IN-64
91297
CR

SERIAL-PARALLEL MULTIPLICATION IN GALOIS FIELDS

p 11

Technical Report II

to

NASA
Goddard Space Flight Center
Greenbelt, Maryland

Grant Number NAG 5-931

Shu Lin
Principal Investigator
Department of Electrical Engineering
University of Hawaii at Manoa
Honolulu, Hawaii 96822

(NASA-CR-181210) SERIAL-PARALLEL MULTIPLICATION IN GALOIS FIELDS (Hawaii Univ.) 11 p Avail: NTIS HC A02/MF A01 CSCL 12A
N87-27469
Unclas
G3/64 0091297

SERIAL-PARALLEL MULTIPLICATION IN GALOIS FIELDS

Shu Lin
University of Hawaii at Manoa
Honolulu, Hawaii 96822

Tadao Kasami
Osaka University
Toyonaka, Osaka 560, Japan

ABSTRACT

In this report, a method for multiplying two elements from the Galois field $GF(2^{ms})$ is presented. This method provides a tradeoff between speed and complexity.

SERIAL-PARALLEL MULTIPLICATION IN GALOIS FIELDS

1. Multiplication over Subfields

In this note, we present a method for multiplying two elements from a Galois field over a subfield. Consider the Galois field $GF(2^{ms})$. This field contains the field $GF(2^s)$ as a subfield and may be regarded as an extension field of $GF(2^s)$. Let α be a primitive element in $GF(2^{ms})$. Then the set, $\{1,\alpha,\alpha^2,\ldots,\alpha^{m-1}\}$, forms a basis for $GF(2^{ms})$ over the subfield $GF(2^s)$. Any element z in $GF(2^{ms})$ can be expressed as a linear sum of $\alpha^0 = 1,\alpha,\alpha^2,\ldots,\alpha^{m-1}$ over $GF(2^s)$ as follows:

$$z = z_0\alpha^0 + z_1\alpha + z_2\alpha^2 + \ldots + z_{m-1}\alpha^{m-1} \tag{1}$$

where $z_i \in GF(2^s)$ for $0 \le i < m$. There is a one-to-one correspondence between z and the m-tuple $(z_0,z_1,\ldots,z_{m-1})$ over $GF(2^s)$ with respect to the basis $\{1,\alpha,\alpha^2,\ldots,\alpha^{m-1}\}$. The basis, $\{1,\alpha,\ldots,\alpha^{m-1}\}$, is called the *polynomial basis*.

The *trace* of an element z in $GF(2^{ms})$ with respect to $GF(2^s)$ is defined as

$$T_m(z) \triangleq z + z^{2^s} + z^{2^{2s}} + \ldots + z^{2^{(m-1)s}} \tag{2}$$

which is an element in $GF(2^s)$ [p. 111, 1]. The trace has the following properties:

1. For any $a \in GF(2^s)$ and $z \in GF(2^{ms})$,

$$T_m(az) = a\, T_m(z);$$

2. For any two elements y and z in $GF(2^{ms})$,

$$T_m(y+z) = T_m(y) + T_m(z) .$$

With respect to the polynomial basis $\{1,\alpha,\alpha^2,\ldots,\alpha^{m-1}\}$, there exists another basis $\{\beta_0,\beta_1,\ldots,\beta_{m-1}\}$ for $GF(2^{ms})$ over $GF(2^s)$ such that

$$T_m(\alpha^i\beta_j) = \begin{cases} 0, & \text{for } i \ne j \\ 1, & \text{for } i = j \end{cases} \tag{3}$$

with $0 \le i, j < m$. The basis $\{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ is called the *dual* (or *complementary*) basis to $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ over $GF(2^s)$. Any element z in $GF(2^{ms})$ can be expressed in either of the following two forms:

1. polynomial form

$$z = a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{m-1}\alpha^{m-1},$$

2. dual form

$$z = b_0\beta_0 + b_1\beta_1 + b_2\beta_2 + \ldots + b_{m-1}\beta_{m-1},$$

where a_i and b_i are elements in $GF(2^s)$ for $0 \le i < m$. These two forms can be converted to each other as follows:

1. $a_i = T_m(z\beta_i)$, and
2. $b_i = T_m(z\alpha^i)$,

for $0 \le i < m$.

