# Efficient Lattice Reduction Algorithm and Cryptography

Masaya Yasuda

Institute of Mathematics for Industry, Kyushu University

January 7, 2016

# Introduction to Lattice-Based Cryptography

1. Let $\mathbf{b}_1, \ldots, \mathbf{b}_n$ be $n$ linearly independent column vectors of $\mathbb{Z}^m$. Set $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n] \in \mathbb{Z}^{m \times n}$, and let

$$L = \mathcal{L}(\mathbf{B}) := \left\{ \sum_{i=1}^{n} x_i \mathbf{b}_i : x_i \in \mathbb{Z} \ (1 \leq \forall i \leq n) \right\}.$$

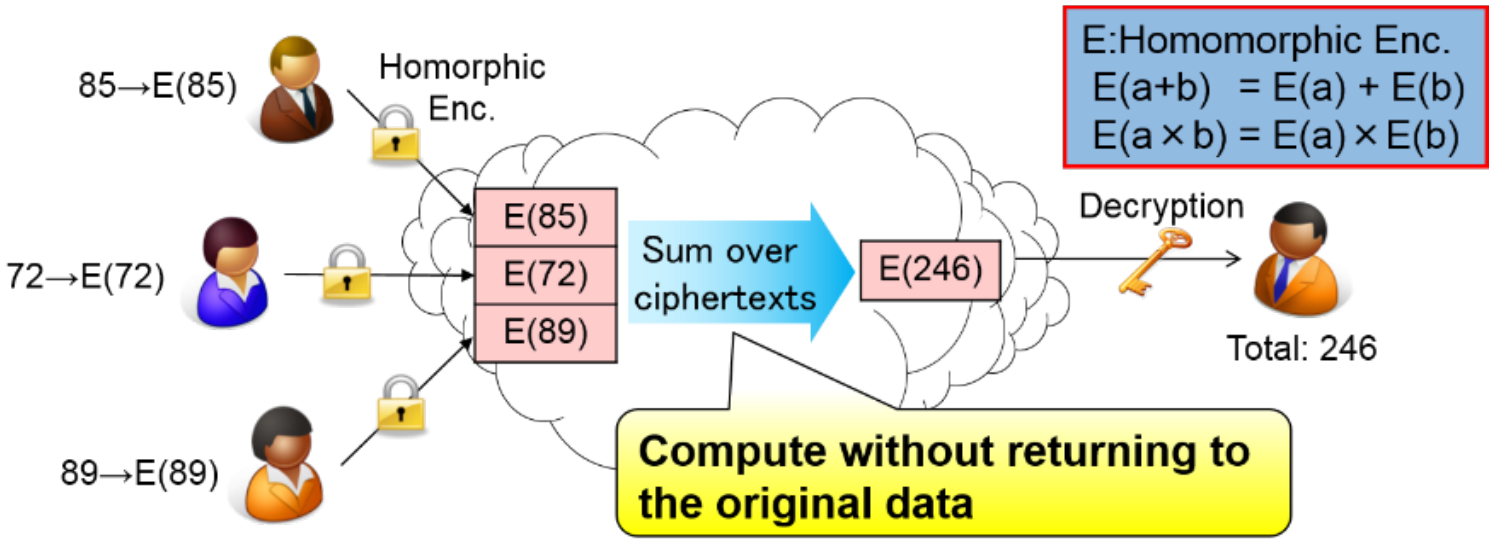
   Then $L$ is called a lattice of dimension $n$, and $\mathbf{B}$ a basis.

2. Lattice-based cryptography has been paid attention as
   - a candidate of post-quantum cryptography
     (i.e. still secure against attacks using quantum computing)
   - application to encryption with high functionality
     (e.g. homomorphic encryption)

# Applications of Lattice-Based Cryptography

## Homomorphic encryption (HE)

1. enables to operate encrypted data without decryption
2. suitable for cloud computing
   - Clients can securely outsource their private data to the cloud
   - The total score can be computed so that the cloud cannot know any score




HE enables a variety of computations while preserving the data confidentiality (it may be applied for cybersecurity).

# Security of Lattice-Based Cryptography

The security of lattice-based cryptography relies on the computational hardness of lattice problems such as

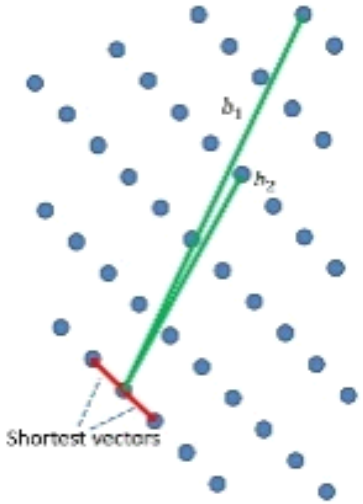
- Shortest Vector Problem (SVP), and
- Closest Vector Problem (CVP).

At present, no efficient algorithm is known to solve SVP and CVP in high dimensional lattices (e.g. $n \geq 100$).

In this talk, we focus on

**SVP**

Given a basis $\mathbf{B}$ of a lattice $L$, SVP is to find a non-zero shortest vector $\mathbf{v} \in L$.




SVP is proved to be NP-hard. In cryptography, shortest vectors are used as a secret key.

To evaluate the security of lattice-based cryptography, we need to estimate the computational hardness of lattice problems.

