$GF(2^m)$상의 고속 타원곡선 암호 프로세서 - Part I 워드레벨 ALU 설계

*김창훈, **권윤기, **권순학, *홍춘표

* 대구대학교 ** 성균관대학교

chkim@dsp.daegu.ac.kr shkwon@skku.edu

High Performance Elliptic Curve Cryptographic Processor - Part I Word Level ALU Design

*Chang Hoon Kim, **Yoon Ki Kwon, **Soonhak Kwon, and *Chun Pyo Hong

Daegu Univ. Sungkyunkwan Univ.

요 약

본 논문에서는 Gaussian Normal Basis(GNB)를 이용하여 $GF(2^m)$상의 타원곡선 암호 프로세서를 위한 새로운 ALU를 제안한다. 제안한 ALU는 $\lceil m/w \rceil$ 사이클 마다 곱셈의 연산을 출력하며, $\{\lfloor \log_2(m-1) \rfloor + H(m-1)\} \times \lceil m/w \rceil$ 사이클 마다 역원 연산을 출력한다. 여기서 w는 워드크기이고 H는 주어진수의 이진 표현에 대한 Hamming Weight이다. 따라서, 본 논문에서 제안된 ALU는 워드크기 w의 선택에 따라 처리시간 및 하드웨어 면적에 있어 상충관계를 개선 할 수 있다.

1. 서 론

타원곡선 암호 시스템(Elliptic Curve Cryptosystem: ECC)는 유한체 상에서 구현되며, 사용되는 유한체는 $GF(p)$, $GF(p^m)$ 그리고 $GF(2^m)$이 있다 (여기서 p는 소수이다). 이중 $GF(2^m)$은 0과 1을 원소로 같는 $GF(2)$의 m차원 확장 필드로 특히 하드웨어 구현에 적합하다. ECC를 위해 NIST[1] 및 IEEE 1363[2]에서 권고하는 $GF(2^m)$의 원소 표기법에는 GNB와 PB(Polynormial Basis)가 있다. 각 기저표기법은 장단점을 가지는데, PB를 이용할 경우 규칙적인 하드웨어구조를 얻기 쉽고 GNB를 이용할 경우 $GF(2^m)$상의 임의의 원소 A^{2^s}는 간단히 s-비트만큼 순환 쉬프트 연산으로 구할 수 있다. 또한 GNB를 이용할 경우 m이 정해진다면, Itoh-Tsujii 알고리즘을 이용하여 역원 연산을 고속으로 수행 할 수 있다.

본 논문에서는 ECC를 위해 GNB를 이용하여 $GF(2^m)$상의 새로운 ALU를 제안한다. 제안된 ALU는 워드레벨의 곱셈기를 사용하며, 역원 연산을 위해 Itoh-Tsujii 알고리즘[5]을 멀티플렉서를 이용하여 직접적으로 구현한다. 따라서 제안된 연산기는 $\lceil m/w \rceil$ 사이클 마다 곱셈의 연산을 출력하며, $\{\lfloor \log_2(m-1) \rfloor + H(m-1)\} \times \lceil m/w \rceil$ 마다 역원 연산을 출력한다. 여기서 w는 워드크기이고 H는 주어진수의 이진 표현에 대한 Hamming Weight이다.

2. GNB를 이용한 $GF(2^m)$상의 워드레벨 곱셈기

2.1 GNB를 이용한 $GF(2^m)$상의 비트-레벨 곱셈 알고리즘

유한체 $GF(2^m)$은 $GF(2)$상의 m차원 벡터 공간으로 $GF(2^m)$상의 원소 A는 기저 $\{\alpha_0, \alpha_1, \cdots, \alpha_{m-1}\}$에 대해

$$A = \sum_{i=0}^{m-1} a_i \alpha_i = a_0\alpha_0 + a_1\alpha_1 + \cdots + a_{m-1}\alpha_{m-1}, \quad a_i \in GF(2) \quad (1)$$

와 같이 표현할 수 있으며, $N = \{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{m-1}}\}$ 형태의 기저를 NB(Normal Basis)라 한다. $GF(2^m)$상에서 ECC의 높은 안전성을 위해서 소수인 m을 요구한다. 이러한 조건은 Pohlig-Hellman 형태의 공격을 회피하기 위해 필요하다. 예를 들면, NIST[1]와 IEEE P1363[2]에서 ECDSA(Elliptic Curve Digital Signature Algoritym)을 위해 권고하는 필드 사이즈 m=163, 233, 283, 409, 571로서 m은 모두 홀수인 소수이다. 따라서 본 논문에서는 m이 홀수인 경우에 대해서만 고려한다.

정의 1. m, k를 소수 $p \neq 2$에 대해, $p=mk+1$인 양의 정수라 하고, $K = \langle \tau \rangle$는 $GF(p)$에서 위수(order) k인 유일한 부분군이라 하자. β가 $GF(2^{mk})$상의 단위원(unity)에 대한 p번째 원시근이라면, 다음 원소