정 보 보 호 학 회 지
제 33 권 제1호, 2023. 2

격자 기반 양자내성암호 Crystals-Kyber/Dilithium 안전성 분석 동향

이 석 준*

요 약

1994년 피터 쇼어에 의해, 대규모 큐비트 연산이 가능한 양자 컴퓨터가 개발된다면 RSA와 같은 현재 공개키 암호 알고리즘이 공격을 당할 수 있음을 이론적으로 가능하게 해주는 쇼어 알고리즘이 소개된 이후, 공개키암호시스템의 붕괴에 대한 가능성은 점점 현실로 다가오고 있다. 물론, 공개키암호시스템은 향후 10~20년은 여전히 안전할 가능성이 높지만, NIST는 최악의 상황에 대비하여 2017년부터 양자내성암호(Post-Quantum Cryptography)에 대한 표준화 작업을 수행하고 있으며, 2022년 4종의 표준화 대상 알고리즘을 선정한 바 있다.

이 중에서도 NIST는 Crystals-Kyber(PKE/KEM)와 Crystals-Dilithium(DSA)를 기본 알고리즘으로 언급하며 우수한 성능과 강한 보안성으로 대부분의 응용에서 잘 동작할 것이라고 예측한 바 있다. 이들 알고리즘은 3라운드의 경쟁 알고리즘 대비 보안 강도가 다소 약한 측면에 있었음에도 우수한 성능, 다양한 환경에서의 적용 가능성 등에 따라 선정된 것으로 보인다. 그럼에도 최근 일부 연구에서는 하이브리드 Dual 공격을 제안함으로써 최초 주장하는 보안 강도와 비교하여 안전성이 더 약화될 가능성이 제기된 바 있다. 본 논문에서는 이들 알고리즘에 대한 안전성 분석 방법을 살펴보고, 최근 논문에서 제기된 새로운 안전성 분석 방법과 그에 따르는 보안 강도를 분석한다.

Ⅰ. 서 론

1994년 피터 쇼어에 의해, 대규모 큐비트 연산이 가능한 양자 컴퓨터가 개발된다면 RSA와 같은 현재 공개키 암호 알고리즘이 공격을 당할 수 있음을 이론적으로 가능하게 해주는 쇼어 알고리즘[1]이 소개된 이후, 많은 전문가 및 글로벌 대기업이 양자 컴퓨터에 대한 연구개발에 집중하였다. 2012년 존 프레스킬은 양자우월성이라는 개념을 제안하였으며, 어떤 문제에 대해서 양자 컴퓨터의 성능이 고전 컴퓨터(슈퍼컴퓨터 등)보다 훨씬 우월함을 의미하는데, 이는 2019년 구글에 의해 달성되었다고 알려져 있다.

구글의 양자우월성이 곧 RSA 및 ECC와 같은 공개키암호시스템의 붕괴를 의미하는 것은 아니며, 공개키암호시스템은 향후 10~20년은 여전히 안전할 가능성이 높지만, NIST는 이러한 최악의 상황에 대비하여 2017년부터 RSA, ECC 등을 대체하기 위한 양자내성암호(PQC, Post-Quantum Cryptography)에 대한 표준화 작업을 수행하고 있다. 이 표준화 작업은 크게 공개키 암호 및 키캡슐화 메커니즘(PKE/KEM)과 디지털 서명 알고리즘(DSA)의 2가지 카테고리로 진행해 왔으며, 2022년 7월 NIST는 4종의 최종 표준화 대상 알고리즘(PKE/KEM 1종 및 DSA 3종)을 선정한 바 있다.

이러한 PQC는 기반 문제에 따라 분류하면 격자, 코드, 다변수 이차식, 해시, 타원곡선 아이소제니 등 다양한 방식이 존재한다. 이 중 격자기반 방식의 양자내성암호는 LWE(Learning with Errors), LWR(Learning with Rounding) 등 양자/고전 컴퓨터상에서의 수학적 난제를 기반으로 구성된 공개키암호 알고리즘이다. NIST PQC 표준화 과정에서는 상대적으로 많은 수의 격자 기반 PQC 알고리즘 후보가 제안되었으며 최종 표준화 대상 알고리즘 4종 중 3종이 선정되었다. 격자기반 방식이 다른 방식과 비교하여 우세한 이유는 수학적 기반 문제에 대한 안전성 연구가 많이 이루어지

본 연구는 정부(과학기술정보통신부)의 재원으로 한국연구재단의 실제 양자컴퓨터 환경을 고려한 격자기반 양자내성암호 양자안전성 분석 연구(No. NRF-2022R1F1A1073211) 및 정보통신기획평가원의 미래컴퓨팅 환경에 대비한 계산 복잡도 기반 암호 안전성 검증 기술개발(No. 2019-0-00033)의 연구결과로 수행되었음
* 가천대학교 IT융합대학 컴퓨터공학부 스마트보안전공 (교수, junny@gachon.ac.kr)

고, 암호문/서명문의 길이, 공개키/비밀키의 길이 및 암복호·서명 속도, TLS와 같은 보안프로토콜과의 결합시 오버헤드 등이 상대적으로 우수하기 때문으로 보인다.

