NAF와 타입 II 최적정규기저를 이용한 $GF(2^n)$ 상의 효율적인 지수승 연산

정회원 권 순 학*, 고 병 환*, 준회원 구 남 훈*, 정회원 김 창 훈**°

NAF and Optimal Normal Basis of Type II and Efficient Exponentiation in $GF(2^n)$

Soonhak Kwon*, Byeonghwan Go* ***Regular Members***, Namhun Koo* ***Associate Member***,
Chang Hoon Kim**° ***Regular Member***

요 약

지수의 signed digit representation을 사용하여 타입 II 최적정규기저에 의해 결정되는 $GF(2^n)$상의 효율적인 지수승 알고리즘을 제안한다. 제안하는 signed digit representation은 $GF(2^n)$에서 non-adjacent form(NAF)를 사용한다. 일반적으로 signed digit representation은 정규기저가 주어진 경우 사용하기 어렵다. 이는 정규 원소의 역원연산이 상당한 지연시간을 갖기 때문이다. 반면에 signed digit representation은 다항식 기저를 이용한 체에 쉽게 적용가능하다. 하지만 본 논문의 결과는 타입 II 최적정규기저(optimal normal basis, ONB), 라는 특별한 정규 기저가 지수의 signed digit representation을 이용한 효율적인 지수승 연산에 이용될 수 있음을 보인다.

Key Words : Gaussian normal basis, Optimal normal basis, Exponentiation, Signed digit representation, NAF (non-adjacent form)

ABSTRACT

We present an efficient exponentiation algorithm for a finite field $GF(2^n)$ determined by an optimal normal basis of type II using signed digit representation of the exponents. Our signed digit representation uses a non-adjacent form (NAF) for $GF(2^n)$. It is generally believed that a signed digit representation is hard to use when a normal basis is given because the inversion of a normal element requires quite a computational delay. However our result shows that a special normal basis, called an optimal normal basis (ONB) of type II, has a nice property which admits an effective exponentiation using signed digit representations of the exponents.

I. 서 론

유한체의 산술 연산은 최근에 많은 암호학 분야에서 다양하게 적용되고 있다. 특히 빠른 지수승 연산은 Diffie-Hellman 키 교환과 의사 랜덤 비트 생성기(pseudo random bit generator)와 같은 응용에 매우 중요하다. 비록 지수승 연산이 많은 소비시간과 복잡한 산술 연산을 갖고 있지만 Diffie-Hellman 키 교환과 같은 몇 가지 경우에는 효율적인 지수승 연산 알고리즘을 구현할 수 있다. $GF(q^n)$이 q가 소

※ 이 논문은 2006년도 정부재원(교육인적자원부 학술연구조성사업비)으로 한국학술진흥재단의 지원을 받아 연구되었음. (KRF-2006-312-C00064)

* 성균관대학교 수학과(shkwon@skku.edu, kobhh@skku.edu, komaton@skku.edu)
** 대구대학교 컴퓨터 · IT공학부(kimch@daegu.ac.kr)(° : 교신저자)

논문번호 : KICS2008-08-352, 접수일자 : 2008년 8월 19일, 최종논문접수일자 : 2008년 11월 29일

수일 때, q^n개 원소를 갖는 유한체라고 하자. 그리고 g를 $GF(q^n)$의 원시 원소(primitive element)라 하자. 임의의 값에 s에 대하여 g^s의 계산 값은 크게 두 가지 방향으로 연구되고 있다. 먼저 BGMW 방법[1]과 같이 벡터 덧셈 체인 및 precomputation을 사용하는 것이 있다. 그리고 이 방법은 Lim과 Lee의 연구[2]와 Rooij[3]의 연구로 발전되었다.

다른 방법으로는 Gao등[4,5,6]이 제안한 방법으로서 $GF(q)$상에서 $GF(q^n)$의 정규 기저를 생성하는 타입 k의 가우스 주기(Gauss period of type k)이라 불리는 특별한 원시 원소를 사용하는 것이다. BGMW 방법 등은 임의의 유한체 $GF(q^n)$에 적합하고 매우 유연하나 이 방법의 이상적인 버전은 $GF(q^n)$상에서 $O(n\log q/\log(n\log q))$의 메모리와 $O(\log(n\log q))$만큼의 곱셈연산을 요구한다. 편의상 $GF(q^n)$상에서의 한 번의 곱셈이 $n^2\log^2 q$번의 비트 덧셈으로 구현가능하다고 가정하면 BGMW 방법은 $O(n^2\log^2 q(n\log q))$만큼의 복잡도를 가진다. BGMW 방법과 비교할 때 Gao등이 제안한 알고리즘은 모든 유한체에 (특히 $GF(p)$와 같이 표수가 큰 유한체) 적용하지는 못한다. 하지만 이 알고리즘은 precomputation이 필요하지 않고 알고리즘의 복잡도는 $O(kqn^2)$만큼의 비트 덧셈연산이다. 그래서 만약 q가 작고 또한 작은 값인 타입 k와 높은 위수를 갖는 가우스 주기가 있다면, Gao등의 방법은 precomputation 방법보다 성능이 낫다.

