논문 2008-45SD-10-4

$GF(3^m)$의 Digit-Serial 유한체 곱셈기

(Digit-Serial Finite Field Multipliers for $GF(3^m)$)

장 남 수*, 김 태 현*, 김 창 한**, 한 동 국***, 김 호 원****

(Nam Su Chang, Tae-Hyun Kim, Chang Han Kim, Dong-Guk Han, and Ho Won Kim)

요 약

최근 페어링 기반의 암호시스템에 대한 연구가 활발히 진행되고 있으며, 암호시스템의 효율성은 기존의 공개키 암호시스템과 같이 유한체에 의존한다. 페어링 기반의 암호시스템의 경우 주로 GF(3^m)에서 고려되며 유한체 연산에서 곱셈 연산이 효율성에 가장 큰 영향을 미친다. 본 논문에서는 삼항 기약다항식 기반의 새로운 GF(3^m) MSD-first Digit-Serial 곱셈기를 제안한다. 제안하는 MSD-first Digit-Serial 곱셈기는 모듈러 감산 연산부를 병렬화하여 공간복잡도는 기존의 결과와 거의 같으나 Critical Path Delay가 기존의 1MUL+(log $\lceil n \rceil$ +1)ADD에서 1MUL+(log $\lceil n+1 \rceil$)ADD으로 감소한다. 따라서 Digit이 2^k가 아닌 경우 1번의 덧셈에 대한 시간 지연이 감소한다.

Abstract

Recently, a considerable number of studies have been conducted on pairing based cryptosystems. The efficiency of pairing based cryptosystems depends on finite fields, similar to existing public key cryptosystems. In general, pairing based ctyptosystems are defined over finite fields of chracteristic three, $GF(3^m)$, based on trinomials. A multiplication in $GF(3^m)$ is the most dominant operation. This paper proposes a new most significant digit(MSD)-first digit-serial multiplier. The proposed MSD-first digit-serial multiplier has the same area complexity compared to previous multipliers, since the modular reduction step is performed in parallel. And the critical path delay is reduced from 1MUL+(log $\lceil n \rceil$ +1)ADD to 1MUL+(log $\lceil n+1 \rceil$)ADD. Therefore, when the digit size is not 2^k, the time delay is reduced by one addition.

Keywords : Digit-Serial Multiplier, Elliptic Curve Cryptosystem, Pairing Based Cryptosystem, Hardware Architecture

I. 서 론

최근 페어링(pairing)의 겹선형성(bilinearity)과 같은 특성들이 새로운 암호시스템에 사용되면서 페어링 연산의 효율성에 대한 관심과 연구가 증가하고 있다. 페어링 기반의 암호시스템(Pairing Based Cryptosystem)은 유한체 연산 중 곱셈 연산을 주된 연산으로 한다.

타원곡선 암호시스템에서 사용되는 유한체 $GF(p)$와 $GF(2^m)$에 대한 하드웨어 연구는 많이 진행되었다. 하지만 페어링 기반 암호시스템의 효율성을 높이기 위한 Duursma-Lee[5]알고리즘과 η_T 페어링[1]등의 사용으로 인하여 유한체 $GF(3^m)$에 대한 하드웨어 구현

* 학생회원, 고려대학교 정보경영공학전문대학원
(Graduate School of Information Management and Security, Korea University)
** 정회원, 세명대학교 정보통신학부
(School of Information & Communication systems, Semyung University)
*** 정회원, 한국전자통신연구원
(Electronics and Telecommunications Research Institute)
**** 정회원, 부산대학교 정보컴퓨터공학부
(Dept of Computer Science & Engineering, Pusan University)
※ 본 연구는 지식경제부 및 정보통신연구진흥원의 대학 IT연구센터 지원사업의 연구결과로 수행되었음 (IITA-2008-(C1090-0801-0025))
접수일자: 2008년1월30일, 수정완료일: 2008년10월6일

방법이 필요하게 되었다. 다항식 기저(polynomial basis)를 이용한 $GF(3^m)$ 연산 방법들은 [3, 8~9]에서 연구되었다. [3~4]에서는 Bit-Serial과 Digit-Serial 방법의 MSB- first(MSD-first) 타입과 LSB-first (LSD-first) 타입의 곱셈기를 소개하였다. [10]에서는 기본적인 MSB-first Bit-Serial 곱셈기를 Digit-Serial로 확장한 곱셈기를 제안하였으며, [11]에서는 [10]의 곱셈기에서 부분곱의 모듈러 연산부를 제거한 Digit-Serial 곱셈기를 제안하였다.

본 논문에서는 새로운 MSD-first Digit-Serial 곱셈기를 제안한다. 제안하는 곱셈기는 삼항 기약다항식을 기반으로 설계되며, 삼항 기약다항식이 사용되는 페어링 기반의 암호시스템의 $GF(3^m)$에 기반한다. 제안하는 곱셈기는 기존의 MSD-first 곱셈기에 비하여 작은 시간지연을 가지며, 표수에 의존하지 않고 적용가능하다.따라서 기존의 곱셈기와 비교하여 공간 복잡도는 거의 같으나 Critical Path Delay가 기존의 1MUL+(log $\lceil n \rceil + 1$)ADD에서 1MUL+(log $\lceil n+1 \rceil$)ADD으로 감소한다. 따라서 Digit이 2^k가 아닌 경우 1번의 덧셈에 대한 시간 지연이 감소한다.

