격자기반암호 공격 알고리즘 연구 동향 및 분석

배재영, 이준우
중앙대학교

go0102@cau.ac.kr, jwlee2815@cau.ac.kr

A Survey on Attack Algorithms against Lattice-Based Encryption

Bae Jae-Young
Chung-Ang Univ.

요 약

최근 CRYSTALS-Kyber 와 CRYSTALS-Dillithium 과 같은 양자내성암호가 LWE 문제에 기반을 두고 있다. 이에 따라 격자기반암호의 안전성 검증을 위한 격자기반암호 공격 알고리즘의 발전이 이루어지고 있다. BKZ 알고리즘을 이용한 primal attack 과 dual attack 이 격자기반암호를 대상으로 이루어졌고, 다양한 기법의 개발로 연구가 가속화되고 있다. 따라서, 본 논문에서는 격자기반암호 대상 공격 알고리즘에 대해 분석하고 동향 파악 및 향후 연구 방향에 대해 기술하고자 한다.

Ⅰ. 서 론

지난, 2004년 Regev[10]의 Learning With Errors (LWE) 문제가 제시된 이후 많은 암호시스템의 기반으로 사용되고 있다. NIST가 양자내성암호 표준화 공모전에서 Final Round에 선택한 CRYSTALS-Kyber[1]와 CRYSTALS-Dillithium[11]이 LWE를 기반으로 하고 있다. 이러한 LWE기반 암호시스템들의 등장과 발전으로 인해 해당 현대암호의 안전성을 시험해보려는 시도도 많아지고 있다.

1982년 Lenstra[9]가 제안한 LLL(Lenstra-Lenstra-Lovász) 알고리즘은 다항 시간내에 Lattice reduction을 가능하게 한다. LLL Reduction을 기반하여 격자기반문제를 풀 수 있는 공격 방법들이 제안되기 시작했다. 먼저, 1993년 Schnorr[8]가 BKZ(Block Korkin-Zolotarev) reduction을 사용한 Primal Attack을 제안하면서 58차원 이하의 모든 Subset Sum Problem을 풀 수 있음을 보였다. 이후, 2011년 Schnorr[8]의 BKZ 공격을 발전시켜 dual lattice에서 shortest vector를 찾는 dual attack을 보인 BKZ 2.0[7]은 격자기반문제 공격의 발전에 박차를 가하게 만들었다.

따라서 본 논문에서는 격자기반암호 공격 알고리즘의 유형과 동향에 대해 분석하고자 한다. LWE 기반 현대암호의 각광받기 이전부터 격자기반문제를 해결하고자 하는 문제는 지속되어 왔으며, 기존 논문 및 표준 공모전 제출물에 포함된 공격 알고리즘의 공격 방법과 분석에 대해 기술한다.

Ⅱ. 격자기반암호 공격 알고리즘 종류 및 특징

격자기반암호 공격 알고리즘은 크게 2종류로 구분된다.

2.1 Primal Attack

Schnorr[8]가 제안한 공격 방법으로 LWE문제로부터 unique-SVP instance를 생성한 후, BKZ 알고리즘을 통해 shortest vector를 찾는 방법이다. LWE문제가 대두되기 이전의 방법으로 Subset Sum Problem을 해결하는 목적으로 사용되었으며, BKZ알고리즘의 blocksize 20으로 58차원까지의 모든 Subset Sum Problem을 해결할 수 있음을 보여주었다.

Schnorr[8]가 제안한 공격 방법으로 LWE문제로부터 unique-SVP instance를 생성한 후, BKZ 알고리즘을 통해 shortest vector를 찾는 방법이다. LWE문제가 대두되기 이전의 방법으로 Subset Sum Problem을 해결하는 목적으로 사용되었으며, BKZ알고리즘의 blocksize 20으로 58차원까지의 모든 Subset Sum Problem을 해결할 수 있음을 보여주었다.

2.2 Dual Attack

Chen 의 [7]에서 새롭게 제안된 Dual Attack 은 dual lattice 에서 shortest vector 를 찾는 방법을 보여주고 있다. Dual

lattice 에서 찾은 벡터 (x, y)를 LWE 문제에 대입했을 때, 그 결과가 가우시안 분포로 분포된다면 해당 벡터는 LWE 샘플로 분류된다. 해당 벡터가 가우시안 분포로 분포되지 않는다면, 해당 벡터는 균등분포로부터 나온 벡터로 분류한다.