본 논문에서는 지수의 signed digit representation을 이용한 타입 II의 가우시안 정규 기저 (타입 II 최적 정규기저) 를 갖는 $GF(2^n)$상의 새로운 지수승 연산 알고리즘을 제안한다. 제안하는 signed digit representation은 non-adjacent form (NAF)를 사용하며 이를 이용하여 제안된 새로운 지수승 알고리즘은 타입 II 가우시안 정규 기저를 사용한 기존의 알고리즘보다 33%정도 더 빠른 알고리즘이다. 그리고 제안한 방법과 기존의 signed digit representation을 이용한 trinomial 기저를 사용한 방법과 비교 분석을 통하여 제안한 알고리즘이 삼항식 (trinomial) 기저방법보다 적어도 33%정도 빠르다는 것을 보인다.

Ⅱ. GF(q^n)에서 타입 k 가우시안 정규 기저 및 Gao의 방법

이 장에서는 가우스 주기 이론과 Gao등의 방법을 주로 설명한다[4,5]. n, k는 양의 정수이며 $nk+1=p$를 소수라 하자. 여기서 p는 q를 나누지 않는 소수라 가정한다. 그리고 $K = \langle\tau\rangle$는 $GF(p)^\times$안의 위수 k인 유일한 부분군이라고 하자. β가 $GF(q^{nk})$의 p번째 원시근이라 하면, 다음 원소

$$\alpha=\sum_{j=0}^{k-1}\beta^{\tau^j} \tag{1}$$

를 타입 (n, k) (혹은 타입 k) 가우스 주기(Gauss period)라 한다. $\mathrm{ord}_p q$를 mod p에 대한 q의 위수라 하고, $\gcd(nk/\mathrm{ord}_p q,\ n)=1$이라고 가정하면, α는 $GF(q^n)$상의 정규 원소이다. 즉, $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{n-1}}\}$은 $GF(q^n)$의 기저이고, 이를 타입 k 가우시안 정규기저(Gaussian normal basis, GNB)라 부른다. $K=\langle\tau\rangle$가 순환군 $GF(p)^\times$안의 위수 k인 부분군이기 때문에, 잉여군(quotient group) $GF(p)^\times/K$역시 위수 n인 순환군이고, 군의 생성원은 qK이다. 따라서 $GF(p)^\times$의 coset decomposition을 식 (2)와 같이 disjoint union으로 나타낼 수 있다.

$$GF(p)^\times=K_0\cup K_1\cup K_2\cup\cdots\cup K_{n-1} \tag{2}$$

여기서 $K_i=q^iK$ $(0\le i\le n-1)$로 정의되고 따라서 $GF(p)^\times$의 모든 원소는 적당한 $0\le s\le k-1$과 $0\le t\le n-1$에 대해 $\tau^s q^t$로 유일하게 표현된다. 이를 이용하여 $0\le i\le n-1$에 대해 다음의 식을 얻을 수 있다.

$$\alpha\alpha^{q^i}=\sum_{s=0}^{k-1}\beta^{\tau^s}\sum_{t=0}^{k-1}\beta^{\tau^t q^i}=\sum_{s=0}^{k-1}\sum_{t=0}^{k-1}\beta^{\tau^s(1+\tau^{t-s}q^i)} \tag{3}$$
$$=\sum_{s=0}^{k-1}\sum_{t=0}^{k-1}\beta^{\tau^s(1+\tau^t q^i)}$$

$GF(p)^\times$의 원소인 -1에 대하여 $-1=\tau^u q^v$ 을 만족하는 유일한 $0\le u\le k-1$와 $0\le v\le n-1$가 있다. 만약 $t\neq u$이거나 $i\neq v$ 이면, t와 i에 종속인 $0\le\sigma(t,i)\le n-1$가 존재하여 원소 $1+\tau^t q^i$는 $K_{\sigma(t,i)}$에 속한다. 그래서 적당한 t'에 대해 $1+\tau^t q^i = \tau^{t'} q^{\sigma(t,i)}$를 얻을 수 있다.

