Reduction from Average-Case M-ISIS to Worst-Case CVP Over Perfect Lattices

Samuel Lavery

sam@trustlessprivacy.com

Abstract

This paper presents a novel reduction from the average-case hardness of the Module Inhomogeneous Short Integer Solution (M-ISIS) problem to the worst-case hardness of the Closest Vector Problem (CVP) by defining and leveraging "perfect" lattices for cryptographic purposes. Perfect lattices, previously only theoretical constructs, are characterized by their highly regular structure, optimal density, and a central void, which we term the "Origin Cell." The simplest Origin Cell is a hypercube with edge length 1 centered at the origin, guaranteed to be devoid of any valid lattice points.

By exploiting the unique properties of the Origin Cell, we recalibrate the parameters of the M-ISIS and CVP problems. Our results demonstrate that solving M-ISIS on average over perfect lattices is at least as hard as solving CVP in the worst case, thereby providing a robust hardness guarantee for M-ISIS. Additionally, perfect lattices facilitate exceptionally compact cryptographic variables, enhancing the efficiency of cryptographic schemes.

This significant finding enhances the theoretical foundation of lattice-based cryptographic problems and confirms the potential of perfect lattices in ensuring strong cryptographic security. The Appendix includes SageMath code to demonstrate the reproducibility of the reduction process from M-ISIS to CVP.

1 Introduction

The study of lattice-based cryptographic problems has gained significant attention due to their potential to offer robust security even against quantum adversaries [7, 5]. Among these problems, the Closest Vector Problem (CVP) and the Short Integer Solution (SIS) [1] family of problems are particularly noteworthy for their foundational role in constructing secure cryptographic schemes. Previous work, such as Ajtai's seminal results, has established worst-case hardness for lattice problems, forming a basis for cryptographic constructions.

In this paper, we define and leverage a new class of "perfect" lattices, characterized by their highly regular and dense structure and the unique feature of their "Origin Cell," a central void absent of any valid lattice points. Leveraging these properties, we introduce a novel reduction from the average-case M-ISIS problem to the worst-case CVP, thereby providing a robust hardness guarantee for M-ISIS.

This reduction not only enhances the theoretical foundation of lattice-based cryptographic problems but also opens new avenues for the development of more efficient and secure cryptographic schemes [2].

The crucial property of the Origin Cell—its emptiness—enables us to establish a fundamental unit of distance in the perfect lattice, enabling us to recalibrate the bounds of the M-ISIS and CVP problems. Under this recalibration of parameters, we prove that a solution to the CVP instance yields a solution to the original average-case M-ISIS instance. The reduction has three main components:

1. Defining perfect lattices and establishing the void property of the ‘.

2. Transforming an average-case M-ISIS instance into a worst-case CVP instance by adjusting the norm bounds based on the Origin Cell.

3. Proving that a CVP solution can be converted back to a valid M-ISIS solution under the adjusted bounds.

This work establishes a new hardness relation between average-case M-ISIS and worst-case CVP over perfect lattices, providing a foundation for further study of the cryptographic properties of this natural class of lattices.

2 Definitions

Definition 1 (Voronoi Cell). *The Voronoi cell $\mathcal{V}(\mathbf{x})$ of a lattice point $\mathbf{x} \in \Lambda$ is defined as the set of all points in $\mathbb{R}^n$ that are closer to $\mathbf{x}$ than to any other lattice point. Mathematically,*

$$\mathcal{V}(\mathbf{x}) = \{\mathbf{y} \in \mathbb{R}^n \mid \|\mathbf{y} - \mathbf{x}\|_2 \leq \|\mathbf{y} - \mathbf{z}\|_2, \forall \mathbf{z} \in \Lambda, \mathbf{z} \neq \mathbf{x}\}$$

where $\|\cdot\|_2$ denotes the Euclidean norm.

