ARTICLE IN PRESS

Discrete Applied Mathematics ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Discrete Applied Mathematics

journal homepage: www.elsevier.com/locate/dam

Low complexity bit-parallel multiplier for $\mathbb{F}_{2^n}$ defined by repeated polynomials☆

Nam Su Chang [a], Eun Sook Kang [b,*], Seokhie Hong [c]

[a] Department of Information Security, Sejong Cyber University, Seoul, Republic of Korea
[b] Department of Mathematics, Korea University, Sejong, Republic of Korea
[c] Center for Information and Security Technologies, Korea University, Seoul, Republic of Korea

ARTICLE INFO

Article history:
Received 28 August 2015
Received in revised form 18 April 2016
Accepted 14 July 2016
Available online xxxx

Keywords:
Finite field
Irreducible polynomial
Polynomial basis
Multiplication

ABSTRACT

Wu recently proposed three types of irreducible polynomials for low-complexity bit-parallel multipliers over $\mathbb{F}_{2^n}$. In this paper, we consider new classes of irreducible polynomials for low-complexity bit-parallel multipliers over $\mathbb{F}_{2^n}$, namely, repeated polynomial (RP). The complexity of the proposed multipliers is lower than those based on irreducible pentanomials. A repeated polynomial can be classified by the complexity of bit-parallel multiplier based on RPs, namely, C1, C2 and C3. If we consider finite fields that have neither a ESP nor a trinomial as an irreducible polynomial when $n \leq 1000$, then, in Wu's result, only 11 finite fields exist for three types of irreducible polynomials when $n \leq 1000$. However, in our result, there are 181, 232(52.4%), and 443(100%) finite fields of class C1, C2 and C3, respectively.

1. Introduction

Finite fields are widely used in cryptography, and in particular in elliptic curve cryptography. In these applications, the multiplication is the most important operation. The design of efficient finite field multipliers is the key to developing efficient hardware implementations for a class of finite fields $\mathbb{F}_{2^n}$. This operation has been considered by researchers from different points of view. A number of efficient $\mathbb{F}_{2^n}$ multiplication approaches and architectures have been proposed in which different basis representations of field elements are used, such as standard basis, dual basis, and normal basis [1]. In [2], a new approach for designing subquadratic area complexity parallel multipliers is outlined.

When implementing an efficient finite field multiplication, irreducible polynomials are major considerations because the efficiency of modular reduction is influenced by the irreducible polynomial. Low-weight irreducible polynomials are useful when implementing the arithmetic of the finite field $\mathbb{F}_2$. Therefore, the finite field $\mathbb{F}_{2^n}$ multipliers offer better space and time complexity when the field is generated by special irreducible polynomials, such as, all-one polynomials (AOPs) [3,4,7], equally spaced polynomials (ESPs) [3,4,7], trinomials [6,7,9,10] and pentanomials [7,8,12]. AOPs and ESPs offer the highest efficiency, but unfortunately AOPs and ESPs are very rare. Therefore, in many standard implementations, a trinomial or pentanomial is used as an irreducible polynomial. When an irreducible trinomial of degree n does not exist, the next best choice is a pentanomial. However, we find that other classes of irreducible polynomials exist, namely, repeated

☆ This research was supported by Next-Generation Information Computing Development Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT & Future Planning (No. NRF-2014M3C4A7030649).

* Corresponding author.
E-mail address: kes@korea.ac.kr (E.S. Kang).

http://dx.doi.org/10.1016/j.dam.2016.07.014
0166-218X/

Please cite this article in press as: N.S. Chang, et al., Low complexity bit-parallel multiplier for $\mathbb{F}_{2^n}$ defined by repeated polynomials, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.07.014

polynomial (RP) where a bit-parallel multiplier using the polynomial basis can be built with lower complexity than that for pentanomials. In this paper, we define and discuss repeated polynomials. In addition, we present how low-complexity bit-parallel multipliers using the polynomial basis can be built based on irreducible RPs. In particular, for the four finite fields using the irreducible pentanomial recommended for an elliptic curve cryptosystem (ANSI X9.62, ANSI X9.63, IEEE P1363, and SEC 1), the irreducible RPs exist in all finite fields ($n = 131, 163, 283, 571$).

