Number theoretic transform(NTT) 연구 동향

송경주*, 장경배*, 김현지*, 양유진*, 서화정**

*한성대학교 (대학원생)

**한성대학교 (교수)

Research Trends on Number theoretic transform(NTT)

Gyeong-Ju Song*, Kyung-Bae Jang*, Hyun-Ji Kim*, Yu-Jin Yang*, Hwa-Jeong Seo*

*Hansung University(Graduate student)

**Hansung University(Professor)

요 약

기존 암호체계는 대규모 양자 컴퓨터의 개발로 인해 위협 받을 수 있다. National Institute of Standards and Technology(NIST)는 안전한 Post-quantum 암호 표준을 정하는 것을 목표로 Post Quantum Conference를 진행하였으며 격자 상의 수학적 난제인 Hard Lattice Problem을 암호 기법에 적용 시킨 격자암호는 Post-quantum 암호로 주목 받고 있다. 격자기반암호의 RLWE 문제에서는 유한필드에서의 다항식 링 곱셈을 기본 연산으로 사용하며 일반적으로 n 길이의 두 다항식에 대해서 $O(n^2)$의 계산 복잡도를 가진다. 이에 대해 Number theoretic transform(NTT)를 사용하면 $O(n \log n)$의 복잡도로 연산이 가능하다. 본 논문에서는 일반적인 NTT 연산과 NTT의 성능을 높이기 위한 연구 동향에 대해 살펴본다.

I. 서론

대규모 양자 컴퓨터의 개발은 현재 암호 체계에 위협이 될 것이라 예상한다. 기존 대칭키 암호와 공개키 암호는 각각 양자 알고리즘인 Grover's algorithm[1]과 Shor's algorithm[2]에 의해 공격 받을 수 있다.

이러한 연구 동기로 National Institute of Standards and Technology(NIST)는 안전한 Post-quantum 암호 표준을 정하는 것을 목표로 총 3라운드의 Post Quantum Conference를 진행하였다. Post-quantum 암호의 후보로는 격자 기반 암호, 코드 기반 암호, 해시 기반 암호, 다변수 기반 암호, 아이소제니 기반 암호 등이 있다. 그 중 격자 기반 암호가 가장 많으며 Finalists 로는 NTRU, CRYSTALS-KYBER, CRYSTALS- DILITHIUM, SABER, FALCON 이 있으며 Alternates 로는 FrodoKEM, NTRU-Prime 이 있다. 격자기반 암호는 Ring Learning With Errors(RLWE), Learning With Errors(LWE), Small Integer Solution(SIS) 등의 문제를 기반으로 하며 RLWE 에서는 유한필드에서 다항식 링 곱셈을 기본연산으로 사용한다. 일반적으로 n길이의 두 다항식에 대해서 $O(n^2)$의 계산 복잡도를 가진다. 이에 대해 Number theoretic transform(NTT)를 사용하면 $O(n \log n)$의 계산 복잡도를 가지므로 기본 연산보다 효율적으로 다항식 곱셈을 수행할 수 있다. 본 논문에서는 이러한 NTT의 연구 동향에 대해 살펴본다.

II. 관련 연구

2.1 격자기반암호

격자기반암호(Lattice-based cryptography)

는 격자(Lattice) 상의 수학적 난제인 Hard Lattice Problem을 암호 기법에 적용시킨 것이다. 여기서 격자(Lattice)는 n차원 공간 R^n에서 점(point)들이 규칙적인 격자무늬 배열로 배치되어 있는 상태를 말하며 식 (1)과 같이 basis matrix(b)의 선형조합으로 표현된다.

$$L(b_1,\cdots,b_n)=\left\{\sum_{i=0}^{n}x_ib_i|x_i\in Z\right\} \quad (1)$$

격자는 기저 벡터(basis vector)들의 선형 결합으로 이루어지므로 격자의 모양은 기저벡터에 의해 결정된다. 1996년 Aitai는 격자 문제의 NP-hardness를 증명하였으며[3] 1997년 Aitai-Dwork은 최악의 시나리오를 기반으로 한 최초의 암호를 구현하였다[4]. 격자기반암호는 수백 차원 격자 상에서의 임의의 위치와 가장 가까운 점을 찾는 어려움을 기반으로 한다. 즉, 격자 상에서의 수학적 난제가 암호 보안성에 기반한다. Cryptography 격자 난제로는 Ring Learning With Errors(RLWE), Learning With Errors(LWE), Small Integer Solution(SIS) 등이 있으며 LWE가 가장 많이 사용된다.

