Quantum Lattice Enumeration in Limited Depth

CRYPTO 2024

Nina Bindel[1] Xavier Bonnetain[2] Marcel Tiepelt[3] Fernando Virdia[4]

[1] SandboxAQ, Palo Alto, CA, USA

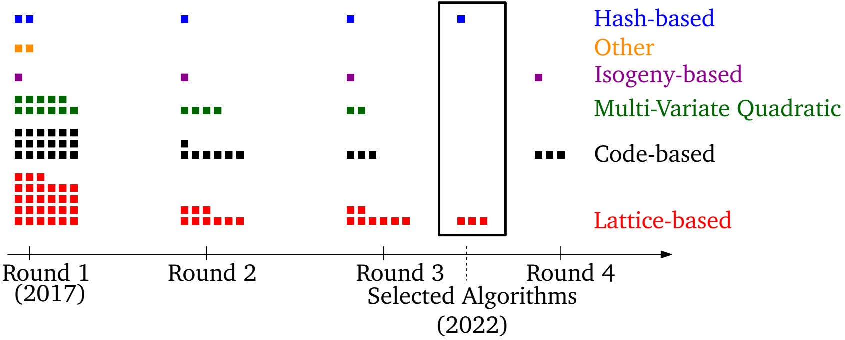
[2] Université de Lorraine, CNRS, Inria, Nancy, France

[3] KASTEL, Karlsruhe Institute of Technology, Karlsruhe, Germany

[4] Univerisdade NOVA de Lisboa, NOVA LINCS, Lisbon, Portugal

Why Lattice Enumeration?

- Lattice-based constructions popular
- 3 out of 4 NIST *post-quantum standards* are based on lattice assumptions



Why Lattice Enumeration as SVP Solver?

- Leading cost of state-of-the-art attacks is cost of SVP solver
- Lattice sieving analyzed in quantum setting[1]
- Quantum lattice enumeration analyzed in *asymptotic* setting[2] and unbounded quantum circuit model[3]

---

[1] [1] Albrecht et al. "Estimating Quantum Speedups for Lattice Sieves"
[5] Chailloux et al. "Lattice Sieving via Quantum Random Walks"
[2] [3] Bai et al. "Concrete Analysis of Quantum Lattice Enumeration"
[3] [2] Aono et al."Quantum Lattice Enumeration and Tweaking Discrete Pruning"

Why Lattice Enumeration as SVP Solver?

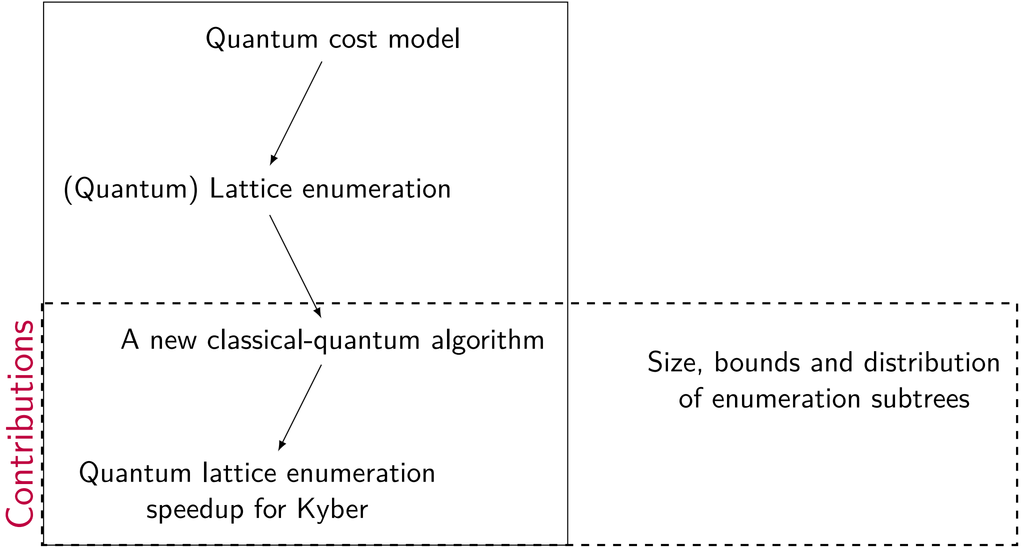
- Leading cost of state-of-the-art attacks is cost of SVP solver
- Lattice sieving analyzed in quantum setting[1]
- Quantum lattice enumeration analyzed in *asymptotic* setting[2] and unbounded quantum circuit model[3]

Concrete speedup of quantum lattice enumeration for practical parameters remains unclear.