이제 $i\neq v$일 때,

$$\alpha\alpha^{q^i}=\sum_{s=0}^{k-1}\sum_{t=0}^{k-1}\beta^{\tau^s(1+\tau^t q^i)}=\sum_{s=0}^{k-1}\sum_{t=0}^{k-1}\beta^{\tau^s(\tau^{t'}q^{\sigma(t,i)})} \tag{4}$$
$$=\sum_{s=0}^{k-1}\sum_{t=0}^{k-1}\beta^{\tau^{s+t'}q^{\sigma(t,i)}}=\sum_{t=0}^{k-1}\alpha^{q^{\sigma(t,i)}}$$

또한 $i=v$일 때,

$$\alpha\alpha^{q^r} = \sum_{s=0}^{k-1}\sum_{t=0}^{k-1}\beta^{r(1+r'q^r)} \quad (5)$$
$$= \sum_{t\neq u}\sum_{s=0}^{k-1}\beta^{r(r'q^{mt+u})} + \sum_{s=0}^{k-1}\beta^{r(1+r'q^r)}$$
$$= \sum_{t\neq u}\sum_{s=0}^{k-1}\beta^{r+r'q^{mt+u}} + \sum_{s=0}^{k-1}1$$
$$= \sum_{l\neq u}\alpha^{q^{mt+u}} + k$$

그러므로 $i\neq v$에 대해 $\alpha\alpha^{q^i}$는 k개만큼의 $\{\alpha, \alpha^q, \alpha^{q^2}, \cdots, \alpha^{q^{m-1}}\}$의 기저 원소의 합으로 계산되어지고 $\alpha\alpha^{q^r}$는 $GF(q)$의 상수 k와 $k-1$개 기저 원소의 합으로 계산된다. 이 개념을 이용하여 Gao등[5]은 다음 결과를 얻었다.

정리 1. $GF(q^n)$상의 타입 k ($k\geq 2$) 가우스 주기를 α라고 하자. 그러면 모든 $0\leq r\leq q^n$에 대해서 α^r은 $(k-1)(q-1)n(n+1)$개의 $GF(q)$상의 덧셈으로 계산되어진다.

증명 스케치. $0\leq r_j<q$에 대해 $r=\sum_{j=0}^{n-1}r_jq^j$ 이라고 하자. 다음 알고리즘은 α^r을 계산하게 한다. 프로베니우스 맵 $\alpha \rightarrow \alpha^q$의 계산량을 무시하면, 식 (4)와 (5)로부터 $A\alpha^{q^i}$는 redundant basis $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}, 1\}$에서 $(k-1)(n+1)$개의 $GF(q)$상 덧셈연산에 의해 계산되어진다. 각 i에 대해서 안쪽의 for-loop $A\leftarrow A\alpha^{q^i}$는 r_i번 수행된다. 그래서 곱셈연산 $A\leftarrow A\alpha^{q^i}$의 총 개수는 $\sum_{i=0}^{n-1}r_i \leq (q-1)n$개다. 따라서 $(k-1)(n+1)(q-1)n=(k-1)(q-1)n(n+1)$개의 $GF(q)$상의 덧셈연산에 의해 α^r이 계산될 수 있고 이는 고정된 k와 q에 대해 $O((k-1)(q-1)n^2)$만큼의 복잡도를 갖는다.

앞의 정리가 실제로 의미를 가지려면, 가우스 주기는 $GF(q^n)$의 원시 원소가 되거나 적어도 높은 위수를 가져야 하나 항상 그런 것은 아니다. 예를 들면, 타입 $(n,1)$ (타입 I) 가우스 주기 α는 결코 원시원소가 되지 않는데 이는 $\alpha^{n+1}=1$이고 $n+1 << q^n$이기 때문이다. 그러나 여러 계산 결과에 따르면 k가 2이상인 경우, $GF(q)$위의 타입 k 가우스 주기 α는 매우 자주 원시근(primitive element)이 되고 α가 원시근이 아닌 경우에도 보통 매우 높은 곱셈위수를 갖는다는 것이 알려져 있다. 예를 들면, [5]에서 알려져 있듯이, n이 1000이하일 때 $GF(2^n)$상에 존재하는 177개의 타입 $(n,2)$ 가우스 주기 α들 중에서 146개의 n값에 대하여 α는 원시근이다. 더군다나 α가 원시근이 아닐 경우에도 매우 높은 위수를 가짐을 알 수 있다. [5]에서 제시된 표에서는 1200이하의 n값들 중 1050개의 값에 대해 타입 k 원시 가우스 주기 (primitive Gauss period)가 존재함이 알려져 있고 많은 경우 k를 20이하로 선택할 수 있다. 이 실험 증거를 뒷받침하는 정리는 Gathen과 Shparlinski[9]에 의해 얻어졌는데 그들은 $GF(q^n)$상의 타입 II 가우스 주기는 무수히 많은 n에 대해 적어도 $2^{\sqrt{2n}-2}$만큼의 위수를 갖는다는 것을 보였다.

