Grover on Lattice

https://youtu.be/wJEjwZAFpcA

CHES'25

- **ML-KEM, ML-DSA에 대한 공격 비용 추정**

- **그러나 몇가지 한계점 존재**
  - 디멘션
  - 검색 범위
  - 그 외

- 전반적으로 표에 대한 설명 누락, 파라미터 명시하지 않음 등의 이유로 정확한 분석은 아니지만..
  - 양자 비용이 높지 않게 제한된 가정에서의 비용 평가를 제시
  - 벡터에 대한 전수조사의 본질이 흐려지는 것 같음 (솔루션 벡터가 커버하는 범위가 적음)

dimension 관련

- $v = [v_0, v_1, \ldots, v_{n-1}]$ 이므로, lattice의 전체 차원 (n)에 대한 입력 벡터 설정이 필요함
- **표3과 표4, q를 기반으로 n (dimension에 해당)를 역계산**
  - ML-KEM-512에서 O_{qs}에서 n은 약 190, O_{dep} 에서 n은 약 17

    → practical 비용을 위해 각각 다르게 제한한 것으로 보임
- **논문에 명시된 값은 아니고, 나와 있는 정보 기반의 추측이긴 함**
  - 여러 수치를 비교했을 때 전체 디멘션 (e.g. 512, 768, 1024) 에 대한 결과라고 보기 어려울 것 같음
  - 제 방식으로 저 정도 세팅으로 돌려보면 거의 비슷한 수준의 자원 나옴

Table 3: The quantum resources for the quantum sieve oracle $\mathcal{O}_{qs}$ and $\mathcal{O}_{qs\text{-}dep.opt.}$

Oracle	Qubit cost	T-count	T-depth
$\mathcal{O}_{qs}$	$\frac{3q^2+(2n+1)q+4}{2}$	$8n(2q^2-1)$	$4n(q^2+q)$
$\mathcal{O}_{qs\text{-}dep.opt.}$	$\frac{3nq^2-nq}{2}+n+2q+1$	$8n(q^2+q-1)$	$2(q^2+(4n-1)q-2n+1)$

Table 4: The quantum resources for our Oracle and Diffusion pair

Algorithm	Parameters	Oracle	#QB	G-cost	D	DW	D^2W
ML-KEM	512	$\mathcal{O}_{qs\text{-}dep.opt.}$	942	$1.03 \cdot 2^{18}$	$1.83 \cdot 2^{10}$	$2^{20.8}$	$2^{31.6}$
		$\mathcal{O}_{qs}$	239	$1.91 \cdot 2^{18}$	$1.82 \cdot 2^{16}$	$2^{24.8}$	$2^{41.6}$
	768	$\mathcal{O}_{qs\text{-}dep.opt.}$	3785	$1.87 \cdot 2^{20}$	$1.15 \cdot 2^{11}$	$2^{23.1}$	$2^{34.3}$
		$\mathcal{O}_{qs}$	694	$1.89 \cdot 2^{21}$	$1.39 \cdot 2^{19}$	$2^{28.9}$	$2^{48.4}$
	1024	$\mathcal{O}_{qs\text{-}dep.opt.}$	5216	$1.72 \cdot 2^{21}$	$1.41 \cdot 2^{11}$	$2^{23.8}$	$2^{35.3}$
		$\mathcal{O}_{qs}$	872	$1.57 \cdot 2^{22}$	$1.95 \cdot 2^{19}$	$2^{29.7}$	$2^{49.7}$
ML-DSA	44	$\mathcal{O}_{qs\text{-}dep.opt.}$	1097	$1.74 \cdot 2^{18}$	$1.09 \cdot 2^{11}$	$2^{21.2}$	$2^{32.3}$
		$\mathcal{O}_{qs}$	289	$1.42 \cdot 2^{19}$	$1.14 \cdot 2^{17}$	$2^{25.4}$	$2^{42.5}$
	65	$\mathcal{O}_{qs\text{-}dep.opt.}$	5757	$1.37 \cdot 2^{21}$	$1.47 \cdot 2^{11}$	$2^{24.0}$	$2^{35.6}$
		$\mathcal{O}_{qs}$	833	$1.34 \cdot 2^{22}$	$1.60 \cdot 2^{19}$	$2^{29.4}$	$2^{49.1}$
	87	$\mathcal{O}_{qs\text{-}dep.opt.}$	8057	$1.09 \cdot 2^{22}$	$1.65 \cdot 2^{11}$	$2^{24.7}$	$2^{36.4}$
		$\mathcal{O}_{qs}$	1089	$1.06 \cdot 2^{23}$	$1.27 \cdot 2^{20}$	$2^{30.4}$	$2^{50.8}$