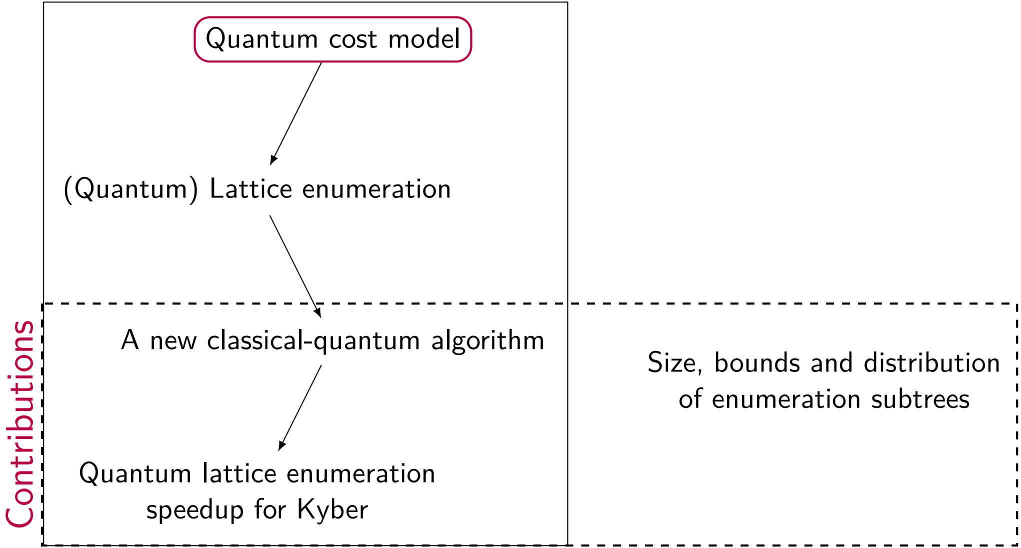
---

[1] [1] Albrecht et al. "Estimating Quantum Speedups for Lattice Sieves"
[5] Chailloux et al. "Lattice Sieving via Quantum Random Walks"
[2] [3] Bai et al. "Concrete Analysis of Quantum Lattice Enumeration"
[3] [2] Aono et al."Quantum Lattice Enumeration and Tweaking Discrete Pruning"

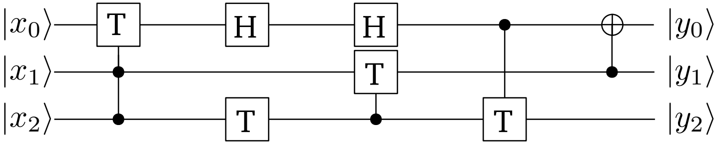
Today


Quantum cost model
(Quantum) Lattice enumeration
A new classical-quantum algorithm
Quantum lattice enumeration speedup for Kyber
Size, bounds and distribution of enumeration subtrees
Contributions

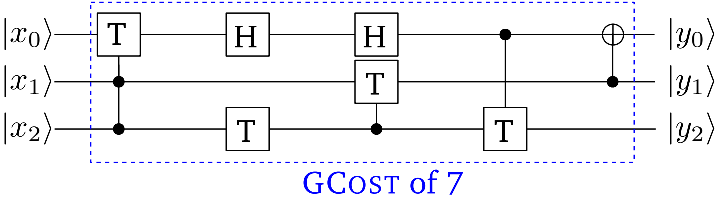
Today


Quantum cost model
(Quantum) Lattice enumeration
A new classical-quantum algorithm
Quantum lattice enumeration speedup for Kyber
Size, bounds and distribution of enumeration subtrees
Contributions

Quantum Cost Model

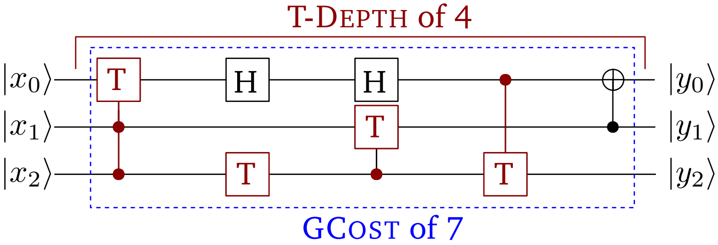


Quantum Cost Model



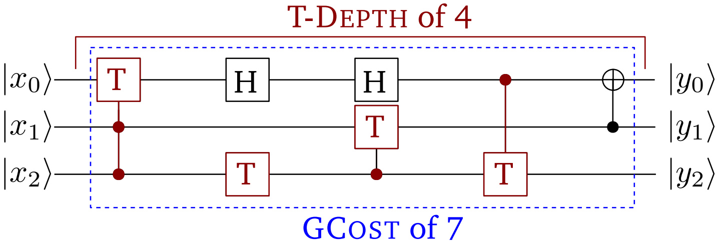
- GCost: Number of quantum gates

Quantum Cost Model



- GCost: Number of quantum gates
- T-Depth: Consecutive gates *(appears to be a main hurdle)*

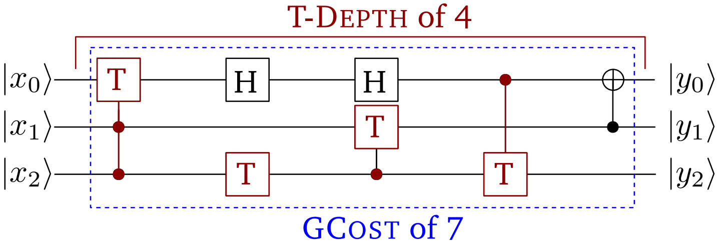
Quantum Cost Model



- GCost: Number of quantum gates
- T-Depth: Consecutive gates *(appears to be a main hurdle)*
- Hypothetical MaxDepth $\in \{2^{40}, 2^{64}, 2^{96}\}$ by NIST[4]:

[4] [9] NIST *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*

Quantum Cost Model

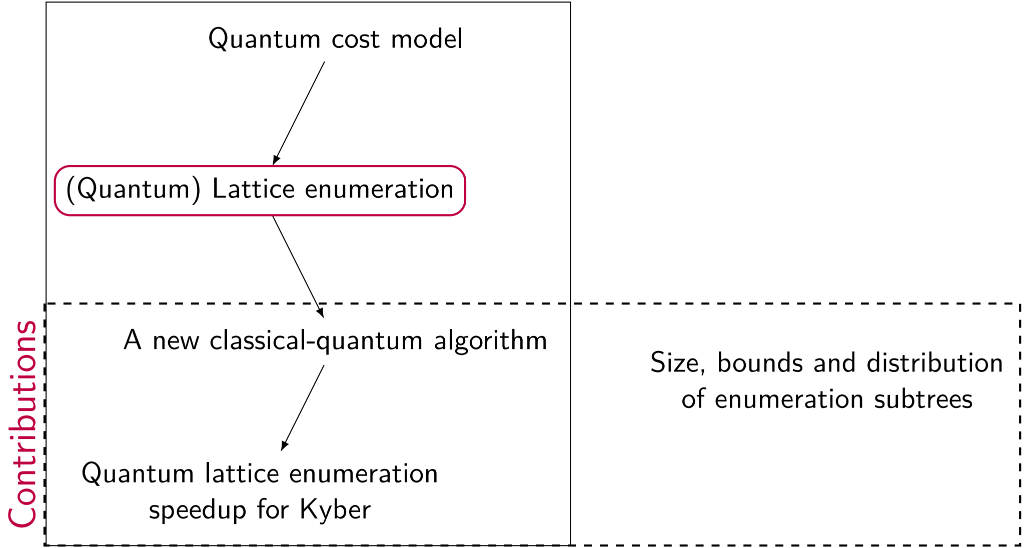


- GCost: Number of quantum gates
- T-Depth: Consecutive gates *(appears to be a main hurdle)*
- Hypothetical MaxDepth $\in \{2^{40}, 2^{64}, 2^{96}\}$ by NIST[4]:

One needs: T-Depth(QEnum) $\leq$ MaxDepth

[4] [9] NIST *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*

Today


Quantum cost model
(Quantum) Lattice enumeration
Contributions
A new classical-quantum algorithm
Quantum lattice enumeration speedup for Kyber
Size, bounds and distribution of enumeration subtrees

Lattice Enumeration

Setup

- Lattice $\mathcal{L}(B)$, dimension n
- Enumeration: Given B, bound R,
  finds $\vec{v}$ s.t. $0 < ||\vec{v}|| \leq R$

Lattice Enumeration

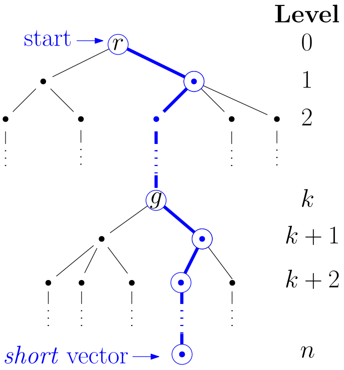
Setup

- Lattice $\mathcal{L}(B)$, dimension n
- Enumeration: Given B, bound R, finds $\vec{v}$ s.t. $0 < ||\vec{v}|| \leq R$

Enumeration with extreme pruning[5]

- DFS defines enumeration tree(s)

One Tree $\mathcal{T}$



[3][6] Gama et al. "Lattice Enumeration Using Extreme Pruning"

Lattice Enumeration

Setup

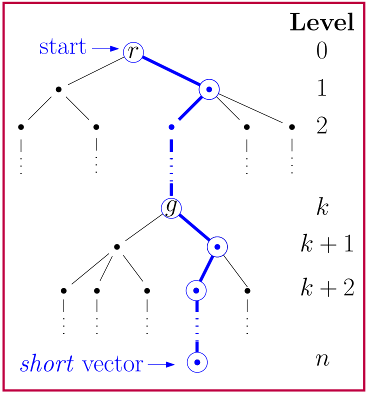
- Lattice $\mathcal{L}(B)$, dimension n
- Enumeration: Given B, bound R, finds $\vec{v}$ s.t. $0 < ||\vec{v}|| \leq R$

Enumeration with extreme pruning[5]

- DFS defines enumeration tree(s)

Gaussian heuristic +GSA gives us $\mathbb{E}_{\text{random tree } \mathcal{T}}[\#\mathcal{T}(r)]$

One Tree $\mathcal{T}$

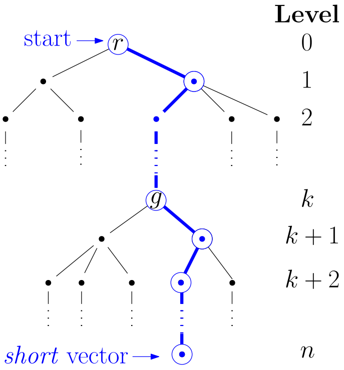


[3][6] Gama et al. "Lattice Enumeration Using Extreme Pruning"

Lattice Enumeration

Time complexity

- Classical: $\mathcal{O}(\#\mathcal{T}(r))$

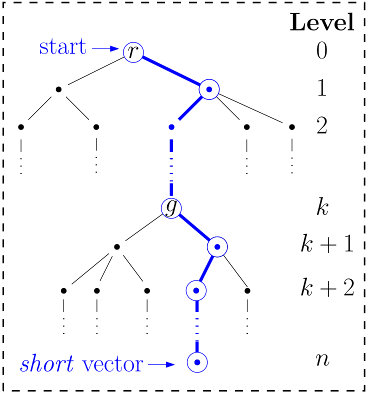


Quantum Lattice Enumeration

Time complexity

- Classical: $\mathcal{O}(\#\mathcal{T}(r))$
- Quantum[6]:
  - QPE: $\mathcal{O}(\sqrt{\#\mathcal{T}(r) \cdot n})$ calls to $\mathcal{W}$
  - $poly(n)$ classical repetitions of QPE($\mathcal{W}$)

QPE($\mathcal{W}$) $\equiv$ Quantum Walk



[6][8] Montanaro's "Quantum-Walk Speedup of Backtracking Algorithms"

