Primal Attack on LWE

Arup Mazumder

September 17, 2025

1 Learning with Errors (LWE)

Let an integer modulus $q \geq 2$, a dimension $n \geq 1$ and an error distribution χ over $\mathbb{Z}$. For an $\mathbf{s} \in \mathbb{Z}_q^n$, the LWE distribution $A_{s,\chi}$ over $\mathbb{Z}_q^n \times \mathbb{Z}_q$ is sampled by choosing a uniformly random $\mathbf{a} \in \mathbb{Z}_q^n$ and an error term $e \leftarrow \chi$, outputting $(\mathbf{a}, b = \langle \mathbf{a}, \mathbf{s} \rangle + e \mod q) \in \mathbb{Z}_q^n \times \mathbb{Z}_q$. The distribution χ is necessary to be 0-centered discrte Gaussian distribution with some standard deviation for having the average-case to worst-case reduction[Reg09][Pei09].

The $\mathbf{search}$ version of the $\mathbf{LWE}_{n,m,q,\chi}$ is, given any desired number of samples $(\mathbf{a}_i, b_i)$ from the LWE distribution $A_{s,\chi}$, one has to find $\mathbf{s}$.

The $\mathbf{decision}$ version of the $\mathbf{LWE}_{n,m,q,\chi}$ is to distinguish given any desired number of samples $(\mathbf{a}_i, b_i)$ from $A_{\mathbf{s},\chi}$ and the same number of samples drawn from the uniform distribution over $\mathbb{Z}_q^n \times \mathbb{Z}_q$.

Very often, we write these problems in matrix form as follows: collecting the vectors $\mathbf{a}_i \in \mathbb{Z}_q^n$ as columns of a matrix $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and the error terms $e_i \in \mathbb{Z}$ and $b_i \in \mathbb{Z}_q$ as the entries of vectors $\mathbf{e} \in \mathbb{Z}^m$, $\mathbf{b} \in \mathbb{Z}_q^m$ respectively, we have the given inputs

$$\mathbf{A}, \mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{e} \mod q \tag{1}$$

and asked to find $\mathbf{s}$, or distinguish the input from a uniformly random $(\mathbf{A}, \mathbf{b})$. If $\mathbf{s}$ is chosen uniformly from $\{0, 1\}$ or $\{-1, 0, 1\}$, then this variant is called Binary-LWE. A particular important fact about the derived encryption schemes in [Reg09, LP10], to reduce the decryption failure it is essential to hold $|e_i| \ll \lfloor q/4 \rfloor$. Neverthless, we can redefine LWE as:

$$\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{e} \mod q, \mathbf{e} = (e_1, e_2, \ldots, e_m) \text{ and } e_i \leftarrow D_{[\![-a,a]\!],\sigma,0} \tag{2}$$

$[\![-a, a]\!] = \{-a, -a+1, \ldots, 0, \ldots, a-1, a\}$ and $a \ll \frac{q}{4}$ and D is 0-centered discrte Gaussian distribution having support $[\![-a, a]\!]$, standard deviation $\sigma > 0$. One can use the uniform distribution [DMQ13, MP13] as an error distribution over $[\![-a, a]\!]$. We denote the uniform distribution over any set S as $\mathcal{U}(S)$.

2 Hardness of LWE

Theorem 1. *[Reg09] (Informal) Let n and q be integers, $\alpha \in (0, 1)$ be such that $\alpha q > 2\sqrt{n}$ and χ be an error distribution that is assumed to be a discrete Gaussian distribution over $\mathbb{Z}$ centred around 0 with a standard deviation αq. If there exists an efficient algorithm that solves search-LWE, then there exists an efficient quantum algorithm that approximates the GapSVP (decision version of the shortest vector problem) and the SIVP (shortest independent vectors problem) to within $\tilde{O}(n/\alpha)$ in the worst case.*

GapSVP and SIVP are two main computational problems on lattices. It is a conjecture that there is no $quantum$ polynomial time algorithm that approximates GapSVP or SIVP to within any polynomial factor. The main theorem can be interpreted as suggesting that, based on this conjecture, the Learning With Errors (LWE) problem is difficult to solve. The only evidence supporting this conjecture is the lack of known quantum algorithms for lattice problems that outperform classical algorithms. This absence of evidence is considered to be one of the most significant open questions in the field of quantum computing.

Theorem 2 (Search-to-Decision, Proposition 3 [MM11])**.** *Let q be positivie integer either prime $q = \Theta(n^c)$ for some constant c or $q = p^e$ for prime $p = \mathrm{poly}(n)$ with distribution $\chi = D_{\mathbb{Z},\sigma}$, $q = p^e = \mathrm{poly}(n)$ with $\chi = \mathcal{U}(\mathbb{Z}_{q^i}), i < e$. Assume there exists a PPT-distinguisher $\mathcal{D}$ that distinguishes decision version of $\mathbf{LWE}_{n,m,q,\chi}$ with non-negligible advantage, then there exits a PPTalgorithm $\mathcal{A}$ that inverts $\mathbf{LWE}_{n,m,q,\chi}$ i.e. solves search version of $\mathbf{LWE}_{n,m,q,\chi}$ with non-negligible success-probabilty.*

So we have search $\mathbf{LWE}_{n,m,q,\chi} \leq$ decision $\mathbf{LWE}_{n,m,q,\chi}$ and decision $\mathbf{LWE}_{n,m,q,\chi} \leq$ search $\mathbf{LWE}_{n,m,q,\chi}$ (obvious!)

Binary-LWE is also hard as both the papers [BLP+13, MP13] proved. The papers relate (n, q)-Binary-LWE to $(n/O(\log q)), q$-LWE. It is clear that one can solve the Binary-LWE in $O(2^n)$ or $O(3^n)$ operations by trying all the choices for $\mathbf{s}$ and testing whether $\mathbf{b} - \mathbf{A}\mathbf{s} \pmod q$ is a short vector.

3 LWE as a Lattice problem

Definition 1. ***Bounded Distance Decoding (BDD):*** *Given a lattice basis $\boldsymbol{B}$ and a target vector $\boldsymbol{t}$ such that dist$(\boldsymbol{t}, \Lambda(\boldsymbol{B})) < \lambda_1(\Lambda(\boldsymbol{B}))$, find the lattice vector $\boldsymbol{v} \in \Lambda(\boldsymbol{B})$ closest to $\boldsymbol{t}$.*

Definition 2. ***Unique Shortest Vector (uSVP):*** *Given a lattice $\boldsymbol{B}$ such that $\lambda_2(\Lambda(\boldsymbol{B})) > \lambda_1(\Lambda(\boldsymbol{B}))$, find a nonzero vector $\boldsymbol{v} \in \Lambda(\boldsymbol{B})$ of length $\lambda_1(\Lambda(\boldsymbol{B}))$. $\gamma = \frac{\lambda_2(\Lambda)}{\lambda_1(\Lambda)}$ is defined as Gap.*

Let n, $m > n$, q be positive integers and a matrix $\mathbf{A} \leftarrow \mathcal{U}(\mathbb{Z}_q^{n\times m})$ of rank n. The rows of $\mathbf{A}$ generates $\mathbb{Z}_q^n$ with probability $1 - \frac{1}{p^{m-n-1}}$ where p is the smallest prime factor of q.

We define:

$$\Lambda_q\left(\mathbf{A}^\top\right) = \{\mathbf{v} \in \mathbb{Z}^m : \mathbf{v} \equiv \mathbf{A}^\top\mathbf{s} \mod q \text{ for some } \mathbf{s} \in \mathbb{Z}^n\}$$

This is a q-ary lattice i.e. $q\mathbb{Z}^m \subset \Lambda_q\left(\mathbf{A}^\top\right) \subset \mathbb{Z}^m$.

$$\text{Note that } \mathbf{A}^\top = \begin{bmatrix}\mathbf{A}_1^\top \\ \mathbf{A}_2^\top\end{bmatrix} \text{ where } \mathbf{A}_1^\top \text{ is invertible of order } n \times n \text{ and } \mathbf{A}_2^\top \text{ of order } (m-n)\times n.$$

Now,

$$\mathbf{v} := \begin{bmatrix}\mathbf{v}_1 \\ \mathbf{v}_2\end{bmatrix} \equiv \mathbf{A}^\top\mathbf{s} \equiv \begin{bmatrix}\mathbf{A}_1^\top \\ \mathbf{A}_2^\top\end{bmatrix}\mathbf{s} \equiv \begin{bmatrix}\mathbf{A}_1^\top\mathbf{s} \\ \mathbf{A}_2^\top\mathbf{s}\end{bmatrix} \mod q$$