본 논문의 구성은 다음과 같다. Ⅱ장에서는 기존의 MSB-first Digit-Serial 곱셈기에 대하여 기술한다. Ⅲ장에서는 제안하는 MSB-first Digit-Serial 곱셈기를 기술한다. Ⅳ장에서는 기존의 결과와 제안하는 곱셈기의 효율성을 비교하고 결론을 내린다.

Ⅱ. 기존의 MSD-first Digit-Serial 곱셈기

$F(x) = x^m + f_t \cdot x^t + f_0$를 $GF(3)$위에서 차수가 m인 삼항 기약다항식이라 하고 α를 $F(x)$의 해라 하자. 그러면 유한체 $GF(3^m)$는 $GF(3)[X]/(F(x))$와 동형이기 때문에 $GF(3^m)$의 원소 $A(\alpha)$는 다항식 기저를 이용해서 다음과 같이 표현할 수 있다.

$$\begin{aligned} A(\alpha) &= a_{m-1}x\alpha^{m-1} + \cdots + a_1\alpha + a_0 \\ &= (a_{m-1}\cdots a_1 a_0), \\ &\quad where\ a_i \in GF(3). \end{aligned}$$

그리고 α는 $F(x)$의 해이므로 $F(\alpha)=0$에 의하여

$$\alpha^m = -f_t\alpha^t - f_0$$

이다. A(α), B(α)$\in GF(3^m)$라 하면, R(α)=A(α)+B(α)는

$$R(\alpha) = A(\alpha) + B(\alpha) = \sum_{i=0}^{m-1}(a_i + b_i)\alpha^i$$

이고 $a_i + b_i$는 GF(3)의 덧셈 연산이다.

1. MSD-first Digit-Serial 곱셈기

본 절에서는 기존의 Digit-Serial 곱셈기에 대하여 기술한다[10~11]. $GF(3^m)$의 곱셈은 두 원소의 케리(Carry) 전파가 없는 다항식 곱셈과 주어진 F(x)를 이용한 모듈러 연산으로 구성된다. 본 논문에서는 일반적인 페어링 기반의 암호 시스템에서 사용하는 삼항 기약다항식 $f(x) = x^m + f_t x^t + f_0$만을 고려한다.

Digit 단위의 연산은 한번의 프로세스에 D개의 계수를 처리하므로 Bit 단위보다 고속처리 가능하다. Digit의 크기를 D라 하면 $GF(3^m)$의 원소 $A(\alpha)$는 다음과 같이 표현된다.

$$\begin{aligned} A(\alpha) &= a_{\lceil m/D \rceil - 1}x\alpha^{\lceil m/D \rceil - 1} + \cdots + a_1\alpha + a_0 \\ &= (a_{\lceil m/D \rceil - 1}\cdots a_1 a_0),\ where\ a_i \in GF(3). \end{aligned}$$

우선 [10]의 MSD-first Digit-Serial 곱셈기에 대하여 살펴본다. [10]의 곱셈기는 전체 $\lceil m/D \rceil$ 클럭 사이클을 수행하며 i번째 반복에서 부분곱 D개의 합은

$$U(\alpha) = \sum_{j=0}^{D-1} a_{Di+j} \cdot B(\alpha) \cdot \alpha^j \mod F(x)$$

이며, 이때 $U(\alpha)$는 m-1차 다항식이다. 다음은 계산된 $U(\alpha)$와 누적값 $R(\alpha)$를 더하는 단계이다. 이와 같은 MSE-first Digit-Serial 곱셈을 알고리즘으로 정리하면 Algorithm 1과 같다.

Algorithm 1. [10]의 MSD-first Digit-Serial 곱셈기

Input : $A(x) = \sum_{i=0}^{m-1} a_i x^i$,

$B(x) = \sum_{i=0}^{m-1} b_i x^i, \quad a_i, b_i \in GF(3)$

Output: $R(\alpha) = A(\alpha) \cdot B(\alpha) = \sum_{i=0}^{m-1} r_i x^i, \quad r_i \in GF(3)$

1. $R(\alpha) = 0$
2. For i = $\lceil m/D \rceil - 1$ to 0 do
   2.1 $U(\alpha) = \sum_{j=0}^{D-1} a_{Di+j} \cdot B(\alpha) \cdot \alpha^j \mod F(x)$
   2.2 $R(\alpha) = R(\alpha) \cdot \alpha^D + U(\alpha) \mod F(x)$
3. Return $R(\alpha)$

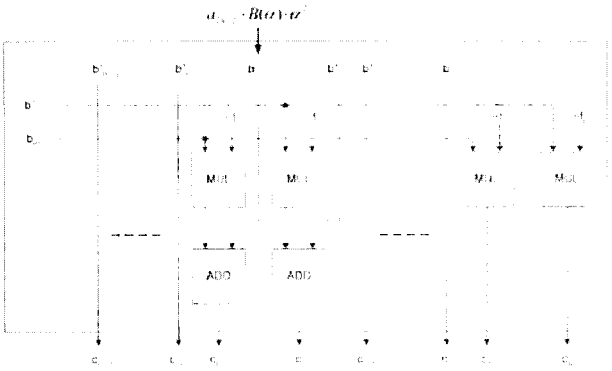

그림 1. $a_{Di+2} \cdot B(\alpha) \cdot \alpha^2 \mod F(x)$의 연산 구조
Fig. 1. The architecture of $a_{Di+2} \cdot B(\alpha) \cdot \alpha^2 \mod F(x)$.