NIST는 최종 표준화 대상 알고리즘 발표에서 MLWE(Module Learning with Errors)를 기반으로 하는 Crystals-Kyber(PKE/KEM)[2,3], Crystals-Dilithium (DSA)[4]를 기본 알고리즘으로 언급하며 우수한 성능과 강한 보안성으로 대부분의 응용에서 잘 동작할 것이라고 예측한 바 있다. 이 알고리즘에 대한 안전성 분석 연구는 현재까지 비교적 많이 이루어져 온 관계로 앞으로도 PQC 전환 과정에서 널리 사용될 가능성이 크다고 볼 수 있다.

따라서, 본 고에서는 PQC 전환 과정에서 가장 우선적으로 고려될 것으로 보이는 Crystals-Kyber와 Crystals-Dilithium, 두 알고리즘에 대하여 저자들이 주장하는 안전성에 대해서 살펴보고, LWE에 대한 최근 안전성 분석 연구 동향에 대해서 소개하고자 한다.

Ⅱ. 격자 기반 PQC 알고리즘

2.1. LWE (Learning with Errors)

2005년 O. Regev[5]가 제안한 LWE 문제는 오류를 포함할 수 있는 선형 함수에 관한 문제로, Search LWE와 Decision LWE으로 나눌 수 있다. Search LWE와 Decision LWE 문제는 동등한 안전성을 갖는다고 알려져 있으며, Decision LWE 문제는 평균적인 경우에 대한 난이도가 곧 최악의 경우 만큼 어렵기 때문에, 공개키 암호의 설계에 많이 사용된다.

Decision LWE 문제는 비밀벡터 $s \in Z_q^n$에 대하여, 임의의 벡터 $a \in Z_q^n$와 분포 χ에서 선택한 작은 크기의 오류 e를 이용하여 구성한 쌍 $(a,b) = (a, a \cdot s + e \pmod q)$을 LWE 샘플이라고 하면, m개의 샘플 $(A,B) \in Z_q^{m \times n} \times Z_q^m$에 대하여, 이 샘플이 LWE 샘플인지 아니면 임의로 선택된 $B \in Z_q^m$인지를 구분하는 문제이다.

2.2. RLWE (Ring-Learning with Errors)

RLWE는 LWE를 변형하여, 유한체 상의 다항식 환 위에서 정의한 문제이다. $a(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_1 x + a_0$라고 정의하면, Decision RLWE 문제는 비밀다항식 $s(x) \in Z_q[x]/\Phi(x)$에 대하여, Z_q^n에서 임의로 계수를 선택한 $a_i(x) \in Z_q[x]/\Phi(x)$와 특정 분포 χ에서 선택한 작은 크기의 오류들로 구성한 다항식 $e_i(x)$를 이용하여 구성한 쌍 $(a_i(x), b_i(x)) = (a_i(x), a_i(x) \cdot s + e_i(x))$을 RLWE 샘플이라고 하면, m개의 샘플 $(a_i(x), b_i(x))$에 대하여, 이 샘플이 RLWE 샘플인지 아니면 임의로 선택된 $b_i(x) \in Z_q[x]/\Phi(x)$인지를 구분하는 문제이다.

RLWE는 격자 기반 주요 문제인 SVP(Shortest Vector Problem)으로부터 다항 시간으로 변환(reduction) 가능한 것으로 알려져 있다.

2.3. MLWE (Module-Learning with Errors)

MLWE는 LWE와 RLWE를 결합하여 일반화한 구조를 가진다. 즉, LWE와 유사한 구조를 가지고 있으나, LWE에서 이용하는 벡터가 Z_q에서 추출한 n차원 요소로 구성되어 있다면 MLWE는 $Z_q[x]/\Phi(x)$에서 추출한 k차원 요소(각 요소는 n차 다항식)로 구성되는 벡터를 이용하게 된다.

따라서 Decision MLWE 문제는 비밀다항식 벡터 $s \in (Z_q[x]/\Phi(x))^k$에 대하여, 임의로 선택한 다항식 벡터 $a_i \in (Z_q[x]/\Phi(x))^k$와 특정 분포 χ에서 선택한 작은 크기의 오류들로 구성한 다항식 벡터 e_i를 이용하여 구성한 쌍 $(a_i, b_i) = (a_i, a_i \cdot s + e_i)$을 MLWE 샘플이라고 하면, m개의 샘플 (a_i, b_i)에 대하여, 이 샘플이 MLWE 샘플인지 아니면 임의로 선택된 (a_i, b_i)인지를 구분하는 문제이다.

2.4. Crystals-Kyber

NIST는 PQC 공모 당시 PKI/KEM 방식에 대한 평가 기준으로 IND-CCA2를 언급[6]하였다. CCA2는 적응 선택 암호문 공격(Adaptive Chosen-Chipertext Attack)으로, 이는 공격자가 언제든지 원하는 암호문에 대한 평문을 얻을 수 있는 환경 상의 공격을 의미하며, IND-CCA2는 이러한 적응 선택 암호문 공격이 가능한 상황(단, 다음의 특정 암호문에 대한 공격은 불

가능)에서, 특정 암호문이 2개의 평문 중 어떤 것인지 공격자가 구별 불가능함(확률적으로 의미 있는 이득이 없음)을 의미한다.

Crystals-Kyber는 IND-CCA2에 안전한 MLWE 기반 키 캡슐화 알고리즘으로 Bos 등에 의해 처음 제안되었다. NIST에 의해 최종 표준화 대상 알고리즘으로 선정되었으며, 공개키 암호화(PKE)를 위한 Kyber.CPAPKE(32비트 메시지 암호화 체계, [그림 1]) 및 이를 기반으로 Fujisaki-Okamoto 변환을 통한 키 캡슐화(KEM) 함수 Kyber.CCAKEM을 지원한다.