Quantum Lattice Enumeration

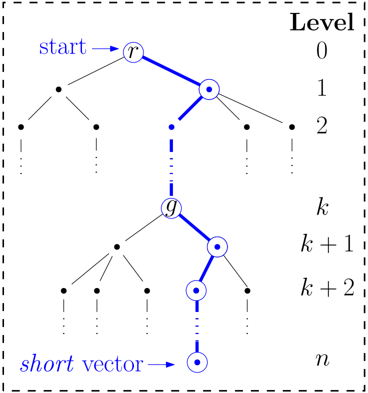
Time complexity

- Classical: $\mathcal{O}(\#\mathcal{T}(r))$
- Quantum[6]:
  - QPE: $\mathcal{O}(\sqrt{\#\mathcal{T}(r) \cdot n})$ calls to $\mathcal{W}$
  - $poly(n)$ classical repetitions of QPE($\mathcal{W}$)

Only QPE($\mathcal{W}$) is a quantum circuit:

$$\text{T-DEPTH}(\text{QENUM}(\mathcal{T}(r))) = \text{T-DEPTH}(\text{QPE}(\mathcal{W}))$$

QPE($\mathcal{W}$) $\equiv$ Quantum Walk



[6] [8] Montanaro's "Quantum-Walk Speedup of Backtracking Algorithms"

Depth of *Full* Quantum Enumeration

! Disclaimer: Very loosely estimated numbers. !

(don't quote us on **these**)

- QPE($\mathcal{W}$) applied to full enumeration tree of depth β
- Ignoring Jensen's Gap $\mathbb{E}[\sqrt{\#\mathcal{T}(r) \cdot h}]$ (we will come back to this later)
- Limitation: $\log_2(\textsc{MaxDepth}) \in \{40, 64, 96\}$

Depth of *Full* Quantum Enumeration

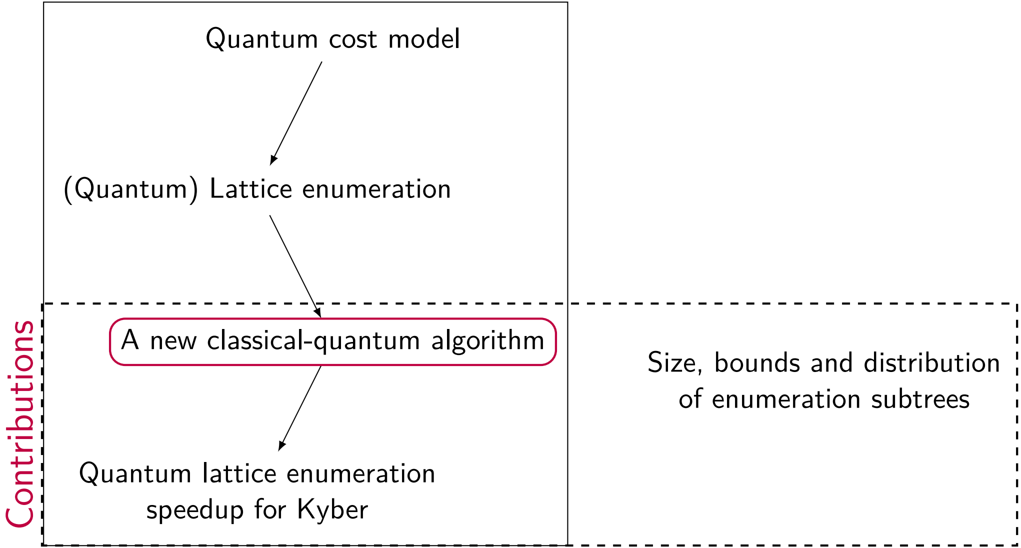
! Disclaimer: Very loosely estimated numbers. !

(don't quote us on **these**)

- QPE($\mathcal{W}$) applied to full enumeration tree of depth β
- Ignoring Jensen's Gap $\mathbb{E}[\sqrt{\#\mathcal{T}(r) \cdot h}]$ (we will come back to this later)
- Limitation: $\log_2(\textsc{MaxDepth}) \in \{40, 64, 96\}$

$$\log_2 \mathbb{E}[\textsc{T-Depth}(\text{QPE}(\mathcal{W}))] \approx \begin{cases} 90 & \text{for Kyber-512} \quad \leq \log(\textsc{MaxDepth}) \\ 166 & \text{for Kyber-768} \quad \gg \log(\textsc{MaxDepth}) \\ 263 & \text{for Kyber-1024} \quad \gg \log(\textsc{MaxDepth}) \end{cases}$$

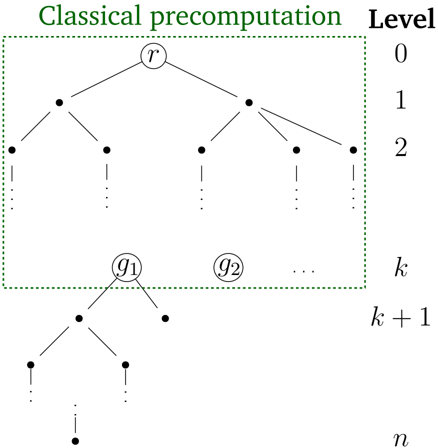
Today



Quantum cost model
(Quantum) Lattice enumeration
A new classical-quantum algorithm
Quantum lattice enumeration speedup for Kyber
Size, bounds and distribution of enumeration subtrees
Contributions

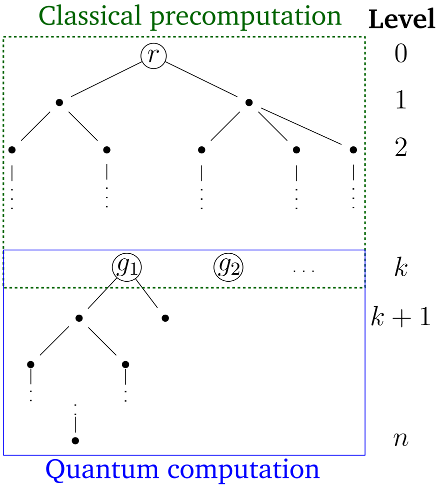
A Quantum-Classical Algorithm (simplified)