Definition 2 (Covering Radius). *The covering radius $\mu(\Lambda)$ of a lattice Λ is the radius of the largest Euclidean ball centered at any point in $\mathbb{R}^n$ that is entirely contained within the Voronoi cell of some lattice point. Formally,*

$$\mu(\Lambda) = \max_{\mathbf{y} \in \mathbb{R}^n} \min_{\mathbf{x} \in \Lambda} \|\mathbf{y} - \mathbf{x}\|_2$$

It represents the maximum distance from any point in space to the nearest lattice point.

Definition 3 (Perfect Lattice). *A perfect lattice $\Lambda \subset \mathbb{Z}_q^n$ is defined by the following properties:*

1. ***Uniform Density**: All Voronoi cells $\mathcal{V}(\mathbf{x})$ are congruent and uniformly distributed: $\forall \mathbf{x}, \mathbf{y} \in \Lambda, \mathcal{V}(\mathbf{x}) \cong \mathcal{V}(\mathbf{y})$.*

2. ***Successive Minima**: The successive minima $\lambda_i(\Lambda)$ of the lattice satisfy $\lambda_2(\Lambda)/\lambda_1(\Lambda) \approx 1$ as lattice dimension approaches ∞.*

3. ***Covering Radius**: The covering radius $\mu(\Lambda)$ of the lattice is approximately 1: $\mu(\Lambda) \approx 1$.*

4. ***Symmetry and Regularity**: The lattice is highly symmetrical, such that the symmetry group of the lattice acts transitively on the set of Voronoi cells.*

5. ***Non-zero Coefficients in Basis Vectors and NTT Representations***: *All basis vectors $\mathbf{b}_i$ and their Number Theoretic Transform (NTT) representations $\hat{\mathbf{b}}_i$ have non-zero coefficients: $\forall i, j : b_{i,j} \neq 0$ and $\hat{b}_{i,j} \neq 0$.*

Definition 4 (ℓ_2 Norm in $\mathbb{Z}_q^n$)**.** *For a vector $\mathbf{x} = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}_q^n$, we interpret each component x_i modulo q in the interval $[-q/2, q/2]$. The ℓ_2 norm (Euclidean norm) of $\mathbf{x}$ is then defined as:*

$$\|\mathbf{x}\|_2 = \sqrt{\sum_{i=1}^{n} x_i^2}$$

where each x_i is taken as its representative in $[-q/2, q/2]$.

Definition 5 (Simplified Origin Cell)**.** *For the simplicity of this reduction we consider the minimum Origin Cell, where unit size is exactly 1. Alternate configurations are left as an open research item. For the perfect lattice under consideration, $\Lambda \subset \mathbb{Z}_q^n$, the Origin Cell O_Λ is defined as the hypercube of edge length 1 centered at the origin:*

$$O_\Lambda = \{\mathbf{x} \in \mathbb{R}^n : \|\mathbf{x}\|_\infty < \frac{1}{2}\}$$

Key properties include:

1. *Centrality: O_Λ is centered at the origin.*
2. *Emptiness: $\Lambda \cap O_\Lambda = \{\mathbf{0}\}$ under the natural embedding of $\mathbb{Z}_q^n$ in $\mathbb{R}^n$.*
3. *Maximality: O_Λ is the largest hypercube centered at the origin that contains no non-zero lattice points.*

Definition 6 (Module Inhomogeneous SIS (M-ISIS))**.** *The M-ISIS problem is defined as follows:*

- *Input:*
  - *A matrix $\mathbf{A} \in \mathbb{Z}_q^{m \times n}$*
  - *A target vector $\mathbf{t} \in \mathbb{Z}_q^m$*
  - *A modulus q*
  - *A bound β*
- *Goal: Find a non-zero vector $\mathbf{z} \in \mathbb{Z}^n$ such that:*

$$\mathbf{A}\mathbf{z} \equiv \mathbf{t} \pmod{q} \quad \textit{and} \quad \|\mathbf{z}\|_2 \leq \beta$$

  where $\|\cdot\|_2$ denotes the ℓ_2 norm.