$\mathbf{s}, \mathbf{e} \leftarrow \chi$
$sk = \mathbf{s}, pk = \mathbf{t} = \mathbf{As} + \mathbf{e}$

$\mathbf{r} \leftarrow \chi$
$\mathrm{e}_1, \mathrm{e}_2 \leftarrow \chi'$
$\mathbf{u} \leftarrow \mathbf{A}^{\mathrm{T}}\mathbf{r} + \mathrm{e}_1$
$v \leftarrow \mathbf{t}^{\mathrm{T}}\mathbf{r} + \mathrm{e}_2 + \mathrm{Enc(m)}$
$c = (\mathbf{u}, v)$

$m = \mathrm{Dec}(v - \mathbf{s}^{\mathrm{T}}\mathbf{u})$

〔그림 1〕 Crystals-Kyber의 CPAPKE 함수 개요

2.5. Crystals-Dilithium

NIST는 PQC 공모 당시 DSA 방식에 대한 평가 기준으로 EUF-CMA를 언급하였다. CMA는 선택 메시지 공격(Chosen Message Attack)으로, 이는 공격자가 선택한 메시지에 대해 정상적인 서명을 계속해서 요청하여 획득할 수 있음을 의미한다. EUF-CMA(Existential UnForgeability under CMA)는 이러한 선택 메시지 공격이 가능한 상황에서도, 공격자가 정상적으로 검증될 수 있는 메시지와 서명 쌍(단, CMA를 통하여 정상 서명을 획득하지 못한 메시지)을 생성할 수 없음을 의미한다.

Crystals-Dilithium은 EUF-CMA에 안전한 MLWE 기반 전자서명 알고리즘으로, NIST에 의해 최종 표준화 대상 알고리즘으로 선정되었으며, 다른 전자서명 알고리즘과 마찬가지로 [그림 2]와 같이 키생성 Gen 함수, 특정 메시지에 대한 서명 생성용 Sign 함수와 서명 검증용 Verify 함수로 구성된다.

Ⅲ. Crystals-Kyber/Dilithium 안전성 주장

3.1. Crystals-Kyber

저자들은 Kyber의 기반이 되는 MLWE 문제의 가장 잘 알려진 공격이 격자에서 Module과 같은 구조를 사용하지 않으며, 따라서 MLWE 문제의 강도를 LWE 문제로서 분석하였다.

저자들은 LWE를 공격하기 위한 많은 알고리즘의 경우, Crystals-Kyber의 파라미터 세트와 관련이 없어, BKW 타입의 공격 및 선형화 공격을 배제할 수 있다고 하였다. 격자의 basis를 줄이기 위한 2가지 BKZ 공격은 여전히 가능한데, 이들은 각각 primal 공격과 dual 공격이다.

BKZ 알고리즘은 SVP 오라클을 사용하여 격자 기저를 더 작은 차원 b로 낮춘다. 해당 오라클로 호출하

Gen
$\mathbf{A} \leftarrow R_q^{k \times l}$
$(\mathrm{s}_1, \mathrm{s}_2) \leftarrow \mathrm{S}_\eta^l \times \mathrm{S}_\eta^k$
$\mathbf{t} = \mathbf{A}\mathrm{s}_1 + \mathrm{s}_2$
Return $(pk = (\mathbf{A}, \mathbf{t}), sk = (\mathbf{A}, \mathbf{t}, \mathrm{s}_1, \mathrm{s}_2))$

Sign
$\mathbf{y} \leftarrow \mathrm{S}_{\gamma_1\text{-}1}^l$
$\mathbf{c} = \mathrm{H}(\mathrm{M}, \mathrm{high}(\mathbf{Ay}, 2\gamma_2))$
$\mathbf{z} = \mathbf{y} + \mathbf{c}\mathrm{s}_1$
If $|\mathbf{z}| > \gamma_1 - \beta$ or $|\mathrm{low}(\mathbf{Ay}\text{-}\mathbf{c}\mathrm{s}_2, 2\gamma_2)| > \gamma_2 - \beta$ restart
signature $= (\mathbf{z}, \mathbf{c})$

Verify
Check $|\mathbf{z}| > \gamma_1 - \beta$
Check $\mathbf{c} = \mathrm{H}(M, \mathrm{high}(\mathbf{Az}\text{-}\mathbf{ct}, 2\gamma_2))$

〔그림 2〕 Crystals-Dilithium 함수 개요

는 수는 다항식 이내이지만, 호출 수를 평가하는 것은 쉽지 않다. 따라서 저자들은 해당 다항식 인자를 무시하고, 오직 차원 b에서 SVP 오라클에 한번의 호출 비용만을 고려하는 분석을 이용하였다. 또한, SVP의 난이도를 위한 매우 단순한 비용 측정을 사용한다. 이 core-SVP hardness 방법은 보안성을 측정하는 방식으로서, E. Alkim 등에 의해 제안[7]되었다. NIST PQC 표준화 라운드 1, 2에서 발생한 암호 분석에서, 이 방법은 정보적으로는 유용하지만, 특히 기존 공격자에 대한 보안 추정을 정확하게 생산하기에 어려웠다고 평가하였으나, 이것은 3 라운드에 추가로 분석한 바 있다.