검색 공간 관련

- **Grover search가 적용되는 부분 → 격자 위의 벡터 w에 대한 전수 조사**
- 격자 위의 벡터 $(i.e., v_0, v_1, w_0)$의 각 요소는 12비트여야 함 (ML-KEM-512 기준)
  - v는 모든 요소에 대해 12비트 사용함 → 즉, 내부 양자 연산 자체는 12비트로 동작

- 그러나 논문에서 검색 대상인 w의 범위를 이를 –T~T로 제한함
  - 양자 비용이 매우 커지기 때문에 practical한 수치를 위해 제한한다고 함
  - 이에 대한 수치나 관련 정보 명시하지 않음
- 역계산하면 약 3~6비트로 추정되며, 이보다 크다고 해도 어쨌든 12비트에 대해 검색하지 않음
  - 이는 실제 격자 상의 벡터가 가지는 계수 범위에 대한 검색이 아님

- 이것은 Grover iteration에 영향을 주며, 검색 공간이 작아지면 전체 비용이 크게 감소
  - 오라클 비용에 영향을 주지는 않음 (12비트에 대한 연산을 하긴 하지만, 중첩으로 두는 부분이 제한된 것)

To keep the quantum search space tractable, we restrict the integer coefficients $x \in \mathbb{Z}^n$ used to generate candidate lattice vectors $w = B \cdot x$ to a bounded hypercube region $[-T, T]^n$. The bound $T \in \mathbb{Z}^+$ is a positive integer parameter that controls the maximum

제곱

- CHES'25에는 제곱에 대한 설명은 없음 (제곱 해서 추가 레지스터에 저장한다 + 단순 수식만 존재)
- **해당 제곱을 썼다는 말은 없지만 AND 게이트 인용하면서, 저자 본인들의 논문 (QIP'25) 참조**
  - **QIP'25가 제곱에 대한 논문**이라서 사용했을 것으로 보임
  - 그리고 QIP'25의 T depth 반영 (Table 3) 하면 CHES'25 논문의 수치 (Table 4)가 비슷하게 나오긴 함
  - Td 비용식도 맞는듯

- **1번의 제곱에 대한 리소스**
  - n=12, Qc = 211, Td = 133
  - Depth opt 버전은 제곱 병렬 (큐비트 추가, 뎁스 그대로)
  - Qubit opt 버전은 제곱 시퀀셜 (큐비트 그대로, 뎁스 추가)

  - 하지만, 그대로 스케일링하면 CHES'25 논문의 표4의 결과만큼 적은 큐비트가 나오지는 않지만 자세히 분석하진 않았기도 하고 구현 상의 뭔가가 있을 것이라고 생각하여 **CHES'25에 제시된 결과 그대로 사용**