표 1. [5]의 지수승 알고리즘

```
Input : r = Σ_{j=0}^{n-1} r_j q^j with 0 ≤ r_j < q
Output : α^r
A ← 1
for (i = 0 to n-1 ; i++)
  if r_i ≠ 0
    for (j = 1 to r_i ; j++)
        A ← Aα^{q^i}
    end for
  end if
end for
```

Ⅲ. Signed digit representation과 타입 II ONB를 사용한 $GF(2^n)$상의 지수승 연산

3.1 이진 NAF (Binary Non-adjacent Form)

모든 정수 $0\leq s<2^n$는 유일한 이진 표현 $s=\sum_{i=0}^{n-1}s_i2^i$ 을 갖는다. 여기서 s_i는 0 또는 1이다. 이와 같은 이진 표현은 $GF(2^n)$상에서의 정규기저를 사용한 지수승 연산을 계산할 때 특별히 유용한데 이는 이 경우 프로베니우스 맵이 자유롭기 때문이다. s_i가 0이 아닌 1인 경우 표 1에서 α^s의 계산을 하는 동안 한 번의 곱셈연산 $A\leftarrow A\alpha$을 수행한다. 임의의 $0\leq s<2^n$의 0이 아닌 비트의 평균 개수는 $n/2$이다. 한편 $s=\sum_{i=0}^{n}s_i2^i$를 s_i가 0, ±1인 3가지 경우를 이용하여 다음의 방법을 따라 표현할 수 있다. 일반적인 s의 이진수 표현으로부터, 만약 $2^{j+1}+2^j$ (즉, $\cdots 11\cdots$)과 같이 0이 아닌 비트가 연속적으로 표현되는 경우, $2^{j+2}-2^j$(즉, $\cdots 10\bar{1}\cdots$ 여기서 $\bar{1}$은 -1)로 바꿔준다. 이와 같은 표현은 유일하고 이를 s의 non-adjacent form(NAF)라고 한다. 사실상 이 표현은 다음 조건에 의해 완벽히 결정되어진다.

정의 2. 정수 $s=\sum_{i=0}^{n}s_i2^i$가 모든 i에 대해 s_i=0, ±1이며 s_is_{i+1}=0을 만족하면 이를 s의 non-adjacent form (NAF)이라 한다.

모든 양의 정수는 유일한 NAF를 갖고 정수 $0 \le s < 2^n$의 NAF 표현에서 0이 아닌 자리수의 평균 개수가 $n/3$인 사실은 [12,14]에서 잘 알려져 있다. 정수의 NAF 표현은 radix $m(m \ge 2)$ 표현의 경우[13,14]로 일반화될 수 있다. [12,13,14]에서는 radix m 표현으로 된 정수의, 길이 n인 NAF의 0이 아닌 자리수의 기대값은 $n\frac{m-1}{m+1}$임을 보여준다. $m \ge 3$ 일때 NAF 를 이용한 개선의 정도는 크지 않다. 이는 m이 클 때 radix m 표현에서 0이 아닌 자리수의 기댓값이 $n\frac{m-1}{m+1} \approx n$이기 때문이다.

3.2 타입 II ONB 및 NAF를 사용한 효율적인 지수승 연산

II장에서 타입 k 가우스 주기 α의 지수승연산은 다항식 시간 복잡도 $O((k-1)(q-1)n^2)$를 갖는다는 것을 보였다. α의 지수승의 signed digit representation을 효율적으로 사용하기 위해서 $GF(2^n)$의 임의의 원소 A에 대해 $A\alpha^{-1}$을 계산하는 것이 필요하고 계산비용은 $A\alpha$ 계산비용보다 적은 비용이어야 한다. 임의의 타입 k 가우스 주기에 대해서 이 문제는 쉽지가 않다. 이는 타입 k 가우스 주기에 의해 결정되는 행렬의, 곱셈에 대한 역원을 찾는 것이 필요하고 보통 가우스 소거법은 많은 시간을 필요로 하기 때문이다. 반면에 k가 2인 경우에는 정규 기저의 치환인 palindromic representation[6,7]이라 불리는 좋은 기저가 있다. $GF(2^n)$상의 타입 II 가우시안 정규 기저 $\{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{n-1}}\}$가 존재하는 것은 $\gcd(2n/\mathrm{ord}_p 2, n) = 1$ (즉, $\mathrm{ord}_p 2 = 2n$ 이거나, n이 홀수이며 $\mathrm{ord}_p 2 = n$) 인 것과 동치이다. 타입 II 가우시안 정규기저를 타입 II 최적 정규 기저(Optimal Normal Basis, ONB)라고도 부르며 위에서 도입된 최적 정규 기저의 정의와 다음 정의가 동치임을 쉽게 알 수 있다[6,7].