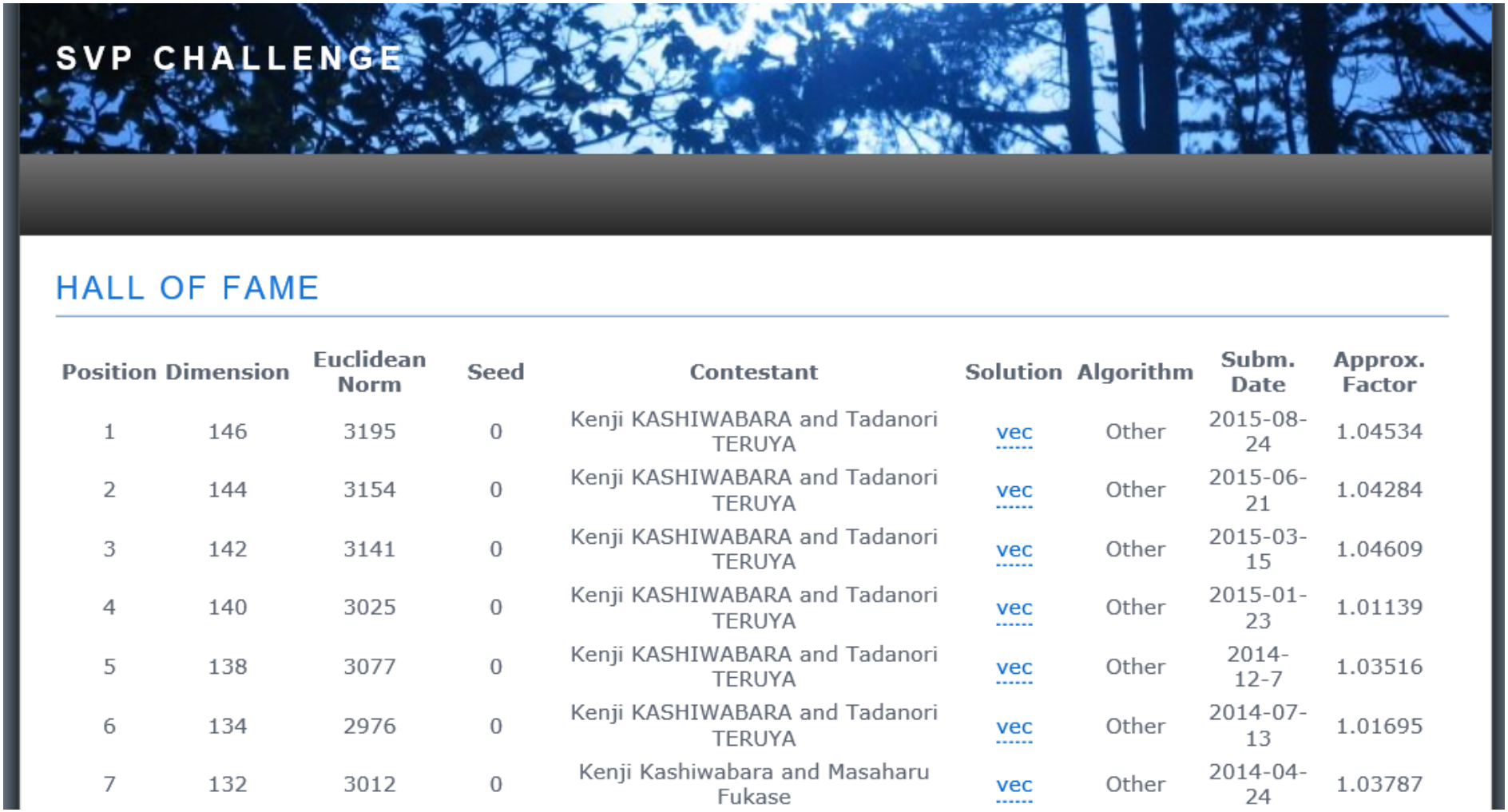
# Main Approaches for SVP

1. Lattice reduction finds a lattice basis with short and nearly orthogonal vectors $[\mathbf{b}_1, \ldots, \mathbf{b}_n]$
   - LLL [6] and BKZ [8] algorithms
2. Enumeration performs to enumerate all lattice points within a sphere $S$ around a target vector
   - Gama-Nguyen-Regev's pruned enumeration [5] for recent work
3. Sieving performs a randomized sampling of $L \cap S$
   - The Ajtai-Kumar-Sivakumar (AKS) algorithm [1]
4. Random sampling samples a number of short lattice vectors until a very short lattice vector is found $\leftarrow$ Our Focus

# Previous Work on Random Sampling

1. In 2003, Schnorr [7] first proposed a random sampling algorithm, called Random Sampling Reduction (RSR)
   - Given a lattice basis $[\mathbf{b}_1, \cdots, \mathbf{b}_n]$, Schnorr's RSR generates $\mathbf{v} \in L$ with $\|\mathbf{v}\|^2 < 0.99 \cdot \|\mathbf{b}_1\|^2$
2. In 2006, Buchmann and Ludwig [2] proposed Simple Sampling Reduction (SSR) to make Schnorr's RSR practical
3. In 2015, Fukase and Kashiwabara [3] proposed a method for SVP
   - Their strategy has been applied to solve Darmstadt's SVP problems of dimensions $134 \sim 146$ by Kashiwabara and Teruya
   - Their method is based on Schnorr's RSR, but their preprocessing is different from others

# Darmstadt's SVP Challenge




## HALL OF FAME

| Position | Dimension | Euclidean Norm | Seed | Contestant | Solution | Algorithm | Subm. Date | Approx. Factor |
|---|---|---|---|---|---|---|---|---|
| 1 | 146 | 3195 | 0 | Kenji KASHIWABARA and Tadanori TERUYA | vec | Other | 2015-08-24 | 1.04534 |
| 2 | 144 | 3154 | 0 | Kenji KASHIWABARA and Tadanori TERUYA | vec | Other | 2015-06-21 | 1.04284 |
| 3 | 142 | 3141 | 0 | Kenji KASHIWABARA and Tadanori TERUYA | vec | Other | 2015-03-15 | 1.04609 |
| 4 | 140 | 3025 | 0 | Kenji KASHIWABARA and Tadanori TERUYA | vec | Other | 2015-01-23 | 1.01139 |
| 5 | 138 | 3077 | 0 | Kenji KASHIWABARA and Tadanori TERUYA | vec | Other | 2014-12-7 | 1.03516 |
| 6 | 134 | 2976 | 0 | Kenji KASHIWABARA and Tadanori TERUYA | vec | Other | 2014-07-13 | 1.01695 |
| 7 | 132 | 3012 | 0 | Kenji Kashiwabara and Masaharu Fukase | vec | Other | 2014-04-24 | 1.03787 |

This page presents sample lattices for testing algorithms that solve SVP
`http://www.latticechallenge.org/svp-challenge/`.