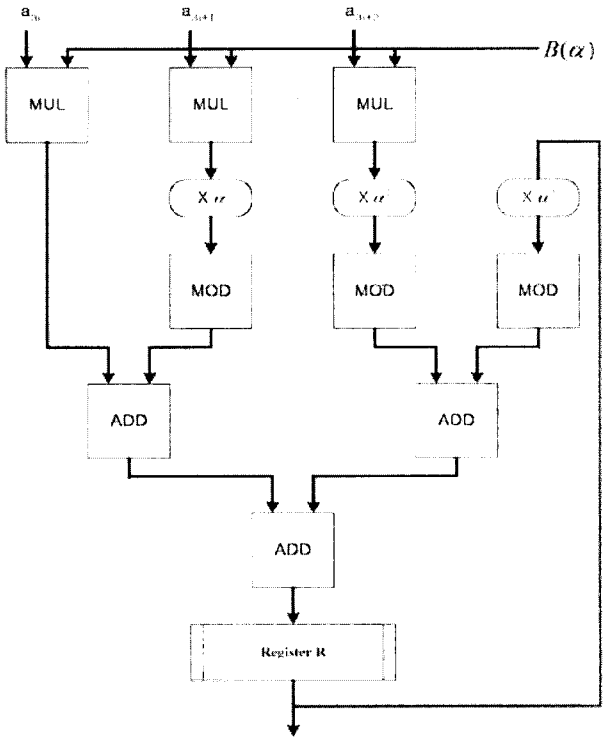

그림 2. [10]의 MSD-first Digit-Serial 곱셈기(D=3)
Fig. 2. MSD-first Digit-Serial Multipier proposed in [10](D=3)

Algorithm 1의 경우 단계 2.1에서 부분곱마다 감산 연산을 수행하므로 이를 병렬화하는 경우 D(D-1)개의 GF(3) 곱셈기와 D(D-1)/2개의 GF(3) 덧셈기가 필요하다. 부분곱의 모듈러 감산연산부 $a_{Di+j} \cdot B(\alpha) \cdot \alpha^j \mod F(x)$는 그림 1과 같다.

$U(\alpha)$는 D개의 m-1차 다항식의 합이므로 GF(3^m) 덧셈기 D-1개로 구성되며 ($\log \lceil D \rceil$)ADD의 시간지연이 소요된다. 또한, $R(\alpha) \cdot \alpha^D \mod F(x)$연산은 $U(\alpha)$와 병렬로 수행되므로 $R(\alpha)$의 계산에서 1ADD의 시간지연이 소요된다. 따라서 Critical Path Delay는 2·MUL+($\log \lceil D+1 \rceil +1$)·ADD이다. Algorithm 1을 하드웨어로 구성하면 그림 2와 같다.

다음으로 [11]에서 제안된 MSD-first Digit-Serial 곱셈기에 대하여 살펴본다. [11]에서는 [10]과 달리 digit 단위의 프로세스 $U(\alpha)$ 계산에서 모듈러 감산을 수행하지 않고 누적값 $R(\alpha)$의 계산에서 한번에 처리한다. 따라서 매단계마다 부분곱의 합 m+D-2차 다항식의 계산은 다음과 같다.

$$U(\alpha) = \sum_{j=0}^{D-1} a_{Di+j} \cdot B(\alpha) \cdot \alpha^j.$$

다음은 계산된 $U(\alpha)$와 누적값 $R(\alpha)$를 더하는 단계이며, 이때 $R(\alpha)$는 m+D-1차 다항식이다. [11]의 곱셈기는 $U(\alpha)$의 계산에서 모듈러 감산부가 없어 시간지연이 [10]보다 효율적이며 각각의 $a_{Di+j} \cdot B(\alpha) \cdot \alpha^j$는 서로 m-1개 항만 더해지므로 공간복잡도 또한 효율적이다. 물론 $R(\alpha)$가 m+D-1차이므로 이의 모듈러 감산연산부가 증가하나 $U(\alpha)$의 모듈러 감산연산부 감소에 비하여 미비하다. 따라서 $R(\alpha)$의 저장공간 D 비트를 제외한 모든 부분에서 [10]보다 효율적이라 할 수 있다. [11]의 MSD-first Digit-Serial 곱셈기는 Algorithm 2와 같다.

Algorithm 2. [11]의 MSD-first Digit-Serial 곱셈기

Input : $A(x) = \sum_{i=0}^{m-1} a_i x^i, \quad a_{m-1} = 0$

$B(x) = \sum_{i=0}^{m-1} b_i x^i, \quad a_i, b_i \in GF(3)$

Output: $R(\alpha) = A(\alpha) \cdot B(\alpha) = \sum_{i=0}^{m-1} r_i x^i, \quad r_i \in GF(3)$

1. $R(\alpha) = 0$
2. For i = $\lceil m/D \rceil - 1$ to -1 do
   2.1 $U(\alpha) = \sum_{j=0}^{D-1} a_{Di+j} \cdot B(\alpha) \cdot \alpha^j$
   2.2 $R(\alpha) = R(\alpha) \cdot \alpha^D + U(\alpha) \mod F(x)$
3. Return $R(\alpha)$

Algorithm 2의 경우 단계 2.1에서 부분곱의 합을 수행하므로 이를 병렬화하는 경우 Dm개의 GF(3) 곱셈기와 (m-1)(D-1)개의 GF(3) 덧셈기가 필요하다. $U(\alpha)$는 m+D-2차 다항식이고 $R(\alpha) \cdot \alpha^D$가 하위 D개의 계수가 0인 m+D-2차 다항식이므로 $R(\alpha)$의 계산에서