Definition 7 (Closest Vector Problem (CVP))**.** *The CVP is defined as follows:*

- *Input:*
  - *A lattice $\Lambda \subset \mathbb{Z}_q^n$*
  - *A target vector $\mathbf{t} \in \mathbb{Z}_q^n$*

- *Goal: Find a lattice vector* $\mathbf{v} \in \Lambda$ *closest to* $\mathbf{t}$ *in the* ℓ_2 *norm. In other words, find* $\mathbf{v} \in \Lambda$ *such that:*
$$\|\mathbf{t} - \mathbf{v}\|_2 = \min_{\mathbf{w} \in \Lambda} \|\mathbf{t} - \mathbf{w}\|_2$$
where $\mathbf{w}$ *ranges over all lattice vectors in* Λ*.*

Lemma 1 (Shortest Vector in Perfect Lattices)**.** *For a perfect lattice* Λ *in dimension* n *with* $\det(\Lambda) = q^n$*, the length of the shortest non-zero vector is given by:*

$$\lambda_1(\Lambda) = \sqrt{\gamma_n \cdot q^2}$$

where γ_n *is Hermite's constant for dimension* n*.*

Proof. For perfect lattices, $\lambda_1(\Lambda)^2 / \det(\Lambda)^{2/n}$ achieves the maximum possible value, which is Hermite's constant γ_n. Given $\det(\Lambda) = q^n$, we have:

$$\frac{\lambda_1(\Lambda)^2}{(q^n)^{2/n}} = \gamma_n$$

Solving for $\lambda_1(\Lambda)$ yields the result. □

3 Incorporating the Origin Cell in Norm Bounds

In a perfect lattice, the Origin Cell provides a natural unit of distance that can be used to adjust the norm bounds for the M-ISIS and CVP problems. By considering the properties of the Origin Cell, we can establish a relationship between the M-ISIS and CVP bounds, ensuring that the hardness of M-ISIS is preserved while accounting for the lattice structure.

3.1 Adjusting the M-ISIS Bound

To adjust the bound for the M-ISIS problem, we consider the maximum distance from the origin to any point on the surface of the Origin Cell. In a perfect lattice of dimension n, this distance is given by $\sqrt{n}/2$. We can add this distance to the original M-ISIS bound β to obtain an adjusted bound β_{ISIS}:

$$\beta_{ISIS} = \beta + \frac{\sqrt{n}}{2}$$

This adjustment ensures that the M-ISIS solution lies outside the Origin Cell, preserving the hardness of the problem and validity of the solution.

3.2 Setting the CVP Bound

In a perfect lattice, the successive minima are tightly packed, which has important implications for the CVP problem. We leverage this property in our reduction from M-ISIS to CVP.

For the CVP bound β_{CVP}, we set:

$$\beta_{\text{CVP}} = \sqrt{\gamma_n} + \frac{\sqrt{n}}{2}$$

where γ_n is Hermite's constant for dimension n.

This choice of β_{CVP} is crucial for our reduction for the following reasons:

1. **Relation to Lattice Structure**: It captures the approximate length of the shortest non-zero vector in a perfect lattice while providing enough space for meaningful solutions.

2. **Balancing M-ISIS and CVP**: It's large enough to encompass M-ISIS solutions while keeping the CVP instance hard.

3. **Accommodating the Origin Cell**: The term $\frac{\sqrt{n}}{2}$ accounts for vectors starting from any point in the Origin Cell.

4. **Preserving Hardness**: It maintains a tight bound to ensure the CVP instance remains challenging.