# Strategy of Fukase et al. [3] for Short Lattice Vectors

Let $L$ be a lattice of dimension $n$. Fix $1 \leq u < n$. Given $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$, Schnorr's Sampling Algorithm (SA) samples $\mathbf{v} = \sum_{i=1}^{n} \nu_i \mathbf{b}_i^* \in L$ with

$$\nu_i \in \begin{cases} (-1/2, 1/2] & \text{if } 1 \leq i < n-u, \\ (-1, 1] & \text{if } n-u \leq i < n, \\ \{1\} & \text{if } i = n, \end{cases} \tag{1}$$

where $[\mathbf{b}_1^*, \ldots, \mathbf{b}_n^*]$ denotes the Gram-Schmidt vectors of $\mathbf{B}$.
Set $S_{u,\mathbf{B}} = \{\mathbf{v} \in L \text{ with } (1)\}$. By calling SA up to $\#S_{u,\mathbf{B}} = 2^u$ times, Schnorr's RSR generates $\mathbf{v} \in L$ with $\|\mathbf{v}\|^2 < 0.99 \cdot \|\mathbf{b}_1\|^2$.
The strategy of Fukase-Kashiwabara [3] is as follows:

Step 1. (New Preprocessing) Given $\mathbf{B}$, we decrease $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ to obtain a new basis $\mathbf{B}$ of $L$ with small $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$.

Step 2. With such $\mathbf{B}$, we find a short lattice vector $\mathbf{v} = \sum_{i=1} \nu_i \mathbf{b}_i^* \in S_{u,\mathbf{B}}$ by Schnorr's RSR.

# Statistical Analysis of [3] on Lattices

The below analysis implies that smaller the sum $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ becomes, *shorter* lattice vectors can be sampled.

## Distribution of $\|\mathbf{v}\|^2$

The distribution of $\|\mathbf{v}\|^2 = \sum_{i=1}^{n} \nu_i^2 \|\mathbf{b}_i^*\|^2$ follows $\mathcal{N}(\mu, \sigma^2)$ with

$$\mu = \frac{\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2}{12} \text{ and } \sigma = \left( \frac{\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^4}{180} \right)^{1/2}.$$

The probability of finding $\mathbf{v} \in L$ shorter than given $\eta$ is

$$\frac{1}{\sqrt{2\pi}\sigma} \int_{-\infty}^{\eta^2} \exp\left( -\frac{(x-\mu)^2}{2\sigma^2} \right) dx = \frac{1}{2} \left( 1 + \mathrm{erf}\left( \frac{\eta^2 - \mu}{\sqrt{2}\sigma} \right) \right),$$

where $\mathrm{erf}(x) = \frac{2}{\sqrt{\pi}} \int_0^x \exp(-t^2) dt$ denotes the error function.

# Basic Method to Decrease $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ in Step 1

To decrease $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$, Fukase-Kashiwabara [3] consider to insert a certain short vector $\mathbf{v} \in L$ into $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ to obtain a new basis

$$\mathbf{C} := [\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{v}, \mathbf{b}_k, \ldots, \mathbf{b}_{n-1}].$$

To reduce $\mathbf{C}$ by LLL or BKZ, the sum $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ is *sometimes* decreased.

## Definition: Insertion Index of $\mathbf{v}$ [3, Definition 4]

Let $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ be a basis of $L$. For fixed $0 < \alpha \leq 1$, the insertion index $k$ of $\mathbf{v} \in L$ is determined by

$$k = \min\left\{1 \leq j \leq n : \|\pi_j(\mathbf{v})\|^2 < \alpha \|\mathbf{b}_j^*\|^2\right\}, \quad \text{(we here set } \alpha = 1\text{)}$$

where let $\pi_j : \mathbb{R}^n \to V_{j-1}^{\perp}$ denote the orthogonal projection over the orthogonal supplement of $V_{j-1} = \langle \mathbf{b}_1^*, \ldots, \mathbf{b}_{j-1}^* \rangle_{\mathbb{R}}$.

# Our Motivation

- **Problem:** No guarantee is known to strictly decrease $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$
- **Motivation:** We would like to give a condition of $\mathbf{v} \in L$ that the sum $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ is strictly decreased
- Given an LLL-reduced basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ and a vector $\mathbf{v} \in L$ with insertion index $k$, we consider

$$\mathbf{B} \xrightarrow{\text{insertion of } \mathbf{v}} \mathbf{C} = [\mathbf{c}_1, \ldots, \mathbf{c}_n] := [\mathbf{b}_1, \ldots, \mathbf{b}_{k-1}, \mathbf{v}, \mathbf{b}_k, \ldots, \mathbf{b}_{n-1}]$$
$$\xrightarrow{\text{LLL reduction}} \mathbf{B}' = [\mathbf{b}'_1, \ldots, \mathbf{b}'_n].$$

Our goal is to give a condition of $\mathbf{v} \in L$ satisfying

$$\sum_{i=1}^{n} \|\mathbf{b}_i'^*\|^2 < \sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$$

# Gram-Schmidt Orthogonalization of $\mathbf{C}$

Let $\mathbf{v} = \sum_{i=1}^{n} \nu_i \mathbf{b}_i^* \in L$ with insertion index $k$.

## Proposition: Gram-Schmidt orthogonalization $[\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*]$ of $\mathbf{C}$

Set $m = \max\{k \le i \le n \mid \nu_i \neq 0\}$. Then we have

$$\mathbf{c}_j^* = \begin{cases} \displaystyle\sum_{i=k}^{m} \nu_i \mathbf{b}_i^* & \text{for } j = k, \\ \displaystyle\frac{D_j}{D_{j-1}} \mathbf{b}_{j-1}^* - \sum_{i=j}^{m} \frac{\nu_i \nu_{j-1} \|\mathbf{b}_{j-1}^*\|^2}{D_{j-1}} \mathbf{b}_i^* & \text{for } k+1 \le j \le m+1, \\ \mathbf{b}_{j-1}^* & \text{for } m+2 \le j \le n+1, \end{cases}$$

where $D_\ell = \sum_{i=\ell}^{m} \nu_i^2 \|\mathbf{b}_i^*\|^2$ for $1 \le \ell \le m$. In particular, $\mathbf{c}_{m+1}^* = \mathbf{0}$.
For $k+1 \le j \le m$, we have

$$\|\mathbf{c}_j^*\|^2 = \frac{D_j}{D_{j-1}} \|\mathbf{b}_{j-1}^*\|^2.$$

# Gap between $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ and $\sum_{i=1}^{n} \|\mathbf{c}_i^*\|^2$

Let $\mathbf{v} = \sum_{i=1}^{n} \nu_i \mathbf{b}_i^* \in L$ with $\nu_n = 1$ (i.e. $m = n$) and insertion index $k$.