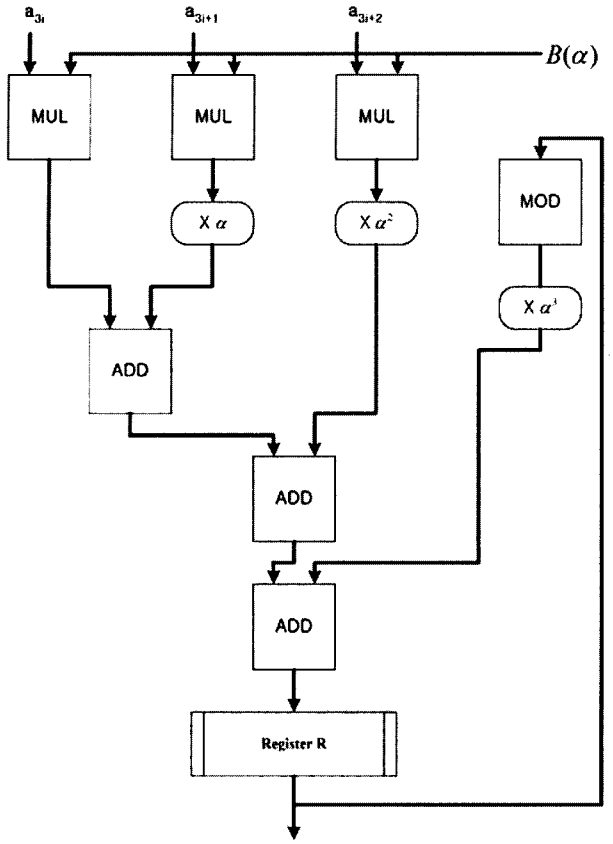

그림 3. [11]의 MSD-first Digit-Serial 곱셈기(D=3)
Fig. 3. MSD-first Digit-Serial Multipier proposed in [11](D=3).

(m-1)개의 GF(3) 덧셈기가 필요하다. 따라서 전체 공간 복잡도는 (Dm+D)의 GF(3) 곱셈기와 (D(m-1)+D)개의 GF(3) 덧셈기가 필요하다. 시간복잡도의 경우 $U(\alpha)$의 계산에서 D개의 m-1차 다항식의 부부곱의 합이므로 1MUL+(log $\lceil D \rceil$)ADD의 시간지연이 소요된다. 또한, $R(\alpha)$ mod F(x)는 $U(\alpha)$와 병렬로 수행되므로 $R(\alpha)$의 계산에서 1ADD의 시간지연이 소요된다. 따라서 Critical Path Delay는 2·MUL+(log $\lceil D \rceil + 1$)·ADD이며 마지막 $R(\alpha)$의 모듈러 연산을 위하여 1번 추가반복한다. Algorithm 2을 하드웨어로 구성하면 그림 3과 같다.

III. 제안하는 MSD-first Digit-Serial 곱셈기

본 절에서는 새로운 GF(3^m) MSD-first Digit-Serial 곱셈기를 제안한다. 제안하는 곱셈기는 [11]에서 제안된 곱셈기의 모듈러 감산 연산부의 병렬화에 기반한다. Algorithm 2에서 $R(\alpha)$는

$$R(\alpha)\cdot\alpha^D \mod F(x) = \sum_{i=0}^{m-1} r_i\alpha^{i+D} \mod F(x)$$
$$= \sum_{i=0}^{D-1} r_{m-1+i}\alpha^{m+i} + \sum_{i=0}^{m-2} r_i\alpha^{i+1} \mod F(x)$$
$$= \sum_{i=0}^{D-1} r_{m-1+i}\left(-f_t\alpha^{t+i} - f_0\alpha^i\right) + \sum_{i=0}^{m-2} r_i\alpha^{i+1} \mod F(x),$$

이다. 또한 Algorithm 2의 반복문에서 i가 $\lceil m/D \rceil - 1$에서 -1까지 감소하는 것을 고려하여 i번째의 $R(\alpha)$를 다음과 같이 표기한다.

$$R(\alpha)^{(i)} = \sum_{j=0}^{m-1} r_j^{(i)}\alpha^j := R(\alpha)^{(i+1)}\cdot\alpha^D + \sum_{j=0}^{D-1} a_{Di+j}\cdot B(\alpha)\cdot\alpha^j \mod F(x).$$

이때, $R(\alpha)^{(\lceil m/D \rceil - 1)} = 0$이다.

Definition 1. A(α)가 GF(3^m)의 원소라 하고 기약 다항식을 F(x)에 대하여 $\widetilde{F}_i(x) = F(x)\cdot x^i (D \le i < 2D)$라 하면,

$$\overline{A}(\alpha) = A(\alpha) - \sum_{i=D}^{2D-1} a_{t+i}\cdot f_t\cdot F(\alpha)\alpha^i$$
$$= A(\alpha) - \sum_{i=D}^{2D-1} a_{t+i}\cdot f_t\cdot \widetilde{F}_i(\alpha)$$

이다. ■

Theorem 1. $A(\alpha), B(\alpha) \in GF(3^m)$이면, Definition 1에 의하여 두 원소의 곱은

$$A(\alpha)B(\alpha) \mod F(x) = (A(\alpha)B(\alpha)\alpha^D \bmod F(x)x^D)/\alpha^D$$
$$= \{\widetilde{A}(\alpha)b(\alpha) \bmod \widetilde{F}_D(x)\}/\alpha^D$$
$$= \{\widetilde{A}(\alpha)\cdot\overline{B}(\alpha) \bmod \widetilde{F}_D(x)\}/\alpha^D$$