또한, BKZ 알고리즘에서 SVP 오라클을 위한 두 가지 알고리즘적 접근 방식이 있는데 이는 각각 Enumeration 알고리즘과 Sieving 알고리즘이다. 이들은 특성이 다르며, Sieving 알고리즘의 경우 성공적으로 공격한 격자 차원으로부터 Crystals-Kyber 공격을 위한 더 큰 차원으로 어떻게 실제 성능이 확장되는지를 예측하는 것이 어렵다. Enumeration 알고리즘은 실행 시간이 super-exponential인 반면, Sieving 알고리즘은 exponential한 실행 시간을 갖는다. 여러 실험 결과에 다르면 Enumeration 알고리즘이 작은 차원에서 더 효율적이며, 어느 정도의 차원에서 Sieving 알고리즘이 더 효율적인지는 알려지지 않은 것으로 보이며, 특정 연구 결과에서는 80차원 수준에서 Sieving 알고리즘이 더 우수한 경우가 있었다. 다만, 메모리 사용량을 고려해야 하며, Sieving 알고리즘이 더 많은 메모리를 사용하기 때문에 명확한 안전성 분석이 필요할 것이다.

다만, 저자들은 보수적인 접근을 위하여 심지어 지수적 수준의 대용량 메모리조차도 비용없이 접근할 수 있다고 가정하였다.

3.1.1. Primal 공격

Primal 공격은 LWE 문제에서 고유-SVP 인스턴스를 구성하고, BKZ 알고리즘을 사용하여 해결하는 방식이다. 저자들은 답을 찾기 위하여 BKZ를 위해 필요한 블록 차원 b가 얼마나 큰지를 검토하였다. LWE 인스턴스 $(A, b = As + e)$에 대해, $d = m + kn + 1$ 차원, 볼륨은 q^n이며, 고유-SVP 솔루션 $v = (s, e, 1)$을 가지는 격자 $\Lambda = \{x \in Z^{m+kn+1} : (A | I_m | -b)x = 0 \bmod q\}$를 구성한다. 단, 여기에서 norm $\lambda \approx \varsigma\sqrt{kn+m}$ 으로 ς는 에러와 비밀 정보의 표준 편차를 의미한다. 사용된 샘플의 수 m은 0과 $(k+1)n$ 사이에서 선택할 수 있으며, 저자들은 이 선택을 최적화하였다.

공격에 대한 성공 조건은 다음과 같다. 공격자 관점에서 유리한 것으로 알려진 기하 급수 가정을 사용하여 BKZ 알고리즘의 행동을 모델링한다. 여기에서는 Gram-Schmidt norm이 $\| b_i^* \| = \delta^{d-2i-1} \cdot Vol(\Lambda)^{1/d}$ (단, $\delta = ((\pi b)^{1/b} \cdot b/2\pi e)^{1/2(b-1)}$)로 주어지는 기저(basis)를 발견하고자 한다. 유일한 SVP 솔루션 v는 마지막 b개의 Gram-Schmidt 벡터들에 의해 확장되는 벡터 공간에 벡터 v의 사영이 b_{d-b}^*보다 짧으면 찾을 수 있다. 투영된 벡터의 크기는 $\varsigma\sqrt{b}$로 예상할 수 있는데, 이는 곧 공격이 성공할 필요충분조건이 $\varsigma\sqrt{b} \le \delta^{2b-d-1} \cdot q^{m/d}$임을 의미한다.

3.1.2. Dual 공격

Dual 공격은 Dual 격자 $w \in \Lambda' = \{(x,y) \in Z^m \times Z^{kn} : A^t x = y \bmod q\}$에 서 의 짧은 벡터를 찾는 방식이다. 길이가 l인 벡터 (x,y)를 찾았다고 가정하고, $z = v^t \cdot b = v^t As + v^t e = w^t s + v^t e \bmod q$를 계산하자. 단, 여기에서 만약 (A,b)가 LWE 샘플이라면 해당 값은 표준편차 $l\varsigma$의 가우시안 분포를 따를 것이다. 이 두 분포의 최대 분산 차이는 $\epsilon = 4\exp(-2\pi^2\tau^2)$ (단, $\tau = l\varsigma/q$이내)이며, 이는 길이 l인 벡터가 주어지면 결정 LWE에 대한 이득 ϵ을 얻을 수 있음을 의미한다.

BKZ 알고리즘에서 주어지는 벡터의 길이 l 은 $l = \| b_0 \|$ 로 주어진다. Λ'이 차원 $d = m + kn$과 볼륨 q^{kn}임을 알기 때문에, $l = \delta^{d-1} q^{kn/d}$를 얻을 수 있다. 따라서, ϵ-distinguisher를 얻기 위해서는 차원 b를 갖는 BKZ 알고리즘 실행이 필요하다. (단, $-2\pi^2\tau^2 \ge \ln(\epsilon/4)$)

공유된 키는 해시 알고리즘을 거치기 때문에 작은 이득 ϵ은 큰 의미가 없다. 공격자는 공유된 키의 검색 공간을 크게 줄이기 위하여 최소 1/2의 이득을 필요로 한다. 따라서 공격자는 $1/\epsilon^2$개의 많은 짧은 벡터를 구성함으로써 성공 확률을 증폭시켜야 한다. sieving 알고리즘이 $2^{0.2075b}$ 벡터를 제공하는 만큼, 공격은 적어도 $R = \max(1, 1/(2^{0.2075b}\epsilon^2))$번 반복하여야 한다.