Now we consider multiplying two elements from $GF(2^{ms})$. If one element is expressed in polynomial form and the other element is expressed in the dual form, then the multiplication can be achieved in a serial-parallel manner over the subfield $GF(2^s)$. This would give a trade-off between the complexity and speed in the implementation of a multiplier. Let x and y be two arbitrary elements in $GF(2^{ms})$. Express x and y in terms of the polynomial basis $\{1, \alpha, \alpha^2, \ldots, \alpha^{m-1}\}$ and its dual basis $\{\beta_0, \beta_1, \ldots, \beta_{m-1}\}$ respectively.

$$x = x_0 + x_1\alpha + x_2\alpha^2 + \ldots + x_{m-1}\alpha^{m-1}, \quad (4)$$

$$y = y_0\beta_0 + y_1\beta_1 + y_2\beta_2 + \ldots + y_{m-1}\beta_{m-1} \quad (5)$$

where x_i and y_i are in $GF(2^s)$ for $0 \le i < m$. Consider the product $z = xy$ and express z in dual form,

$$\begin{aligned} z &= xy \\ &= z_0\beta_0 + z_1\beta_1 + \ldots + z_{m-1}\beta_{m-1} \end{aligned} \quad (6)$$

where

$$z_i = T_m(z\alpha^i) \tag{7}$$

for $0 \le i < m$.

Next we show how the coefficients of z can be obtained from the coefficients of x and y in a serial manner. It follows from (5) to (7) that

$$\begin{aligned} z_i &= T_m(xy\alpha^i) \\ &= T_m\left(\sum_{\ell=0}^{m-1} y_\ell x\ \beta_\ell \alpha^i\right) \\ &= y_0 T_m(x\beta_0\alpha^i) + y_1 T_m(x\beta_1,\alpha^i) + \ldots + y_{m-1}\ T_m(x\beta_{m-1}\alpha^i) \end{aligned} \tag{8}$$

Setting i=0 in (8), we obtain

$$z_0 = y_0 T_m(x\beta_0) + y_1 T_m(x\beta_1) + \ldots + y_{m-1}\ T_m(x\beta_{m-1}) \tag{9}$$

Since $T_m(x\beta_i) = x_i$ for $0 \le i < m$, it follow from (9) that

$$z_0 = x_0 y_0 + x_1 y_1 + \ldots + x_{m-1}\ y_{m-1}\ . \tag{10}$$

In order to obtain the other m-1 coefficients of z, we define

$$y^{(i)} = y\alpha^i\ , \tag{11}$$

$$y^{(i+1)} = y^{(i)}\alpha\ . \tag{12}$$

Note that $y^{(0)} = y$. We express both $y^{(i)}$ and $y^{(i+1)}$ in dual forms:

$$y^{(i)} = y_0^{(i)}\beta_0 + y_1^{(i)}\beta_1 + \ldots + y_{m-1}^{(i)}\beta_{m-1}\ , \tag{13}$$

$$y^{(i+1)} = y_0^{(i+1)}\beta_0 + y_1^{(i+1)}\beta_1 + \ldots + y_{m-1}^{(i+1)}\beta_{m-1}\ . \tag{14}$$

where

$$y_j^{(i)} = T_m\left(y^{(i)}\alpha^j\right)\ , \tag{15}$$

$$y_j^{(i+1)} = T_m\left(y^{(i+1)}\alpha^j\right) \tag{16}$$

It follows from (12) that, for $0 \le j < m$,

$$\begin{aligned} y_j^{(i+1)} &= T_m\left(y^{(i+1)}\alpha^j\right) \\ &= T_m\left(y^{(i)}\alpha^{j+1}\right) = y_{j+1}^{(i)} \end{aligned} \tag{17}$$