So,

$$\mathbf{v}_1 \equiv \mathbf{A}_1^\top\mathbf{s} \mod q \text{ and } \mathbf{v}_2 \equiv \mathbf{A}_2^\top\mathbf{s} \mod q \implies \mathbf{v}_2 \equiv \mathbf{A}_2^\top\left(\mathbf{A}_1^\top\right)^{-1}\mathbf{s} \mod q \implies \mathbf{v}_2 = \mathbf{A}_2^\top\left(\mathbf{A}_1^\top\right)^{-1}\mathbf{v}_1 + q\mathbf{u} \text{ for some } \mathbf{u} \in \mathbb{Z}^{m-n}$$

Hence,

$$\mathbf{v} = \begin{bmatrix}\mathbf{v}_1 \\ \mathbf{v}_2\end{bmatrix} = \begin{bmatrix}\mathbf{v}_1 \\ \mathbf{A}_2^\top\left(\mathbf{A}_1^\top\right)^{-1}\mathbf{v}_1 + q\mathbf{u}\end{bmatrix} = \begin{bmatrix}\mathbf{I}_n & \mathbf{0} \\ \mathbf{A}_2^\top\left(\mathbf{A}_1^\top\right)^{-1} & q\mathbf{I}_{m-n}\end{bmatrix}\begin{bmatrix}\mathbf{v}_1 \\ \mathbf{u}\end{bmatrix}$$

So, we can write any $\mathbf{v} \in \Lambda\left(\mathbf{A}^\top\right)$ as $\mathbf{v} = \mathbf{B}\mathbf{w}$ for some $\mathbf{w} \in \mathbb{Z}^m$ where

$$\mathbf{B} = \begin{bmatrix}\mathbf{I}_n & \mathbf{0} \\ \mathbf{A}_2^\top\left(\mathbf{A}_1^\top\right)^{-1} & q\mathbf{I}_{m-n}\end{bmatrix}$$

and $\mathbf{B}$ is an invertible matrix with the determinant q^{m-n}, hence it is a basis of the lattice $\Lambda_q\left(\mathbf{A}^\top\right)$.

Now, if $\mathbf{e}$ is small $\left(||\mathbf{e}||_2 < \frac{\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)}{2}\right)$, the $\mathbf{LWE}_{n,m,q,\chi}$ can be seen as follows: given a point $\mathbf{b}$ as a target vector, one has to find the lattice point $\mathbf{v}$ in $\Lambda_q\left(\mathbf{A}^\top\right)$ so that $\mathbf{e} = \mathbf{b} - \mathbf{v} = \mathbf{b} - \mathbf{B}\mathbf{u}$ for some $\mathbf{u} \in \mathbb{Z}^m$. So we have reduced $\mathbf{LWE}_{n,m,q,\chi}$ to a BDD problem on the lattice $\Lambda_q\left(\mathbf{A}^\top\right)$. Now we will embed $\Lambda_q\left(\mathbf{A}^\top\right)$ into an $m+1$ dimensional lattice $\Lambda = \Lambda(\mathbf{B}')$ where

$\mathbf{B}' = \begin{bmatrix}\mathbf{B} & \mathbf{b} \\ \mathbf{0} & \mu\end{bmatrix}$, where μ is called the embedding constant and the best choice is $\mu = ||\mathbf{e}||_2$ (by Theorem 1 of [LM09]).

Note that:

$$\begin{bmatrix}\mathbf{e} \\ \mu\end{bmatrix} = \begin{bmatrix}-\mathbf{B}\mathbf{u} + \mathbf{b} \\ \mu\end{bmatrix} = \mathbf{B}'\begin{bmatrix}-\mathbf{u} \\ 1\end{bmatrix}$$

We will show that if $\mu = ||\mathbf{e}||_2$ and $\left(||\mathbf{e}||_2 < \frac{\lambda_1(\Lambda_q(\mathbf{A}^\top))}{2}\right)$, then $\Lambda(\mathbf{B}')$ will contain a unique shortest vector $\mathbf{v}' = \begin{bmatrix}\mathbf{e}\\ \mu\end{bmatrix}$. Thus, finding such a vector will solve the BDD problem and so the $\mathbf{LWE}_{n,m,q,\chi}$. $||\mathbf{v}'||_2 = \sqrt{\mu^2+\mu^2} = \sqrt{2}\mu$. Our claim is that all the other vectors in $\Lambda(\mathbf{B}')$ that are not linearly dependent to $\mathbf{v}'$ is of length at least $\frac{\lambda_1(\Lambda_q(\mathbf{A}^\top))}{\sqrt{2}}$. We will prove our claim by contradiction. Let there exist a vector $\mathbf{w}' \in \Lambda(\mathbf{B}')$ such that $||\mathbf{w}'||_2 < \frac{\lambda_1(\Lambda_q(\mathbf{A}^\top))}{\sqrt{2}}$ that is linearly independent of $\mathbf{v}'$. Rewrite $\mathbf{w}' = \begin{bmatrix}\mathbf{B} & \mathbf{b}\\ \mathbf{0} & \mu\end{bmatrix}\begin{bmatrix}\mathbf{x}\\ y\end{bmatrix} = \begin{bmatrix}\mathbf{Bx}+y\mathbf{b}\\ y\mu\end{bmatrix} = \begin{bmatrix}\mathbf{w}+y\mathbf{b}\\ y\mu\end{bmatrix}$, y is an negative integer and $\mathbf{w} = (\mathbf{Bx}) \in \Lambda_q\left(\mathbf{A}^\top\right)$.

$$\|\mathbf{w}'\|_2 = \sqrt{\|\mathbf{w}+y\mathbf{b}\|_2^2 + (y\mu)^2} < \frac{\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)}{\sqrt{2}}$$

$$\implies y\mu < \frac{\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)}{\sqrt{2}} \quad \text{and} \quad \|\mathbf{w}+y\mathbf{b}\|_2 < \sqrt{\frac{\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)^2}{2} - (y\mu)^2}$$

Consider $\mathbf{w}+y\mathbf{v} \in \Lambda_q\left(\mathbf{A}^\top\right)$ and we have assumed that $\mathbf{w}'$ is linearly independent of $\mathbf{v}'$, so $\mathbf{w}+y\mathbf{v}$ is a non-zero lattice vector(why?). To get the contradiction, we will show that the length of the vector $\mathbf{w}+y\mathbf{v}$ is strictly less than $\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)$.

$$||\mathbf{w}+y\mathbf{v}||_2 = ||\mathbf{w}+y\mathbf{b}+y(\mathbf{b}-\mathbf{v})||_2 \leq ||\mathbf{w}+y\mathbf{b}||_2 + y||\mathbf{b}-\mathbf{v}||_2 \leq \sqrt{\frac{\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)^2}{2} - (y\mu)^2} + y\mu$$

The above inequality is maximized when $y = \frac{\lambda_1(\Lambda_q(\mathbf{A}^\top))}{2}$ and therefore for all y,

$$||\mathbf{w}+y\mathbf{v}||_2 < \sqrt{\frac{\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)^2}{2} - (y\mu)^2} + y\mu \leq \lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)$$

which gives the contradiction.

4 Uniqueness of the Solution

It is a trivial question that, does LWE consist unique solution? To be more precise, on what conditions on the parameters m and n, there is only one solution to an LWE problem. As we saw in the previous section, LWE can be reduced to a BDD problem on the lattice $\Lambda_q\left(\mathbf{A}^\top\right)$. This is exactly the same as the "Decoding Problem" in coding theory. The decoding problem refers to the challenge of recovering the original message (or code word) from a received message that may have been corrupted during transmission over a noisy channel. So the question is under what conditions on the m and n and the error $\mathbf{e}$, can we recover the solution of the LWE? The $||\mathbf{e}||_2$ has to be strictly lesser than $\frac{\lambda_1(\Lambda_q(\mathbf{A}^\top))}{2}$, otherwise the BDD problem has no unique solution. Next, if we assume that the $\text{LWE}_{m,n,q,\chi}$ has an unique solution, and already we have the condition $||\mathbf{e}||_2 < \frac{\lambda_1(\Lambda_q(\mathbf{A}^\top))}{2}$, then by the Gaussian Heuristic: $\lambda_1\left(\Lambda_q\left(\mathbf{A}^\top\right)\right) \approx \sqrt{\frac{m}{2\pi e}}\,\text{Vol}\left(\Lambda_q\left(\mathbf{A}^\top\right)\right)^{\frac{1}{m}} = \sqrt{\frac{m}{2\pi e}}q^{\frac{m-n}{m}}$ and since the error distribution χ is taken to be discrete Gaussian, then expected norm of the error vector $\mathbf{e}$ is $\approx \sqrt{m}\alpha q$, we have :

$$\sqrt{m}\alpha q < \frac{\sqrt{\frac{m}{2\pi e}}q^{\frac{m-n}{m}}}{2} \implies m > k \times n \times \log q, k = \frac{1}{\log \frac{1}{2\alpha\sqrt{2\pi e}}} > 0 \tag{3}$$

where k is a positive real number. So to keep a unique solution of an $\text{LWE}_{m,n,q,\chi}$, we have to set the values of m, n, q, α so that Eq. 3 holds.