3.1.3. 대수적 공격

Kyber 기반의 MLWE 인스턴스에 대한 가장 잘 알려진 공격은 격자의 구조를 사용하지 않지만 저자들은 공격의 최신 동향에 대해서 여전히 논의 중임을 언급하였다. 특히, 최근 제안된 Ideal-SVP에 대한 새로운 양자 알고리즘들은, 이상적인 격자에서의 SVP 문제를 풀고자 한다. Cramer 등[8]은 RLWE에 대한 양자 공격에 대한 어려움을 언급하였음에도 MLWE를 사용할 것을 제안하고 있으며, Albrecht 등[9]은 MLWE에서 RLWE로 변환(reduction)을 구성하여였으며, 이는 특정 매개변수를 사용하여 RLWE에 대한 다항식 시간 알고리즘이 MLWE에 대한 다항식 시간 알고리즘으로 변환된다는 의미한다. 그러나 실질적으로 이 공격은 모듈의 차원이 증가함에 따라 상당한 속도 저하가 발생하므로, 모듈의 차원이 늘리면 더 안전해질 수 있음을 의미한다.

3.2. Crystals-Dilithium

전자 서명에 대한 표준 보안 개념은 선택 메시지 공격에 대한 보안성을 나타내는 UF-CMA 보안이다. 이 보안 모델에서 공격자는 공개키를 얻고 자신이 선택한 메시지에 대한 서명 오라클에 액세스할 수 있습니다. 공격자의 목표는 새 메시지의 유효한 서명을 만드는 것이며, 더 강력한 보안 요구 사항인 SUF-CMA(Strong Unforgeability under CMA)는 공격자가 이미 확인한 메시지의 다른 서명값을 생성할 수 있는 환경에서 공격에 성공할 수 없어야 함을 의미한다.

(고전적인) 랜덤 오라클 모델에서 Dilithium은 표준 MLWE 및 MSIS(Module Short Integer Solution) 격자 문제의 어려움에 기반한 SUF-CMA를 제공한다. 또한, 양자 공격자의 경우 중첩된 입력을 해시 함수에 쿼리(QROM)할 수 있으므로, 이 체계의 보안을 고려해야 한다. 그러나 변환으로 인하여 보안에 크게 영향을 주는 것으로 보이지는 않으며, Grover와 같은 전체 탐색 알고리즘 정도만 양자 알고리즘의 효과를 누릴 수 있는 것으로 보인다.

저자들은 변환(reduction)을 이용한 공격이 없었던 이유는 아마도 양자 변환 하에서도 전자서명의 UF-CMA 보안과 거의 동일한 문제가 있기 때문일 것으로 추측하였으며, 수학 문제의 구조와 해시 함수 사이에 관계가 없는 한 이 문제를 푸는 것은 수학 문제를 해결하는 것보다 쉽지 않을 것으로 보고 있다.

저자들은 Dilithium의 SUF-CMA이 기반으로 하는 난이도에 대한 가정을 소개하였는데, 처음 두 가정인 MLWE와 MSIS는 LWE, Ring-LWE, SIS 및 Ring-SIS를 일반화한 표준 격자 문제이다. 세 번째 문제인 SelfTargetMSIS는 앞서 언급한 MSIS와 해시 함수 H의 결합 난이도을 기반으로 하는 문제이다.

3.2.1. MSIS 문제

MSIS에서는 MLWE와 유사하게 $Z_q[x]/\Phi(x)$에서 추출한 k차원 요소(각 요소는 n차 다항식)로 구성되는 벡터를 이용하게 된다. 임의로 선택한 다항식 벡터 $a_i \in (Z_q[x]/\Phi(x))^k$들에 대하여 $\sum_{i=0}^{m-1} a_i \bullet b_i = 0 \bmod q$와 어떤 β에 대하여 $0 < \| b \| \leq \beta$를 만족하는 $b_i \in (Z_q[x]/\Phi(x))^k$를 찾는 문제 혹은 이렇게 추출한 샘플인지 임의로 선택된 (a_i, b_i)인지를 구분하는 결정 문제이다.

3.2.2. 기본 공격

Crystals-Dilithium 역시 Kyber와 마찬가지로 MLWE를 사용하므로, Kyber에서 시도한 SVP 및 MLWE에 대한 공략은 유사하게 접근할 수 있다. 따라서, SVP 오라클을 사용하여 격자 기저를 더 작은 차원 b로 낮추는 BKZ 알고리즘의 활용 가능성과 함께, MLWE 혹은 RLWE 문제를 공략하려는 시도들도 동일하게 활용할 수 있다.

3.2.3. 그 외의 분석

core-SVP Hardness 측정이 도입되었을 때 Sieving의 구현은 Becker 등의 방법론[10]에 의해 보수적인 추정치로 제안된 $2^{0.292b}$ CPU cycle보다 훨씬 나쁜 성능을 보였다. 이는 Becker 등의 기법에서 제안된 $2^{0.292b+o(b)}$의 복잡도 분석에서 숨겨진 상당한 다항식 또는 심지어 sub-지수 오버헤드 때문이다. 이전에도 Enumeration을 통한 SVP 비용에 기반하여 하여 훨씬 더 공격적인 매개변수를 설정하게 되었 차후 개선된 BKZ 알고리즘이 LWE를 푸는데 있어 다른 예측이 이

루어지기도 하였다.

Enumeration과 Sieving 알고리즘을 통하여 SVP 문제를 풀기 위한 부분은 3.1절에서 기술한 내용을 참고할 수 있다.