$$
\begin{aligned}
E(\mathbf{v}, k) &:= \sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2 - \sum_{i=1}^{n} \|\mathbf{c}_i^*\|^2 \\
&= \sum_{i=k}^{n} \|\mathbf{b}_i^*\|^2 - \left( D_k + \sum_{j=k+1}^{n} \frac{D_j}{D_{j-1}} \|\mathbf{b}_{j-1}^*\|^2 \right) \\
&= \sum_{j=k}^{n-1} \nu_j^2 \|\mathbf{b}_j^*\|^2 \left( \frac{\|\mathbf{b}_j^*\|^2}{D_j} - 1 \right) \quad (\text{Recall } D_j = \sum_{i=j}^{n} \nu_i^2 \|\mathbf{b}_i^*\|^2)
\end{aligned}
$$

- To decrease $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$, we need to take $\mathbf{v} \in L$ with $E(\mathbf{v}, k) > 0$
- However, in most cases, $E(\mathbf{v}, k)$ is negative when $\mathbf{v} \in L$ is generated by Schnorr's SA
- Then we need to carefully consider the LLL reduction for $\mathbf{C}$

# LLL-Reduction for Basis $\mathbf{C}$

The LLL algorithm for $\mathbf{C}$ consists of the following two steps:
From $i = 2$ to $n$,

Step 1. Size-reduce $\mathbf{C} = [\mathbf{c}_1, \ldots, \mathbf{c}_n]$

- Note that this procedure does not change the lengths of the Gram-Schmidt vectors $[\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*]$ by [4, Lemma 17.4.1].

Step 2. Swap $\mathbf{c}_i$ with $\mathbf{c}_{i-1}$ if the Lovász condition is not satisfied:

$$\|\mathbf{c}_i^*\|^2 \geq (\delta - \xi_{i,i-1}^2)\|\mathbf{c}_{i-1}^*\|^2$$

In this case, set $i \leftarrow \max\{2, i-1\}$. Otherwise set $i \leftarrow i+1$. Then go back to Step 1.

- $\delta$: the reduction parameter satisfying $1/4 < \delta < 1$
- The parameter was initially set as $\delta = \frac{3}{4}$ in [6], but we used $\delta = 0.99$ in our experiments

# Key Lemma [4, Lemma 17.4.3]

The vectors $[\mathbf{c}_1^*, \ldots, \mathbf{c}_n^*]$ are changed by swapping $\mathbf{c}_\ell$ with $\mathbf{c}_{\ell+1}$ as follows:

(i) For $1 \leq i < \ell$ and $\ell + 1 < i \leq n$, the vector $\mathbf{c}_i^*$ is unchanged.

(ii) The new vector for $\mathbf{c}_\ell^*$ is given by $\mathbf{c}_\ell'^* := \mathbf{c}_{\ell+1}^* + \xi_{\ell+1,\ell}\mathbf{c}_\ell^*$, and

$$C_\ell' := \|\mathbf{c}_\ell'^*\|^2 = C_{\ell+1} + \xi_{\ell+1,\ell}^2 C_\ell, \quad \xi_{i,j} := \frac{\langle \mathbf{c}_i, \mathbf{c}_j^* \rangle}{\|\mathbf{c}_j^*\|^2}$$

where $C_i = \|\mathbf{c}_i^*\|^2$ for $1 \leq i \leq n$.

(iii) The new vector for $\mathbf{c}_{\ell+1}^*$ is by $\mathbf{c}_{\ell+1}'^* := \frac{C_{\ell+1}}{C_\ell'}\mathbf{c}_\ell^* - \frac{\xi_{\ell+1,\ell} C_\ell}{C_\ell'}\mathbf{c}_{\ell+1}^*$, and

$$C_{\ell+1}' := \|\mathbf{c}_{\ell+1}'^*\|^2 = \frac{C_\ell C_{\ell+1}}{C_\ell'}.$$

If we set $\delta_\ell' := \frac{C_\ell'}{C_\ell} = \frac{C_{\ell+1}}{C_\ell} + \xi_{\ell+1,\ell}^2$, then $\delta_\ell' < \delta$.