정의 4. $GF(2^n)$를 원소가 2^n개인 유한체라고 하자. 여기서 $2n+1=p$은 소수이다. 이 때

(*) 2가 mod p로 볼 때 원시근이다.

(**) -1이 mod p에 대한 이차 비잉여(quadratic non-residue)이고 2의 적당한 지수승들이 mod p에 대한 모든 이차 잉여(quadratic residue)를 생성한다.

위의 두 조건중 하나가 만족되면 다음의 정규기저 $\{\alpha, \alpha^2, \cdots, \alpha^{2^{n-1}}\}$를 $GF(2^n)$상의 타입 II 최적 정규 기저 (혹은 타입 II 가우시안 정규기저)라고 한다. 여기서 $\alpha = \beta + \beta^{-1}$이고 β는 $GF(2^{2n})$상에서의 p번째 원시근 (p-th primitive root of unity)이다.

위 정의에 있는 가정을 사용하면 다음 식을 쉽게 구할 수 있다.

$$\alpha^{2^s} = (\beta + \beta^{-1})^{2^s} = \beta^{2^s} + \beta^{-2^s} = \beta^t + \beta^{-t} \qquad (7)$$

여기서 t는 $2s \equiv t \pmod p$이며 $0 < t < p = 2n+1$를 만족한다. 만약 $n+1 \le t \le 2n$이면 t대신 $p-t$를 대입하여 $\{\alpha, \alpha^2, \cdots, \alpha^{2^{n-1}}\}$과 $\{\beta + \beta^{-1}, \beta^2 + \beta^{-2}, \cdots, \beta^n + \beta^{-n}\}$이 같은 집합임을 알 수 있다. 즉, $\{\alpha^{2^s} | 0 \le s \le n-1\}$과 $\{\beta^s + \beta^{-s} | 1 \le s \le n\}$은 같은 집합이다. 이 결과를 이용하기 위하여 다음을 정의한다.

정의 5. β를 $GF(2^{2n})$상의 p-th ($p=2n+1$) 원시근이라고 하자. 각 정수 s에 대해서 α_s를 다음으로 정의하자.

$$\alpha_s = \beta^s + \beta^{-s} \qquad (8)$$

그러면 각 정수 s와 t에 대해서 다음 식을 쉽게 구한다.

$$\alpha_s \alpha_t = (\beta^s + \beta^{-s})(\beta^t + \beta^{-t}) = \alpha_{s-t} + \alpha_{s+t} \qquad (9)$$

다시 말하면, 두 기저 원소의 곱셈은 두 기저 원소의 합으로 표현할 수 있다.

보조정리 6. $\alpha_0 = 0$ 이고 $\alpha_s = \alpha_t$인 것은 $s \pm t \equiv 0 \pmod{2n+1}$과 동치이다.

증명. $\alpha_0 = \beta^0 + \beta^0 = 2 = 0$이고 $\alpha_s = \beta^s + \beta^{-s}$는 $\beta^{2n+1} = 1$이므로 $s \pmod{2n+1}$의 잉여 클래스에만 의존한다. 그리고 $\alpha_{2n+1-s} = \beta^{2n+1-s} + \beta^{-(2n+1-s)} = \beta^{-s} + \beta^s = \alpha_s$이다.

위로부터 두 기저 $\{\alpha, \alpha^2, \cdots, \alpha^{2^{n-1}}\}$와 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$는 집합으로 보면 같고 원소의 순서만 바꾸었다는 것을 알 수 있다. 체 연산의 복잡도를 줄이기 위해 임의의 s와 t에 대해 (9)식이 자주 사용될 것이다. 유한체 $GF(2^n)$ 상의 기저 $\{\alpha_1, \alpha_2, \cdots, \alpha_n\}$를 생각하자. 여기서 $\alpha = \alpha_1 = \beta + \beta^{-1}$는 타입 II ONB 원소라고 하자. $GF(2^n)$상의 원소 $A = \sum_{i=1}^n a_i \alpha_i$, $B = \sum_{i=1}^n b_i \alpha_i$가 다음 관계식을 만족한다고 하자.

$$B = A\alpha^{-1} \qquad (10)$$

표 2. 타입 II ONB를 갖는 $GF(2^n)$상의 signed digit representation을 이용한 새로운 지수승 알고리즘

Input : $r=\sum_{j=0}^{n} r_j 2^j$ with $r_j=0,\pm 1$
Output : α^r
$A \leftarrow 1$
for ($i=n$ to 0 ; $i--$)
  $A \leftarrow A^2\alpha^{r_i}$
end for

그러면 식 (9)와 보조정리 6을 이용하여 다음 식을 얻는다.