이고, 이때 $A(\alpha)\alpha^D = \widetilde{A}(\alpha) = \sum_{i=0}^{m+D-1} \widetilde{a}_i\alpha^i$이다. 그리고 F(x)가 삼항 기약다항식이면, $B(\alpha) \equiv \overline{B}(\alpha) \bmod F(x)$이고 t+D항부터 t+2D-1까지의 계수는 0이다. (단, t<m-2D이다.) ■

GF(3)의 0이 아닌 임의의 원소 a_i는 자신의 역원이므

로 $a_i^2=1$이다. 따라서 $\overline{B}(\alpha)$의 t+D항부터 t+2D-1항 까지의 계수는

$$b_{t+i}\alpha^{t+i}-b_{t+i}\cdot f_t\cdot f_t\alpha^{t+i}=(b_{t+i}-b_{t+i})\alpha^{t+i}$$

이므로, 항상 0이다.($D\leq i<2D$) 따라서 $R(\alpha)\equiv R(\alpha)\cdot\alpha^D+\sum_{j=0}^{D-1}\left(A_{Di+j}\alpha^i\cdot B(\alpha)\right)\bmod F(x)$는 Theorem 1에 의해 $R(\alpha)\equiv R(\alpha)\cdot\alpha^D+\tilde{a}_i\cdot\overline{B}(\alpha)\bmod+\sum_{j=0}^{D-1}\left(a_{Di+j}\alpha^i\cdot B(\alpha)\right)\bmod F(x)$이며 반복 연산을 고려하여 표현하면 다음과 같으며 $\widetilde{F_D}(x)$가 m+D차이므로 $\tilde{R}(\alpha)^{(i+1)}$은 m+D-1차이다.

$$\begin{aligned}R(\alpha)^{(i)}&\equiv R(\alpha)^{(i+1)}\cdot\alpha^D+\tilde{a}_i\cdot\overline{B}(x)\\&\quad+\sum_{j=0}^{D-1}\left(a_{Di+j}\alpha^i\cdot B(\alpha)\right)\bmod\widetilde{F_D}(x)\\&=\tilde{R}(\alpha)^{(i+1)}+\tilde{a}_i\cdot\overline{B}(x)\\&\quad+\sum_{j=0}^{D-1}\left(a_{Di+j}\alpha^i\cdot B(\alpha)\right)\bmod\widetilde{F_D}(x)\\&=\sum_{j=D}^{2D-1}\left(\tilde{r}_{m+j}^{(i+1)}+\tilde{a}_i\cdot\overline{b}_{(m+j)}\right)\alpha^{(m+j)}\\&\quad+\sum_{j=0}^{m+D-1}\left\{\left(\tilde{r}_j^{(i+1)}+\tilde{a}_i\overline{b}_j\right)\right.\\&\quad\left.+\left(\sum_{k=1}^{D-1}\tilde{a}_ib_{j-k}\right)\right\}\alpha^j\bmod\tilde{F}_D(x)\qquad(1)\end{aligned}$$

이고, 이때 b_j에서 j<0이면 $b_j=0$이다. 식 (1)에서 $\tilde{r}_j^{(i+1)}+\tilde{a}_i\overline{b}_j$를 $\delta^{(i,j)}$라 하면 $\delta^{(i,j)}\cdot\alpha^{(m+j)}$는

$$-\delta^{(i,j)}\cdot\tilde{f}_{j,t+j}\alpha^{(t+j)}-\delta^{(i,j)}\cdot\tilde{f}_{j,j}\alpha^j\}$$

이고, 이를 식 (1)에 적용하여 정리하면 $R(\alpha)^{(i)}$의 계수는 다음과 같다.(이때, $\tilde{f}_{j,t+j}$는 $\tilde{F}_j$의 t+j항 계수이다.)

$$r_j^{(i)}\equiv\begin{cases}\widetilde{r_j^{(i+1)}}+\tilde{a}_i\overline{b}_j-\delta^{(i,j)}\tilde{f}_{j,j}+\left(\sum_{k=1}^{D-1}\tilde{a}_i\cdot b_{j-k}\right) & .D\leq j<2D\\ \widetilde{r_j^{(i+1)}}+\tilde{a}_i\overline{b}_j-\delta^{(i,j)}\tilde{f}_{j-t,j}+\left(\sum_{k=1}^{D-1}\tilde{a}_i\cdot b_{j-k}\right) & .t+D\leq j<t+2D.\\ \widetilde{r_j^{(i+1)}}+\tilde{a}_i\overline{b}_j+\left(\sum_{k=1}^{D-1}\tilde{a}_i\cdot b_{j-k}\right) & .otherwise\end{cases}\quad(2)$$

Theorem 2. $\tilde{r}_{m+j}^{(i+1)}+\tilde{a}_i\overline{b}_{m+j}$를 $\delta^{(i,j)}$라 하고, $D\leq j<2D$일 때 $\widetilde{a_{i+1}}\overline{b_{j-D}}+\tilde{a}_i\overline{b}_j$를 $\lambda^{(i,j)}$이라 하면,

$$r_j^{(i)}\equiv\begin{cases}\widetilde{r_j^{(i+1)}}+\tilde{a}_i\overline{b}_j-\delta^{(i,j)}\tilde{f}_{j,j}+\left(\sum_{k=1}^{D-1}\tilde{a}_i\cdot b_{j-k}\right) & .D\leq j<2D\\ \widetilde{r_j^{(i+1)}}+\tilde{a}_i\overline{b}_j-\delta^{(i,j)}\tilde{f}_{j-t,j}+\left(\sum_{k=1}^{D-1}\tilde{a}_i\cdot b_{j-k}\right) & .t+D\leq j<t+2D.\\ \widetilde{r_j^{(i+1)}}+\tilde{a}_i\overline{b}_j+\left(\sum_{k=1}^{D-1}\tilde{a}_i\cdot b_{j-k}\right) & .otherwise\end{cases}$$