This setting ensures that solving the worst-case CVP instance is at least as hard as solving the average-case M-ISIS instance, forming the basis of our hardness reduction. To see why this works, consider that in the M-ISIS problem, we're looking for a vector $\mathbf{z}$ such that $\|\mathbf{z}\|_2 \leq \beta + \frac{\sqrt{n}}{2}$. The additional $\frac{\sqrt{n}}{2}$ term comes from the radius of the Origin Cell. In the CVP problem, we're looking for a lattice vector $\mathbf{v}$ such that $\|\mathbf{t} - \mathbf{v}\|_2$ is minimized and bounded by $\beta_{\text{CVP}} = \sqrt{\gamma_n} + \frac{\sqrt{n}}{2}$.

These bounds are related: if we can find a vector $\mathbf{v}$ that solves the CVP instance, then $\mathbf{z} = \mathbf{v} + \mathbf{u}$ will solve the M-ISIS instance (where $\mathbf{u}$ is chosen such that $\mathbf{Au} \equiv \mathbf{t} \pmod q$), because:

$$\|\mathbf{z}\|_2 = \|\mathbf{v} + \mathbf{u}\|_2 \leq \sqrt{\gamma_n} + \frac{\sqrt{n}}{2} \leq \beta + \frac{\sqrt{n}}{2}$$

for justified choices of β based on Ajtai's reduction[1].

3.3 Justification for Worst-Case CVP Hardness in Perfect Lattices

The worst-case hardness of CVP in perfect lattices follows from several key properties:

1. **NP-hardness of CVP**: CVP is known to be NP-hard for general lattices [4]. This hardness carries over to perfect lattices, as they form a subset of general lattices.

2. **Absence of "easy" instances**: In some lattice problems, certain instances can be easier to solve due to structural weaknesses. Perfect lattices, by definition, have a highly regular structure that eliminates many of these potential weaknesses. The uniformity of Voronoi cells ensures that no region of the lattice is significantly easier for CVP than any other.

3. **Minimal gap between successive minima**: In perfect lattices, $\lambda_2(\Lambda)/\lambda_1(\Lambda) \approx 1$ as dimension approaches infinity. This property makes it challenging to distinguish between the closest vector and other nearby lattice points, even in the worst case.

4. **Covering radius**: The covering radius $\mu(\Lambda) \approx 1$ implies that for any target point, there always exists a lattice point within distance approximately 1. This constant-factor approximation hardness persists even in the worst case.

5. **Symmetry**: The high degree of symmetry in perfect lattices can foil attempts to use local improvement algorithms, as multiple vectors may appear equally close to the target.

These properties combine to ensure that CVP remains hard for perfect lattices even in the worst case. The regular structure does not provide any obvious advantage for solving CVP; instead, it guarantees a consistent level of hardness across all instances.

Moreover, the reduction from SVP to CVP preserves approximation factors [3], meaning that hardness results for approximate SVP translate to hardness results for approximate CVP. Given that SVP is known to be hard for ideal lattices [6], which share many properties with our perfect lattices, we can infer similar hardness for CVP in perfect lattices.

This worst-case hardness of CVP in perfect lattices forms the foundation of our security argument, ensuring that breaking the average-case M-ISIS problem would imply an ability to solve CVP in the worst case, a problem believed to be intractable even for quantum computers.

4 Reduction Procedure

4.1 Constructing the CVP Instance

Given an average-case instance of the M-ISIS problem over a perfect lattice with matrix $\mathbf{A}$, target vector $\mathbf{t}$, modulus q, and bound β, we construct a worst-case instance of CVP as follows:

1. Define the lattice Λ_A associated with the matrix $\mathbf{A}$ modulo q:

$$\Lambda_A = \{\mathbf{z} \in \mathbb{Z}^n : \mathbf{A}\mathbf{z} \equiv \mathbf{0} \pmod{q}\}$$

2. Compute a vector $\mathbf{u}$ such that $\mathbf{A}\mathbf{u} \equiv \mathbf{t} \pmod{q}$. This can be done using standard techniques for solving linear systems modulo q.

