EFFICIENT PARALLEL GAUSSIAN NORMAL BASES
MULTIPLIERS OVER FINITE FIELDS

Yongtae Kim

Abstract. The normal basis has the advantage that the result of squaring an element is simply the right cyclic shift of its coordinates in hardware implementation over finite fields. In particular, the optimal normal basis is the most efficient to hardware implementation over finite fields. In this paper, we propose an efficient parallel architecture which transforms the Gaussian normal basis multiplication in $GF(2^m)$ into the type-I optimal normal basis multiplication in $GF(2^{mk})$, which is based on the palindromic representation of polynomials.

1. Introduction

In hardware implementation, finite field arithmetic depends on the basis representation, and the type-I optimal normal basis generated by the irreducible All One Polynomial(AOP) is the best known efficient among normal bases implementations. From [3,6,13,14], we recognize that the parallel multiplier with the type-I optimal normal basis is the most efficient. We thus like to embed the finite field $GF(2^m)$ with the Gaussian normal basis of type-k into its extension field $GF(2^{mk})$ with the type-I optimal normal basis[12]. It is well known that if the finite field $GF(2^m)$ has the Gaussian normal basis of type $k$, and the multiplicative subgroup modulo $mk + 1$ denoted by $GF(mk + 1)^*$ is equal to

---

Received June 1, 2007. Accepted August 22, 2007.

2000 Mathematics Subject Classification: 11Y40, 94A60.

Key words and phrases: Finite fields, Massey-Omura multiplier, Gaussian Normal Basis, ECC.

This paper was partially supported by Gwangju National University of Education 2006.
the multiplicative cyclic group generated by 2 modulo $mk + 1$ denoted by $< 2 >$, then not only $GF(2^m)$ is the subfield of $GF(2^{mk})$ but also $GF(2^{mk})$ contains the type-I optimal normal basis. In this case $GF(2^m)$ can be embedded into $GF(2^{mk})$ with the type-I optimal normal basis. NIST recommended two elliptic curves over the fields $GF(2^{163})$ and $GF(2^{409})$ which have type-IV Gaussian normal bases. For $m \leq 2000$, nearly half of them having Gaussian normal bases of type-II,VI and X contained in IEEE draft P1363, ANSI and X9.63[1] satisfy the condition $GF(mk + 1)^* = < 2 >$ when $m$ is odd, and moreover ECC is mainly implemented over the field $GF(2^m)$ for odd prime $m$. So there need efficient algorithms over the field $GF(2^m)$ for odd prime $m$. For odd $m$, it is well known that if $GF(2^m)$ has the Gaussian normal basis of type $k$ and $GF(2^{mk})$ as the extension field of $GF(2^m)$ has the type-I optimal normal basis, then the product of two elements of $GF(2^m)$ with respect to the Gaussian normal basis can be represented with respect to the type-I optimal normal basis of $GF(2^{mk})$, which is based on the palindromic representation of polynomials. Applying this property, we, in this paper, propose an architecture for an efficient parallel multiplier which transforms the Gaussian normal basis multiplication in $GF(2^m)$ into the type-I optimal normal basis multiplication in $GF(2^{mk})$.

2. Preliminaries

Throughout this paper, each element of the finite field will be represented with respect to the normal basis. We denote the multiplicative subgroup of the finite field $GF(mk + 1)$ modulo $mk + 1$ and the multiplicative cyclic group generated by 2 modulo $mk + 1$ by $GF(mk + 1)^*$ and $< 2 >$ respectively. We now outline the process of the construction of normal bases of low complexity. Let $m, k$ be positive integers, $n = mk$ and $n + 1 \neq 2$ prime. Let $\tau$ be the element of $GF(n + 1)^*$, the multiplicative subgroup modulo $n + 1$, of order $k$, i.e., $k$ is the least