5 The Primal Attack

The primal attack on the Learning With Errors (LWE) problem was first formally introduced in the [ADPS16]. Specifically, the technique is discussed in the NewHope paper, where it was outlined, reducing LWE to a unique Shortest Vector Problem (uSVP) using lattice embedding, then applying lattice reduction algorithms to recover the secret. We also have discussed a lattice embedding technique, called Kannan's embedding, which is the first form of the so-called Primal Attack. We will first see how many LWE samples are required to perform the primal attack via Kannan's embedding. Gama and Nguyen [GN08] have given a heuristic approach to estimate the capability of lattice basis reduction algorithms. Let us consider a lattice basis reduction algorithm which takes as input for a lattice L of dimension m, and outputs a list of vectors $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_m$. The root Hermite factor $\delta \in \mathbb{R}^+$ of a lattice basis reduction algorithm is:

$$\delta = \frac{||\mathbf{b}_1||_2^{\frac{1}{m}}}{\mathrm{Vol}(\Lambda)^{\frac{1}{m^2}}} \tag{4}$$

The paper [GN08] argues that $\delta = 1.01$ is about the limit of the practical algorithm BKZ. The paper [CN11] extended the study to algorithms with greater running time. Their heuristic argument is that $\delta = 1.006$ might be reachable with an algorithm performing around 2^{110} operations. In section 3.3 of [GN08], the authors drew attention to solving unique-SVP. If one knows that there is a large gap γ, then a lattice basis reduction can solve the unique-SVP with some Hermite factor δ. Gama and Nguyen observed that the practical algorithms succeed if $\gamma > c\delta^m$ for some small constant $c < 1$. This Gama-Nguyen heuristic is called "**Estimate 2008**". The lower the value of δ, the lattice basis reduction algorithms need to perform more operations. The root hermite factor δ is related to the BKZ block size β [Che13] by:

$$\delta(\beta) = \left(\frac{\beta}{2\pi e} \cdot (\pi\beta)^{1/\beta}\right)^{\frac{1}{2(\beta-1)}}, \quad \beta \geq 50 \tag{5}$$

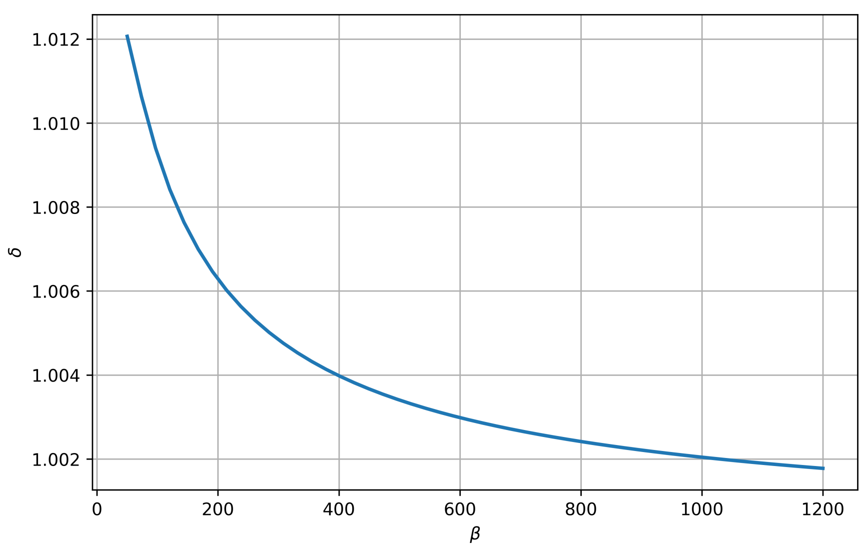

Figure 1: Graph of $\delta(\beta)$ for $50 \leq \beta \leq 1200$

Now we will see how "**Estimate 2008**" will help us to determine the sample size of LWE to perform a standard attack. Consider running the embedding technique on an LWE instance, using the lattice Λ given by the matrix $\mathbf{B}'$. We will have a good chance of getting the right result if the error vector $\mathbf{e}$ is very short compared with the second shortest vector in the lattice Λ, which we assume to be the shortest vector in the original lattice Λ_q. We know by the Gaussian heuristic that the euclidean length of the shortest vector in the lattice Λ_q is approximately $\sqrt{\frac{m}{2\pi e}}q^{\frac{m-n}{m}}$. But Λ_q has also some known vectors named "q-vectors" of Euclidean length q. Hence we have

$$\lambda_2(\Lambda(\mathbf{B}')) \approx \lambda_1(\Lambda_q(\mathbf{B})) \approx \min\left(q, \sqrt{\frac{m}{2\pi e}}q^{\frac{m-n}{m}}\right).$$

On the other hand, the vector $\mathbf{e}$ has expected euclidean length is $\sqrt{m}\alpha q$ as components of $\mathbf{e}$ are from Gaussian over $\mathbb{Z}$ with standard deviation αq and so the expected length of the vector $\begin{bmatrix} \mathbf{e} \\ \mu \end{bmatrix}$ is $\sqrt{2m}\alpha q$ when $\mu = \sqrt{m}\alpha q$. Assume that $\lambda_1(\Lambda(\mathbf{B}')) \approx \sqrt{2m}\alpha q$. Hence the gap:

$$\gamma(m) = \frac{\lambda_2(\Lambda(\mathbf{B}'))}{\lambda_1(\Lambda(\mathbf{B}'))} \approx \frac{\min\left(q, \sqrt{\frac{m}{2\pi e}} q^{\frac{m-n}{m}}\right)}{\sqrt{2m}\alpha q}$$

For a successful attack, we want this gap γ to be large, so we need:

$$\sqrt{2m}\alpha q \ll \sqrt{\frac{m}{2\pi e}} q^{\frac{m-n}{m}} < q$$

To determine whether an LWE instance can be solved using the embedding technique and a lattice reduction algorithm with a given root Hermite factor δ, one chooses a sample size m and verifies the gap condition $\gamma(m) > c\delta^{m+1}$ for a suitable value c. Since c is unknown so we can maximize the function f for fixed n, q, δ to determine the optimal m, $f(m) = \frac{q^{-\frac{n}{m}}}{2\sqrt{\pi e}\alpha\delta^{m+1}}$. Taking the log of both sides and the first derivative test tells us

$$\frac{n}{m^2} \log q = \log \delta \implies m = \sqrt{\frac{n \log q}{\log \delta}}$$

One can check that at $m = \sqrt{\frac{n \log q}{\log \delta}}$, f attains its global maxima.

Parameters	1	2	3	4	5	6	7	8	9	10
n	128	256	512	1024	1280	1536	1624	1792	1824	2048
δ	1.007200	1.006444	1.005689	1.004933	1.004178	1.003422	1.002667	1.001911	1.001156	1.000400
m	534	798	1200	1822	2213	2678	3118	3869	5018	9036

Table 1: Old Attack's Parameters $n, \delta, m, q = 8380417$

A New Attack due to Bai-Galbraith Embedding

Now, we will discuss another embedding technique where we will get a smaller sample size as compared to the prior. Bai and Galbraith [BG14] introduced a new attack on Binary-LWE. They used the fact that $\mathbf{s}$ is short. The previous attack on LWE can't use this shortness of $\mathbf{s}$. Let us have an LWE instance $(\mathbf{A}^\top_{m\times n}, \mathbf{b})$.
Now write,

$$\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{e} \pmod q \implies \mathbf{b} = [\mathbf{A}^\top | \mathbf{I}_m] \begin{bmatrix} \mathbf{s} \\ \mathbf{e} \end{bmatrix} \pmod q \tag{6}$$

