격자 기반 암호 분석을 위한 Approximate 알고리즘에 대한 조사

김현지[1], 김덕영[1], 윤세영[1], 서화정[2]
[1]한성대학교 IT융합보안학과 대학원생
[2]한성대학교 IT융합보안학과 교수
khj1594012@gmail.com, dudejrdl123@gmail.com, sebbang99@gmail.com,
hwajeong84@gmail.com

A survey of approximation algorithms for cryptanalysis for lattice-based cryptography.

Hyun-Ji Kim[1], Duk-Young Kim[1], Se-Young Yoon[1], Hwa-Jeong Seo[2]
[1]Dept. of IT Convergence Security, Han-sung University
[2]Dept. of IT Convergence Security, Han-sung University

요 약

최근 양자컴퓨터와 양자컴퓨팅 기술이 발전하면서, 수학적 난제에 기반을 둔 현대 암호들이 위협받고 있다. 이에 양자 내성 암호에 대한 활발한 연구들이 진행되고 있으며, 이와 동시에 양자 내성 암호를 분석하기 위한 노력들도 존재한다. 양자 내성 암호 중 한 종류인 격자 기반 암호는 NP-hard 문제에 속하는 격자 문제를 기반으로 하며, 해당 격자 문제가 해결된다면 격자 기반 암호 시스템에도 큰 위협이 될 수 있다. 본 논문에서는 이러한 격자 기반 문제를 해결하기 위한 기법 중, 고차원 격자를 대상으로 하는 Approximate algorithm의 기술 동향에 대해 알아보고, 현재의 알고리즘 개발 동향을 기반으로 향후 진행되어야 할 연구 방향에 대해 살펴본다.

1. 서론

2019년 10월 구글에서 54 큐비트의 양자 프로세서를 개발함과 동시에 양자 우월성을 달성함으로써 현존하는 슈퍼컴퓨터의 성능을 능가할 수 있음이 증명되었다. IBM 또한 양자 컴퓨터 개발에 투자하고 있으며, 2022년 11월 10일에는 433 큐비트를 갖는 양자 컴퓨터 개발에 성공하였다. 이처럼 전세계적으로 앞으로 다가올 양자 컴퓨터 시대에 대한 대비를 위해 많은 연구들이 진행되고 있다.

양자 컴퓨터는 특정 문제에 있어서 기존의 컴퓨터가 수행할 수 없었던 복잡한 연산을 다항 시간 안에 수행할 수 있다. 따라서 이를 활용하면 인공지능, 대규모 시뮬레이션, 빅데이터 처리와 같은 높은 연산 부하를 갖는 난제들을 해결할 수 있으나, 난제에 기반을 둔 암호학에서는 양자 컴퓨터의 개발이 큰 위협으로 다가오고 있다.

2. 관련 연구

2.1. 격자 기반 암호 시스템

격자 기반 암호는 양자 내성 암호의 한 종류에 해당하며, 격자 공간을 기반으로 하는 공개키 암호이다. 격자 기반 암호의 안전성은 격자 기반 문제를 해결하기 어렵다는 사실에 근거한다. 대표적인 격자 기반 문제로는 SVP가 있다. SVP는 격자 내에서 0이 아닌 가장 짧은 벡터를 찾는 것이며, NP-hard 문제 [1]에 속한다. SVP [2]를 해결하기 위해서는 격자상의 벡터를 입력으로 사용하여 격자 상에서 가장 짧은 벡터를 찾는다. 그러나 벡터는 동일한 크기의 다른 벡터를 가질 수 있으므로 해는 고유하게 결정되지 않으며, 만약 좋지 않은 (길이가 긴) 기저 벡터가 입력되면 SVP를 해결하는 작업이 어려워진다. 이에 비해 좋은 기저 (길이가 짧은)를 입력으로 사용하면 가장 짧은 벡터가 입력 기저 내에 이미 존재할 가능성이 더 높다. 따라서, 격자의 차원이 증가함에 따라 해당 격자에 속하는 벡터의 길이가 길어지므로, 해당 문제는 점점 더 복잡해진다.

암호 시스템에 사용되는 격자는 최소 500차원 이상이므로 솔루션을 찾는 것이 매우 어렵다. 또한 앞서 언급했듯이 좋지 않은 기저 (공개키)에서 좋은 기저 (개인키)를 도출하는 것은 정보 비대칭으로 인해 어렵다. 격자 기반 암호화의 복잡성은 주로 단방향 프로세스 (한 방향에서는 쉬우나, 다른 방향에서는 어려운 문제)에 의존하기 때문이다. 이러한 격자 기반

암호 시스템을 손상시키기 위해서는 근본적인 격자 기반 문제를 해결해야한다. 즉, 격자 문제 중 하나인 SVP를 해결함으로써 Learning with Error (LWE) [3]와 같은 격자 기반 암호화 방식을 위협할 수 있다.