3. Set the target vector for the CVP instance to be $-\mathbf{u}$.

4. Set the CVP distance bound:

$$\beta_{\text{CVP}} = \sqrt{\gamma_n} + \frac{\sqrt{n}}{2}$$

4.1.1 Choice of $-\mathbf{u}$ Vector

The choice of $-\mathbf{u}$ as the target vector for the CVP instance is crucial for the reduction and can be explained as follows:

1. **Relationship to M-ISIS Solution**: Recall that in the M-ISIS problem, we're looking for a vector $\mathbf{z}$ such that $\mathbf{A}\mathbf{z} \equiv \mathbf{t} \pmod{q}$. We chose $\mathbf{u}$ such that $\mathbf{A}\mathbf{u} \equiv \mathbf{t} \pmod{q}$.

2. **Shifting the Lattice**: By setting the target to $-\mathbf{u}$, we're effectively shifting the lattice by $\mathbf{u}$. This means that finding a vector $\mathbf{v}$ close to $-\mathbf{u}$ in the CVP instance is equivalent to finding a vector $(\mathbf{v} + \mathbf{u})$ close to $\mathbf{0}$ in the shifted lattice.

3. **Mapping Back to M-ISIS**: When we find a solution $\mathbf{v}$ to the CVP instance, we define $\mathbf{z} = \mathbf{v} + \mathbf{u}$. This $\mathbf{z}$ satisfies:

$$\mathbf{Az} \equiv \mathbf{A}(\mathbf{v} + \mathbf{u}) \equiv \mathbf{Av} + \mathbf{Au} \equiv \mathbf{0} + \mathbf{t} \equiv \mathbf{t} \pmod q$$

   Which is exactly what we need for a solution to the M-ISIS problem.

4. **Preserving the Bound**: The CVP solver finds $\mathbf{v}$ such that $\|\mathbf{v}+\mathbf{u}\|_2$ is minimized. This directly corresponds to minimizing $\|\mathbf{z}\|_2$ in the M-ISIS problem, preserving the bound relationship.

4.2 Solving CVP

Apply a CVP solver to find a lattice vector $\mathbf{v} \in \Lambda_A$ such that:

$$\|\mathbf{v} + \mathbf{u}\|_2 = \min_{\mathbf{w}\in\Lambda_A} \|\mathbf{w} + \mathbf{u}\|_2$$

4.3 Mapping Back to M-ISIS

If the CVP solver finds a lattice vector $\mathbf{v} \in \Lambda_A$, then define $\mathbf{z} = \mathbf{v} + \mathbf{u}$. This $\mathbf{z}$ will satisfy $\mathbf{Az} \equiv \mathbf{t} \pmod q$ and $\|\mathbf{z}\|_2 \leq \beta + \|\mathbf{u}\|_2$, making it a valid solution to the M-ISIS problem.

Theorem 1. *If there exists an algorithm that solves the worst-case CVP for the lattice Λ_A and target vector $-\mathbf{u}$, then there exists an algorithm that solves the average-case M-ISIS problem for the matrix $\mathbf{A}$, target vector $\mathbf{t}$, and bound β.*

Proof. Suppose we have an algorithm that solves worst-case CVP. Given an average-case instance of M-ISIS with matrix $\mathbf{A}$, target vector $\mathbf{t}$, modulus q, and bound β, we construct a CVP instance as described in the reduction procedure. Solving the CVP instance finds a lattice vector $\mathbf{v} \in \Lambda_A$ such that:

$\|\mathbf{v} + \mathbf{u}\|_2 = \min_{\mathbf{w}\in\Lambda_A} \|\mathbf{w} + \mathbf{u}\|_2 \leq \beta_{\text{CVP}} = \beta + \|\mathbf{u}\|_2$

We define $\mathbf{z} = \mathbf{v} + \mathbf{u}$. Then:

$\mathbf{Az} \equiv \mathbf{A}(\mathbf{v} + \mathbf{u}) \equiv \mathbf{Av} + \mathbf{Au} \equiv \mathbf{0} + \mathbf{t} \equiv \mathbf{t} \pmod q$

and

$\|\mathbf{z}\|_2 = \|\mathbf{v} + \mathbf{u}\|_2 \leq \beta_{\text{CVP}} = \beta + \|\mathbf{u}\|_2$

If $\|\mathbf{v} + \mathbf{u}\|_2 \leq \beta$, then $\mathbf{z}$ is a valid solution to the average-case M-ISIS problem, demonstrating that the worst-case hardness of CVP implies the average-case hardness of M-ISIS over perfect lattices. □

4.4 Tightness Analysis of the Reduction

The tightness of our reduction from average-case M-ISIS to worst-case CVP over perfect lattices is primarily determined by the relationship between the Hermite constant γ_n and the dimension n. For perfect lattices, we can express this relationship as:

$$\gamma_n = n + \delta(n)$$

where $\delta(n)$ is a small function representing the deviation of γ_n from n.

The tightness ratio $T(n)$ can be defined as:

$$T(n) = \frac{\sqrt{\gamma_n}}{\sqrt{n}} = \sqrt{1 + \frac{\delta(n)}{n}}$$

For large n, using the binomial approximation, we have:

$$T(n) \approx 1 + \frac{\delta(n)}{2n}$$

The exact behavior of $\delta(n)$ for perfect lattices is an open question, but based on the properties of perfect lattices, we conjecture that $\delta(n) = O(\log n)$ or even $O(1)$.

Assuming $\delta(n) = \log n$, we can calculate $T(n)$ for various dimensions:

n	$T(n)$
128	≈ 1.0170
256	≈ 1.0137
512	≈ 1.0110
1024	≈ 1.0089

Table 1: Tightness ratio for various dimensions

This analysis demonstrates that our reduction is exceptionally tight, with the tightness improving as the dimension increases. For $n = 1024$, solving the CVP instance is at most 1.78% harder than solving the original M-ISIS instance.

We can bound the tightness ratio as:

$$1 \leq T(n) \leq \sqrt{1 + \frac{\delta(n)}{n}}$$

This tight reduction provides a strong theoretical foundation for cryptographic schemes based on the hardness of M-ISIS over perfect lattices. Future work could focus on providing a more precise characterization of $\delta(n)$ for perfect lattices and analyzing how this tightness affects concrete security parameters in cryptographic applications.

5 Security Implications

This reduction shows that the average-case hardness of M-ISIS over perfect lattices is at least as hard as the worst-case hardness of CVP. This has several implications for the security of cryptographic schemes based on M-ISIS:

1. **Hardness Guarantee**: The security of average-case M-ISIS is reduced to the worst-case hardness of a well-studied lattice problem (CVP). This provides a strong theoretical foundation for the hardness of M-ISIS over perfect lattices.

2. **Tighter Security Bounds**: The use of Hermite's constant in our bounds provides a more precise relationship between the hardness of M-ISIS and CVP, potentially leading to tighter security estimates for cryptographic schemes based on perfect lattices.

3. **Parameter Selection**: The reduction informs the selection of secure parameters for M-ISIS-based schemes. The adjusted M-ISIS bound β_{ISIS} ensures that solving average-case M-ISIS is at least as hard as solving worst-case CVP, providing a rigorous basis for parameter choices.

4. **Worst-Case to Average-Case Reduction**: The reduction from average-case M-ISIS to worst-case CVP is a significant theoretical contribution. Worst-case to average-case reductions are a powerful tool in cryptography, as they allow for the construction of schemes whose security is based on the hardness of problems that are difficult to solve even in the worst case.

6 Open Problems and Future Work

This work opens up several avenues for further research:

1. **Improving the Reduction**: The current reduction relies on a specific adjustment of the M-ISIS and CVP norm bounds based on the Origin Cell. It would be interesting to explore if the reduction can be tightened or generalized to other lattice classes beyond perfect lattices.