2.2 Number theoretic transform(NTT)

Number theoretic transform(NTT)는 Fast Fourier transform에서 도메인을 정수 필드로 일반화 한 것이다[5]. NTT는 긴 다항식의 곱을 효율적으로 계산할 수 있으며 주로 Lattice 기반 암호에서 곱셈을 효율적으로 수행하기 위해 사용한다. NTT를 사용하면 n길이의 두 다항식 곱셈에 대한 복잡도를 $O(n^2)$에서 $O(n\log n)$로 줄일 수 있다. NTT는 $Z_q[x]/(x^n+1)$ 에서의 곱셈을 수행하며 여기서 n은 2의 제곱이며, q는 $q\equiv 1\,(\bmod\ 2n)$을 만족하는 소수이다. $a=(a[0],\cdots,a[n-1])\in Z_q^n$ 이고 ω는 Z_q에서의 n번째 제곱근 $\omega^n\equiv 1\,(\bmod\, q)$이라고 할 때, $\tilde{a}\equiv NTT(a)$는 식 (2)로 계산된다.

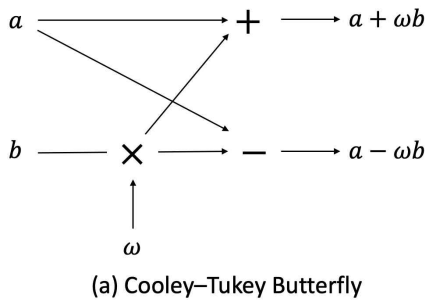
$$\tilde{a}\equiv\sum_{j=0}^{n-1}a[j]w^{ij}\,(\bmod\, q),\ i=0,1,\cdots,n-1 \quad (2)$$

NTT는 두 방정식 $a=a_0,\ldots,a_n$, $b=b_0,\ldots,b_n$이 주어지면 링 (x^n+1) 상에서의 곱셈을 구할 수 있으며 이때 링 (x^n+1)의 차원을 낮춰 서브 링으로 표현하여 계산을 수행한다.

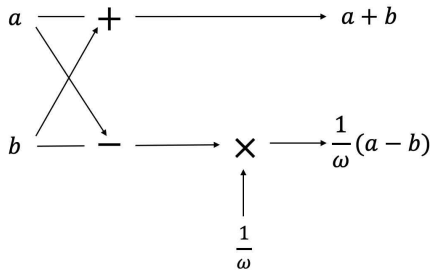
III. 연구동향

3.1 Classic NTT (Butterfly)

일반적인 NTT는 소위 butterfly라고 불리는 연산을 통해 계산된다. butterfly 방식에는 Cooley-Tukey[6], Gentleman-Sande[7] 방식이 있으며 NTT 식 (2)는 미리 계산된 제곱근 ω을 사용하여 그림 (1)과 같이 Butterfly 방식으로 계산된다.



(a) Cooley–Tukey Butterfly



(b) Gentleman–Sande Butterfly

(그림 1) (a) Cooley-Tukey Butterfly (2) Gentleman-Sande Butterfly

3.2 Montgomery NTT[8]

기존 NTT 연산에 Montgomery 곱셈을 활용하여 속도를 높이는 방법이 있다. 식 (3)의 Montgomery 곱셈은 모듈러 상에서의 곱셈 속도를 높이는 방법이며 곱셈보다 느린 연산인 나눗셈을 곱셈으로 대체하여 속도를 높인다.