3.3. Crystals-Kyber/Dilithium의 보안성

NIST IR 8413(NIST PQC 표준화 3라운드 결과에 대한 보고)[11]에서는 3라운드 후보들에 대한 성능, 안전성 등 최종 표준화 대상 알고리즘을 선정하기 위한 여러 평가 내용을 포함하고 있다. 특히 부록 D의 표 10과 11에서는 격자 기반 PQC 후보에 대한 고전 및 양자 안전성에 대한 메트릭을 소개하고 있으며, Crystals-Kyber/Dilithium을 요약하면 [표 1]과 같다.

〔표 1〕 Crystals-Kyber/Dilithium 안전성 메트릭

PQC 후보	보안 강도	core-SVP 측정	게이트 수	메모리
Kyber512	Level 1	C: 118bits Q: 107bits	2^{151}	2^{94}
Kyber768	Level 3	C: 183bits Q: 166bits	2^{215}	2^{139}
Kyber1024	Level 5	C: 256bits Q: 232bits	2^{287}	2^{190}
Dilithium	Level 2	C: 123bits Q: 112bits	2^{159}	2^{98}
Dilithium	Level 3	C: 182bits Q: 165bits	2^{217}	2^{139}
Dilithium	Level 5	C: 252bits Q: 229bits	2^{285}	2^{187}

Ⅳ. 최근 안전성 분석 연구 동향

여러 연구자들에게 알려진 바와 같이 격자 기반 암호에 대해서, primal 공격과 dual 공격이 가장 효과적인 공격으로 알려져 있다. 한편, 이 외에 추가로 고려해야 할 공격 중 하나는 2007년 NTRU를 공격하기 위해 제안한, lattice-reduction 공격과 MITM(Meet-in-the-middle) 공격을 결합한 하이브리드 공격[12]이다.

하이브리드 공격은 비밀의 일부를 추측하고 나머지 부분에 대해 일부 공격을 수행한다. 추측이 문제의 차원을 줄이면 나머지 부분에 대한 격자 공격 비용이 줄어들게 되며, 또한 일반적으로 격자 공격 컴포넌트는 여러 추측에 재사용할 수 있다. 추측 비용이 격자 공격 비용과 일치할 때 최적의 공격이 달성된다.

격자 공격 컴포넌트가 primal 공격 혹은 dual 공격인 하이브리드 공격이 가능하며, 일반적으로 추측을 위해서 MITM 기술을 많이 사용하지만 Pruning이나 Matrix Multiplication 등 다른 방식이 사용되는 경우도 있다.

Bi 등[13]은 2022년 임의의 secret을 갖는 LWE에 대한 하이브리드 dual 공격 2가지를 제안하였다. 저자들은 이 공격은 secret의 분포와 관계없이 기존의 dual 공격의 성능을 향상시켰다고 주장하였다.

첫 번째 하이브리드 dual 공격(Hybrid-1)은 전체 검색을 통해 "추측"을 수행하는 단순한 전략으로 출발한다. 하이브리드 공격에는 격자 감소 단계와 추측 단계의 두 가지 구성 요소가 있으며, 격자 감소 단계부터 시작한다. 입력으로 m개의 LWE 인스턴스 $(A, b = A \cdot s + e \bmod q)$가 주어지면 비밀 벡터 s와 공개 행렬 A를 파라미터화된 r에 따라 두 부분으로 나누게 된다.

$$s = \begin{pmatrix} s_1 \\ s_2 \end{pmatrix} \in Z_q^r \times Z_q^{n-r}$$
$$A = (A_1, A_2) \in Z_q^{m \times r} \times Z_q^{m \times (n-r)}$$

추측 단계에서는 차원 r의 벡터에 대해 작동하고 s_1의 계수를 식별하고자 한다. dual 공격에서도 유사하게 A_2에 대한 격자도 다음과 같이 정의한다.

$$\Lambda_{dual}^E(A_2) = \{(w, v) \in Z^m \times Z^{n-r} : wA_2 = v \bmod q\}$$

$\Lambda_{dual}^E(A_2)$는 높은 확률로 차원 $d = m + n - r$ 및 볼륨 q^{n-r}을 가진다. 이 다음으로는 격자 감소 알고리즘을 통하여 $\langle w, b \rangle$를 계산할 수 있도록 만들어주는 어떤 짧은 벡터 $(w, v) = \Lambda_{dual}^E$을 얻을 수 있다.

$$\begin{aligned} \langle w, e \rangle &= w(As + e) \\ &= wA_1 s_1 + wA_2 s_2 + \langle w, e \rangle \\ &= wA_1 s_1 + \langle v, s_2 \rangle + \langle w, e \rangle \bmod q \end{aligned}$$

상기 식은 아래 식으로 변환하는 경우, 새로운 LWE 샘플 $(\hat{a}, \hat{b} = \langle \hat{a}, s_1 \rangle + \hat{e})$로 볼 수도 있다.

$$\hat{b} = \langle w, b \rangle \bmod q$$
$$\hat{a} = wA_1 \bmod q$$
$$\hat{e} = \langle v, s_2 \rangle + \langle w, e \rangle \bmod q$$

다음은 추측 단계이다. $\widetilde{s_1}$가 추측 공간에서의 한 후보로 정하자. 그러면, $\hat{e} = \hat{b} - \langle \hat{a}, \widetilde{s_1} \rangle \bmod q$는 $\widetilde{s_1}$이 제대로 된 추측이라면 가우시안 분포를 따를 것이며, 그렇지 않다면 Z_q 상에서 균일 분포를 따르게 된다.

s_1을 완전히 복구하기 위해, $\Lambda_{dual}^{E}(A_2)$로부터 대량의 짧은 벡터가 필요하다. sieving 알고리즘이 $2^{0.2075b}$ 벡터를 제공하는 만큼, 이는 격자 감소 단계에서 얻을 수 있다.