Expression (17) gives a relationship between the coefficients of $y^{(i+1)}$ and those of $y^{(i)}$. From (14) and (17), we obtain

$$y^{(i+1)} = y_1^{(i)}\beta_0 + y_2^{(i)}\beta_1 + \dots + y_{m-1}^{(i)}\beta_{m-2} + y_m^{(i)}\beta_{m-1} \ . \tag{18}$$

where

$$y_m^{(i)} = T_m\left(y^{(i)}\alpha^m\right) \ . \tag{19}$$

The coefficient $y_m^{(i)}$ can be determined as follows

$$\begin{aligned} y_m^{(i)} &= T_m\left(y^{(i)}\alpha^m\right) = T_m\left(\alpha^m \sum_{\ell=0}^{m-1} y_\ell^{(i)}\beta_\ell\right) \\ &= y_0^{(i)}T_m\left(\beta_0\alpha^m\right) + y_1^{(i)}T_m\left(\beta_1\alpha^m\right) + \dots + y_{m-1}^{(i)}\ T_m\left(\beta_{m-1}\alpha^m\right) \ . \end{aligned} \tag{20}$$

From (18) and (20), we see that the coefficients of $y^{(i+1)}$ are completely determined by the coefficients of $y^{(i)}$.

Now we return to the coefficients of z. It follows from (7) that, for $0 \le i < m-1$,

$$\begin{aligned} z_{i+1} &= T_m\left(z\alpha^{i+1}\right) \\ &= T_m\left(xy\alpha^{i+1}\right) = T_m\left(xy^{(i)}\alpha\right) \\ &= T_m\left(\sum_{j=0}^{m-1} x_j y^{(i)}\ \alpha^{j+1}\right) \\ &= \sum_{j=0}^{m-1} x_j T_m\left(y^{(i)}\alpha^{j+1}\right) \ . \end{aligned} \tag{21}$$

Combining (15) and (21), we have

$$z_{i+1} = x_0y_1^{(i)} + x_1y_2^{(i)} + \dots + x_{m-2}\ y_{m-1}^{(i)} + x_{m-1}y_m^{(i)} \ . \tag{22}$$

Putting (10), (17) to (22) altogether, we see that the coefficients, z_0, z_1, ..., z_{m-1} of the product $z = xy$ in dual form can be generated from the coefficients of x and y in a serial manner with m steps,

$$z_0 = x_0 y_0^{(0)} + x_1 y_1^{(0)} + \ldots + x_{m-2}\, y_{m-2}^{(0)} + x_{m-1}\, y_{m-1}^{(0)}$$

$$z_1 = x_0 y_1^{(0)} + x_1 y_2^{(0)} + \ldots + x_{m-2}\, y_{m-1}^{(0)} + x_{m-1}\, y_m^{(0)}$$

$$z_2 = x_0 y_1^{(1)} + x_1 y_2^{(1)} + \ldots + x_{m-2}\, y_{m-1}^{(1)} + x_{m-1}\, y_m^{(1)} \qquad (23)$$

$$\vdots$$

$$z_{m-1} = x_0 y_1^{(m-2)} + x_1 y_2^{(m-2)} + \ldots + x_{m-2}\, y_{m-1}^{(m-2)} + x_{m-1}\, y_m^{(m-2)}$$

where

(1) $y_i^{(0)} = y_i$ for $0 \le i < m$, (24)

(2) $y_j^{(i+1)} = y_{j+1}^{(i)}$ for $0 \le i < m-1$ and $1 \le j < m$, (25)

(3) $y_m^{(i)} = y_0^{(i)} T_m(\beta_0 \alpha^m) + y_1^{(i)} T_m(\beta_1 \alpha^m) + \ldots + y_{m-1}^{(i)} T_m(\beta_{m-1} \alpha^m)$. (26)