In 6, we have just converted an LWE instance to an ISIS instance. $\begin{bmatrix} \mathbf{s} \mid \mathbf{e} \end{bmatrix}^\top$ is our short vector. Now, we will reduce this ISIS problem to a closest vector problem.
Let $\mathbf{w} = \begin{bmatrix} \mathbf{0} \\ \mathbf{b} \end{bmatrix}$ be a target vector and consider the lattice $L = \{\mathbf{v} \in \mathbb{Z}^{m+n} : [\mathbf{A}^\top | \mathbf{I}_m]\mathbf{v} \equiv \mathbf{0} \; mod \; q\}$. To solve the CVP instance $(L, \mathbf{w})$, we have to construct a basis of the lattice L. A basis can be constructed as:

$$\begin{aligned} & [\mathbf{A}^\top \mid \mathbf{I}_m]\mathbf{v} \equiv 0 \pmod q \\ \implies & [\mathbf{A}^\top \mid \mathbf{I}_m]\mathbf{v} = q\mathbf{u}, \quad \mathbf{u} \in \mathbb{Z}^m \\ \implies & \mathbf{A}^\top \mathbf{v}_1 + \mathbf{v}_2 = q\mathbf{u}, \quad \text{where } \mathbf{v} = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} \\ \implies & \mathbf{v}_2 = q\mathbf{u} - \mathbf{A}^\top \mathbf{v}_1 \\ \implies & \mathbf{v} = \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{v}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{v}_1 \\ q\mathbf{u} - \mathbf{A}^\top \mathbf{v}_1 \end{bmatrix} \\ & = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ -\mathbf{A}^\top & q\mathbf{I}_m \end{bmatrix} \begin{bmatrix} \mathbf{v}_1 \\ \mathbf{u} \end{bmatrix} \end{aligned}$$

So, $\mathbf{B} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} \\ -\mathbf{A}^\top & q\mathbf{I}_m \end{bmatrix}$ is a generating matrix and has determinant q^m. So $\mathbf{B}$ is a basis of L. Now to solve CVP instance $(L, \mathbf{w})$, one seeks a vector $\mathbf{v} \in L$ so that $\mathbf{v} = \mathbf{B}\mathbf{z}$ for some $\mathbf{z} \in \mathbb{Z}^{m+n}$. So it is expected that $\mathbf{w} - \mathbf{v} = \begin{bmatrix}\mathbf{s} \mid \mathbf{e}\end{bmatrix}^\top$ and $\mathbf{v} = \begin{bmatrix} -\mathbf{s} \\ \mathbf{b} - \mathbf{e} \end{bmatrix}$. Here, the main observation is CVP finds an unbalanced solution $\begin{bmatrix}\mathbf{s} \mid \mathbf{e}\end{bmatrix}^\top$ because of $||\mathbf{s}||_2 < ||\mathbf{e}||_2$. Assume that $\mathbf{s} \xleftarrow{\$} \{-1, 0, 1\}^n$. So to get a balanced solution (i.e. $\alpha q||\mathbf{s}||_2 \approx ||\mathbf{e}||_2$) $\begin{bmatrix} -\alpha q\mathbf{s} \\ \mathbf{e} \end{bmatrix} = \mathbf{w} - \mathbf{v}$, one has to multiply the first n rows of $\mathbf{B}$ with αq to seek $\mathbf{v} = \begin{bmatrix} -\alpha q\mathbf{s} \\ \mathbf{b} - \mathbf{e} \end{bmatrix} = \begin{bmatrix} \alpha q\mathbf{I}_n & \mathbf{0} \\ -\mathbf{A}^\top & q\mathbf{I}_m \end{bmatrix} \begin{bmatrix} -\mathbf{s} \\ \mathbf{0} \end{bmatrix}$. When $\mathbf{s} \xleftarrow{\$} \{0, 1\}^n$, then to balance the solution, so that the components of $\mathbf{s}$ will be symmetric about 0 (i.e. each component of $\mathbf{s}$ will be either $-\alpha q$ or $+\alpha q$),

1. update the target vector from $\mathbf{w} = \begin{bmatrix} \mathbf{0} \\ \mathbf{b} \end{bmatrix}$ to $\mathbf{w}_{\text{updated}} := \mathbf{w} - (\alpha q, \alpha q, \ldots, \alpha q, 0, \ldots, 0)^\top$
2. multiply first n rows of $\mathbf{B}$ with $2\alpha q$.

Let us see how 1 and 2 helps us to get the balanced solution. We want a balanced solution $(\pm\alpha q, \pm\alpha q, \ldots, \pm\alpha q, e_1, \ldots, e_m)^\top = \mathbf{w}_{\text{updated}} - \mathbf{v}$. To get this, one seeks $\mathbf{v} = \begin{bmatrix} 2\alpha q\mathbf{I}_n & \mathbf{0} \\ -\mathbf{A}^\top & q\mathbf{I}_m \end{bmatrix} \begin{bmatrix} -\mathbf{s} \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} -\mathbf{2}\alpha q\mathbf{s} \\ \mathbf{A}^\top\mathbf{s} \end{bmatrix} = \begin{bmatrix} -\mathbf{2}\alpha q\mathbf{s} \\ \mathbf{b} - \mathbf{e} \end{bmatrix}$. The vector $-2\alpha q\mathbf{s}$ has each component is either 0 or $-2\alpha q$. When we subtract $\mathbf{v}$ from $\mathbf{w}_{\text{updated}}$ then the first n components of the resultant vector will be either $-\alpha q$ or $+\alpha q$ and rest respective m components are $e_1, \ldots, e_m$.
By re-balancing, the volume of the lattice got increased by the factor $(\alpha q)^n$ for the case $\{-1, 0, 1\}$ and $(2\alpha q)^n$ for the case $\{0, 1\}$. So it is expected that the *gap* in the re-scaled lattice is larger than compared in the original lattice.

The basis of the embedded lattice, for the $\mathbf{s} \in \{-1, 0, 1\}^n$, is $\mathbf{B}' = \begin{bmatrix} \alpha q\mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ -\mathbf{A}^\top & q\mathbf{I}_m & \mathbf{b} \\ \mathbf{0} & \mathbf{0} & 1 \end{bmatrix}$. Consider the lattice $L' = \{\mathbf{x} \in (\alpha q\mathbb{Z})^n \times \mathbb{Z}^{m+1} : \left(\frac{1}{\alpha q}\mathbf{A}^\top|\mathbf{I}_m| - \mathbf{b}\right)\mathbf{x} \equiv \mathbf{0} \ (\ mod\ q)\}$ which has the basis $\mathbf{B}'$. So we have the explicit form of the embedded lattice. Note that $\mathbf{u} = \begin{bmatrix}\alpha q\mathbf{s} \mid \mathbf{e} \mid 1\end{bmatrix}^\top \in L'$. To expect $\mathbf{u}$ is the unique shortest vector in L', it is essential to keep

$$\alpha q\sqrt{m+n} < \sqrt{\frac{m+n}{2\pi e}} \left(q^m(\alpha q)^n\right)^{\frac{1}{m+n}} \implies \alpha^{\frac{m}{m+n}} < \frac{1}{\sqrt{2\pi e}} \tag{7}$$

So assuming 7 and we have $\lambda_1(L') \approx \alpha q\sqrt{m+n}$ and $\lambda_2(L') \approx \sqrt{\frac{m+n}{2\pi e}} \left(q^m(\alpha q)^n\right)^{\frac{1}{m+n}}$. To determine the optimal m, consider $f(m) = \frac{\lambda_2(L')}{\lambda_1(L')\cdot\delta^{m+n+1}} = \frac{\alpha^{\frac{-m}{m+n}}\sqrt{\frac{m+n}{2\pi e}}}{\sqrt{m+n}\cdot\delta^{m+n+1}} = \frac{\alpha^{\frac{-m}{m+n}}}{\sqrt{2\pi e}\cdot\delta^{m+n+1}}$. Taking the log of both sides and the first derivative test tells us that m attains the max value:

$$-\frac{n}{(m+n)^2}\log\alpha - \log\delta = 0 \implies m = \sqrt{\frac{n(\log q - \log\sigma)}{\log\delta}} - n, \sigma := \alpha q$$

Parameters	1	2	3	4	5	6	7	8	9	10
n	128	256	512	1024	1280	1536	1624	1792	1824	2048
δ	1.004100	1.003689	1.003278	1.002867	1.002456	1.002044	1.001633	1.001222	1.000811	1.000400
m	505	675	866	1029	1188	1415	1766	2316	3261	5605

Table 2: New Attack's Parameters n, δ, $\alpha q = 2\sqrt{n}$, and m values for $q = 8380417$.

From the Graph-1, Table-1 and Table-2, one can observe that for the dimension $n = 1024$ the required size of LWE samples are reduced from 1822 to 1029 in the new attack and to recover the unique shortest vector, the block size β is needed around $600 - 650$. The cost of BKZ reduction is dominated by its shortest vector problem (SVP) oracle, which in the state-of-the-art setting is based on lattice sieving. The best known classical sieving algorithms [BDGL16] solve SVP in time approximately $2^{0.292\beta}$ and space $2^{0.207\beta}$, where β is the BKZ block size. Since bit security is defined as the base-2 logarithm of the attack cost, the security level against classical attacks is estimated as about 0.292β bits. For example, block sizes of $\beta = 300, 400$, and 500 correspond to roughly $(\log_2(2^{0.292\beta}) = 0.292\beta) = 88, 117$, and

146 bits of classical security, respectively. In the quantum setting, Grover-accelerated sieving [Laa16] improves the running time to $2^{0.265\beta}$, yielding an estimated 0.265β bits of security. Polynomial overheads in the lattice dimension contribute only negligible factors, so security analyses typically rely on these linear approximations when relating β to bit security.