두 번째 하이브리드 dual 공격(Hybrid-2)은 Optimal pruning과 결합하는 방식이다. 이는 하이브리드 dual 공격 비용이 너무 많이 들거나 모든 후보를 추측할 수 없을 정도일 때 다른 비밀 분포를 위한 비밀 후보의 optimal 부분집합을 찾는 방식이 적용된다. 여기에서도 Hybrid-1과 유사하게 추측 시간이 BKZ의 비용을 근사할 필요가 있기 때문에, 후보 중 제한된 수만 추측할 수 있다. 성공 확률을 최적화하기 위하여 가능한 한 큰 성공 확률을 보이는 후보들의 적당량을 발견해야 한다. 성공 확률 p_c를 최적화하려면 성공 확률이 가능한 한 큰 특정 수의 후보 모음을 찾아야 한다. 즉, 후보 수가 제한되어 있을 때 성공 확률을 최대화하려고 한다. 이것은 $\max_{|C|<d} p(C)$로 표현할 수 있는데, 여기서 C는 추측된 후보의 모음이고 c는 $|C|$의 상한이며 $p(C) = pr[s_1 \in C]$는 올바른 S_1가 C에 있을 확률이다.

Algorithm: Hybrid Dual Attack

Input: $(\mathbf{A}, \mathbf{b}) \in \mathbb{Z}_q^{m \times n} \times \mathbb{Z}_q^m, r \in \mathbb{Z}$
Output: LWE distribution or Uniform

$\mathbf{P} \leftarrow$ permutation matrix;
$(\mathbf{A_1}, \mathbf{A_2}) \leftarrow \mathbf{A} \cdot \mathbf{P}$ with $\mathbf{A_1} \in \mathbb{Z}_q^{m \times r}$ and $\mathbf{A_2} \in \mathbb{Z}_q^{m \times (n-r)}$;
M short vector $(\mathbf{w_i}, \mathbf{v_i})_{i \in [M]} \leftarrow$ N calls to BKZ on $\Lambda_{\mathrm{dual}}^{\mathrm{E}}(\mathbf{A_2})$;
for $i \in \{1, \ldots, M\}$ **do**
  calculate $\widehat{b_i} = \langle \mathbf{w_i}, \mathbf{b} \rangle \bmod q$ and $\widehat{\mathbf{a_i}} = \mathbf{w_i A_1} \bmod q$;
for each $\widetilde{s_1} \in C$ do
  for $i \in \{1, \ldots, M\}$ **do**
    calculate $\widetilde{e_1} = \widehat{b_i} - \langle \widehat{\mathbf{a_i}}, \widetilde{\mathbf{s_1}} \rangle \bmod q$;
  if $\tilde{e}_{i \in [M]}$ follow modular Gaussian distribution **then**
    return LWE distribution;
return Uniform;

〔그림 3〕 하이브리드 Dual 공격

$(N \cdot T_{BKZ} + T_{guess})/p_c$를 최소화하는 최적의 매개변수는 $p_c < \frac{1}{2}$로 만들 수 있다. 성공 확률 p_c를 높이기 위해, 비밀의 다른 부분(r 차원)을 추측하여 공격을 반복하는데, 최소 $\lfloor n/r \rfloor$번 반복할 수 있다. 최적의 추측 전략은 낮은 확률을 갖는 일부 후보를 무시할 수 있기 때문에 $\lfloor n/r \rfloor$번 동안 공격이 실패할 수도 있으나, p_c가 너무 작지 않은 한 이런 일이 발생할 확률은 매우 낮다. 따라서 공격은 실용적이라고 볼 수 있다.

이 두가지 공격에 대하여 기존 해당 알고리즘의 보안 강도에 대한 주장, 기본 Dual 공격, Bi 등의 하이브리드 공격에 의한 공격 강도를 [표 2]에서 비교하였다. 하이브리드 공격은 Hybrid-2에 따라 계산된 수치이며, 가정 1은 SVP 오라클로서 Sieving을 사용할 때 BKZ 알고리즘으로부터 짧은 벡터를 $2^{0.2075b}$개 얻을 수 있다는 가정이며, 가정 2는 가정 1에 동일한 환경에서 BKZ 알고리즘에 의해 생성되는 가장 짧은 벡터보다 대부분의 벡터가 $\sqrt{\frac{4}{3}}$ 배 더 길다는 가정을 포함하는 것이다.

가정 2에서는 Crystals-Kyber/Dilithium에 의한 보안 강도와 본 논문의 하이브리드 기법을 통한 보안 강도의 차이가 거의 없으나, 가정 1에서는 3~9비트 정도 줄어듬을 확인할 수 있다.