이고, i+1번째 반복문에서 $\delta^{(i,j)}$와 $\lambda^{(i,j)}$를 계산할 수 있으면 i번째 반복문에서 $R(\alpha)^{(i)}$의 모든 계수는 한번의 GF(3) 곱셈과 $\lceil\log(D+1)\rceil$번의 덧셈 연산으로 계산된다. ■

$\overline{B}(\alpha)$의 t+D항부터 t+2D-1 까지의 계수는 0이므로 $D\leq j<2D$에 대하여 $r_{t+j}^{(i)}=\widetilde{r_{t+1}^{(i+j)}}+\widetilde{a_i\overline{b_{t-j}}}-\delta^{(i,j)}\cdot\tilde{f}_{j,t+j}=\tilde{r}_{t+1}^{(i+j)}-\delta^{(i,j)}\tilde{f}_{j,t+j}$이고, $\tilde{r}_j^{(i+j)}$는 $r_j^{(i+1)}{}_D$이므로 $\lambda^{(i,j)}$를 $\tilde{a}_{i+1}\overline{b}_{j-D}+\tilde{a}_i\overline{b}_j$이라 하면 $r_j^{(i)}=\widetilde{a_{i+1}}\overline{b_{j-D}}+\tilde{a}_i\overline{b}_j-\delta^{(i,j)}\widetilde{f_{j,j}}+\left(\sum_{k=1}^{D-1}\tilde{a}_ib_{j-k}\right)=\lambda^{i,j}-\delta^{(i,j)}\widetilde{f_{j,j}}+\left(\sum_{k=1}^{D-1}\tilde{a}_ib_{j-k}\right)$이다. 따라서 $\lambda^{(i,j)}$는 i+1번째 반복에서 계산 가능하다. 또한, $\tilde{r}_{m+D}^{(i+1)}=r_m^{(i+1)}=\tilde{r}_m^{(i+2)}+\tilde{a}_{i+1}\overline{b_m}$이고 Definition 1에 의하여 $\overline{b_m}$은 0이므로 $\delta^{(i,j)}=\widetilde{r_m^{(i+2)}}+\widetilde{a_i\overline{b_{m+j}}}$는 i+1번째 반복에서 계산 가능하다. 따라서 $R\alpha)^{(i)}$의 모든 계수는 한번의 GF(3) 곱셈과 $\lceil\log(D+1)\rceil$번의 덧셈 연산으로 계산된다. 제안하는 MSD-first Digit-Serial 곱셈기를 정리하면 Algorithm 3와 같다.

제안하는 Algorithm 3에 대하여 기술하면 다음과 같다. 제안하는 알고리즘은 한번의 곱셈과 $\log\lceil D-1\rceil$번의 덧셈을 $\lceil m/D\rceil+3$번 반복하며 각각 연산에서 (a), (b), (c)는 병렬로 동작한다. (a)는 $\overline{B}(\alpha)$를 초기화하는 과정으로 실제값은 $\overline{B}(\alpha)=B(\alpha)-\left(\sum_{j=0}^{D-1}b_{t+D+j}\cdot f_t\cdot F(\alpha)\alpha^{D+j}\right)$의 계산 값이므로 $0\leq j<D$일 때 $\overline{b}_{m+D+j},\overline{b}_{D+j}$은 F(x)의 계수에 의하여 갱신되며 $\overline{b}_{m+j},\overline{b}_{t+D+j}$은 0 그리고 나머지 $\overline{b}_i$는 b_i와 같다. 따라서 $\overline{b}_{m+D+j},\overline{b}_j$만 계산하면 된다. (b)는 Theorem 2의 $r_j^{(i)}$를 계산하는 부분이다. (c)는 Theorem 2의 $\delta^{(i,j)},\lambda^{(i,j)}$를 계산하는 부분이므로 i번째의 $\delta^{(i,j)},\lambda^{(i,j)}$는 i+1번째에서 계산되어야 한다. 따라서 알고리즘은 i가 $\lceil m/D\rceil+2$일때 $\overline{B}(\alpha)$를 초기화하고 i가 $\lceil m/D\rceil+1$일때 다음 사용할 $\delta^{(m,j)},\lambda^{(m,j)}$를 계산해야 하므로 $\tilde{a}_{m+3D-1},\tilde{a}_{m+D}$을

Algorithm 3. 제안하는 MSD-first Digit-Serial 곱셈

Input : $\tilde{A}(\alpha)=A(\alpha)\alpha^D=\sum_{i=0}^{m+3D-1}\tilde{a}_i\alpha^i=(\overbrace{0,\cdots,0}^{2D},\overbrace{\cdots,0,,a_{m-1},\cdots,a_0}^{\lceil m/D\rceil},,0\overbrace{0,\cdots,0}^{D})$,

$B(\alpha)=\sum_{i=0}^{m-1}b_i\alpha^i=(b_{m-1},\cdots,b_0),\quad a_i,b_i\in GF(3),$

$-f_t,-f_0,-f_tf_0\in GF(3)$

Output: $R(\alpha)=A(\alpha)B(\alpha)\bmod F(x)=\sum_{i=0}^{m-1}r_i\alpha^i,\quad r_i\in GF(3)$