2. Serial-Parallel Multiplier

From the expressions of (23) to (26), we see that, if we multiply two elements x and y from $GF(2^{ms})$ in mixed forms, the coefficients of the product z in dual form over $GF(2^s)$ can be determined from the coefficients of x (in polynomial form) and y (in dual form) in a serial manner with m steps. At the i-th step, the coefficient

$$z_i = x_0 y_1^{(i-1)} + x_1 y_2^{(i-1)} + \ldots + x_{m-1}\, y_m^{(i-1)}$$

is formed. To form z_i, m multiplications over $GF(2^s)$ are required. These m multiplications can be carried out in a parallel (or direct) manner using either m $GF(2^s)$ array multipliers or m look-up tables. The coefficients $y_1^{(i-1)}$, $y_2^{(i-1)}$, ..., $y_{m-1}^{(i-1)}$ must be formed separately. From (26), we have

$$y_m^{(i-1)} = y_0^{(i-1)} T_m\left[\beta_0 \alpha^m\right] + y_1^{(i-1)} T_m\left[\beta_1 \alpha^m\right] + \ldots + y_{m-1}^{(i-1)}\; T_m\left[\beta_{m-1} \alpha^m\right] \qquad (27)$$

To form $y_m^{(i-1)}$, m multiplications over $GF(2^s)$ are needed. Each of these multiplications involves a fixed element, $T_m(\beta_i \alpha^m)$, from $GF(2^s)$. As a result, the implementation is simpler. A general serial-parallel multiplier which realizes the multiplication algorithm presented in a previous section is shown in Figure 1. It consists of two parts, the top part forms the coefficients, $z_0, z_1, \ldots, z_{m-1}$ of the product z, which is called the z_i-circuit. The lower part of Figure 1 forms the coefficients, $y_m^{(0)}, y_m^{(1)}, \ldots, y_m^{(m-1)}$, which is called the $y_m^{(i)}$-circuit. The multiplication is completed in m steps (or in m clock times). The z_i-circuit requires m $GF(2^s)$-multipliers, each multiplying two arbitrary elements from $GF(2^s)$. The $y_m^{(i)}$-circuit requires m $GF(2^s)$-multipliers, each multiplying a fixed element and an arbitrary element from $GF(2^s)$. The overall multiplier also needs two ms-input s-output adders.

Suppose we implement the serial-parallel multiplier of Figure 1 by using $GF(2^s)$ array multipliers. Each $GF(2^s)$ array multiplier with two arbitrary inputs requires s^2 AND gates to form the partial products, $(s-1)^2$ two-input X-OR gates to add the partial products and then approximately $(s-1)(\ell-1)$ two-input X-OR gates to reduce the sum to a s-bit symbol in $GF(2^s)$. A $GF(2^4)$ array multiplier with generating polynomial X^4+X+1 is shown in Figure 2. A $GF(2^s)$ array multiplier with one fixed input requires no AND gates and less than $(s-1)^2+(s-1)(\ell-1)$ two-input X-OR gates. Now consider the implementation of the serial-parallel multiplier using look-up tables (ROMs). For multiplying two arbitrary elements from $GF(2^s)$, a single look-up table requires a ROM of 2s inputs, s outputs and 2^{2s} s-bit words. For multiplying an arbitrary element with a fixed element, the look-up table requires a ROM of s inputs, s outputs and 2^s s-bit words.

The multiplication of two elements from $GF(2^{ms})$ can be achieved by using a single Berlekamp's bit-serial multiplier [2]. This implementation is extremely simple, however it takes ms clock times to complete the multiplication, which is s times longer than the serial-parallel multiplier over $GF(2^s)$ of Figure 1. If speed is critical, we may multiply two elements from $GF(2^{ms})$ directly by using a single $GF(2^{ms})$ array multiplier or a single look-up table. A single $GF(2^{ms})$ array multiplier would require $(ms)^2$ AND gates and approximately $(ms-1)^2 + (ms-1)(L-1)$ two-input X-OR gates where L is the number of terms in the generating polynomial for $GF(2^{ms})$. For the serial-parallel multiplier using $GF(2^s)$ array multipliers, a total of $m \cdot s^2$ AND gates and no more than $2m[(s-1)^2 + (s-1)(\ell-1)]$ two-input X-OR gates are needed. For large m ($m \geq 3$), a single $GF(2^{ms})$ array multiplier requires much more AND and X-OR gates than the serial-parallel multiplier over $GF(2^s)$.