Short-Secret LWE

Recall the definition 2 and assume that errors are coming from $\mathcal{U}[\![-a,a]\!]$. According to [ACPS09, MR09, LP10, BCD$^+$16] secret and error, both can be chosen from the same distribution.

Definition 3. *Let m,n and q be positive integers, $\boldsymbol{s} \leftarrow \mathcal{U}[\![-a,a]\!]^n$ and $\boldsymbol{e} \leftarrow \mathcal{U}[\![-a,a]\!]^m$ where $d \ll \frac{q}{4}$. Given $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}$ and $\boldsymbol{b} = \boldsymbol{A}^\top \boldsymbol{s} + \boldsymbol{e} \mod q$, one has to find $\boldsymbol{s}$, or distinguish the input from a uniformly random $(\boldsymbol{A}, \boldsymbol{b})$.*

The LWE in the definition 3 is called the Short-Secret LWE and we denote it by $\mathbf{LWE}_{m,n,q,a}$.

Lemma 1. *search $\mathbf{LWE}_{m,n,q,a} \leq$ search $\mathbf{LWE}_{n,m,q,\chi}$ with $\chi = \mathcal{U}[\![-a,a]\!]$*

Proof. Let $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{e} \mod q$ be a $\mathbf{LWE}_{m,n,q,a}$ instance and $\mathbf{d} \in \mathbb{Z}_q^n$. Now $\mathbf{b}' = \mathbf{b} + \mathbf{A}^\top \mathbf{d} \mod q \implies \mathbf{b}' = \mathbf{A}^\top \mathbf{s} + \mathbf{e} + \mathbf{A}^\top \mathbf{d} \mod q \implies \mathbf{b}' = \mathbf{A}^\top(\mathbf{s}+\mathbf{d}) + \mathbf{e}$, where $\mathbf{s}+\mathbf{d} \in \mathbb{Z}_q^n$. Then $(\mathbf{A}, \mathbf{b}')$ is an $\mathbf{LWE}_{n,m,q,\chi}$ instance with $\chi = \mathcal{U}[\![-a,a]\!]$. ☐

Lemma 2. *search $\mathbf{LWE}_{n,m,q,\chi} \leq$ search $\mathbf{LWE}_{m-n,n,q,a}$ with $\chi = \mathcal{U}[\![-a,a]\!]$*

Proof. Let $\mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{e} \mod q$ be a $\mathbf{LWE}_{n,m,q,\chi}$ instance with $\chi = \mathcal{U}[\![-a,a]\!]$.

$$\mathbf{b} = \begin{bmatrix} \mathbf{b}_1 \\ \mathbf{b}_2 \end{bmatrix} = \begin{bmatrix} \mathbf{A}_1^\top \\ \mathbf{A}_2^\top \end{bmatrix} \mathbf{s} + \begin{bmatrix} \mathbf{e}_1 \\ \mathbf{e}_2 \end{bmatrix}$$

where $\mathbf{A}_1^\top$ is invertible matrix in $\mathbb{Z}_q$ with high probability of order n. Let $\bar{\mathbf{A}} = -\mathbf{A}_2^\top(\mathbf{A}_1^\top)^{-1}$. Then $\bar{\mathbf{b}} = \bar{\mathbf{A}}\mathbf{b}_1 + \mathbf{b}_2 = \bar{\mathbf{A}}\mathbf{e}_1 + \mathbf{e}_2$. Thus $(\bar{\mathbf{A}}, \bar{\mathbf{b}})$ is an search $\mathbf{LWE}_{m-n,n,q,a}$ instance. ☐

Theorem 3. *search short-secret LWE and search LWE are equivalent.*

Proof. Apply lemma 1 and lemma 2. ☐

A new estimate and Primal Attack

Formally, we define Primal Attack, as defined in [ADPS16], is consists of constructing a unique-SVP instance from the LWE problem and solving it using BKZ. Given an LWE instance $(\mathbf{b}, \mathbf{b} = \mathbf{A}^\top \mathbf{s} + \mathbf{e})$, one can construct a lattice $\Lambda = \{\mathbf{x} \in \mathbb{Z}^{m+n+1} : (\mathbf{A}_{m\times n}^\top | \mathbf{I}_m | -\mathbf{b})\mathbf{x} \equiv \mathbf{0} \mod q\}$ consisting a basis $\mathbf{B} = \begin{bmatrix} \mathbf{I}_n & \mathbf{0} & \mathbf{0} \\ -\mathbf{A}^\top & q\mathbf{I}_m & \mathbf{b} \\ \mathbf{0} & \mathbf{0} & 1 \end{bmatrix}$. Note that $\mathrm{Vol}(\Lambda) = q^m$ and Λ contains a unique SVP solution $\begin{bmatrix} \mathbf{s} \mid \mathbf{e} \mid 1 \end{bmatrix}^\top$. BKZ-$\beta$ will find $\begin{bmatrix} \mathbf{s} \mid \mathbf{e} \mid 1 \end{bmatrix}^\top$ if and only if

$$\sqrt{\frac{\beta}{d}} || \begin{bmatrix} \mathbf{s} \mid \mathbf{e} \mid 1 \end{bmatrix}^\top ||_2 \leq \delta^{2\beta-d}\,\mathrm{Vol}(\Lambda)^{\frac{1}{d}} \tag{8}$$

where $d = m+n+1$ is the dimension of the lattice Λ and β is block size. The success condition of BKZ is called "**Estimate 2016**". This estimate had been investigated extensively by Albrecht et al. in [AGVW17]. They also show that the lattice reduction experiments largely follow the behaviour expected from the "**Estimate 2016**".

But what the new estimate is saying?

We will see after some facts on orthogonal projection operator.

Definition 4. *Let V be an inner product space, W be any subset of V. We define $W^\perp := \{x \in V : \langle x, y\rangle = 0; \forall y \in W\}$ and $W^\perp$ is called orthogonal complement of W. If W is a subspace of V then $W^\perp$ is also a subspace of V.*

Theorem 4. *Let V be a d dimensional inner product space, W be any subspace of V and $\boldsymbol{y} \in V$. Then $\exists$ unique vectors $\boldsymbol{u} \in W$ and $\boldsymbol{z} \in W^\perp$ such that $\boldsymbol{y} = \boldsymbol{u} + \boldsymbol{z}$. Moreover if $\{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_k^*\}$ is an orthogonal basis for W, then $\{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_k^*\}$ can be extended to an orthogonal basis $\{\boldsymbol{b}_1^*, \boldsymbol{b}_2^*, \ldots, \boldsymbol{b}_k^*, \boldsymbol{b}_{k+1}^*, \ldots, \boldsymbol{b}_d^*\}$ for V and $\{\boldsymbol{b}_{k+1}^*, \boldsymbol{b}_{k+2}^*, \ldots, \boldsymbol{b}_d^*\}$ is an orthogonal basis of $W^\perp$.*

Corollary 1. *The vector $\boldsymbol{z}$ is the unique vector in $W^{\perp}$ that is "closest" to $\boldsymbol{y}$ i.e.* $\operatorname{dist}(\boldsymbol{y}, W^{\perp}) = \|\boldsymbol{y} - \boldsymbol{z}\|_2$.

Definition 5. *The $\boldsymbol{z}$ in corollary1 is called the Orthogonal Projection of $\boldsymbol{y}$ onto $W^{\perp}$.*

From now, we write $\hat{\mathbf{x}} :=$ the orthogonal projection of a vector $\mathbf{x} \in V$ onto $W^{\perp}$. Since $\hat{\mathbf{x}}$ is unique, so we can define a map $P : V \to W^{\perp}$ by $P(\mathbf{x}) = \hat{\mathbf{x}}$. It is easy to check that P is a linear map.

