Quantum Sieving for Decoding Linear Codes

Investigating Quantum Nearest-Neighbor and Sieving Techniques in Code-Based Cryptography

Omar Abul-Hassan
Department of Mathematics
Stanford University

March 23, 2025

Overview

Introduction and Motivation

- **Quantum Threat to Cryptography**
  - Shor's algorithm breaks RSA and ECC.
  - Necessity for quantum-resistant cryptography (NIST PQC standardization).
- **Code-Based Cryptography**
  - Security relies on difficulty of decoding random linear codes.
  - Syndrome Decoding Problem known to be NP-hard.
- **Quantum Algorithms and Security**
  - Quantum techniques offer speedups for decoding tasks.
  - Impact on code-based cryptographic schemes like McEliece.

Goal: Investigate quantum sieving algorithms to understand their implications on decoding complexity and post-quantum security.

Linear Codes and the Decoding Problem

- **Linear Codes**
  - A linear code C of length n over $\mathbb{F}_2$ is a subspace of $\mathbb{F}_2^n$.
  - Parameters: dimension k, length n, denoted as $[n, k]$ code.
- **Parity-Check Matrix**
  - For a linear code C, parity-check matrix H defined such that:

$$C = \{c \in \mathbb{F}_2^n \mid Hc^T = 0\}$$

  - Syndrome of received vector $y = c + e$ computed as:

$$s = Hy^T = H(c + e)^T = He^T$$

- **Syndrome Decoding Problem (SDP)**
  - Given (H, s, t), find error vector e such that $He^T = s$ and $\mathrm{wt}(e) \leq t$.
  - Known to be NP-hard (Berlekamp–McEliece–van Tilborg, 1978).

Classical Decoding Techniques: ISD

Syndrome Decoding as a Search Problem

- Decoding goal: Given a syndrome s, find the error vector e such that:

$$He^T = s, \quad \mathrm{wt}(e) \leq t]$$

- Equivalently, this can be viewed as nearest-neighbor search in a high-dimensional Hamming space.

Information Set Decoding (Prange, 1962)

- Fundamental idea: select *information set*, a set of coordinates assumed error-free.
- Solve the linear equation on this set:

$$H_I e_I^T = s \quad \Rightarrow \quad e_I = H_I^{-1} s$$

- Verify solution correctness by checking weight.

Complexity Improvements

- Original Prange complexity: $O(2^{0.1207n})$.
- Subsequent improvements: Stern (1989), Dumer (1991), BJMM (2012) use structured search methods (meet-in-the-middle, birthday paradox).
- Current best classical complexity around $O(2^{0.096n})$ (BJMM, 2012).

Quantum Algorithms: Grover's Search

Why Quantum Algorithms?

- Quantum computing utilizes quantum superposition and interference, providing computational speedups over classical counterparts.

Grover's Search Algorithm (Grover, 1996)

- General quantum search technique for unstructured search problems.
- Classically: searching an unstructured database of size N takes $O(N)$.
- Grover's algorithm improves to quantum complexity $O(\sqrt{N})$.

Lemma: Grover's Complexity (Bernstein, 2010)

Applying Grover's algorithm to Information Set Decoding (ISD) reduces Prange's decoding complexity exponent approximately by half:

$$2^{0.1207n} \to 2^{0.06035n}$$

Quantum Walks: Structured Quantum Search

From Grover to Quantum Walks

- Grover's algorithm offers quadratic improvement, but no further structural insights.
- Quantum walks generalize Grover's algorithm by exploiting the structure of the search space, achieving superior complexities for structured search problems.

Quantum Walk Techniques

- Represent search space as graph: nodes as partial solutions, edges as feasible transitions between solutions.
- Quantum walks efficiently explore this graph, reducing complexity by combining structured search with quantum parallelism.

Theorem (Quantum ISD Complexity, Kachigar–Tillich, 2017)

Quantum Information-Set Decoding algorithms leveraging quantum walks achieve complexity approximately:

$$T_{QW\text{-}ISD} \approx 2^{0.05869n},$$

surpassing Grover's quadratic improvement by exploiting structured search.

Key Intuition: Why Quantum Walks Improve Complexity

Quantum Walk vs Classical Search

- Classical ISD algorithms (like Stern and BJMM) use structured searches (meet-in-the-middle, collision-finding) in exponentially large sets.
- Quantum walks leverage quantum amplitudes to simultaneously explore multiple structured solutions, amplifying probability of successful collisions.
- Specifically, quantum amplitude amplification (similar to Grover) boosts successful candidate probabilities.