- Classical precomputation: up to level k



A Quantum-Classical Algorithm (simplified)

- Classical precomputation: up to level k
- $\textsc{QEnum}(\mathcal{T}(g_i))$ for every node g_i on level k

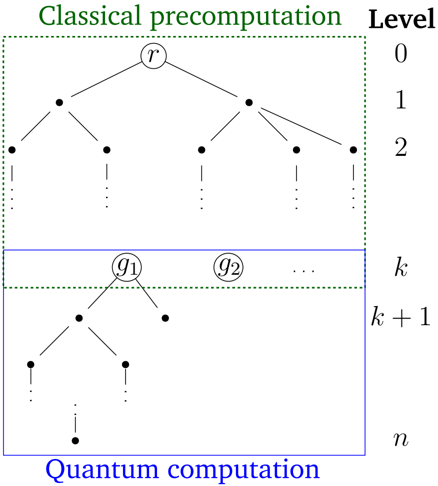


A Quantum-Classical Algorithm (simplified)

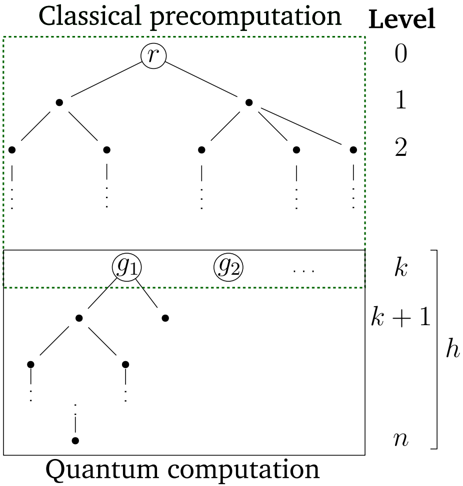
- Classical precomputation: up to level k
- $\textsc{QEnum}(\mathcal{T}(g_i))$ for every node g_i on level k
- Choose level k such that

$$\textsc{T-Depth}(QPE(\mathcal{W})) \leq \textsc{MaxDepth}$$

... and also reducing overall cost.

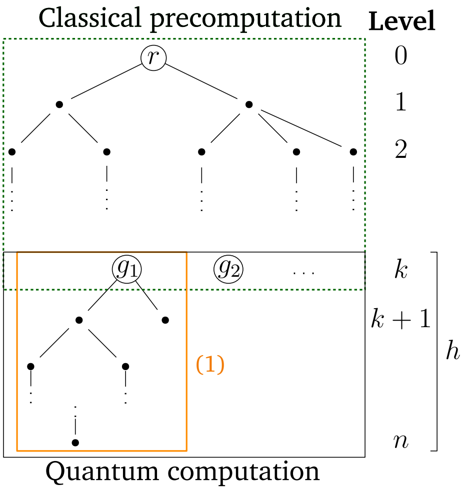


Quantum Cost Estimation



Quantum Cost Estimation

(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

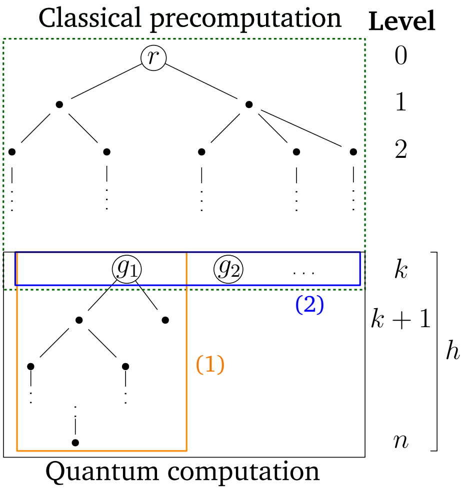


[7] [4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Quantum Cost Estimation

(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

(2) Distribution of subtrees[7]



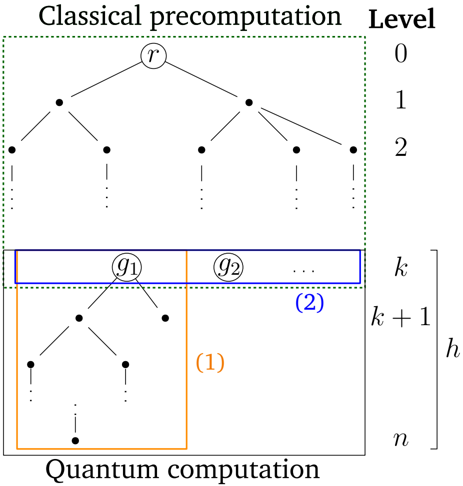
[7] [4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Quantum Cost Estimation

(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

(2) Distribution of subtrees[7]

(3) #calls to $\mathcal{W}$[7]: $\sqrt{\#\mathcal{T}(g_i) \cdot h}$



[7] [4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Quantum Cost Estimation

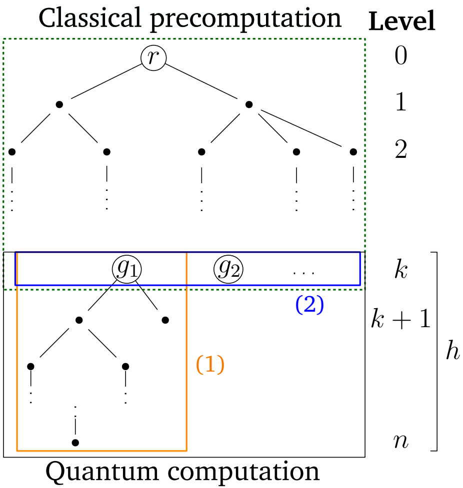
(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