In $\mathbb{F}_{2^n}$, multiplication can be computed with the addition (XOR) and multiplication (AND) over the ground field $\mathbb{F}_2$. Therefore, the space complexity of bit-parallel multipliers in $\mathbb{F}_{2^n}$ is often represented in terms of the total number of AND and XOR gates used. The corresponding time complexity is given in terms of the maximum delay faced by a signal due to one two-input AND and XOR gate. In this paper, we denote the total number of a two-input AND gates and the total number of a two-input XOR gates as N_A and N_X, respectively. In addition, let T_A, T_X and T_C be the delay of a two-input AND gate, that of a two-input XOR gate and the total gate delay, respectively.

The remainder of this paper is organized as follows: in Section 2, we provide a brief review of finite field multiplication using the polynomial basis in $\mathbb{F}_{2^n}$. In Section 3, the definition of the RP is given. In addition, we present how low-complexity bit-parallel multipliers using the polynomial basis can be built based on irreducible RPs. Efficient bit-parallel multipliers based on RPs are introduced in Section 4. In Section 5, complexity comparisons are made between the proposed multipliers and the previous proposals. Finally, conclusions are given in Section 6.

2. Polynomial basis multiplication over $\mathbb{F}_{2^n}$

Let $f(x) = x^n + \sum_{i=1}^{n-1} f_i x^i + 1$ be an irreducible polynomial of degree n over $\mathbb{F}_2$, where $f_i \in \mathbb{F}_2$. Let α be a root of $f(x)$. Since the finite field $\mathbb{F}_{2^n}$ is isomorphic to $\mathbb{F}_2[x]/(f(x))$ the polynomial or standard basis is defined by the set $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. Let $a(\alpha) = \sum_{i=0}^{n-1} a_i \alpha^i$ and $b(\alpha) = \sum_{i=0}^{n-1} b_i \alpha^i$ be any two elements in $\mathbb{F}_{2^n}$. Then, $c(\alpha) = \sum_{i=0}^{n-1} c_i \alpha^i \in \mathbb{F}_{2^n}$, the product of $a(\alpha)$ and $b(\alpha)$ can be obtained in two steps:

1. Polynomial multiplication:

$$s(\alpha) = a(\alpha)b(\alpha) = \sum_{i=0}^{2n-2} s_i \alpha^i,$$
$$\text{where} \quad s_i = \sum_{j+h=i} a_j b_h, \ 0 \le j, h \le n-1, \ 0 \le i \le 2n-2.$$

2. Reduction modulo the irreducible polynomial:

$$c(\alpha) = s(\alpha) \mod f(\alpha), \quad \text{where } c(\alpha) = \sum_{i=0}^{n-1} c_i \alpha^i, \ c_i \in \mathbb{F}_2.$$

The complexity of the polynomial multiplication is independent of the choice of irreducible polynomial $f(x)$. The polynomial multiplication step requires n^2 AND gates and $(n-1)^2$ XOR gates. The time delay is $T_A + \lceil \log_2 n \rceil T_X$. The product $c(\alpha)$ in the reduction step is given as follows:

$$c(\alpha) = s(\alpha) \mod f(\alpha) = \sum_{i=0}^{n-1} s_i \alpha^i + \left(\sum_{i=n}^{2n-2} s_i \alpha^i \mod f(\alpha) \right).$$

We define a $(n-1) \times n$ multiplication matrix $\mathbf{T} = (t_{i,j})_{(n-1)\times n}$ as

$$\begin{bmatrix} \alpha^n \\ \alpha^{n-1} \\ \vdots \\ \alpha^{2n-2} \end{bmatrix} = \mathbf{T} \times \begin{bmatrix} \alpha^{n-1} \\ \alpha^{n-2} \\ \vdots \\ 1 \end{bmatrix}.$$

Clearly,

$$\alpha^{n+i} \bmod f(\alpha) = \sum_{j=0}^{n-1} t_{i,j} \alpha^{n-j-1}, \tag{1}$$

for $i = 0, 1, \ldots, n-2$. Then, the formula of $c(\alpha)$ can be rewritten as

$$c(\alpha) = s(\alpha) \mod f(\alpha) = \sum_{i=0}^{n-1} s_i \alpha^i + \left(\sum_{i=n}^{2n-2} s_i \alpha^i \mod f(\alpha) \right)$$

Please cite this article in press as: N.S. Chang, et al., Low complexity bit-parallel multiplier for $\mathbb{F}_{2^n}$ defined by repeated polynomials, Discrete Applied Mathematics (2016), http://dx.doi.org/10.1016/j.dam.2016.07.014