Underlying Principle

- Quantum walks replace classical exhaustive pairing with quantum collision finding, significantly faster due to amplitude amplification.
- Each quantum step is analogous to *simultaneous classical checks*, leveraging quantum parallelism.

Result: Quantum walks structurally refine Grover's speedup, yielding best known quantum complexity $\approx 2^{0.058n}$.

Quantum Sieving: Origin and Motivation

- **Historical Context**
  - Originated from lattice cryptography: Ajtai–Kumar–Sivakumar lattice sieving (2001).
  - Successfully adapted to code-based cryptography by leveraging structural similarities in search problems.
- **Why Quantum Sieving for Linear Codes?**
  - Classical sieving techniques effectively reduce complexity through structured searching, but remain exponentially expensive.
  - Quantum computing can supercharge these methods by performing structured searches using quantum parallelism.
  - Quantum techniques exploit search-space structure more deeply than generic algorithms like Grover's.
- **Quantum Techniques in Sieving**
  - Quantum nearest-neighbor search efficiently identifies close pairs of vectors.
  - Quantum walks and amplitude amplification significantly improve complexity, surpassing classical and basic quantum search methods.

Result: Quantum sieving lowers complexity exponents beyond Grover-based methods, crucially impacting cryptographic security analysis.

Quantum Sieving: Step-by-Step Construction (1)

Step 1: List Generation

- Generate an exponentially large structured list L of partial error vectors:

$$L = \{v_i \in \mathbb{F}_2^n \mid \text{partial solutions to } He^T = s\}$$

- List size typically set as $|L| \approx 2^{\lambda n}$, where λ is optimized to minimize overall complexity.
- Each vector represents a candidate partial solution to the decoding problem.

Intuition:

- Large lists increase collision probability but also computational overhead.
- Optimal λ balances collision likelihood with complexity.

Quantum Sieving: Step-by-Step Construction (2)

Step 2: Quantum Nearest-Neighbor Search

- Goal: Efficiently find pairs (v_i, v_j) from list L with small Hamming distance.
- Key criterion: Identify pairs where:

$$d(v_i, v_j) \leq \gamma n, \quad 0 < \gamma < 1$$

- Quantum superposition over all vector pairs enables simultaneous searching:

$$\frac{1}{|L|} \sum_{v_i, v_j \in L} |v_i, v_j\rangle$$

- Quantum walks, combined with amplitude amplification (Grover), substantially speed up the search.

Lemma (May–Ozerov, 2015)

Quantum nearest-neighbor search complexity for lists of size $2^{\lambda n}$ is:

$$O\left(2^{\frac{\lambda n}{1-\gamma}}\right) \quad \text{(classically: } 2^{\lambda n}\text{)}$$

Quantum Sieving: Step-by-Step Construction (3)

Step 3: Collision Identification and Error Reconstruction

- Once candidate pairs (v_i, v_j) are found, form potential solutions:

$$e = v_i + v_j$$

- Check the syndrome condition classically:

$$He^T \stackrel{?}{=} s$$

- Each collision (v_i, v_j) yields a candidate for the original error vector.
    - Candidates satisfying the syndrome equation are valid decoding solutions.
- Quantum walks enhance the probability of obtaining good candidates through amplitude amplification: probability of selecting a correct pair significantly boosted by quantum interference effects.
- Final classical verification is still required to ensure solution accuracy

Result: Quantum sieving finds valid decoding solutions faster than classical sieving methods, dramatically reducing complexity.

Quantum Complexity Analysis

- **Classical Complexity Baseline**
  - Information-Set Decoding (ISD) complexity (e.g., BJMM algorithm):

$$T_{\text{ISD}} \approx 2^{0.096n}$$

- **Quantum Speedups Overview**
  - Grover's algorithm provides generic quadratic speedups.
  - Quantum walks offer additional efficiency by structured solution-space exploration.