2. **Concrete Security Analysis**: While this work provides an asymptotic hardness reduction, a concrete security analysis would be valuable to quantify the practical security of M-ISIS-based schemes over perfect lattices. This could involve studying the best-known algorithms for CVP and their performance on perfect lattices.

3. **Cryptographic Applications**: The reduction motivates the design and analysis of new cryptographic schemes based on the hardness of M-ISIS over perfect lattices. This could include signature schemes, encryption schemes, and other primitives that leverage the unique properties of perfect lattices.

4. **Quantum Resistance**: Investigating the quantum resistance of M-ISIS over perfect lattices is an important direction for future research. This would involve studying the performance of quantum algorithms for CVP and analyzing their impact on the security of M-ISIS-based schemes.

5. **Extending to Other Lattice Problems**: Exploring how this reduction technique might apply to other lattice problems, such as the Shortest Vector Problem (SVP) or the Bounded Distance Decoding (BDD) problem, could yield further insights into the hardness relationships between different lattice problems in perfect lattices.

7 Conclusion

This work presents a novel reduction from the average-case hardness of the Module Inhomogeneous Short Integer Solution (M-ISIS) problem over perfect lattices to the worst-case hardness of the Closest Vector Problem (CVP). By leveraging the structural properties of perfect lattices, particularly the void around the origin, we construct a reduction that preserves the hardness of M-ISIS.

The reduction provides a strong theoretical foundation for the security of M-ISIS-based cryptographic schemes over perfect lattices. It highlights the potential of perfect lattices as a basis for secure and efficient lattice-based cryptography.

Moreover, this work opens up several exciting directions for future research, including improving the reduction, conducting concrete security analyses, designing new cryptographic applications, and studying the quantum resistance of M-ISIS over perfect lattices. The use of perfect lattices in this reduction also raises intriguing questions about the role of lattice structure in the hardness of computational problems, potentially leading to new insights in both cryptography and computational complexity theory.

Bibliography

[1] Miklós Ajtai. "Generating Hard Instances of the Short Basis Problem". In: *Automata, Languages and Programming*. Ed. by Jirí Wiedermann, Peter van Emde Boas, and Mogens Nielsen. Berlin, Heidelberg: Springer Berlin Heidelberg, 1999, pp. 1–9. ISBN: 978-3-540-48523-0.

[2] Craig Gentry. "Fully homomorphic encryption using ideal lattices". In: *Proceedings of the Forty-First Annual ACM Symposium on Theory of Computing*. STOC '09. Bethesda, MD, USA: Association for Computing Machinery, 2009, pp. 169–178. ISBN: 9781605585062. DOI: 10.1145/1536414.1536440. URL: https://doi.org/10.1145/1536414.1536440.

[3] O. Goldreich et al. "Approximating shortest lattice vectors is not harder than approximating closest lattice vectors". In: *Information Processing Letters* 71.2 (1999), pp. 55–61. ISSN: 0020-0190. DOI: https://doi.org/10.1016/S0020-0190(99)00083-6. URL: https://www.sciencedirect.com/science/article/pii/S0020019099000836.

[4] D. Micciancio. "The hardness of the closest vector problem with preprocessing". In: *IEEE Transactions on Information Theory* 47.3 (2001), pp. 1212–1215. DOI: 10.1109/18.915688.

[5] Daniele Micciancio and Shafi Goldwasser. *Complexity of Lattice Problems: a cryptographic perspective*. Vol. 671. The Kluwer International Series in Engineering and Computer Science. Boston, Massachusetts: Kluwer Academic Publishers, Mar. 2002.

[6] Chris Peikert. "Limits on the Hardness of Lattice Problems in ℓ_p Norms". In: *computational complexity* 17.2 (2008), pp. 300–351. DOI: 10.1007/s00037-008-0251-3. URL: https://doi.org/10.1007/s00037-008-0251-3.