2.2. 격자 기반 문제

격자 기반 암호에 대한 암호 분석은 크게 Approximate 알고리즘과 exact 알고리즘의 두 과정으로 구성된다. 먼저, 암호 시스템에 사용되는 격자는 500차원으로 매우 크므로, 이것을 빠르게 줄여나갈 수 있는 Approximate 알고리즘이 사용된다. 즉, Approximate 알고리즘은 높은 차원의 격자에서 어느 정도 짧은 벡터들을 찾아나가면서 격자 범위를 축소하는 알고리즘이며, 해당 알고리즘에는 LLL (Lenstra - Lenstra - Lovász) [4] 알고리즘, Block Korkine-Zolotarev (BKZ) [5] 알고리즘 등이 존재한다. 이후, 격자의 차원이 약 50~60 차원까지 줄어들면, 짧은 벡터를 찾아내기 위한 exact 알고리즘을 사용한다. 대표적인 exact 알고리즘에는 AKS [6] NV Sieve [7], Gauss Sieve [8] 등이 있으며, 해당 알고리즘들의 목적은 짧은 벡터의 손실을 최소화 하면서 격자의 차원을 줄여나감으로써 가장 짧은 벡터를 정확히 찾아내는 것이다. 즉, 어느 정도 짧은 벡터들을 찾아내는 Approximate 기법과 정확히 짧은 벡터를 찾아내는 Exact 기법이 결합되어야 한다.

3. 격자 기반 암호 분석을 위한 Approximate algorithm에 대한 기술 조사

3.1. LLL 알고리즘

LLL 알고리즘은 격자의 기저 (b_0, b_1)를 입력 받은 후, 동일 격자에 대한 축소 기저를 출력하는 알고리즘이다. 해당 알고리즘은 크게 두 단계로 구성되어 있다. Gram-Schimist 직교화 정리를 적용하여 첫 번째 조건을 확인한다. 이후, Lov´asz condition을 체크한 뒤, 조건을 만족하지 않으면 b_0와 b_1을 Swap한다. 전체 알고리즘은 다음과 같다.

먼저, 격자의 입력 기저 (b_0, b_1)에 대해 격자 축소를 진행한다. 이를 위해 b_0, b_1에 Gram-Schmidt 직교화 정리를 적용하여 b_0^*, b_1^*를 얻는다. 해당 값을 활용하여 μ을 구한 뒤, 해당 값이 0.5보다 크다면 size reduction을 수행하여 입력 기저를 교체한다. 이후, Lov´asz condition ($\| b_i^* \|^2 \leq \| b_{i+1}^* \|^2 + \mu_{i+1,i}^2 \| b_i^* \|^2$)을 체크하고 해당 조건이 만족된다면, k값을 증가 (초기화 시, $k=1$) 시키고, 다시 μ를 구하는 과정을 진행하고, 만족하지 않는다면 b_0와 b_1에 대해 swap 연산을 수행한다.

3.1.2 Quantum LLL 알고리즘

최근에는 양자컴퓨터상에서의 quantum LLL [9] 알고리즘이 제안되었다. 해당 연구는 LLL 알고리즘에 대한 첫 양자 회로 구현이며, 양자 알고리즘을 이용해 Mersenne Number 암호체계를 공격하는 방법에 대해서도 논한다. 또한, 이 공격에 필요한 상당한 양의 자원, 특히 큐비트 수에 대해 강조하며, 향후 암호체계의 안전성을 재평가할 필요성을 제시한다. Quantum LLL 알고리즘의 핵심 요소는 다음과 같다. LLL의 두 단계인 Gram-Schimist 직교화 정리와 벡터 사이즈 축소 등을 모두 양자 회로로 구현한다. 이 과정에서 필요한 덧셈기로는 Cuccaro 덧셈기[10] 및 Gidney 덧셈기[11]를 사용하였다. 또한, 이들은 T-depth가 1인 토폴리 게이트를 사용하여 자원 절약적인 양자 회로를 설계하였다.

3.2. BKZ 알고리즘

BKZ (Block Korkin-Zolotarev) 알고리즘은 격자 기반 암호 분석에 주로 사용되며, LLL을 확장하여 더 큰 블록 크기에서 로컬 최적화를 수행하여 LLL보다 더 짧고, 더 정확하게 직교하는 기저를 찾는다. BKZ의 입력 기저 $B = (b_0, ..., b_n)$를 블록으로 나눈다. 이후 내부에서는 LLL과 같이 μ를 업데이트하고, 다음 반복에서 다음 블록에 대한 LLL 격자 축소를 진행하는 방식이다.

BKZ가 LLL보다 복잡하고 요구되는 계산량이 크지만, LLL에 비해 더 효율적이라는 장점이 있다. 또한, Quantum LLL과 같이 양자 컴퓨팅의 맥락에서 BKZ 또한 더 효율적으로 동작할 수 있는 잠재력이 있다고 여겨진다.