Cost measures	Q-counts	T-counts	T-depths
[1]	n^2+2n+1	$15n^2-17n+2$	$5n^2-3n-2$
[2]	n^2+n	$16n^2+13n+3$	$5n^2+12n-1$
[3]	$0.5n^2+6.5n+0.5$	$18n^2-14n-6$	$6n^2-4n-5$
[4]	$0.5n^2+3.5n+1$	$20n^2-8n-9$	$8n^2-8n-11$
[11]	$0.5n^2+2.5n+2$	$22n^2-24n-12$	$8n^2-6n-8$
[10] (n-even)	$1.5n^2+n-2$	$5n^2-4n-4$	$2.5n^2-2n-2$
[10] (n-odd)	$1.5n^2-1.5$	$5n^2-6n-3$	$2.5n^2-3n-1.5$
Proposed	$1.5n^2-0.5n+1$	$4n^2-4n$	n^2-n+1

Td 비교

- 현재 제 구현과 CHES'25의 Table 4에 제시된 비용 중 Td 및 큐비트 수 비교 (CHES'25 세팅에 맞춰 ; 추정이긴 함)
  - q= 12비트, dimension = 17

  1. **v+w에 대한 시퀀셜 덧셈 Td** → 17*17 = 289

  2. 제곱 한 번 → 20 + 21 + 12 = 53
     모든 디멘션에 대한 제곱 Td = 17 x 53 = 901

  3. 마지막 **비교 Td** → 13

  - Ours: 시퀀셜 덧셈, 제곱, 마지막 비교 더하면 총 1203 → 리버스 포함 총 Td : **2406**
  - Ours: 큐비트 수 → 677 – 56 (구현 편의상 추가했지만 idle 큐빗이라 56개 제외) = **621**

  - CHES'25의 Table 4 → Td = **1874**, Qubit = **982**
  - Ours → Td = 2406, Qubit = 621

  - **Td x Qubit가 18.8퍼 감소**
    - CHES'25 = 1840268
    - Ours = 1494126

논문 수정 방향

- **현재 제가 가진 구현은 full dimension과 full search space를 대상으로 했음**
  - CHES'25는 공격 가능한 제한된 범위에 대한 리소스 추정 (feasible bound)
  - 따라서 제 구현이 비용이 높게 나올 수 밖에 없음 (동일 조건이 아니어서)
  - 지금 시간 내에 작성할 수 있는 방향
    - 1. 실제 ML-KEM/DSA의 실제 파라미터에 대한 공격 비용이다
      → 개선은 조금 (약 18%) 되었으며, 전체 비용 추정으로 해서 다이렉트 비교는 최소화
    - 2. KpqC에 대한 양자 시브 비용이다 → KpqC를 우리나라 말고 다른데서 관심을 가지는지가 걱정

- **현재, Asiacrypt 냈을 때 제출한 구현에서 조금 변경**
  - 제곱에서 큐비트 재사용 최대화했음 (병렬 제거)
  - 비용은 새로 추정함

- **구현 자체에 대한 설명은 거의 없어서 어떤 구조인지 파악하기 어려움**
  - 또한 몇 개의 비용 테이블에 대한 설명이 누락 / 결과 누락되어 있어서 완전하게 이해하기 어려움
  - 동일한 가정에서의 개선이 아니니까 그들이 사용한 것으로 예상되는 파라미터로 비교
    - 제한된 그 세팅에서 우리 거가 조금 더 좋다고 하고, 그 이후로는 전체 시브 비용 제시 (이후로는 직접 비교 안 함) → 이렇게 해도 될까요?
  - **런타임 및 피지컬 리소스 추가 예정**

변경한 구현 결과

- 전에는 디멘션에 대한 병렬 제곱을 해서 안실라 큐비트가 너무 과도하게 필요했음 (뎁스는 최소화)
  - 수정한 구현에서는 뎁스는 증가했지만 큐빗을 많이 줄임

- Qubit x Depth trade off에서 전보다 개선된 결과 (딜리시움은 진행 중)
  - 저의 기존 구현보다 94퍼 감소 (FD-M and Td-M)

ML-KEM	512	768	1024
Qubit	807	812	812
Full depth	826814	1240136	1653430
Td	75802	113690	151578

Thank you.

감사합니다.