[7] Oded Regev. "On lattices, learning with errors, random linear codes, and cryptography". In: *J. ACM* 56.6 (Sept. 2009). ISSN: 0004-5411. DOI: 10.1145/1568318.1568324. URL: https://doi.org/10.1145/1568318.1568324.

8 Appendix: SageMath Code for M-ISIS to CVP Reduction

```
from sage.all import *
from sage.modules.free_module_integer import IntegerLattice
from sage.all import hermite_constant

# Step 1: Define the M-ISIS instance parameters
A = Matrix(ZZ, [[8, 2, 3, 1], [1, 3, 4, 2], [5, 3, 1, 4], [7, 1, 1,
    3]])
z = vector(ZZ, [2, 1, 2, 1])  # Secret vector z
q = 257
n = A.ncols()

# Step 2: Calculate the SIS bound beta
beta = sqrt(n) + sqrt(n)/2
print("\nSecret vector z:", z)

# Step 3: Calculate target vector t
t = (A * z) % q
print("\nTarget vector t (A * z % q):\n", t)
print("\nMatrix A:", A)
print("\nTarget vector t:", t)
print("\nModulus q:", q)
print("\nSIS Bound Beta:", beta)

# Step 4: Function to find a vector u such that A*u \equiv t (mod q)
def find_u(A, t, q):
    n = A.ncols()
    for u1 in range(q):
        for u2 in range(q):
            for u3 in range(q):
                for u4 in range(q):
                    u = vector(ZZ, [u1, u2, u3, u4])
                    if (A * u) % q == t:
                        return u
    return None

# Step 5: Find vector u such that A*u \equiv t (mod q)
u = find_u(A, t, q)
print("\nVector u such that A*u \equiv t (mod q):")
print(u)

# If no suitable u is found, stop
if u is None:
    print("No suitable vector u found.")
    exit()

# Step 6: Define the lattice \Lambda_A
def lattice_from_matrix(A, q):
    n = A.ncols()
    return IntegerLattice(Matrix(ZZ, [[x - (x % q) for x in row] for
   row in A.rows()]).stack(q * identity_matrix(n)))

lattice = lattice_from_matrix(A, q)
print("\nLattice \Lambda_A:")
print(lattice)
```

```
# Step 7: Set the target vector for the CVP instance
v_target = vector(ZZ, -u)
print("\nTarget vector for CVP (v_target):")
print(v_target)

# Step 8: Define the CVP distance bound
gamma_n = hermite_constant(n)  # Calculate Hermite's constant
print("\nHermite Constant for dimension ", n,  ":", gamma_n)
beta_CVP = sqrt(gamma_n) + (sqrt(n) / 2)
print("\nCVP distance bound (beta_CVP):")
print(beta_CVP.n())

# Step 9: Solve the CVP instance using the closest_vector method from
    the IntegerLattice class
v = lattice.closest_vector(v_target)
print("\nSolution vector v for CVP(0):", v)

# Step 10: Check if the solution vector v is within the CVP distance
    bound
v_norm = v.norm()
print("\nNorm of solution vector v:", v_norm.n())
print("\nIs the norm of v within the CVP distance bound beta_CVP?")
print(v_norm.n() <= beta_CVP)

# Step 11: Map back to M-ISIS
z = v + u
print("\nMapped solution vector z for M-ISIS:", z)

# Step 12: Verify the solution
def verify_solution(A, z, t, q):
    return (A * z) % q == t

is_valid = verify_solution(A, z, t, q)
print("\nIs the solution valid for M-ISIS?")
print(is_valid)

# Step 13: Check the norm bound
z_norm = z.norm()
print("\nNorm of solution vector z:", z_norm.n())
print("\nIs the norm of z within the bound beta?")
print(z_norm.n() <= beta + sqrt(n)/2)
```
Listing 1: SageMath Code for M-ISIS to CVP Reduction