〔표 2〕 Crystals-Kyber/Dilithium의 새로운 안전성 분석

PQC 후보	보안 강도	기존	가정 1		가정 2	
			Dual	H1	Dual	H2
Kyber512	Level 1	118	117	114	122	119
Kyber768	Level 3	183	181	175	188	182
Kyber1024	Level 5	256	253	245	263	254
Dilithium	Level 2	123	123	121	126	124
Dilithium	Level 3	182	181	179	186	183
Dilithium	Level 5	252	251	246	257	252

Ⅴ. 결 론

본 고에서는 NIST PQC 표준화 대상 알고리즘으로 선정된 격자 기반(MLWE)의 Crystals-Kyber/Dilithium 안전성을 정리하고 최근 동향을 분석하였다. 엄밀히 보면 NIST PQC 라운드 3의 다른 후보 알고리즘과 비

교하여 Crystals-Kyber/Dilithium은 주장하는 보안 강도면에서 볼 때 우수하다고 보기는 어렵다. 예를 들어, Level 1의 경우 Crystals-Kyber512의 보안 강도는 118비트로 주장되었으나, NTRU는 134~144비트였으며, Kyber1024의 보안 강도는 256비트이나 Fire Saber는 260비트였다.

그럼에도 Crystals-Kyber/Dilithium는 우수한 성능과 다양한 환경에서의 적용 가능성으로 다른 격자 방식 알고리즘과의 경쟁에서 승리하였다.

그러나, 아직까지도 이들 암호의 안전성에 대한 연구가 계속 이루어지고 있는 상태에서 현재의 보안 강도는 확정적이라고 보기 어렵다. Bi 등의 연구에서도 실제 보안 강도는 주장하는 강도 대비 더 감소할 가능성이 제기되었다. 따라서 앞으로도 Crystals-Kyber/Dilithium 뿐만 아니라 표준화 대상 알고리즘 및 라운드 4 후보 전체에 대한 보안 강도 분석 연구는 계속 이루어져야 할 것으로 보인다.

참 고 문 헌

[1] P. W. Shor, “Algorithms for quantum computation: Discrete logarithms and factoring”, in Proc. 35th Annual Symposium on Foundation of Computer Science, pages 124-134, 1994

[2] J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, and D. Stehle. “CRYSTALS-Kyber: a CCA-secure module-lattice-based KEM”, In 2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018

[3] R. Avanzi, J. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehle, “CRYSTALS-Kyber: Algorithm Specifications And Supporting Documentation (version 3.02)”, https://pq-crystals.org/kyber/, 2021

[4] S. Bai, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler and D. Stehle, “CRYSTALS-Dilithium: Algorithm Specifications and Supporting Documentation (Version 3.1)”, https://pq-crystals.org/dilithium/index.shtml, 2021

[5] O. Regev, “On lattices, learning with errors, random linear codes, and cryptography”, In STOC ’05, Proceedings of the thirty-seventh annual ACM symposium on Theory of computing, pages 84-93. ACM, 2005

[6] L. Chen, S. Jordan, Y. Liu, D. Moody, R. Peralta, R. Perlner, and D. Smith-Tone, “Report on Post-Quantum Cryptography”, NIST IR 8105, 2016

[7] E. Alkim, L. Ducas, T. Poppelmann, and Peter Schwabe, “Post-quantum key exchange - a new hope”, In Proceedings of the 25th USENIX Security Symposium, pages 327-343. USENIX Association, 2016

[8] R. Cramer, L. Ducas, and B. Wesolowski, “Short Stickelberger class relations and application to Ideal-SVP”, In Jean-Sebastien Coron and Jesper Buus Nielsen, editors, Advances in Cryptology . EUROCRYPT 2017, volume 10210 of LNCS, pages 324-348. Springer, 2017

[9] M. Albrecht and A. Deo, “Large modulus Ring-LWE ≥ Module-LWE”, Advances in Cryptology, ASIACRYPT 2017: 23rd International Conference on the Theory and Applications of Cryptology and Information Security, Springer, 2017

[10] A. Becker, L. Ducas, N. Gama, and T. Laarhoven, “New directions in nearest neighbor searching with applications to lattice sieving”, In SODA ’16 Proceedings of the twenty-seventh annual ACM-SIAM symposium on Discrete Algorithms, pages 10-24, SIAM, 2016

[11] G. Alagic, D. Apon, D. Cooper, Q. Dang, T. Dang, J. Kelsey, J. Lichtinger, Y. Liu, C. Miller, D. Moody, R. Peralta, R. Perlner, Angela Robinson and D. Smith-Tone, “Status Report on the Third Round of the NIST Post-Quantum Cryptography Standardization Process”, NIST IR 8413-upd1, 2022

[12] N. Howgrave-Graham, “A hybrid lattice-reduction and meet-in-the-middle attack against NTRU”, Advances in Cryptology, CRYPTO

2007, volume 4622 of LNCS, pages 150-169. Springer, 2007

[13] L. Bi, X. Lu, J. Luo, K. Wang and Z. Zhang, “Hybrid dual attack on LWE with arbitrary secrets”, Cybersecurity, 5(1), 1-27, 2022

〈저자소개〉

이 석 준 (Sokjoon Lee)

종신회원

1998년 2월 : 서울대학교 컴퓨터공학과 졸업

2000년 2월 : 서울대학교 컴퓨터공학과 석사

2019년 8월 : KAIST 전산학과 박사

2000년 2월~2022년 2월 : 한국전자통신연구원 정보보호연구본부 책임연구원/PL

2022년 3월~현재 : 가천대학교 IT융합대학 컴퓨터공학부 스마트보안전공 교수

<관심분야> 암호 양자분석, 암호엔지니어링, 제로트러스트, 위험관리