(2) Distribution of subtrees[7]

(3) #calls to $\mathcal{W}$[7]: $\sqrt{\#\mathcal{T}(g_i) \cdot h}$

(4)

$$\underbrace{\underset{\substack{\text{random} \\ \text{tree } \mathcal{T}}}{\mathbb{E}} [\sqrt{\#\mathcal{T}(g_i) \cdot h}]}_{\text{what we need}}$$



[7] [4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Quantum Cost Estimation

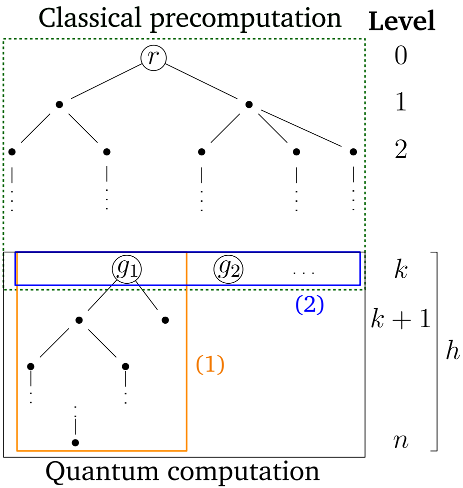
(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

(2) Distribution of subtrees[7]

(3) #calls to $\mathcal{W}^7$: $\sqrt{\#\mathcal{T}(g_i) \cdot h}$

(4)

$$\underbrace{\mathbb{E}_{\text{random tree } \mathcal{T}}\left[\sqrt{\#\mathcal{T}(g_i) \cdot h}\right]}_{\text{what we need}} \qquad \underbrace{\mathbb{E}_{\text{random tree } \mathcal{T}}\left[\#\mathcal{T}(g_i) \cdot h\right]}_{\text{what we know (Gaussian heuristic + GSA)}}$$



[7][4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Quantum Cost Estimation

(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

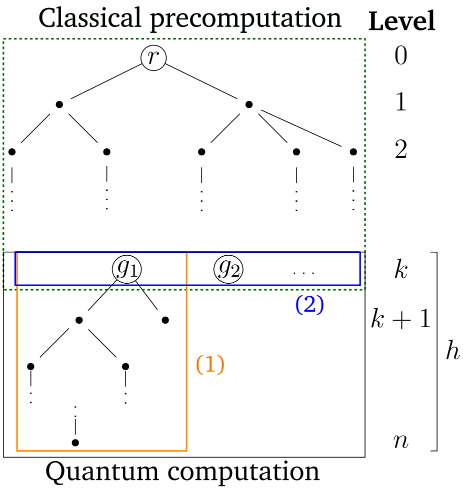
(2) Distribution of subtrees[7]

(3) #calls to $\mathcal{W}$[7]: $\sqrt{\#\mathcal{T}(g_i) \cdot h}$

(4)

$$\underbrace{\mathop{\mathbb{E}}_{\substack{\text{random}\\\text{tree } \mathcal{T}}}\left[\sqrt{\#\mathcal{T}(g_i) \cdot h}\right]}_{\text{what we need}} \qquad \underbrace{\sqrt{\mathop{\mathbb{E}}_{\substack{\text{random}\\\text{tree } \mathcal{T}}}\left[\#\mathcal{T}(g_i) \cdot h\right]}}_{\substack{\text{what we know}\\\text{(Gaussian heuristic + GSA)}}}$$

Jensen's Inequality: $\mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$



[7] [4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Quantum Cost Estimation

(1) Size $\#\mathcal{T}(g_i)$ of subtrees[7]

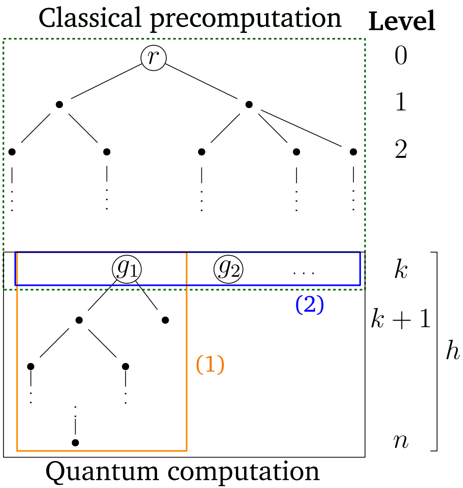
(2) Distribution of subtrees[7]

(3) #calls to $\mathcal{W}$[7]: $\sqrt{\#\mathcal{T}(g_i) \cdot h}$

(4) Multiplicative Jensen's Gap 2^z: (property of the trees)

