c3+                  d2+               a1+   b1+   b3
            c4+                  d3+            a2+      b2+   b4
               c5+                  d4+         a3+         b3+   b5
c0+               c6+                  d5+      a4+b0+         b4+   b6
   c1+               c7+d0+               d6+   a5+   b1+         b5+   b7
   c1+                  d0+                  d7+a6+   b1+            b6
c0+c1+                  d0+                     a7+b0+b1+               b7


c0+ A+c2+                  d1+                  a0+   b1+b2
         c3+                  d2+               a1+   b1+   b3
            c4+                  d3+            a2+      b2+   b4
               c5+                  d4+         a3+         b3+   b5
                  c6+                  d5+      a4+ B+         b4+   b6
    A+               c7+                  d6+   a5+   b1+         b5+   b7
    C+                                       d7+a6+                  b6
    C+                                          a7+ B+                  b7

A=c1+d0  B=b0+c0  C=A+b1     38 XORs
```

(10)

G. $f = 0x1c3$ PB($R = 1$) Hadamard INVOLUTORY (e1 e3 1 2)

```
(e1 e3 1 2):
                   d7 + d0 + d1 + a0 + b7 + c0 + c1
                   d7 + d0 + d2 + a1 + b0 + b7 + c2
                        c3 + d1 + d3 + a2 + b1
                        c4 + d2 + d4 + a3 + b2
                        c5 + d3 + d5 + a4 + b3
                   d6 + c6 + d0 + d4 + a5 + b4 + c0
                   c7 + d0 + d5 + a6 + b5 + b7 + c0
                   d6 + d7 + d0 + a7 + b6 + b7 + c0
```

```
                    C + d1 + a0 + c1
                    A + d0 + d2 + a1 + b0 + c2
                        c3 + d1 + d3 + a2 + b1
                        c4 + d2 + d4 + a3 + b2
                        c5 + d3 + d5 + a4 + b3
                   d6 + c6 + d4 + a5 + b4 + B
                   c7 + d5 + a6 + b5 + b7 + B
                   d6 + a7 + b6 +  C

         A=b7+d7  B=d0+c0  C=A+B     36 XORs
```

(11)

H. $f = 0x187$ SPB($R = x^{-4}$) Hadamard NON-INVOLUTORY (2 8 10 20) (5 14 28 50) 33+40=73

```
(2 8 10 20):  37-4=33XORs
                a0 + a2 + a3 + b0 + b1 + c0 + d7
             a1 + a2 + a4 + b0 + b2 + c1 + d0 + d7
                     a5 + b3 + c2 + d1 + d7
                       a6 + b4 + c3 + d2
                     a0 + a7 + b5 + c4 + d3
                       a1 + b6 + c5 + d4
                  a0 + a2 + b0 + b7 + c6 + d5
                  a1 + a2 + b0 + c7 + d6 + d7

                a0 + (a2 + b0) + a3 + b1 + c0 + d7
             (a1 + d7) + (a2 + b0) + a4 + b2 + c1 + d0
                     a5 + b3 + c2 + d1 + d7
                       a6 + b4 + c3 + d2
                     a0 + a7 + b5 + c4 + d3
                       a1 + b6 + c5 + d4
                  a0 + (a2 + b0) + b7 + c6 + d5
                  (a1 + d7) + (a2 + b0) + c7 + d6


(5 14 28 50):  40 XORs

 a0 + a2 + a3 + a4 + b0 + b1 + b2 + c0 + c1 + c7 + d0 + d6 + d7
           a1 + a2 + a5 + b0 + b3 + c2 + c7 + d1 + d6
        a4 + a6 + b2 + b4 + c1 + c3 + c7 + d0 + d2 + d6
        a0 + a5 + a7 + b3 + b5 + c2 + c4 + d1 + d3 + d7
             a1 + a6 + b4 + b6 + c3 + c5 + d2 + d4
           a2 + a7 + b0 + b5 + b7 + c4 + c6 + d3 + d5
           a0 + a3 + b1 + b6 + c0 + c5 + c7 + d4 + d6
      a1 + a2 + a3 + b0 + b1 + b7 + c0 + c6 + c7 + d5 + d6

       I+                                Z+          Y+                   O
   a1+ I+                                               X+             A
                                                     Y+    W+          A
                                                        X+    V+          O
   a1+                                                     W+    T
                                                              V+    U
a0+                                      Z+                      T
   a1+                                   Z+                         U

   A=c7+d6  B=c6+d5  C=c5+d4  D=c4+d3  E=c3+d2  F=c2+d1  G=c1+d0
   H=b1+c0  I=a2+b0  J=a4+b2  K=a5+b3  L=a6+b4  M=a7+b5  O=a0+d7
```

```
Y=J+G  X=K+F  W=L+E  V=M+D     R=H+a3  S=B+b7  T=C+b6      Z=R+A  U=I+S
```

(12)