# Decreasing Value by One Swap for $\mathbf{C}$ ($C_i = \|\mathbf{c}_i^*\|^2$)

The decreasing value by *one swap* at the $\ell$-th index is estimated as

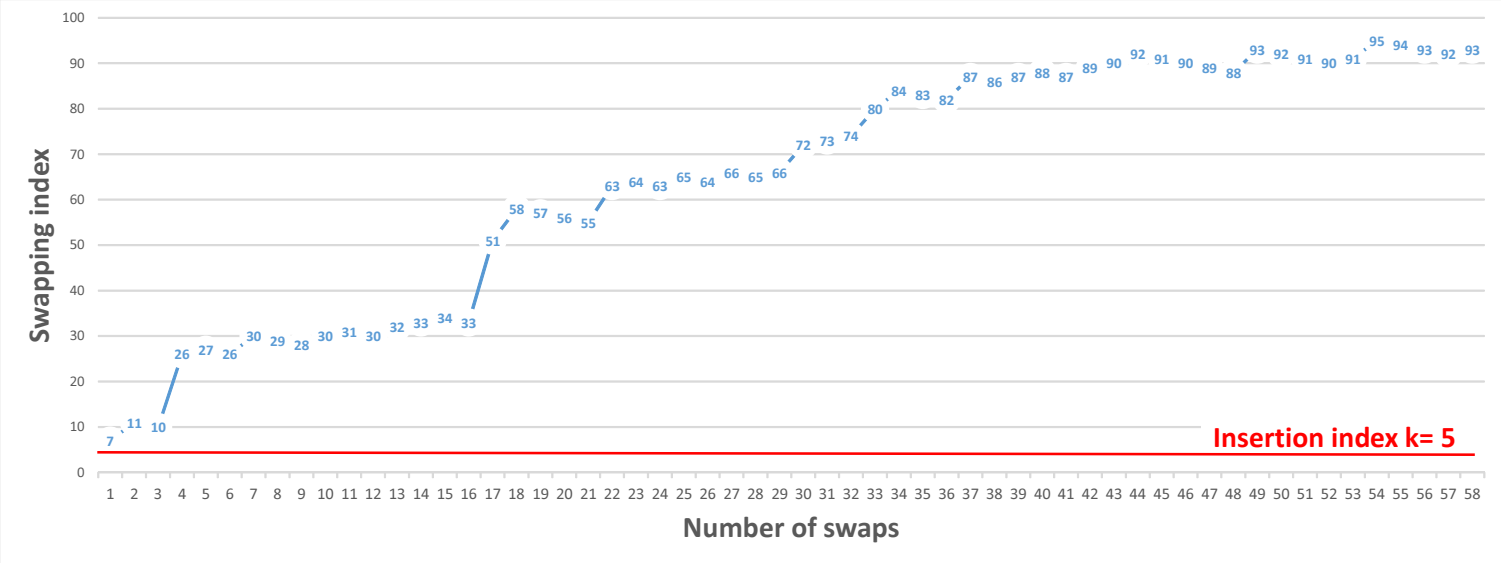
$$\begin{aligned}(C_\ell + C_{\ell+1}) - (C'_\ell + C'_{\ell+1}) &= (1 - \xi_{\ell+1,\ell}^2) C_\ell - \frac{C_\ell C_{\ell+1}}{C'_\ell} \\ &= \frac{\xi_{\ell+1,\ell}^2 (1 - \delta'_\ell)}{\delta'_\ell} C_\ell > \frac{\xi_{\ell+1,\ell}^2 (1 - \delta)}{\delta} C_\ell > 0.\end{aligned}$$

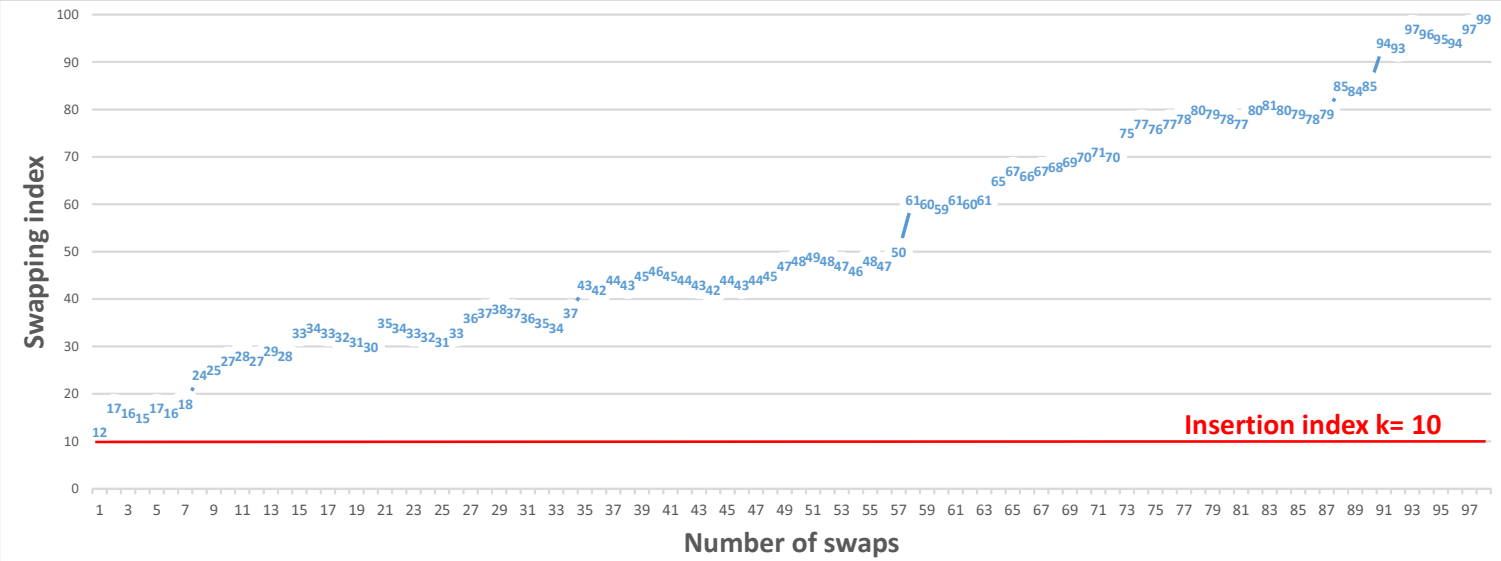
Let $\mathbf{v} \in L$ with $\|\mathbf{v}\|^2 = D_k < \|\mathbf{b}_k^*\|^2$ ($k$: the insertion index).
If $(\mathbf{c}_k, \mathbf{c}_{k+1}) = (\mathbf{v}, \mathbf{b}_k)$ is swapped at the beginning of the LLL algorithm, then $(\mathbf{c}'_k, \mathbf{c}'_{k+1}) = (\mathbf{b}_k, \mathbf{v})$ with $C'_k = \|\mathbf{b}_k^*\|^2$ and $C'_{k+1} = D_{k+1}$. However,

$$\begin{aligned}(C_k + C_{k+1}) - (C'_k + C'_{k+1}) &= \left( D_k + \frac{D_{k+1}}{D_k} \|\mathbf{b}_k^*\|^2 \right) - \left( \|\mathbf{b}_k^*\|^2 + D_{k+1} \right) \\ &= \left( \frac{D_k - D_{k+1}}{D_k} \right) (D_k - \|\mathbf{b}_k^*\|^2) < 0.\end{aligned}$$

A contradiction. This implies that $(\mathbf{c}_k, \mathbf{c}_{k+1})$ cannot be swapped at the beginning of the LLL algorithm.