최근 학회에서 제시되고 있는 다양한 공격 알고리즘들은 주로 Dual Attack 에 기반을 하고 있다. 우선, BKZ 2.0[7]이 이전의 BKZ 알고리즘들을 활용한 공격들을 뛰어넘는 성능을 보여주었다. 기존의 Primal Attack 에서의 BKZ blocksize 의 크기가 40 을 넘어서면 실용적 결과를 보이지 못한 데에 비해 BKZ 2.0 은 Darmstadt's Challenge 에서 blocksize 90 으로 750 과 775 차원의 격자에서 문제를 해결할 수 있음을 처음으로 보여주었다. 또한, 525~725 사이의 차원에서도 shortest vector 를 찾을 수 있음을 보였다.

Nguyen[6]이 제안한 shortest vector problem 에 사용되는 Sieve 알고리즘을 도입한 Dual Sieve 공격은 많은 발전을 이끌어냈다. 2018 년 Ducas 의 "Dimensions for free"기법은 shortest vector 를 주어진 문제의 차원인 b 보다 조금 작은 $b' = b - d4f$ 차원에서 sieving 을 통해 찾을 수 있음을 보였다.

Guo의 [5]와 MATZOV[4]에서는 "Independence Heuristic"을 바탕으로 여러 개의 LWE 샘플에서 서로 독립적인 다수의 shortest vector를 추출할 수 있다는 가정하에 빠르게 LWE문제를 해결할 수 있음을 보였다. 게다가, FFT(Fast-Fourier Transform)을 이용하여 shortest vector를 찾는 연산을 가속화했다. MATZOV는 "modulus switching"기법을 도입하여 격자의 basis를 더 낮은 차원의 격자로 투영시켜 Sieving을 진행할 수 있음을 보여주었다.

하지만, 2023 년 Ducas 는 [4]와 [5]에서의 "Independence Heuristic"의 오류를 지적하며 여러 LWE 샘플들 사이에서 추출되는 shortest vector 들이 충분히 상호 독립적이지 않다고 반박하면서 Dual-Sieve 공격은 다소 후퇴한 상황이다.

Ⅲ. 결론 및 향후 연구 방향

본 논문에서는 격자기반암호 공격 알고리즘의 2가지 종류에 대한 동향을 알아보고 성능을 분석하였다. 현재 NIST 양자내성암호 표준안들을 대상으로 LWE를 공격하는 알고리즘은 Dual-Sieve 공격 위주로 이루어지고 있다. 향후에는 기존 공격 알고리즘들에 사용한 기법들을 바탕으로 shortest vector들의 독립성 증명과 차원 감소를 중점으로 최적화 연구가 진행될 것으로 보이며, 연산 가속화 방안에 대한 연구들도 함께 진행될 것으로 예측된다.

참 고 문 헌

[1] Roberto Avanzi, Joppe Bos, Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, John M.Schank, Peter Schwabe, Gregor Seiler, Damien Stehle, "CRYSTALS-Kyber Algorithm Specification And Supporting Documentation", NIST PQC round, 2021

[2] Leo Ducas. "Shortest vector from lattice sieving: a few dimensions for free." In Annual International Conference on the Theory and Applications of Cryptographic Techniques, pages 125-145, 2018

[3] Leo Ducas, Ludo N. Pulles. "Does the dual-sieve attack on learning with errors even work?" CRYPTO 2023, 2023

[4] MATZOV. "Report on the security of LWE: Improved dual lattice attack", 2022

[5] Qian Guo, Thomas Johansson. "Faster dual lattice attacks for solving LWE with applications to CRYSTALS" ASIACRYPT 2021, 2021

[6] Phong Q. Nguyen, Thomas Vidick. "Sieve algorithms for the shortest vector problem are pratical." Journal of Mathematical Cryptology, 2008

[7] Yuanmi Chen, Phong Q. Nguyen. "BKZ 2.0: Better lattice security estimates" ASIACRYPT 2011, 2011

[8] Claus-Peter Schnorr, Martin Euchner. "Lattice basis reduction: improved practical algorithms and solving subset sum problems" Mathematical Programming, 66(1-3):181-199, 1994

[9] A.K. Lenstra, H.W. Lenstra, L.Lovasz. "Factoring polynomials with rational coefficients," Mathematische Annalen 261, 515-534, 1983

[10] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography," 2009

[11] Leo Ducas, Eike Kiltz, Tancrede Lepoint, Vadim Lyubashevsky, Peter Schwabe, Gregor Seiler, Damien Stehle. "CRYSTALS-Dillithium: A Lattice-Based Digital Signature Scheme" NIST PQC round, 2021