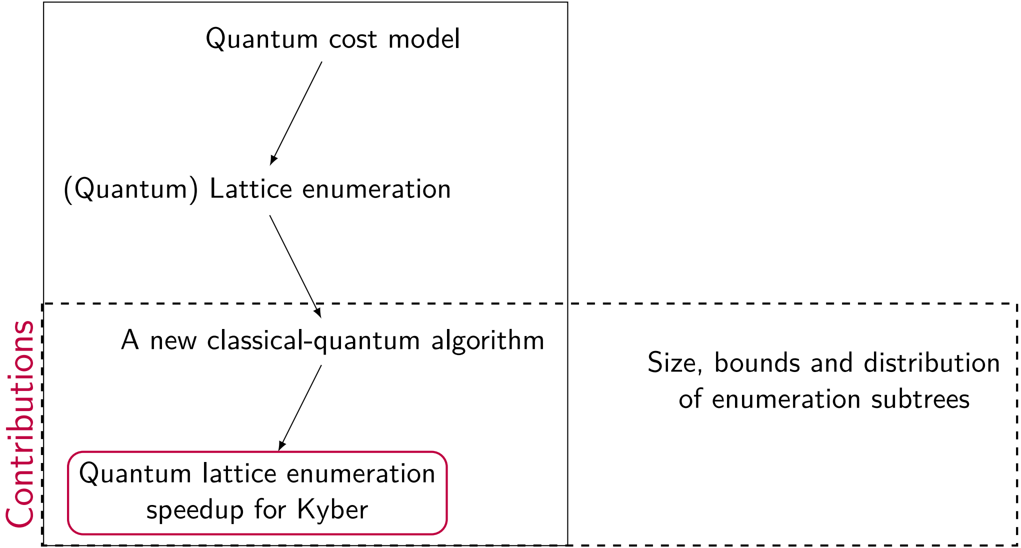
$$2^z \cdot \underbrace{\mathop{\mathbb{E}}_{\substack{\text{random}\\ \text{tree } \mathcal{T}}}\left[\sqrt{\#\mathcal{T}(g_i) \cdot h}\right]}_{\text{what we need}} = \underbrace{\sqrt{\mathop{\mathbb{E}}_{\substack{\text{random}\\ \text{tree } \mathcal{T}}}\left[\#\mathcal{T}(g_i) \cdot h\right]}}_{\substack{\text{what we know}\\ \text{(Gaussian heuristic + GSA)}}}$$

Jensen's Inequality: $\mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$



[7] [4, Conj. 1, 2, 3] This work. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*

Today


Quantum cost model
(Quantum) Lattice enumeration
A new classical-quantum algorithm
Quantum lattice enumeration speedup for Kyber
Size, bounds and distribution of enumeration subtrees
Contributions

Computing Results: Quantum Cost Estimation

Compute

$$\textbf{Total Cost} = \text{Classical Precomputation} + \mathop{\mathbb{E}}_{\substack{\text{random}\\ \text{tree } \mathcal{T}}}\left[\sum_{\substack{g_i \\ \text{on level k}}} \textsc{GCost}(\textsc{QEnum}(\mathcal{T}(g_i))\right]$$

Computing Results: Quantum Cost Estimation

Compute

$$\textbf{Total Cost} = \text{Classical Precomputation} + \mathop{\mathbb{E}}_{\substack{\text{random}\\ \text{tree } \mathcal{T}}} \left[\sum_{\substack{g_i \\ \text{on level k}}} \textsc{GCost}(\textsc{QEnum}(\mathcal{T}(g_i)) \right]$$

with level k such that

$$\textsc{T-Depth}(\mathsf{QPE}(\mathcal{W})) \leq \textsc{MaxDepth}\,,$$

Computing Results: Quantum Cost Estimation

Compute

$$\textbf{Total Cost} = \text{Classical Precomputation} + \underset{\substack{\text{random}\\ \text{tree } \mathcal{T}}}{\mathbb{E}} \left[\sum_{\substack{g_i \\ \text{on level k}}} \textsc{GCost}(\textsc{QEnum}(\mathcal{T}(g_i))) \right]$$

with level k such that

$$\textsc{T-Depth}(\mathsf{QPE}(\mathcal{W})) \leq \textsc{MaxDepth}\,,$$

compare **Total Cost** to running Grover's algorithm on AES[8].

[8][7] Jaques et al. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC"

Computing Results: Quantum Cost Estimation

Compute

$$\textbf{Total Cost} = \text{Classical Precomputation} + \mathop{\mathbb{E}}_{\substack{\text{random}\\ \text{tree } \mathcal{T}}}\left[\sum_{\substack{g_i \\ \text{on level k}}} \textsc{GCost}(\textsc{QEnum}(\mathcal{T}(g_i))\right]$$

with level k such that

$$\textsc{T-Depth}(\text{QPE}(\mathcal{W})) \leq \textsc{MaxDepth}\,,$$

compare **Total Cost** to running Grover's algorithm on AES[8].

Find Jensen's Gap 2^z such that

Total Cost $\leq$ Cost of Grover on AES with $\textsc{T-Depth}(\text{QPE}(\mathcal{W})) \leq \textsc{MaxDepth}$

[8] [7] Jaques et al. "Implementing Grover Oracles for Quantum Key Search on AES and LowMC"

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"hypothetical lower bounds" for $\#\mathcal{T}(g_i)$ (LB/UB in our paper)

more likely to be feasible → less likely to be feasible						
	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"hypothetical lower bounds" for $\#\mathcal{T}(g_i)$ (LB/UB in our paper)

more likely to be feasible → less likely to be feasible						
	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"hypothetical lower bounds" for $\#\mathcal{T}(g_i)$ (LB/UB in our paper)

more likely to be feasible → less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 0$	$z \geq 0$	$z \geq 2$	$z \geq 17$	$z \geq 50$	$z > 64$
2^{64}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 17$	$z \geq 49$	$z > 64$
2^{96}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 19$	$z \geq 51$	$z > 64$

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

“hypothetical lower bounds” for $\#\mathcal{T}(g_i)$ (LB/UB in our paper)

more likely to be feasible ⟶ less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 0$	$z \geq 0$	$z \geq 2$	$z \geq 17$	$z \geq 50$	$z > 64$
2^{64}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 17$	$z \geq 49$	$z > 64$
2^{96}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 19$	$z \geq 51$	$z > 64$

quantum speedup... ...may be possible

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"hypothetical lower bounds" for $\#\mathcal{T}(g_i)$ (LB/UB in our paper)

more likely to be feasible — less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 0$	$z \geq 0$	$z \geq 2$	$z \geq 17$	$z \geq 50$	$z > 64$
2^{64}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 17$	$z \geq 49$	$z > 64$
2^{96}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 19$	$z \geq 51$	$z > 64$

quantum speedup... ...may be possible (Kyber-512) ...may be possible for "trivial" quantum operator (Kyber-768)