Lemma (Grover's Speedup for ISD, Bernstein 2010)

Applying Grover's algorithm to ISD reduces the complexity exponent roughly by half:

$$T_{\text{Grover-ISD}} \approx 2^{0.06035n}$$

Theorem (Quantum Walks Complexity, Kachigar–Tillich 2017)

Quantum walks combined with ISD achieve complexity:

$$T_{\text{QuantumWalk-ISD}} \approx 2^{0.05869n}$$

Security Implications for Code-Based Cryptography

- **Impact on McEliece Cryptosystem**
  - Security fundamentally relies on hardness of syndrome decoding.
  - Quantum sieving significantly reduces this hardness:

$$2^{0.096n} \to 2^{0.05806n}$$

Security Margin Reduction

Quantum sieving substantially reduces effective security level:

- Classical 128-bit security parameters reduce to about 77 bits against quantum sieving.

- **Reassessing Security Parameters**
  - Increased complexity demands adjusting parameters to retain security:

$$n_{\text{quantum}} \approx 1.6 \cdot n_{\text{classical}}$$

Theorem (Quantum Security Margin)

To maintain equivalent security levels under quantum sieving attacks, code length parameters must increase by approximately 60% compared to classical scenarios.

Quantum Implementation and Practical Challenges

- **Quantum Resource Requirements**
  - Quantum sieving algorithms rely heavily on quantum random access memory (QRAM).
  - Current quantum hardware faces significant limitations in qubit coherence and circuit depth.
- **Quantum Error Correction (QEC)**
  - Practical implementation necessitates extensive quantum error correction.
  - Additional overhead due to logical qubits significantly increases quantum resource demand.
- **Complexity vs. Practicality Trade-offs**
  - Quantum sieving achieves theoretical complexity gains but practical quantum architectures lag.
  - Important to balance theoretical complexity with realistic hardware capabilities.
- **Current Status and Outlook**
  - Quantum attacks are currently impractical due to hardware constraints.
  - Ongoing quantum hardware advancements may alter this status in the next decades.

Future Directions and Open Questions

- **Algorithmic Improvements**
  - Explore further reductions in complexity through new quantum algorithmic paradigms.
  - Investigate hybrid quantum-classical sieving methods for efficiency.
- **Practical Quantum Architectures**
  - Develop quantum architectures optimized specifically for cryptanalysis tasks.
  - Examine feasibility of specialized quantum circuits or fault-tolerant designs tailored for sieving algorithms.
- **Cryptographic Parameter Optimization**
  - Refine methods for determining secure parameters considering quantum advances.
  - Identify new cryptographic constructions resilient to quantum sieving.
- **Open Questions**
  - Can quantum sieving complexity be further significantly reduced beyond current results?
  - What quantum hardware improvements would realistically threaten code-based cryptosystems in practice?

Conclusion

- **Quantum Sieving and Complexity**
  - Quantum sieving substantially reduces decoding complexity from classical $2^{0.096n}$ to quantum $2^{0.05806n}$.
  - Despite quantum improvements, decoding complexity remains exponential.
- **Implications for Code-Based Cryptography**
  - Security margins significantly impacted; cryptographic parameters require reassessment and possible scaling.
- **Current Practical Security**
  - Practical quantum attacks remain challenging due to hardware limitations.
  - Immediate threat low, but proactive parameter adjustments necessary for long-term security.
- **Research Importance**
  - Continued research on quantum sieving critical for assessing future post-quantum cryptographic security.

Quantum sieving illustrates significant theoretical improvements, underscoring the need for continued vigilance and research in quantum-resistant cryptography.

References

[Prange, 1962] E. Prange (1962).
"The Use of Information Sets in Decoding Cyclic Codes".
IRE Trans. Inf. Theory.

[Stern, 1989] J. Stern (1989).
"A method for finding codewords of small weight".
Coding Theory and Applications.

[Bernstein, 2010] D. J. Bernstein (2010).
"Grover vs. McEliece".
PQCrypto.

[Kachigar–Tillich, 2017] G. Kachigar and J.-P. Tillich (2017).
"Quantum Information Set Decoding Algorithms".
PQCrypto.

[Kirshanova, 2018] E. Kirshanova (2018).
"Improved Quantum Information Set Decoding".
PQCrypto.

[May-Ozerov, 2015] A. May and I. Ozerov (2015).
"On Computing Nearest Neighbors with Applications to Decoding".
Eurocrypt.

[Ajtai, Kumar, Sivakumar, 2001] M. Ajtai, R. Kumar, and D. Sivakumar (2001).
"A sieve algorithm for the shortest lattice vector problem".
STOC.

[NIST PQC, 2022] NIST (2021).
"Post-Quantum Cryptography Standardization".
`https://csrc.nist.gov/projects/post-quantum-cryptography`.