$$a\cdot b\equiv c\,(\bmod\, m),\ m<2^n \quad (3)$$

이러한 Montgomery를 NTT의 modulus 나눗셈에 사용하여 속도를 높일 수 있다. 하지만 NTT 이전의 필드를 Montgomery 표현으로 변환하고 INTT 이후의 필드를 다시 Montgomery 이전으로 변환해야 한다는 단점이 있다. 유한 필드 요소 x를 몽고메리 형식으로 변환하는 방식으로 모듈식 축소 함수 redc를 x와 사전 계산된 상수 $R^2 \bmod q$ 의 곱에 적용하는 것이다. 단순히 redc을 적용하여 원래 형식으로 다시 변환한다. 알고리즘 1은 전체 reduction에 대한 redc 함수의 동작이다.

```
int_t redc (int_dt T)
{
    unit_t m = (unit_t)T*N;
    int_t V = ((unit_dt)m*q+T)>>WL;
    V-=q; V+=(V>>(WL-1))&q;
    return V;
}
```

(알고리즘 1) 모듈식 축소 함수 redc

3.3 Speed up NTT

Longa et al.은 특정 계수에 대한 모듈러 축소 알고리즘을 제시하여 NTT의 속도를 높였다[9]. 제안한 모듈러 축소 기법을 사용한 NTT 알고리즘을 키 교환에 적용하여 성능을 크게 향상시켰다. NTT의 속도를 높이기 위한 [9]의 주요 아이디어는 곱셈 후에만 K-RED를 적용하여 내부 루프에서의 반복당 한 번 감소시킨다. K-RED 함수는 모든 정수인 C 에 대해 입력으로 받아 동작한다. 이후 $D \equiv kC (\bmod q)$ 및 $|D| < q + |C|/2^m$ 의 정수 D를 반환한다.

```
function K-RED(C)
{
    C0 ← C mod 2^m
    C1 ← C / 2^m
    return kC0 − C1
}
```

(알고리즘 2) K-RED 함수

IV.결론

본 논문에서는 긴 다항식의 모듈러 곱셈 연산을 효율적으로 수행하는 Number Theoretic Transform (NTT)의 동향을 살펴보았다. NTT는 $O(n \log n)$의 계산 복잡도를 가지며 격자기반암호에서의 곱셈에 사용할 수 있어 여러 최적화 방식이 연구되고 있다. 일반적으로 butterfly 방식을 사용하여 NTT 연산을 수행하며 속도를 높이기 위한 연구들이 진행되고 있다. 본 논문에는 일반적인 butterfly 방식의 NTT와 기존 NTT에 Montgomery 곱셈을 활용하여 속도를 높이는 연구 및 특정 계수에 대한 모듈러 축소 알고리즘을 활용하여 속도를 높이는 연구 동향을 살펴보았다.

V.Acknowledgement

이 논문은 2022년도 정부(과학기술정보통신부)의 재원으로 정보통신기획평가원의 지원을 받아 수행된 연구임 (<Q|Crypton>, No.2019-0-00033, 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발, 100%)

[참고문헌]

[1] Grover, Lov K. "A fast quantum mechanical algorithm for database search." Proceedings of the twenty-eighth annual ACM symposium on Theory of computing. 1996.

[2] Shor, Peter W. "Algorithms for quantum computation: discrete logarithms and factoring." Proceedings 35th annual symposium on foundations of computer science. Ieee, 1994.

[3] Ajtai, Miklós. "Generating hard instances of lattice problems." Proceedings of the twenty-eighth annual ACM symposium on Theory of

computing. 1996.

[4] Ajtai, Miklós, and Cynthia Dwork. "A public-key cryptosystem with worst-case/average-case equivalence." Proceedings of the twenty-ninth annual ACM symposium on Theory of computing. 1997.

[5] Scott, Michael. "A note on the implementation of the number theoretic transform." IMA International Conference on Cryptography and Coding. Springer, Cham, 2017.

[6] Cooley, James W., and John W. Tukey. "An algorithm for the machine calculation of complex Fourier series." Mathematics of computation 19.90 (1965): 297-301.

[7] Gentleman, W. Morven, and Gordon Sande. "Fast Fourier transforms: for fun and profit." Proceedings of the November 7-10, 1966, fall joint computer conference. 1966.

[8] Scott, Michael. "A note on the implementation of the number theoretic transform." IMA International Conference on Cryptography and Coding. Springer, Cham, 2017.

[9] Longa, Patrick, and Michael Naehrig. "Speeding up the number theoretic transform for faster ideal lattice-based cryptography." International Conference on Cryptology and Network Security. Springer, Cham, 2016.