# Examples of Swaps for $\mathbf{C}$ (lattice dimension $n = 100$)



# Average of Decreasing Value of $\sum_{i=1}^{n} \|\mathbf{c}_i^*\|^2$ by One Swap

## Lemma: Decreasing Value by One Swap

If a swap occurs at the $\ell$-th index, then $\sum_{i=1}^{n} C_i = \sum_{i=1}^{n} \|\mathbf{c}_i^*\|^2$ is reduced at least

$$\frac{\xi_{\ell+1,\ell}^2(1-\delta)}{\delta} C_m$$

for some $m$ (in most cases $m = \ell$, sometimes $m = \ell+1, \ell+2$ or so on).

Assumption 1. The value $\xi_{\ell+1,\ell}$ is uniformly distributed over the range $\left[-\frac{1}{2}, \frac{1}{2}\right]$ (then we expect $E[\xi_{\ell+1,\ell}^2] = \frac{1}{12}$)

Assumption 2. Swap indices $\ell$ are roughly distributed over the range from $k$ to $n-1$ *evenly* (uniformly)

Under these assumptions, the expected value $E[C_m]$ can be estimated as

$$\begin{aligned} E[C_m] &\approx \frac{1}{(n-k)} \sum_{m=k}^{n-1} C_m \geq \left( \prod_{m=k}^{n-1} C_m \right)^{1/(n-k)} \\ &= \left( D_k \cdot \left( \frac{D_{k+1}}{D_k} \|\mathbf{b}_k^*\|^2 \right) \cdots \left( \frac{D_n}{D_{n-1}} \|\mathbf{b}_{n-1}^*\|^2 \right) \right)^{1/(n-k)} \\ &= \mathrm{vol}(\pi_k(L))^{2/(n-k)}. \end{aligned}$$

## Proposition: Average of Decreasing Value of $\sum_{i=1}^{n} \|\mathbf{c}_i^*\|^2$

We can roughly estimate that the average of decreasing values of the sum $\sum_{i=1}^{n} C_i = \sum_{i=1}^{n} \|\mathbf{c}_i^*\|^2$ by one swap is greater than

$$\frac{1-\delta}{12\delta} \cdot \mathrm{vol}(\pi_k(L))^{2/(n-k)}.$$

# Expected Number of Swaps in LLL for $\mathbf{C}$

## Definition: Loop Invariant

The *loop invariant* of a lattice basis $\mathbf{S} = [\mathbf{s}_1, \ldots, \mathbf{s}_n]$ is defined as

$$\mathcal{LI}(\mathbf{S}) = \prod_{i=1}^{n-1} \left( \prod_{\ell=1}^{i} \|\mathbf{s}_\ell^*\|^2 \right) = \prod_{i=1}^{n-1} \|\mathbf{s}_i^*\|^{2n-2i},$$

where $[\mathbf{s}_1^*, \ldots, \mathbf{s}_n^*]$ denotes the Gram-Schmidt vectors of $\mathbf{S}$.

The invariant plays an important role for the number of swaps. If swapping $(\mathbf{s}_\ell, \mathbf{s}_{\ell+1})$ to obtain $\mathbf{T} = [\mathbf{t}_1, \ldots, \mathbf{t}_n]$ with $\mathbf{t}_\ell = \mathbf{s}_{\ell+1}, \mathbf{t}_{\ell+1} = \mathbf{s}_\ell$, we have

$$\mathcal{LI}(\mathbf{T}) = \mathcal{LI}(\mathbf{S}) \times \frac{\|\mathbf{t}_\ell^*\|^2}{\|\mathbf{s}_\ell^*\|^2} \text{ and } \delta_\ell := \frac{\|\mathbf{t}_\ell^*\|^2}{\|\mathbf{s}_\ell^*\|^2} = \eta_{\ell+1,\ell}^2 + \frac{\|\mathbf{s}_{\ell+1}^*\|^2}{\|\mathbf{s}_\ell^*\|^2},$$

where $\eta_{\ell+1,\ell} = \dfrac{\langle \mathbf{s}_{\ell+1}, \mathbf{s}_\ell^* \rangle}{\|\mathbf{s}_\ell^*\|^2}$.

## Lemma: Relation between $\mathcal{LI}(\mathbf{B})$ and $\mathcal{LI}(\mathbf{C})$

Let $B_i = \|\mathbf{b}_i^*\|^2$ and $C_i = \|\mathbf{c}_i^*\|^2$ for $1 \leq i \leq n$. Then we have

$$\mathcal{LI}(\mathbf{C}) = \mathcal{LI}(\mathbf{B}) \times \frac{D_k \cdots D_{n-1}}{B_k \cdots B_{n-1}}.$$

Let $\mathbf{B}' \leftarrow \mathrm{LLL}(\mathbf{C})$. Then

$$\mathcal{LI}(\mathbf{B}') = \prod_{i=1}^{N} \delta(i) \times \prod_{i=k}^{n-1} \frac{D_i}{B_i} \times \mathcal{LI}(\mathbf{B}) \text{ for some } \delta(i),$$

where let $N$ denote the number of swaps. Each $\delta(i)$ is defined as

$$\delta(i) = \xi(i)^2 + \frac{C_{\ell(i)+1}^{(i-1)}}{C_{\ell(i)}^{(i-1)}},$$

where $\mathbf{C}^{(s)} = \left[\mathbf{c}_1^{(s)}, \ldots, \mathbf{c}_n^{(s)}\right]$ denotes the basis obtained by $s$ times swaps and size-reduced for $1 \leq s \leq N$, and $C_i^{(s)} = \|\mathbf{c}_i^{(s)*}\|^2$ ($\ell(i) =$ the swap position of the $i$-th swap, $\xi(i) =$ the normalized inner product).