Theorem 5. *Let the columns of a $d \times k$ matrix $\boldsymbol{X}$ form a basis for a subspace $S^{\perp} \subseteq \mathbb{R}^d$. Then the matrix $\boldsymbol{P}$ is an orthogonal projection onto $S^{\perp}$ if and only if*

$$\boldsymbol{P} = \boldsymbol{X}\big(\boldsymbol{X}^{\top}\boldsymbol{X}\big)^{-1}\boldsymbol{X}^{\top}.$$

Proof. Let $\mathbf{v} \in \mathbb{R}^d$ and $\mathbf{P} = \mathbf{X}\left(\mathbf{X}^{\top}\mathbf{X}\right)^{-1}\mathbf{X}^{\top}$. Then $\hat{\mathbf{v}} = \mathbf{P}\mathbf{v} = \mathbf{X}\left(\mathbf{X}^{\top}\mathbf{X}\right)^{-1}\mathbf{X}^{\top}\mathbf{v} = \mathbf{X}\mathbf{u} \in S^{\perp}$ where $\mathbf{u} = \left(\mathbf{X}^{\top}\mathbf{X}\right)^{-1}\mathbf{X}^{\top}\mathbf{v}$. Now for any $\mathbf{y} \in \mathbb{R}^k$, we have $\mathbf{z} = \mathbf{X}\mathbf{y} \in S^{\perp}$ and by using $\langle \mathbf{z}, \mathbf{v} - \hat{\mathbf{v}} \rangle = \mathbf{z}^{\top}(\mathbf{v} - \hat{\mathbf{v}})$

$$\underbrace{(\mathbf{X}\mathbf{y})^{\top}}_{\mathbf{z}^{\top}}\underbrace{\left[\mathbf{v} - \mathbf{X}(\mathbf{X}^{\top}\mathbf{X})^{-1}\mathbf{X}^{\top}\mathbf{v}\right]}_{\mathbf{v}-\mathbf{P}\mathbf{v}} = \mathbf{y}^{\top}\left[\mathbf{X}^{\top}\mathbf{v} - \underbrace{\mathbf{X}^{\top}\mathbf{X}(\mathbf{X}^{\top}\mathbf{X})^{-1}}_{I_k}\mathbf{X}^{\top}\mathbf{v}\right] = 0.$$

Conversely, let $\mathbf{P}$ be an orthogonal projection onto S. We will prove that for any $\mathbf{v} \in \mathbb{R}^d$, $\hat{\mathbf{v}} = \mathbf{X}(\mathbf{X}^{\top}\mathbf{X})^{-1}\mathbf{X}^{\top}\mathbf{v}$. Note that $\mathbf{X}^{\top}\mathbf{X}$ is invertible. By definition $\hat{\mathbf{v}} \in S^{\perp} = \operatorname{Col}(\mathbf{X})$, so there is a vector $\mathbf{c} \in \mathbb{R}^d$ with $\mathbf{X}\mathbf{c} = \hat{\mathbf{v}}$. Also $\mathbf{v} - \hat{\mathbf{v}} = \mathbf{v} - \mathbf{X}\mathbf{c} \in S = \operatorname{Nul}(\mathbf{X}^{\top})$ as because $\operatorname{Nul}(\mathbf{X}^{\top})^{\perp} = \operatorname{Col}(\mathbf{X})$. So $\mathbf{0} = \mathbf{X}^{\top}(\mathbf{v} - \mathbf{X}\mathbf{c}) = \mathbf{X}^{\top}\mathbf{v} - \mathbf{X}^{\top}\mathbf{X}\mathbf{c} \implies \mathbf{c} = (\mathbf{X}^{\top}\mathbf{X})^{-1}\mathbf{X}^{\top}\mathbf{v}$. Hence $\hat{\mathbf{v}} = \mathbf{X}\mathbf{c} = \mathbf{X}(\mathbf{X}^{\top}\mathbf{X})^{-1}\mathbf{X}^{\top}\mathbf{v}$. ☐

Corollary 2. *Let $\boldsymbol{U}$ be a $d \times k$ matrix with orthogonal columns and $S = \operatorname{span}(\boldsymbol{U})$. Then $\boldsymbol{P} = \boldsymbol{U}\boldsymbol{U}^{\top}$.*

Corollary 3. *$\boldsymbol{P}^2 = \boldsymbol{P}^{\top} = \boldsymbol{P}$. More over $\boldsymbol{P}$ is similar to the diagonal matrix with k many 1s and $d - k$ many 0s.*

Projected Lattice

Let $\mathcal{L} = \mathcal{L}(\mathbf{B})$,where $\mathbf{B} = \{\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k, \mathbf{b}_{k+1}, \ldots, \mathbf{b}_d\} \in \mathbb{R}^{d\times d}$ is invertible, be a lattice of rank d and $\tilde{\mathbf{B}} = \{\mathbf{b}_1^*, \mathbf{b}_2^*, \ldots, \mathbf{b}_k^*, \mathbf{b}_{k+1}^*, \ldots, \mathbf{b}_d^*\}$ be Gram-Schmidt orthogonalized basis. We define $k(< d)$-th projection of a vector

$$\mathbf{v}(\in \mathbb{R}^d) = \sum_{i=k}^{d} c_i\, \mathbf{b}_i^*, c_i \in \mathbb{R}$$

with

$$\pi_k(\mathbf{v}) = \sum_{i=k}^{d} c_i\, \mathbf{b}_i^*$$

So it is easy to observe that we are projecting all the vectors $\mathbf{v}$ onto a $d - k + 1$ dimensional subspace having a basis $\{\mathbf{b}_k^*, \mathbf{b}_{k+1}^*, \ldots, \mathbf{b}_d^*\}$ and $\pi_k(\mathbf{b}_{k-1}) = \mathbf{0}$, $\pi_k(\mathbf{b}_k) = \mathbf{b}_k^*$, $\pi_k(\mathbf{b}_{k+1}) = \mathbf{b}_{k+1}^* + \mu_{k+1,k}\mathbf{b}_k^*$ and so on. Now we consider the set $\pi_k(\mathcal{L}) = \{\pi_k(\mathbf{v}) : \mathbf{v} \in \mathrm{L}\}$. Clearly the k-th projection of $\mathbf{0} \in \mathcal{L}$, is in $\pi_k(\mathcal{L})$. If $\mathbf{u}, \mathbf{v} \in \mathcal{L}$ then $c\pi_k(\mathbf{u}) - \pi_k(\mathbf{v}) = \pi_k(c\mathbf{u} - \mathbf{v}) \in \pi_k(\mathcal{L})$. Since $\mathcal{L}$ is discrete, so for any $\mathbf{u}, \mathbf{v} \in \mathcal{L}$,

$$\|\mathbf{u} - \mathbf{v}\|_2 = \ell(> 0) \implies \|\pi_k(\mathbf{u}) - \pi_k(\mathbf{v})\|_2 = \ell^{'} > 0$$

So $\pi_k(\mathcal{L})$ is also a discrete subgroup of $\mathbb{R}^d$.

Definition 6. *We define π_k-th projection of a lattice L is $\pi_k(\mathcal{L}) = \{\pi_k(\boldsymbol{v}) : \boldsymbol{v} \in \mathcal{L}\}$.*

Lemma 3. *$\{\pi_k(\boldsymbol{b}_k), \pi_k(\boldsymbol{b}_{k+1}), \ldots, \pi_k(\boldsymbol{b}_d)\}$ is a basis of $\pi_k(\mathcal{L})$.*

Proof. Let $\mathcal{L} = \mathcal{L}(\mathbf{b}_1, \ldots, \mathbf{b}_d)$. Any $\mathbf{v} \in \mathcal{L}$ can be written as

$$\mathbf{v} = \sum_{i=1}^{d} c_i \mathbf{b}_i, \qquad c_i \in \mathbb{Z}.$$

Applying π_k gives

$$\pi_k(\mathbf{v}) = \sum_{i=1}^{d} c_i \pi_k(\mathbf{b}_i).$$

Since $\pi_k(\mathbf{b}_i) = \mathbf{0}$ for all $i < k$, we obtain

$$\pi_k(\mathbf{v}) = \sum_{i=k}^{d} c_i \pi_k(\mathbf{b}_i).$$

Thus every element of $\pi_k(\mathcal{L})$ is an integer linear combination of $\pi_k(\mathbf{b}_k), \ldots, \pi_k(\mathbf{b}_d)$, so they generate $\pi_k(\mathcal{L})$. Now let

$$\sum_{i=k}^{d} c_i \pi_k(\mathbf{b}_i) = \mathbf{0}$$

$$\implies c_k \mathbf{b}_k^* + c_{k+1}(\mathbf{b}_{k+1}^* + \mu_{k+1,k}\mathbf{b}_k^*) + \ldots + c_n(\mathbf{b}_n^* + \sum_{j<d}^{k} \mu_{d,j}\mathbf{b}_j^*) = \mathbf{0}$$

Assmbling all the coefficients of $\mathbf{b}_i^*$'s, and since $\{\mathbf{b}_k^*, \mathbf{b}_{k+1}^*, \ldots, \mathbf{b}_d^*\}$ is linearly independent, we have $c_n = c_{n-1} = \ldots = c_d = 0$. Hence $\{\pi_k(\mathbf{b}_k), \pi_k(\mathbf{b}_{k+1}), \ldots, \pi_k(\mathbf{b}_d)\}$ is a basis of $\pi_k(\mathcal{L})$. □