$$\begin{aligned} A=B\alpha &= \sum_{i=1}^{n} b_i\alpha_i\alpha_1 = \sum_{i=1}^{n} b_i(\alpha_{i-1}+\alpha_{i+1}) \\ &= b_1(2+\alpha_2)+b_2(\alpha_1+\alpha_3)+\cdots \\ &\quad +b_{n-1}(\alpha_{n-2}+\alpha_n)+b_n(\alpha_{n-1}+\alpha_n) \\ &= 2b_1+b_2\alpha_1+(b_1+b_3)\alpha_2+(b_2+b_4)\alpha_3 \\ &\quad +\cdots+(b_{n-2}+b_n)\alpha_{n-1}+(b_{n-1}+b_n)\alpha_n \\ &= 2b_1+b_2\alpha_1+(b_{n-1}+b_n)\alpha_n \\ &\quad +\sum_{i=2}^{n-1}(b_{i-1}+b_{i+1})\alpha_i \end{aligned} \quad (11)$$

정리 7. $GF(2^n)$상에서 기저 $\{\alpha_1,\alpha_2,\cdots,\alpha_n\}$를 사용하면 $B=A\alpha^{-1}$을 계산하는 데 $n-1$번의 $GF(2)$상의 덧셈이 필요하다.

증명. 식 (11)로부터 $2b_1=0$이고,

$$\begin{aligned} &a_1=b_2,\ a_n=b_{n-1}+b_n, \\ &\text{and } a_i=b_{i-1}+b_{i+1} \text{ for } 2\le i\le n-1 \end{aligned} \quad (12)$$

이다. 그러므로 위의 관계를 이용하여 다음과 같이 짝수인 i에 대해서 반복적으로 값 b_i를 구하게 된다.

$$\begin{aligned} &b_2=a_1, b_4=b_2+a_3, b_6=b_4+a_5, \\ &\cdots, b_{2s}=b_{2s-2}+a_{2s-1} \end{aligned} \quad (13)$$

여기서 $s=\lfloor \frac{n}{2} \rfloor$, 즉 n은 $2s$ 또는 $2s+1$이다. 만약 $n=2s$이면, 식 (12)을 다시 사용하고 다음과 같이 홀수인 i에 대해서 반복적으로 b_i값을 구하게 된다.

$$\begin{aligned} &b_{n-1}=b_n+a_n, b_{n-3}=b_{n-1}+a_{n-2}, \\ &b_{n-5}=b_{n-3}+a_{n-4}, \cdots, b_1=b_3+a_2 \end{aligned} \quad (14)$$

그리고 만약 $n=2s+1$이면, 즉 $2s=n-1$이면, 홀수 i에 대해서 다음 식을 구하게 된다.

$$\begin{aligned} &b_n=b_{n-1}+a_n, b_{n-2}=b_n+a_{n-1}, \\ &b_{n-4}=b_{n-2}+a_{n-3}, \cdots, b_1=b_3+a_2 \end{aligned} \quad (15)$$

그러므로 b_i ($i\neq 2$, $1\le i\le n$)의 계산에는 한 번의 덧셈연산이 필요하다 (단 $b_2=a_1$). 따라서 $A\alpha^{-1}$를 계산하는 데에 쓰이는 $GF(2)$상의 덧셈연산의 총 개수는 $n-1$이다.

정리 7을 기반으로 하여 지수의 signed digit representation을 이용한 새로운 지수승 알고리즘을 표2와 같이 제안할 수 있다. 위에 제시한 알고리즘은 다음 식을 계산하는 이진 윈도우 방법의 단순한 형태이다.

$$\alpha^r=\alpha^{\sum_{i=0}^{n} r_i 2^i}=(\cdots(((\alpha^{r_n})^2\alpha^{r_{n-1}})^2\alpha^{r_{n-2}})^2\cdots)^2\alpha^{r_0} \quad (16)$$

제안된 알고리즘은 표 1의 알고리즘과 비교할 때 단지 한번의 for-루프를 갖고 Gao등[5]이 제시한 기존의 알고리즘보다 계산 비용이 상당히 감소함을 알 수 있다.

Ⅳ. 제안한 알고리즘과 Gao등의 방법, Wu와 Hasan의 다항식 기저 방법과의 비교

표 1의 알고리즘에서는 타입 k 가우시안 정규기저를 사용한 지수승 연산의 복잡도는 $(k-1)(q-1)n(n+1)$ 개의 $GF(q)$상의 덧셈연산을 갖는다. 타입 II ONB ($q=2$, $k=2$)의 경우는 $n(n+1)$개의 $GF(2)$상의 덧셈연산을 갖는다. 그러므로, $GF(2^n)$상에서 이진 표현을 사용한 지수 r의 0이 아닌 비트의 개수의 기댓값은 $n/2$이므로 Gao등의 방법을 사용하여 $GF(2^n)$상의 원소 α^r을 계산하는 데에 필요한 $GF(2)$의 덧셈연산의 평균개수는 $\frac{1}{2}n(n+1)\approx\frac{1}{2}n^2$이다.