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"hypothetical lower bounds" for $\#\mathcal{T}(g_i)$ (LB/UB in our paper)

more likely to be feasible → less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 0$	$z \geq 0$	$z \geq 2$	$z \geq 17$	$z \geq 50$	$z > 64$
2^{64}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 17$	$z \geq 49$	$z > 64$
2^{96}	$z \geq 0$	$z \geq 0$	$z \geq 1$	$z \geq 19$	$z \geq 51$	$z > 64$

quantum speedup...

- Kyber-512: ...may be possible
- Kyber-768: ...may be possible for "trivial" quantum operator
- Kyber-1024: ...probably no effect

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"state-of-the-art" bounds for $\#\mathcal{T}(g_i)$ (UB/UB in our paper)

more likely to be feasible → less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{64}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{96}	$z \geq 15$	$z \geq 40$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"state-of-the-art" bounds for $\#\mathcal{T}(g_i)$ (UB/UB in our paper)

more likely to be feasible → less likely to be feasible						
	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{64}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{96}	$z \geq 15$	$z \geq 40$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$

quantum speedup... ...questionable even for "trivial" quantum operator

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"state-of-the-art" bounds for $\#\mathcal{T}(g_i)$ (UB/UB in our paper)

more likely to be feasible → less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{64}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{96}	$z \geq 15$	$z \geq 40$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$

quantum speedup... (Kyber-512:) ...questionable even for "trivial" quantum operator (Kyber-768:) ...probably no effect

Simplified Results

Reminder: Multiplicative Jensen's Gap

$$2^z \cdot \mathbb{E}[\sqrt{X}] \leq \sqrt{\mathbb{E}[X]}$$

"state-of-the-art" bounds for $\#\mathcal{T}(g_i)$ (UB/UB in our paper)

more likely to be feasible → less likely to be feasible

	Kyber-512		Kyber-768		Kyber-1024	
	GCost of quantum walk operator $\mathcal{W}$					
MaxDepth	1	*minimal*	1	*minimal*	1	*minimal*
2^{40}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{64}	$z \geq 20$	$z \geq 36$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$
2^{96}	$z \geq 15$	$z \geq 40$	$z \geq 61$	$z > 64$	$z > 64$	$z > 64$

quantum speedup...

- Kyber-512: ...questionable even for "trivial" quantum operator
- Kyber-768: ...probably no effect
- Kyber-1024: ...probably no effect

Conclusion

There exists a gap between *generous* lower bounds, and actual expected cost.

2^z, $\mathcal{W}$, ... (more in our paper)

Better understanding of degree of uncertainty from properties of enumeration trees.

Conclusion

There exists a gap between *generous* lower bounds, and actual expected cost.

2^z, $\mathcal{W}$, ... (more in our paper)

Better understanding of degree of uncertainty from properties of enumeration trees.

(link to eprint)

Marcel Tiepelt, marcel.tiepelt@kit.edu

ePrint:
https://eprint.iacr.org/2023/1423

Code:
https://github.com/mtiepelt/QuantumLatticeEnumeration

Slides:
https://mtiepelt.github.io/Pages/Publications

Bibliography I

[1] M. R. Albrecht et al. "Estimating Quantum Speedups for Lattice Sieves". In: *Advances in Cryptology – ASIACRYPT 2020*. Cham, 2020. DOI: 10.1007/978-3-030-64834-3_20.

[2] Y. Aono et al. "Quantum Lattice Enumeration and Tweaking Discrete Pruning". In: *Advances in Cryptology – ASIACRYPT 2018*. Cham, 2018.

[3] S. Bai et al. "Concrete Analysis of Quantum Lattice Enumeration". English. In: *Advances in Cryptology ASIACRYPT 2023 - 29th International Conference on the Theory and Application of Cryptology and Information Security, Proceedings*. Germany, 2023. DOI: 10.1007/978-981-99-8727-6_5.

[4] N. Bindel et al. *"Quantum Lattice Enumeration in Limited Depth"*. Cryptology ePrint Archive, Paper 2023/1423. 2023.

Bibliography II

[5] A. Chailloux and J. Loyer. “Lattice Sieving via Quantum Random Walks”. In: *Advances in Cryptology – ASIACRYPT 2021*. Cham, 2021. DOI: 10.1007/978-3-030-92068-5_3.

[6] N. Gama et al. “Lattice Enumeration Using Extreme Pruning”. In: *Advances in Cryptology – EUROCRYPT 2010*. Berlin, Heidelberg, 2010. DOI: 10.1007/978-3-642-13190-5_13.

[7] S. Jaques et al. “Implementing Grover Oracles for Quantum Key Search on AES and LowMC”. In: *Advances in Cryptology - EUROCRYPT 2020 - 39th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Zagreb, Croatia, May 10-14, 2020, Proceedings, Part II*. Vol. 12106. 2020. DOI: 10.1007/978-3-030-45724-2_10.

[8] A. Montanaro. “Quantum-Walk Speedup of Backtracking Algorithms”. In: *Theory Comput.* 14.1 (2018). DOI: 10.4086/TOC.2018.V014A015.

Bibliography III

[9] NIST. *Submission Requirements and Evaluation Criteria for the Post-Quantum Cryptography Standardization Process*. 2016.