Definition 7 (Geometric Series Assumption). *The norms of the Gram-Schmidt vectors after lattice reduction satisfy*

$$\|\boldsymbol{b}_i^*\|_2 = \alpha^{i-1} \cdot \|\boldsymbol{b}_1\|_2 \quad \textit{for some } 0 < \alpha < 1 \tag{9}$$

By 4 we have $\|\mathbf{b}_1\|_2 = \delta^d \cdot \mathrm{Vol}(\Lambda)^{\frac{1}{d}}$ and $\mathrm{Vol}(\Lambda) = \prod_{i=1}^{d} \|\mathbf{b}_i^*\|_2$ as we know from the Gram-Schmidt Orthogonalization $\mathbf{B} = \mathbf{L} \cdot \tilde{\mathbf{B}}$, we get

$$\begin{aligned}
\mathrm{Vol}(\Lambda) &= \|\mathbf{b}_1^*\|_2 \cdot \|\mathbf{b}_2^*\|_2 \ldots \cdot \|\mathbf{b}_d^*\|_2 &(10)\\
&= \|\mathbf{b}_1^*\|_2 \cdot \alpha\|\mathbf{b}_1^*\|_2 \ldots \cdot \alpha^{d-1}\|\mathbf{b}_1^*\|_2 &(11)\\
&= \alpha^{1+2+\ldots+(d-1)}\|\mathbf{b}_1^*\|_2^d &(12)\\
&= \alpha^{d(d-1)/2}\delta^{d^2}\,\mathrm{Vol}(\Lambda) &(13)\\
\therefore \alpha &= \delta^{\frac{-2d}{d-1}} \approx \delta^{-2} \text{ for the GSA.} &(14)
\end{aligned}$$

In [ADPS16], the considered LWE has short secret and the secret is comming from the error distribution χ to be centred arround 0, and used the new attack due to Bai-Galbraith. The uSVP solution will be an embedded vector for which each entry is drawn i.i.d. from a distribution of standard deviation σ and mean $\mu = 0$ with additional constant entry 1 and the solution is $\mathbf{t} = \begin{bmatrix}\mathbf{s} \mid \mathbf{e} \mid 1\end{bmatrix}^\top$. Due to the fact that each component of the secret and the error vectors is coming from the distribution χ,that is why, we do not have to consider the rebalancing. Suppose the distribution χ is the uniform distribution on $[\![-a, a]\!]$. So χ has mean $c = 0$ and variance:

$$\frac{1}{2a+1}\sum_{i=-a}^{a} i^2 = \frac{a(a+1)}{3} \implies \sigma = \sqrt{\frac{a(a+1)}{3}}$$

Suppose each component of the error and the secret vector are coming from $D_{[\![-a,a]\!],\sigma=\sqrt{\frac{a(a+1)}{3}},c=0}$. Then $\|\mathbf{t}\|_2^2$ follows a scaled chi-squared distribution $\sigma^2 \cdot \chi_{d-1}^2$ with $d-1$ degress of freedom, with a fixed 1, resulting in $\mathrm{E}[\|\mathbf{t}\|_2^2] = (d-1)\sigma^2 + 1 \approx d \cdot \sigma^2$. By theorem 5, any k-th projection has the form $\mathbf{P} = \mathbf{X}\big(\mathbf{X}^\top\mathbf{X}\big)^{-1}\mathbf{X}^\top$, where the columns of $\mathbf{X}$ form k dimensional subspace. The $d \times k$ matrix $\mathbf{X}$ has singular value decomposition

$$\mathbf{X} = \mathbf{U}\mathbf{D}\mathbf{V}$$

where $\mathbf{U}$ is a $d \times d$ orthonormal, $\mathbf{D}$ is a $d \times k$ diagonal, and $\mathbf{V}$ is a $k \times k$ orthonormal matrix. So the matrix product

$$\mathbf{X}^\top\mathbf{X} = \mathbf{V}^\top\mathbf{D}^2\mathbf{V},$$

whose inverse is

$$(\mathbf{X}^\top\mathbf{X})^{-1} = \mathbf{V}^\top\mathbf{D}^{-2}\mathbf{V},$$

if $\mathbf{D}$ is non-singular, that is, if $\mathbf{X}$ is basis.

The matrix $\mathbf{P}$ is then

$$\mathbf{X}^\top\mathbf{V}^\top\mathbf{D}^{-2}\mathbf{V}\mathbf{X} = \mathbf{U}\mathbf{U}^\top$$

The distribution of $\mathbf{Pv}$ depends only on the length of the vector a because for each fixed $k \times k$ orthogonal matrix $\mathbf{B}$, the matrix $\mathbf{UB}$ is distributed the same way $\mathbf{U}$ is. It is a consequence of the rotational symmetry built into the $\mathcal{N}(\mathbf{0}, \mathbf{I}_{k\times k})$ distribution.

Thus,

$$\mathbb{E}[\|\mathbf{Pv}\|_2^2] = \|\mathbf{v}\|_2^2\,\mathbb{E}[\mathrm{P}_{11}],$$

as we can take

$$\mathbf{v} = (\|\mathbf{v}\|_2, 0, 0, \ldots, 0)^\top.$$

But what is $\mathbb{E}[\mathrm{P}_{11}]$? Since the distribution of $\mathbf{U}$ is rotation invariant in $\mathbb{R}^d$, so it means the distributions of all diagonal entries $\mathrm{P}_{ii}, 1 \le i \le d$ are identical, so the expectations are equal.

But using lemma 3

$$\mathrm{tr}(\mathbf{P}) = \mathrm{tr}(\mathbf{U}\mathbf{U}^\top) = k,$$

so finally

$$\mathbb{E}[\mathrm{P}_{11}] = \frac{k}{d}, \quad \mathbb{E}[\|\mathbf{Pv}\|_2^2] = \|\mathbf{v}\|_2^2\,\mathbb{E}[\mathrm{P}_{11}] = \|\mathbf{v}\|_2^2\frac{k}{d}.$$

So, the expected ℓ_2 norm of the $d-\beta+1$-th projection of vector $\mathbf{t}$ is $\frac{\sqrt{\beta}}{\sqrt{d}}\|\mathbf{v}\|_2$. But we have assumed all the components of $\mathbf{t} = \left[\mathbf{s} \mid \mathbf{e} \mid 1\right]^\top$ is coming from $D_{[\![-a,a]\!],\sigma=\sqrt{\frac{a(a+1)}{3}},c=0}$, so the expected ℓ_2 norm of $\mathbf{t}$ is $\sigma\sqrt{d}$. So $\mathbb{E}[\|\mathbf{t}\|_2] = \sigma\sqrt{\beta}$. If after basis reduction, the Gram-Schmidt vectors obeying that GSA assumption, then

$$\|\mathbf{b}^*_{d-\beta+1}\|_2 = \alpha^{d-\beta+1-1}\|\mathbf{b}_1\|_2 = \delta^{2\beta-d}\,\mathrm{Vol}(\Lambda)^{\frac{1}{d}}$$

by using 4 and 14. So inequality 8 tells us that in the BKZ analysis of [ADPS16], the success condition is expressed by comparing the projected $\mathbf{t} = \left[\mathbf{s} \mid \mathbf{e} \mid 1\right]^\top$ to the expected Gram–Schmidt profile under the Geometric Series Assumption (GSA). Concretely, after reduction, one considers the projection of the vector $\mathbf{t} = \left[\mathbf{s} \mid \mathbf{e} \mid 1\right]^\top$ orthogonally to the first $d-\beta$ Gram–Schmidt vectors. If $\pi_{d-\beta+1}(\mathbf{t})$ projection is shorter than the expected length of $\mathbf{b}^*_{d-\beta+1}$ under the GSA, then the vector $\pi_{d-\beta+1}(\mathbf{t})$ appears as a shortest vector in the last projected block. As a result, the SVP oracle called on this block of size β is likely to identify it, thereby exposing the short structure that enables the attack. This condition thus provides the heuristic justification for why BKZ with block size β succeeds when the projected error length is sufficiently small relative to the GSA-predicted basis profile. To estimate the cost of the attack, one has to find an optimal BKZ block size β and an optimal $\mathbf{LWE}_{m,n,q,a}$ sample size m so that the unique shortest vector can be recovered from the reduced lattice basis under the GSA. Reader can visit this link and find a $\mathbf{LWE}_{m,n,q,a}$ estimator which was used to estimate parameters regarding primal attack on CRYSTALS-Kyber and CRYSTALS-Dilithium.