이제 표 2에서 제안한 방법의 복잡도를 구하겠다. 식 (11), (12)에 의해서 $GF(2^n)$상의 원소 A에 대하여 $A\alpha$를 계산하는 데에 사용되는 $GF(2)$상의 덧셈연산의 개수는 $n-1$개이다. $GF(2^n)$상에서 지수 r의 NAF를 사용할 때 r의 0이 아닌 비트의 기댓값은 $n/3$이다. 그러므로 정리 7로부터 제안된 알고리즘을 사용하여 $GF(2^n)$상에서 α^r을 계산하는 데에 필요한 $GF(2)$상의 덧셈연산의 평균개수는

표 3. 한 번의 지수승 연산을 위해 필요한 덧셈 연산의 개수 비교

기저	[5] 타입 II ONB	[10,11] trinomial	본 논문의 타입 II ONB
$GF(2^n)$	$\frac{1}{2}n^2$	$\frac{1}{2}n^2$ 또는 $\frac{3}{4}n^2$	$\frac{1}{3}n^2$

$\frac{1}{3}n(n-1) \approx \frac{1}{3}n^2$이다. 그러므로 $GF(2^n)$상에서 새롭게 제안된 알고리즘은 지수승 연산을 위해 필요로 하는 $GF(2)$상의 덧셈연산의 개수를 Gao등[5]의 방법보다 대략 33%정도 감소시켰다.

또한 제안한 방법은 signed digit representation의 다항식 기저방법을 사용한 것보다 효과적이다. 그 이유는 $GF(2^n)$상의 $A \leftarrow A^2$ 계산이 다항식 기저에서는 자유롭지 않으며 한 번의 지수승 연산결과를 얻기 위해 n번의 제곱연산을 반복적으로 수행하는 반면에, 정규기저에서는 모든 제곱연산이 자유롭기 때문이다. 제곱연산의 복잡도는 $GF(2)[X]$상에서 주어진 기약다항식 $f(X)$의 Hamming weight(다항식의 0이 아닌 계수의 개수)에 매우 의존적이나 여러 다항식 중에서 3항다항식 (trinomial) $f(X) = X^n + aX^k + b$ 을 사용하는 지수승 연산 알고리즘의 복잡도가 가장 낮다.

이진체 $GF(2^n)$에 대해, Wu[10]의 결과는 $1 \le k < \frac{n}{2}$ 를 만족하는 k에 대하여 3항다항식 $f(X)=X^n+X^k+1$을 사용하여 한 번의 제곱연산에 필요한 $GF(2)$상의 덧셈연산의 정확한 추정치를 보여준다. 즉, 사용되는 $GF(2)$상의 덧셈연산의 개수는, nk가 홀수일 때 $\frac{n}{2}$이고, nk가 짝수일 때 $\frac{3}{4}n$이다. 또한 α를 3항다항식 $f(X)$의 근이라고 할 때, $A \leftarrow A\alpha^{\pm 1}$의 연산에 필요한 덧셈연산의 개수가 한 개라는 사실은[11] 쉽게 유도된다. 그러므로 [11]의 signed binary 방법을 이용하면, $GF(2^n)$상에서 α^r의 지수승 연산의 복잡도는 nk가 홀수인 경우 $\frac{1}{2}n \cdot n + 1 \cdot \frac{n}{3} \approx \frac{1}{2}n^2$개의 $GF(2)$-덧셈연산이 필요하고, nk가 짝수인 경우 $\frac{3}{4}n \cdot n + 1 \cdot \frac{n}{3} \approx \frac{3}{4}n^2$개의 $GF(2)$-덧셈연산이 필요하다. 표 3은 제안한 지수승 연산 알고리즘이 정규기저 혹은 다항식 기저를 이용한 다른 알고리즘보다 뛰어남을 보여준다. 제안한 방법에서 필요한 $GF(2)$상의 덧셈연산의 개수는 Gao등[5]의 타입 II ONB 방법보다 33%정도 적고, $f(X)=X^n+X^k+1$의 3항기저 (trinomial basis)와 signed bit representation을 사용한 방법[10,11]보다 역시 33%정도 적다.

V. 결 론

유한체 $GF(2^n)$에서 타입 II 최적정규기저 및 지수의 NAF (non-adjacent form)를 이용한 효율적인 지수승 알고리즘을 제안하였다. 정규기저를 사용할 때는 쉽지 않은 $A\alpha^{-1}$의 계산이 타입 II 최적정규기저를 사용할 때에는 $A\alpha$의 계산만큼 쉬움을 보였다. 계산결과는 제안된 알고리즘이, 유한체 $GF(2^n)$상에서 정규 기저 혹은 다항식 기저를 이용한 기존의 알고리즘보다 빠르다는 것을 보여준다.