3.3. HKZ 알고리즘

HKZ (Hermite-Korkin-Zolotarev) 알고리즘 [12]은 LLL과 BKZ를 발전시킨 격자 축소 알고리즘이다. HKZ는 기저의 전역 최적화를 수행함으로써 더욱 강력한 축소 효과를 갖는다. 또한, LLL이 격자 기저를 단계적으로 개선하는 데 반해, HKZ는 격자의 모

든 부분을 고려하여 최적화한다. BKZ는 LLL과 HKZ 사이에서 균형을 이루며, 블록 단위로 로컬 최적화를 수행한다. 이처럼 HKZ는 세 알고리즘 중 이론적으로는 가장 강력하지만, 실제로는 계산 비용이 매우 높다는 한계점이 존재한다. 이러한 점 때문에 LLL 이나 BKZ 같은 실용적인 알고리즘들이 선호되는 경향이 있다. 앞서 설명한 BKZ와 HKZ의 주요 차이점은 최적화의 범위와 계산 복잡도이다. HKZ는 전역 최적화를 목표로 하는 반면 BKZ는 블록 단위로 로컬 최적화를 수행하여 실제 계산에서 더 효율적이고 실용적일 수 있는 것이다.

4. 결론

양자 내성 암호로 주목 받고 있는 격자 기반 암호를 분석하기 위해서는 Approximate 알고리즘과 Exact 알고리즘이 순차적으로 수행되어야 한다. 격자 기반 암호 알고리즘은 최소 500차원 이상의 격자를 기반으로 하므로, Exact 알고리즘만을 수행하여 SVP 문제를 해결하기는 어렵다. 본 논문에서는 Approximate 알고리즘의 종류와 동작 과정에 대해 알아보았다. 가장 기본적인 알고리즘인 LLL 부터, BKZ 및 HKZ 알고리즘에 대해 살펴보았다. 현재 LLL 알고리즘은 양자 컴퓨터상에서의 이점이 있으며 이미 구현된 상태이다. 향후, BKZ 등의 다른 Approximate 알고리즘 또한 양자 이점이 있을 포인트가 존재한다면 양자 컴퓨터상에서 구현하기 위한 연구들이 필요할 것으로 보인다.

5. Acknowledgment

This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government(MSIT) (<Q|Crypton>, No.2019-0-00033, Study on Quantum Security Evaluation of Cryptography based on Computational Quantum Complexity, 100%).

참고문헌

[1] Ajtai, Miklós. "The shortest vector problem in L2 is NP-hard for randomized reductions." Proceedings of the thirtieth annual ACM symposium on Theory of computing. 1998.

[2] Micciancio, Daniele, and Shafi Goldwasser. "Shortest vector problem." Complexity of Lattice Problems: A Cryptographic Perspective. Boston, MA: Springer US, 2002. 69-90.

[3] O Regev, Oded. "The learning with errors problem." Invited survey in CCC 7.30 (2010): 11.

[4] Nguyen, Phong Q., and Brigitte Vallée. The LLL algorithm. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010.

[5] Schnorr, Claus-Peter, and Martin Euchner. "Lattice basis reduction: Improved practical algorithms and solving subset sum problems." Mathematical programming 66 (1994): 181-199.

[6] Ajtai, Miklós, Ravi Kumar, and Dandapani Sivakumar. "A sieve algorithm for the shortest lattice vector problem." Proceedings of the thirty-third annual ACM symposium on Theory of computing. 2001.

[7] Nuyen, Phong Q., and Thomas Vidick. "Sieve algorithms for the shortest vector problem are practical." Journal of Mathematical Cryptology 2.2 (2008): 181-207.

[8] Micciancio, Daniele, and Panagiotis Voulgaris. "Faster exponential time algorithms for the shortest vector problem." Proceedings of the twenty-first annual ACM-SIAM symposium on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2010.

[9] Tiepelt, Marcel, and Alan Szepieniec. "Quantum LLL with an application to mersenne number cryptosystems." Progress in Cryptology – LATINCRYPT 2019: 6th International Conference on Cryptology and Information Security in Latin America, Santiago de Chile, Chile, October 2 – 4, 2019, Proceedings 6. Springer International Publishing, 2019.

[10] Cuccaro, Steven A., et al. "A new quantum ripple-carry addition circuit." arXiv preprint quant-ph/0410184 (2004).

[11] Gidney, Craig. "Halving the cost of quantum addition." Quantum 2 (2018): 74.

[12] Zhang, Wen, Sanzheng Qiao, and Yimin Wei. "HKZ and Minkowski reduction algorithms for lattice-reduction-aided MIMO detection." IEEE transactions on signal processing 60.11 (2012): 5963-5976.