For i=D to 2D-1 do

$\delta_i\leftarrow 0\ ,\ \lambda_i\leftarrow 0,\ \overline{b_{m+i}}\leftarrow 0,\ \ \overline{b_i}\leftarrow 0$

For i = $\lceil m/D\rceil+2$ to 0 do

1. Multiplication

(a) ($\overline{b}(\alpha)$ Initialization) For j=D to 2D-1 do

$\overline{b_{m+j}}\leftarrow b_{t+1}\cdot(-f_t),\quad t_j^1\leftarrow b_{t+j}\cdot(-f_tf_0)$

(b) For j=1 to D-1 do

$v_j\leftarrow a_{Di+j}\cdot B(\alpha)$

end for

$v_0\leftarrow\sum_{\substack{j=0\\0\le j<D,\\2D\le j<t+D,\\t+2D\le j<m}}^{m-1}a_{Di}b_j,$

For j=0 to D-1 do

$v_{0,t+D+j}\leftarrow\delta_j\cdot(-f_t),\ v_{0,D+j}\leftarrow\delta_j\cdot(-f_0)$

end for

(c) (Precomputation) For j=D to 2D-1 do

$t_j^2\leftarrow\overline{b}_{m+j}\cdot\tilde{a}_{D(i-2)+j},\ t_j^3\leftarrow\overline{b_j}\cdot\tilde{a}_{D(i-2)+j}$

2. Addition

(a) ($\overline{b}(\alpha)$ Initialization) For j=D to 2D-1 do

$\overline{b_j}\leftarrow t_j^1+b_j$

(b) $R(\alpha)\leftarrow\sum_{j=2D}^{m-1}(v_{0,j}+r_{j-D})\alpha^j,$

For j=0 to D-1 do

$r_{m+j}\leftarrow r_{m-D+j},\quad r_{D+j}\leftarrow v_{0,D+j}+\lambda_j,\quad r_j\leftarrow v_j$

end for

$R(\alpha)\leftarrow R(\alpha)+\sum_{j=1}^{D-1}v_j,$

(c) (Precomputation) For j=0 to D-1 do

$\delta_j\leftarrow\text{temp2}+t_{j+D}^2+r_{m-D+j},\ \lambda_j\leftarrow t_j^3+v_0$

end for

Return $(R(\alpha)/\alpha^D)$

0으로 할당하여 (a)와 (c)를 준비한다. 제안하는 MSD-first Digit-Serial 곱셈기의 하드웨어 구조는 그림 4와 같다.

그림 4에서 레지스터 R은 2m+2D 비트의 정보를 저

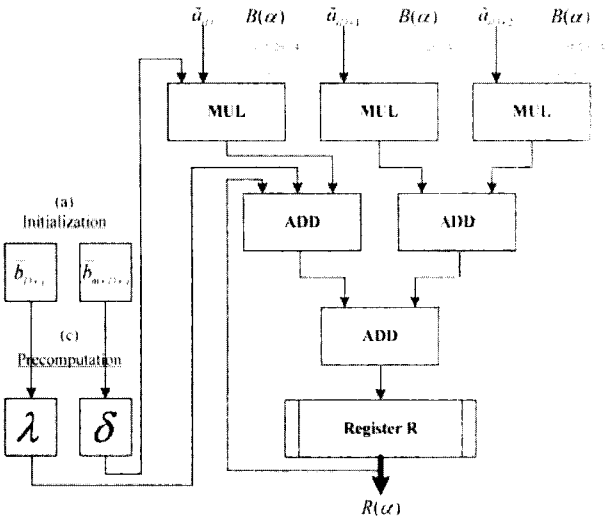

그림 4. 새로운 MSD-first Digit-Serial 곱셈기(D=3)
Fig. 4. The architecture of new MSD-first Digit-Serial Multiplier over GF(3^m)(D=3)

장하며 δ, λ, $\bar{b}_{D+j}$, $\bar{b}_{m-D+j}$는 각각 2D 비트를 저장한다. (a)와 (c)의 구성에서 GF(3) 곱셈기 4D개와 GF(3) 덧셈기 3D개가 소요되며 주 연산부와 병렬로 동작한다. 또한 $A(\alpha)\alpha^D$를 고려하여 동작하므로 2m+2D 비트의 중간값 $R(\alpha)$는 마지막 사이클에서 2m비트의 결과값이 된다.

Ⅳ. 비교 및 결론

본 논문에서는 새로운 MSD-first Digit-Serial 곱셈기를 제안하였다. 제안하는 곱셈기는 삼항기약 다항식의 특징과 모듈러 감산 연산부의 병렬화에 기반한다.

제안하는 곱셈기와 기존의 곱셈기의 시간-공간 복잡도 측면의 효율성을 비교하며 비교 결과는 표 1과 같다. 제안하는 곱셈기는 삼항 기약다항식 기반으로 정의되며, 기존의 곱셈기에 비하여 Critical Path Delay면에서 모두 효율적이고, [11]에 비하여 공간복잡도가 약간 증가한다. 따라서 확장체의 표수가 작은 페어링 기반의 암호시스템에서 고속 동작 가능하므로 고속 연산이 요구되는 장비에 효율적이며 일반적인 삼항 기약다항식 기반의 확장체 GF(p^m)에 모두 적용가능하다.

표 1. MSD-first Digit-Serial 곱셈기의 복잡도 비교
Table 1. Comparison of MSD-first Digit-Serial multipliers.