Assumption 3. $1 \succeq R := \dfrac{\mathcal{LI}(\mathbf{B}')}{\mathcal{LI}(\mathbf{B})}$, where $A \succeq B$ means $A \approx B$ or $A > B$

- Since $\mathbf{B}$ and $\mathbf{B}'$ are LLL-reduced, we roughly expect $\frac{B_i}{B_{i+1}} \approx \frac{B'_i}{B'_{i+1}} \approx q^2$ for any $1 \leq i \leq n-1$ under GSA

Assumption 4. $E\left[\log(\delta(i)\right] \approx \log(\epsilon)$ with $\epsilon = \dfrac{1}{12}$

- We estimate $E\left[\delta(i)\right] \succeq E\left[\xi(i)^2\right] = \dfrac{1}{12}$

**Proposition: Expected Number $N$ of Swaps**

Under the above assumptions, the number $N$ of swaps in the LLL algorithm for $\mathbf{C}$ is roughly estimated as

$$N \approx \sum_{j=k}^{n-1} \log_\epsilon \left(\frac{B_j}{D_j}\right) + \log_\epsilon(R) \succeq \sum_{j=k}^{n-1} \log_\epsilon \left(\frac{B_j}{D_j}\right)$$

# Main Result: Gap between $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ and $\sum_{i=1}^{n} \|\mathbf{b}_i'^*\|^2$

We estimate ($\epsilon = 1/12$, $\delta = 0.99$, $B_j = \|\mathbf{b}_j^*\|^2$, $D_j = \sum_{i=j}^{n} \nu_i^2 \|\mathbf{b}_i^*\|^2$)

$$\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2 - \sum_{i=1}^{n} \|\mathbf{b}_i'^*\|^2 \succeq E(\mathbf{v}, k) + \frac{1-\delta}{12\delta \log(\epsilon)} \cdot \mathrm{vol}(\pi_k(L))^{2/(n-k)} \cdot \sum_{j=k}^{n-1} \log\left(\frac{B_j}{D_j}\right).$$

We expect that $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ could be strictly decreased if the right-hand side value is positive.

## Definition of Mutant Vectors

Given an LLL-reduced basis $\mathbf{B} = [\mathbf{b}_1, \ldots, \mathbf{b}_n]$ of $L$, let $\mathbf{v} = \sum_{i=1}^{n} \nu_i \mathbf{b}_i^* \in L$ with insertion index $k$, sampled by Schnorr's SA. Given a constant $c > 0$, we call $\mathbf{v}$ a *mutant vector with factor c* if

- $k < n - u$ ($u$: the constant of search space bound for SA), and
- $E(\mathbf{v}, k) > c \cdot \mathrm{vol}(\pi_k(L))^{2/(n-k)} \cdot \sum_{j=k}^{n-1} \log\left(\frac{B_j}{D_j}\right)$.

# Experimental Verification

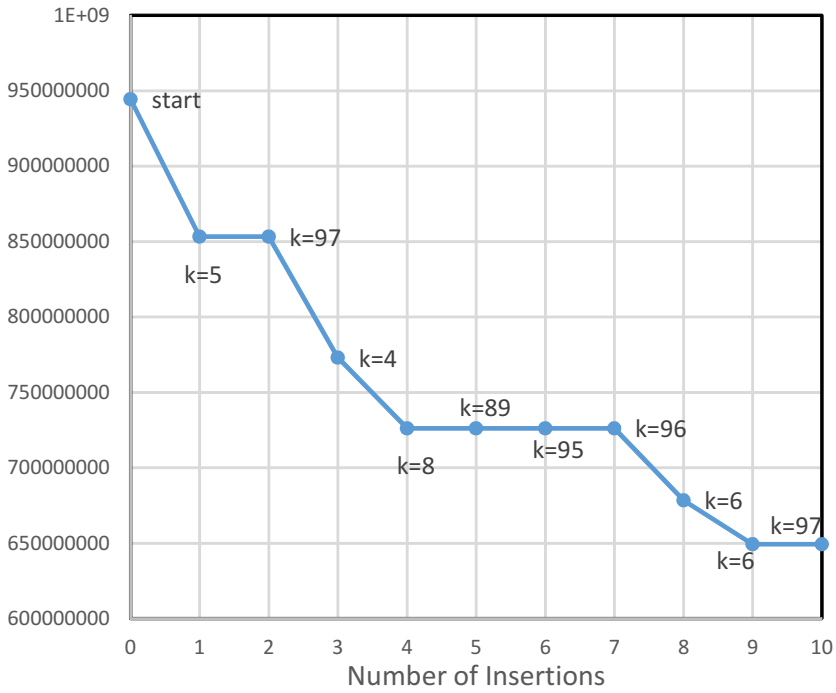
**Aim:** Verify that a mutant vector $\mathbf{v}$ can decrease $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$

**In our experiments:**

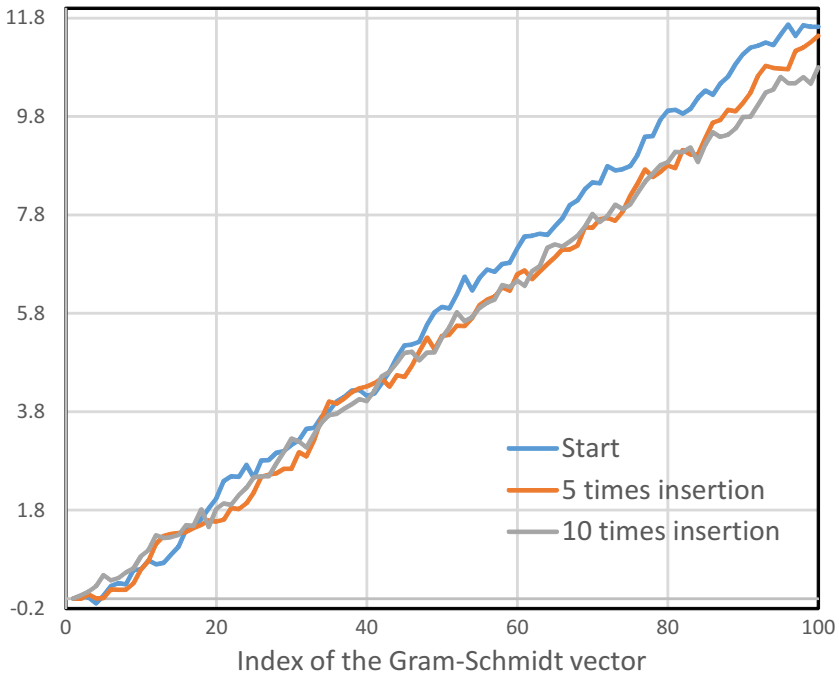
- We used Schnorr's SA with $u = 30$ to sample short vectors $\mathbf{v} \in L$
- PARI library for LLL with $\delta = 0.99$.
- We took $n = 100, 110$ and 120 from Darmstadt SVP challenge
- We set

$$c = 0.25 \quad (\text{resp. } c = 0.35)$$

for $n = 100$ (resp. $n = 110$ and 120). Note that these constants are determined by our experiments.