A single look-up table for direct multiplication of two arbitrary elements from $GF(2^{ms})$ requires a ROM of 2 ms inputs, ms outputs and 2^{2ms} ms-bit words. However, for the serial-parallel multiplier of Figure 1, it requires a total memory of $m(2^{2s}+2^s)$ s-bit words which is much smaller than 2^{2ms} for $m \geq 2$.

In summary, the serial-parallel multiplication over a subfield presented in this note provides a trade-off between speed and complexity.

REFERENCES

1. F.J. MacWilliams and N.J.A. Sloane, *Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977.

2. E.R. Berlekamp, "Bit-Serial Reed-Solomon Encoders," *IEEE Transactions on Information Theory*, Vol. IT-28, No. 6, pp. 869-874, 1982.

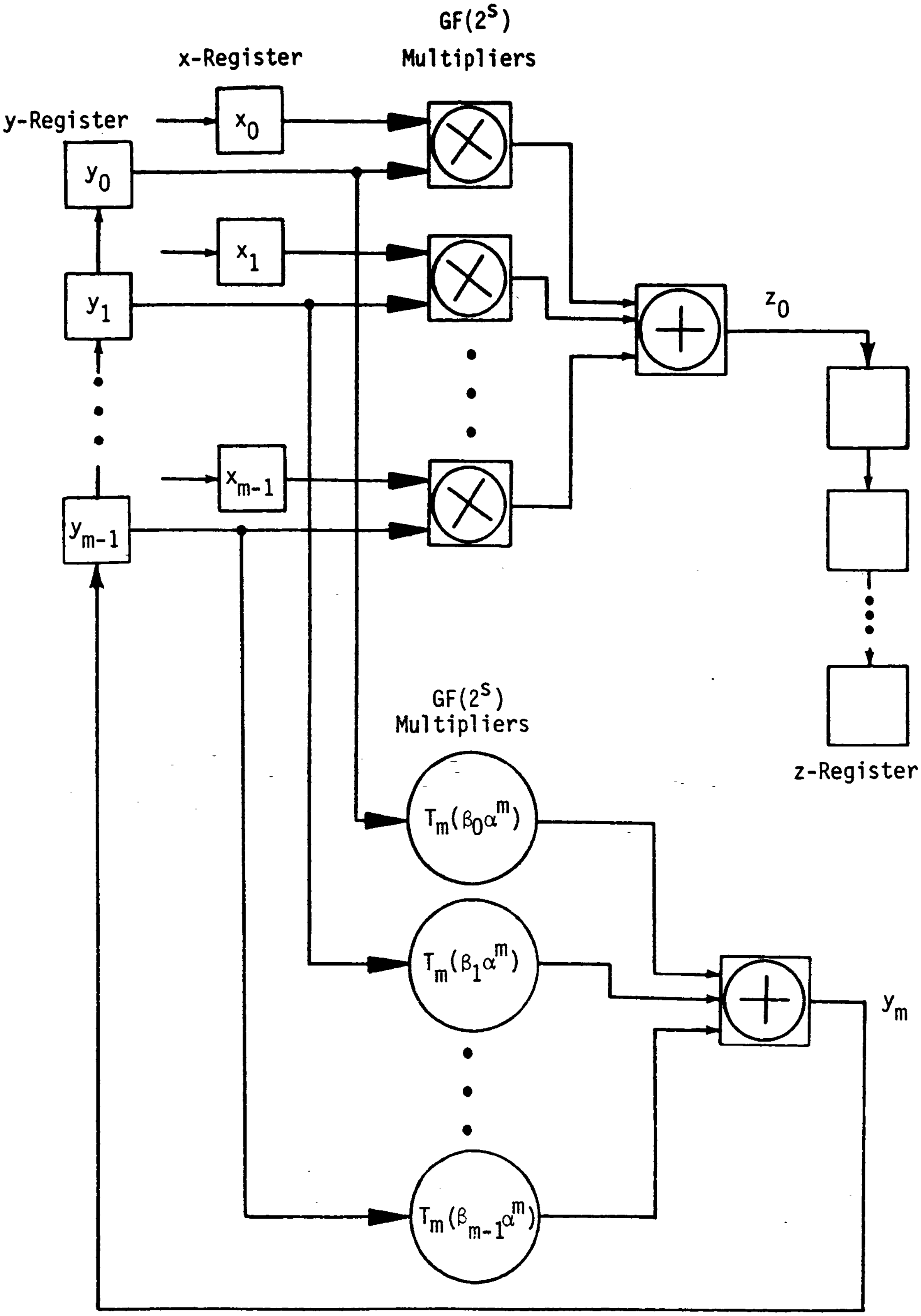

Figure 1 A GF(2^{ms}) serial-parallel multiplier over GF(2^s)

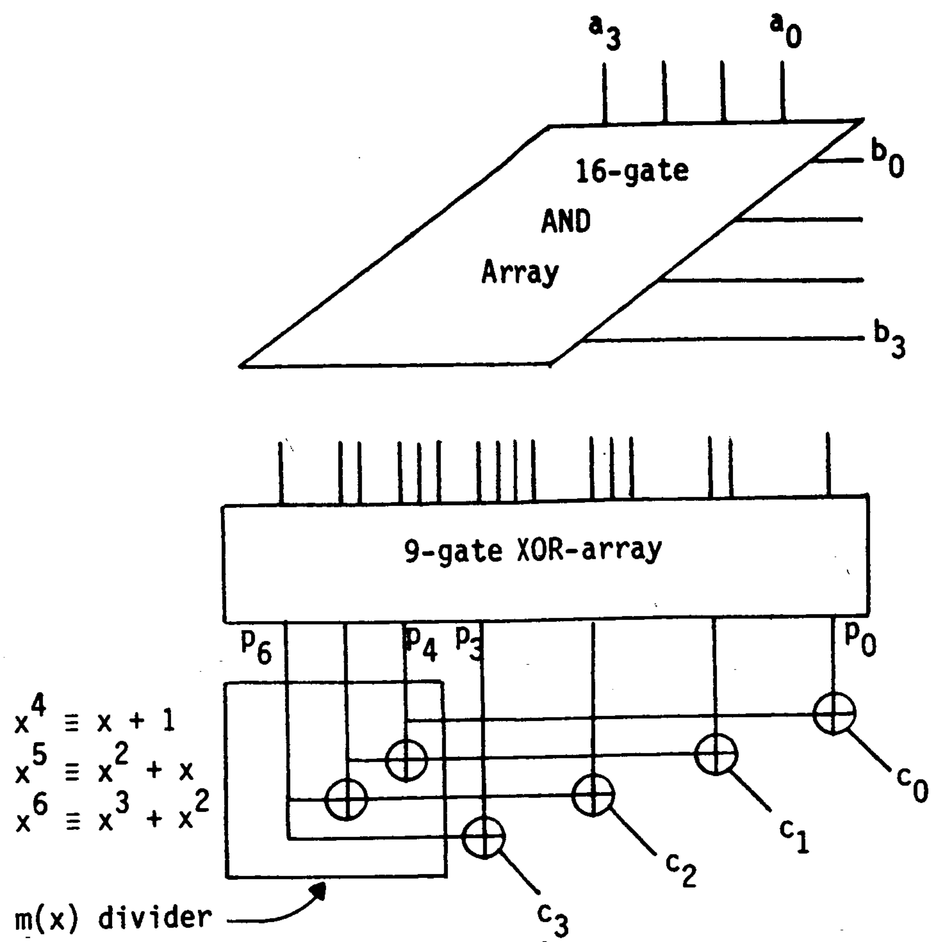

Figure 2 A GF(2^4) multiplier