MSD-first Digit-Serial 곱셈기	Space Complexity			Critical Path Delay	Latency (# clocks)
	MUL	ADD	Register		
[10]의 Digit-Serial 곱셈기	D(m+D-1)	D(m+(D-1)/2)	2m	$\lceil \log(D+1) \rceil + 1$	$\lceil m/D \rceil$
[11]의 Digit-Serial 곱셈기	D(m+1)	Dm	2(m+D)	$\lceil \log(D) \rceil + 1$	$\lceil m/D \rceil + 1$
제안하는 Digit-Serial 곱셈기	D(m+4)	D(m+1)	2(m+5D)	$\lceil \log(D+1) \rceil$	$\lceil m/D \rceil + 3$

※ MUL : GF(3) 곱셈기
※ ADD : GF(3) 덧셈기

참 고 문 헌

[1] P.S.L.M. Barreto, S. Galbraith, C. Ó hÉigeartaigh and M. Scott, "Efficient Pairing Computation on Supersingular Abelian Varieties," *Designs, Codes and Cryptography*, Vol.42, No.3, pp.239-271, 2007.
[2] P.S.L.M. Barreto, H.Y. Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," *CRYPTO 2002, LNCS 2442*, pp.354-368, Springer-Verlag, 2002.
[3] G. Bertoni, J. Guajardo, S. Kumar, G. Orlando C. Paar and T. Wollinger. "Efficient GF(p^m) Arithmetic Architectures for Cryptographic Applications," *CT-RSA 2003, LNCS 2612*, pp.158-175. Springer-Verlag, 2003.
[4] J. Beuchat, T. Miyoshi, Y. Oyama, E. Okamoto, "Multiplication over F_{p^m} on FPGA: A Survey", *ARC-2007, LNCS 4419*, pp.214-225, Springer-Verlag, 2007.
[5] I. Duursma and H.-S. Lee, "Tate pairing implementation for hyperelliptic curves $y^2 = x^p - x + d$," *Asiacrypt 2003, LNCS 2894*, pp.111-123, Springer-Verlag, 2003.
[6] R. Granger, D. Page, and M. Stam, "Hardware and software normal basis arithmetic for pairing based cryptography in characteristic three," *IEEE Transactions on Computers*, Vol.54, No.7, pp.852-860, July 2005.
[7] T. Kerins, W. Marnane, E. Popovici, P. S. L. M. Barreto "Efficient Hardware for the Tate Pairing

Calculation in Characteristic Three," *CHES 2005, LNCS 3659*, pp.398-411, Springer-Verlag, 2005.
[8] T. Kerins, E. M. Popovici and W. P. Marnane. "Algorithms and Architectures for use in FPGA implementations of Identity Based Encryption Schemes," *FPL 2004, LNCS 3203*, pp.74-83, Springer-Verlag, 2004.
[9] D. Page and N. Smart "Hardware Implementation of Finite Fields of Characteristic Three," *CHES 2002, LNCS 2523*, pp.529-539, Springer-Verlag, 2003.
[10] L. Song and K. Parhi, "Low energy digit-serial /parallel finite field multipliers", *Journal of VLSI Signal Processing*, Vol.19, No.2, pp.149-166, July 1998.
[11] C. Shu, S. Kwon, and K. Gaj, "FPGA accelerated Tate pairing based cryptosystemover binary fields", *Cryptography ePrint Archive, Report 2006/179*, 2006.

저 자 소 개

장 남 수(학생회원)-주저자
2002년 2월 서울시립대학교 수학과 학사.
2004년 8월 고려대학교 정보보호 대학원 석사.
2005년~현재 고려대학교 정보경영공학전문대학원 박사과정.
<주관심분야 : 공개키 암호, 암호칩 설계 기술, 부채널 공격 방법론>

김 태 현(학생회원)
2002년 2월 서울시립대학교 수학과 학사.
2004년 8월 고려대학교 정보보호대학원 석사.
2005년~현재 고려대학교 정보경영공학전문대학원 박사과정.
<주관심분야 : 공개키 암호, 부채널 공격, 암호칩 설계 기술>

김 창 한(정회원)-교신저자
1985년 2월 고려대학교 수학과 학사
1987년 2월 고려대학교 수학과 석사
1992년 2월 고려대학교 수학과 박사
1992년 3월~현재 세명대학교 정보통신학부 교수
<주관심분야 : 정수론, 공개키암호, 암호프로토콜>

한 동 국(정회원)
1999년 2월 고려대학교 수학과 학사
2002년 2월 고려대학교 수학과 석사
2005년 2월 고려대학교 정보보호 대학원 박사
2004년 4월 일본 Kyushu Univ., 방문연구원
2005년 4월 일본 Future Univ.-Hakodate, Post.Doc.
2006년 6월 한국전자통신연구원 정보보호연구본부 선임연구원
<주관심분야 : 공개키 암호시스템 안전성 분석 및 고속 구현, 부채널 분석, RFID/USN 정보보호 기술>

김 호 원(정회원)
1993년 경북대학교 전자공학과 학사.
1995년 포항공과대학교 전자전기공학과 석사
1999년 포항공과대학교 전자전기공학과 박사
2003년 7월 독일 Ruhr University Bochum, Post Doc.
1998년 12월 한국전자통신연구원 정보보호연구단 선임연구원/팀장
2008년 부산대학교 정보컴퓨터공학부 조교수
<주관심분야 : RFID 정보보호 기술 및 USN 정보보호 기술, 타원곡선 및 초타원곡선 암호이론, VLSI 설계 >