$GF(2^m)$상의 고속 타원곡선 암호 프로세서 - Part II 타원곡선 암호프로세서 설계

*김창훈, *김태호, **권순학, *홍춘표

* 대구대학교 ** 성균관대학교

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

High Performance Elliptic Curve Cryptographic Processor - Part II Design of Elliptic Curve Cryptographic Processor

*Chang Hoon Kim, *Tae Ho Kim, **Soonhak Kwon, and *Chun Pyo Hong

Daegu Univ. Sungkyunkwan Univ.

요 약

본 논문에서는 GNB(Gaussian Normal Basis)를 이용한 최초의 $GF(2^m)$상의 타원곡선 암호 프로세서를 제안한다. 제안된 암호 프로세서는 Lopez-Dahab Montgomery 알고리즘에 기반하며, 기존의 가장 효율적인 구조에 비해 속도 및 면적 모두에 있어 상당한 성능 향상을 보인다.

1. 서 론

타원곡선 암호시스템 (ECC: Elliptic Curve Cryptosystems)에서 가장 중요한 연산은 kP이다. 여기서 k는 큰 정수이고 P는 타원곡선상의 한 포인트이다. 현재까지 kP연산을 위해 바이너리, m-ary, sliding 윈도우 방법등 다양한 알고리즘들이 제안되었다 [1]. 특히 최근에 발표된 Lopez-Dahab Montgomery 정수 곱셈 알고리즘은 다른 알고리즘에 비해 기본 연산이 매우 규칙적일 뿐만 아니라 분기조건이 없기 때문에 다른 알고리즘에 비해 타이밍, 전력, 전자기장 공격에 높은 면역을 가진다[1,4]. 뿐만 아니라 다른 사영 좌표계보다 훨씬 적은 곱셈을 수행한다. 따라서 ECC 프로세서의 Part II인 본 논문에서는 Lopez-Dahab Montgomery 알고리즘에 기반한 ECC 프로세서를 설계한다.

2. Lopez-Dahab kP 알고리즘

P, P_1과 P_2가 타원곡선 E위의 점들이고, P_2는 P_1과 P의합으로 표현된다고 하자. 또한 P_i의 x좌표 값은 X_i/Z_i로 표현할 수 있다고 하자. 여기서 $i \in \{1,2\}$이다. 그러면 우리는 $2P_i$와 P_1+P_2의 x좌표 값은 사영 좌표계에서 아래의 식 (1)과 같이 나타낼 수 있다[1,4].

$$\begin{cases} x(2P_i) = X_i^4 + bZ_i^4 \\ z(2P_i) = Z_i^2 X_i^2 \end{cases} \quad \begin{cases} x(P_1+P_2) = xZ_3 + (X_1Z_2)(X_2Z_1) \\ z(P_1+P_2) = (X_1Z_2 + X_2Z_1)^2 \end{cases} \tag{1}$$

식 (1)로부터 우리는 아래의 Lopez-Dahab 타원곡선 정수 곱셈 알고리즘을 얻을 수 있으며, 아래 알고리즘의 단계 7은 Projective 좌표계에서 Affine 좌표계로의 변환을 수행한다[4].

알고리즘 1. Lopez-Dahab 타원곡선 정수 곱셈 알고리즘

Input : $P=(x,y) \in E(GF(2^m))$, an integer $k \geq 0$
Output : $kP=(x_0,y_0)$

1. If $k=0$ or $x=0$, then stop and output $kP=O$ or P
2. $k \leftarrow (k_{l-1},\cdots,k_1,k_0)_2$
3. $(X_1,Z_1) \leftarrow (x,1), (X_2,Z_2) \leftarrow (x^4+b, x^2)$
4. for $i=s-2$ down to 0 do
5. $\quad Z_3 \leftarrow (X_1Z_2 + X_2Z_1)^2$
6. $\quad$ if $k_i = 1$ then
   $X_1 \leftarrow xZ_3 + (X_1Z_2)(X_2Z_1)$, $Z_1 \leftarrow Z_3$,
   $X_2 \leftarrow X_2^4 + bZ_2^4$, $Z_2 \leftarrow X_2^2 Z_2^2$
   else
   $X_2 \leftarrow xZ_3 + (X_1Z_2)(X_2Z_1)$, $Z_2 \leftarrow Z_3$,
   $X_1 \leftarrow X_1^4 + bZ_1^4$, $Z_1 \leftarrow X_1^2 Z_1^2$
   end if
   end for
7. $x_0 \leftarrow \dfrac{X_1}{Z_1}$,
   $y_0 \leftarrow \dfrac{1}{x} \cdot (x+\dfrac{X_1}{Z_1})\left\{(x+\dfrac{X_1}{Z_1})(x+\dfrac{X_2}{Z_2})+x^2+y\right\}+y$
9. return $kP=(x_0,y_0)$