참 고 문 헌

[1] E.F. Brickel, D.M. Gordon, K.S. McCurley, and D.B. Wilson, "Fast exponentiation with precomputation," *Eurocrypt 92, Lecture Notes in Computer Science,* Vol.658, pp.200-207, 1992.

[2] C.H. Lim and P.J. Lee, "More flexible exponentiation with precomputation," *Crypto 94, Lecture Notes in Computer Science,* Vol.839, pp.95-107, 1994.

[3] P. de Rooij, "Efficient exponentiation using precomputation and vector addition chains," *Eurocrypt 94, Lecture Notes in Computer Science*, Vol.950, pp.389-399, 1994.

[4] S. Gao, J. von zur Gathen, and D. Panario, "Gauss periods and fast exponentiation in finite fields," *Latin 95, Lecture Notes in Computer Science,* vol 911, pp.311-322, 1995.

[5] S. Gao, J. von zur Gathen, and D. Panario, "Orders and cryptographical applications," *Math. Comp.*, Vol.67, pp.343-352, 1998.

[6] S. Gao and S. Vanstone, "On orders of optimal normal basis generators,," *Math Comp.*, Vol.64, pp.1227-1233, 1995.

[7] A.J. Menezes, I.F. Blake, S. Gao, R.C. Mullin, S.A. Vanstone, and T. Yaghoobian, *Applications of Finite Fields,* Kluwer Academic Publisher, 1993.

[8] S.Feisel, J. von zur Gathen, M. Shokrollahi, "Normal bases via general Gauss periods," *Math. Comp.*, Vol.68, pp.271-290, 1999.

[9] J. von zur Gathen and I. Shparlinski, "Orders of Gauss periods in finite fields," *ISAAC 95, Leture Notes in Computer Science,* Vol.1004, pp.208-215, 1995.

[10] H. Wu, "On complexity of polynomial basis squaring in $GF(2^m)$," *SAC 00, Lecture Notes in Computer Science*, Vol.2012, pp.118-129, 2001.

[11] H. Wu and M.A. Hasan, "Efficient exponentiation of a primitive root in $GF(2^m)$," *IEEE Trans. Computers*, Vol.46, pp.162-172, 1997.

[12] D.M. Gordon, "A survey of fast exponentiation methods," *J. Algorithm*, Vol.27, pp.129-146, 1998.

[13] S. Arno and F.S. Wheeler, "Signed digit representation of minimal hamming weight," *IEEE Trans. Computers*, Vol.42, pp.1007-1010, 1993.

[14] J.H. van Lint, *Introduction to Coding Theory, 3rd*, Springer-Verlag, 1999..

[15] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press, 1996.

[16] D.E. Knuth, *The Art of Computer Programming, 3rd* : Seminumerical algorithms, Vol.II, Addison-Wesley, 2001.

권 순 학 (Soonhak Kwon) 정회원

1990년 2월 KAIST 수학과 학사

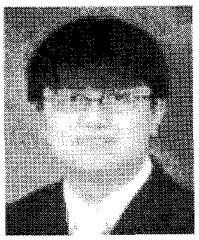
1992년 2월 서울대학교 수학과 석사

1997년 5월 Johns Hopkins University 박사

1998년 3월~현재 성균관대학교 수학과 부교수

<관심분야> 정수론, 암호론, Cryptographic Hardware, USN 보안

고 병 환 (Byeonghwan Go) 정회원



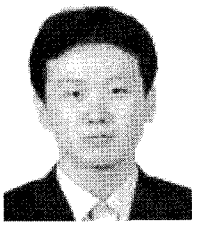
2005년 2월 연세대학교 원주캠퍼스 수학과 학사

2007년 2월 성균관대학교 수학과 석사

2007년 3월~현재 성균관대학교 수학과 박사과정

<관심분야> 공개키 암호시스템, 타원곡선 암호시스템, Pairing 기반 암호시스템, USN 보안

구 남 훈 (Namhun Koo) 준회원



2006년 8월 성균관대학교 수학과 학사

2006년 9월~현재 성균관대학교 수학과 석사과정 재학 중

<관심분야> 공개키 암호 시스템, 타원곡선 암호시스템, Pairing 기반 암호시스템, NTRU 암호시스템, USN 보안

김 창 훈 (Chang Hoon Kim) 정회원

한국통신학회 논문지 제33권 4C호 참조

현재 대구대학교 컴퓨터·IT 공학부 전임강사