Note. *Suppose we have a matrix $\boldsymbol{A} \in \mathbb{Z}_q^{n\times m}, n \le m$ with rank$(\boldsymbol{A}) = n$. Consider the q-ary lattice $\Lambda_q^{\perp}(\boldsymbol{A}) = \{\boldsymbol{x} \in \mathbb{Z}^m : \boldsymbol{A}\boldsymbol{x} \equiv 0 \mod q\}$. $\boldsymbol{A} = [\boldsymbol{A}_1|\boldsymbol{A}_2]$ where $\boldsymbol{A}_1$ is invertible of order $n \times n$ and $\boldsymbol{A}_2$ is of order $n \times (m-n)$. We are interested to find a basis for this lattice. Let $\boldsymbol{x} \in \Lambda_q^{\perp}(\boldsymbol{A})$.*

$$\boldsymbol{A}\boldsymbol{x} = [\boldsymbol{A}_1|\boldsymbol{A}_2]\boldsymbol{x} \equiv \boldsymbol{0} \mod q$$

then,

$$\boldsymbol{A}_1^{-1}\boldsymbol{A}\boldsymbol{x} = [\boldsymbol{I}|\boldsymbol{A}_1^{-1}\boldsymbol{A}_2]\boldsymbol{x} = q\boldsymbol{u}, \boldsymbol{u} \in \mathbb{Z}^n$$

implies,

$$\boldsymbol{x}_1 + \boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{x}_2 = q\boldsymbol{u}, \textit{where } \boldsymbol{x} = \left[\boldsymbol{x}_1 \mid \boldsymbol{x}_2\right]^\top$$

So,

$$\boldsymbol{x} = \begin{bmatrix}\boldsymbol{x}_1\\ \boldsymbol{x}_2\end{bmatrix} = \begin{bmatrix}q\boldsymbol{u} - \boldsymbol{A}_1^{-1}\boldsymbol{A}_2\boldsymbol{x}_2\\ \boldsymbol{x}_2\end{bmatrix} = \begin{bmatrix}q\boldsymbol{I}_n & -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\\ \boldsymbol{0} & \boldsymbol{I}_{m-n}\end{bmatrix}\begin{bmatrix}\boldsymbol{u}\\ \boldsymbol{x}_2\end{bmatrix}$$

$\boldsymbol{B}' = \begin{bmatrix}q\boldsymbol{I}_n & -\boldsymbol{A}_1^{-1}\boldsymbol{A}_2\\ \boldsymbol{0} & \boldsymbol{I}_{m-n}\end{bmatrix}$ *is a basis and volume of the lattice $\Lambda_q^{\perp}(\boldsymbol{A})$ is q^n. The* GSO $\left(\boldsymbol{B}'\right)$ *consists of*

- *For $i = 1, \ldots, n$:*

$$\boldsymbol{v}_i^* = \begin{bmatrix}q\boldsymbol{e}_i\\ \boldsymbol{0}\end{bmatrix}, \qquad \|\boldsymbol{v}_i^*\|_2 = q.$$

- *For $t = 1, \ldots, m-n$:*

$$\boldsymbol{v}_{n+t}^* = \begin{bmatrix}\boldsymbol{0}\\ \boldsymbol{e}_t\end{bmatrix}, \qquad \|\boldsymbol{v}_{n+t}^*\|_2 = 1.$$

First n vectors of $\boldsymbol{B}'$ are being called by q-vectors. For $\Lambda = \{\boldsymbol{x} \in \mathbb{Z}^{m+n+1} : (\boldsymbol{A}_{m\times n}^\top|\boldsymbol{I}_m| - \boldsymbol{b})\boldsymbol{x} \equiv \boldsymbol{0} \mod q\}$, we can also construct a basis like $\boldsymbol{B}'$ having first m many q-vectors. In the simulator this type of basis was considered.

References

[ACPS09] Benny Applebaum, David Cash, Chris Peikert, and Amit Sahai. Fast cryptographic primitives and circular-secure encryption based on hard learning problems. In *Proceedings of the 29th Annual International Cryptology Conference on Advances in Cryptology*, CRYPTO '09, page 595–618, Berlin, Heidelberg, 2009. Springer-Verlag.

[ADPS16] Erdem Alkim, Léo Ducas, Thomas Pöppelmann, and Peter Schwabe. Post-quantum key exchange: a new hope. In *Proceedings of the 25th USENIX Conference on Security Symposium*, SEC'16, page 327–343, USA, 2016. USENIX Association.

[AGVW17] Martin R. Albrecht, Florian Göpfert, Fernando Virdia, and Thomas Wunderer. Revisiting the expected cost of solving usvp and applications to lwe. In Tsuyoshi Takagi and Thomas Peyrin, editors, *Advances in Cryptology – ASIACRYPT 2017*, pages 297–322, Cham, 2017. Springer International Publishing.

[BCD+16] Joppe W. Bos, Craig Costello, Léo Ducas, Ilya Mironov, Michael Naehrig, Valeria Nikolaenko, Ananth Raghunathan, and Douglas Stebila. Frodo: Take off the ring! practical, quantum-secure key exchange from lwe. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, 2016.

[BDGL16] Anja Becker, Léo Ducas, Nicolas Gama, and Thijs Laarhoven. New directions in nearest neighbor searching with applications to lattice sieving. In *Proceedings of the Twenty-Seventh Annual ACM-SIAM Symposium on Discrete Algorithms*, SODA '16, page 10–24, USA, 2016. Society for Industrial and Applied Mathematics.

[BG14] Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE. In Willy Susilo and Yi Mu, editors, *Information Security and Privacy - 19th Australasian Conference, ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 322–337. Springer, 2014.

[BLP+13] Zvika Brakerski, Adeline Langlois, Chris Peikert, Oded Regev, and Damien Stehlé. Classical hardness of learning with errors. In *Proceedings of the Forty-Fifth Annual ACM Symposium on Theory of Computing*, STOC '13, page 575–584, New York, NY, USA, 2013. Association for Computing Machinery.

[Che13] Yuanmi Chen. *Lattice based cryptography: An introduction*. PhD thesis, PhD thesis, Ruhr-Universität Bochum, 2013. Available at Internet Archive.

[CN11] Yuanmi Chen and Phong Q. Nguyen. Bkz 2.0: Better lattice security estimates. In *ASIACRYPT*, volume 7073 of *Lecture Notes in Computer Science*, pages 1–20. Springer, 2011.

[DMQ13] Nico Döttling and Jörn Müller-Quade. Lossy codes and a new variant of the learning-with-errors problem. In *Advances in Cryptology - EUROCRYPT 2013*, volume 7881 of *Lecture Notes in Computer Science*, pages 18–34. Springer, 2013.

[GN08] Nicolas Gama and Phong Q. Nguyen. Predicting lattice reduction. In Nigel P. Smart, editor, *Advances in Cryptology - EUROCRYPT 2008, 27th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Istanbul, Turkey, April 13-17, 2008. Proceedings*, volume 4965 of *Lecture Notes in Computer Science*, pages 31–51. Springer, 2008.

[Laa16] Thijs Laarhoven. Search problems in cryptography: from fingerprinting to lattice sieving. In *PhD Thesis, Eindhoven University of Technology*, 2016.

[LM09] Vadim Lyubashevsky and Daniele Micciancio. On bounded distance decoding, unique shortest vectors, and the minimum distance problem. In Shai Halevi, editor, *Advances in Cryptology - CRYPTO 2009*, pages 577–594, Berlin, Heidelberg, 2009. Springer Berlin Heidelberg.

[LP10] Richard Lindner and Chris Peikert. Better key sizes (and attacks) for LWE-based encryption. Cryptology ePrint Archive, Paper 2010/613, 2010.

[MM11] Daniele Micciancio and Petros Mol. Pseudorandom knapsacks and the sample complexity of lwe search-to-decision reductions. In Phillip Rogaway, editor, *Advances in Cryptology – CRYPTO 2011*, pages 465–484, Berlin, Heidelberg, 2011. Springer Berlin Heidelberg.

[MP13] Daniele Micciancio and Chris Peikert. Hardness of SIS and LWE with small parameters. Cryptology ePrint Archive, Paper 2013/069, 2013.

[MR09] Daniele Micciancio and Oded Regev. *Lattice-based Cryptography*, pages 147–191. Springer Berlin Heidelberg, Berlin, Heidelberg, 2009.

[Pei09] Chris Peikert. Public-key cryptosystems from the worst-case shortest vector problem: extended abstract. In Michael Mitzenmacher, editor, *Proceedings of the 41st Annual ACM Symposium on Theory of Computing, STOC 2009, Bethesda, MD, USA, May 31 - June 2, 2009*, pages 333–342. ACM, 2009.

[Reg09] Oded Regev. On lattices, learning with errors, random linear codes, and cryptography. *J. ACM*, 56(6), September 2009.