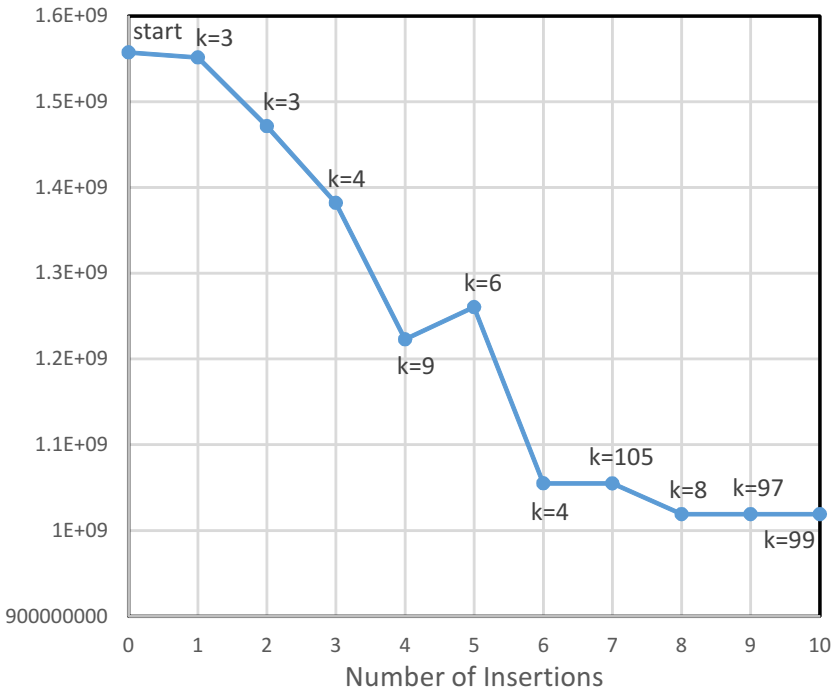



(a) Transition of $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$




(b) The value $\log_2(\|\mathbf{b}_1\|^2/\|\mathbf{b}_i^*\|^2)$

Figure: Transition of the sum $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ and the GSA behavior by insertion of mutant vectors in a lattice of dimension $n = 100$



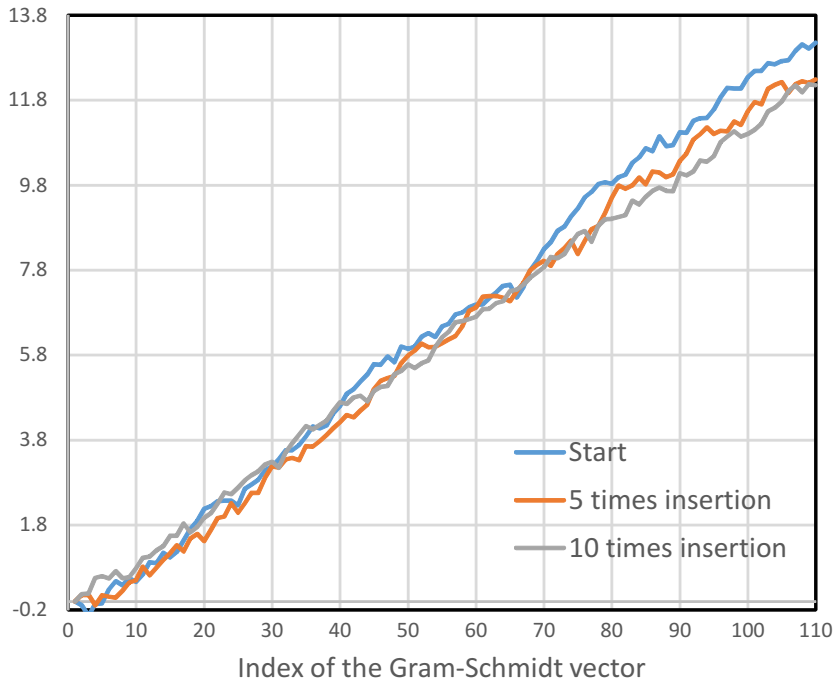
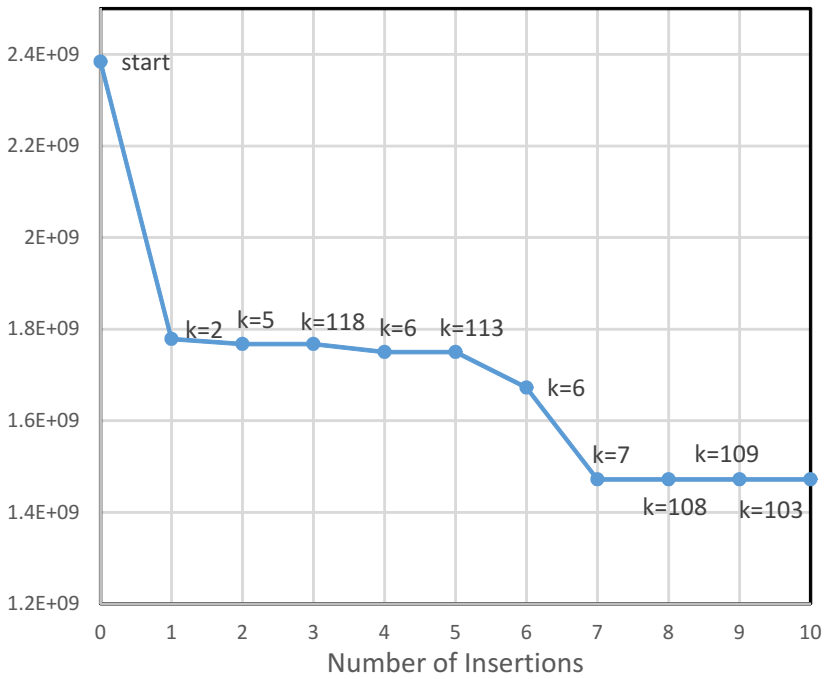




Figure: Same as Figure 1, but the lattice dimension $n = 110$



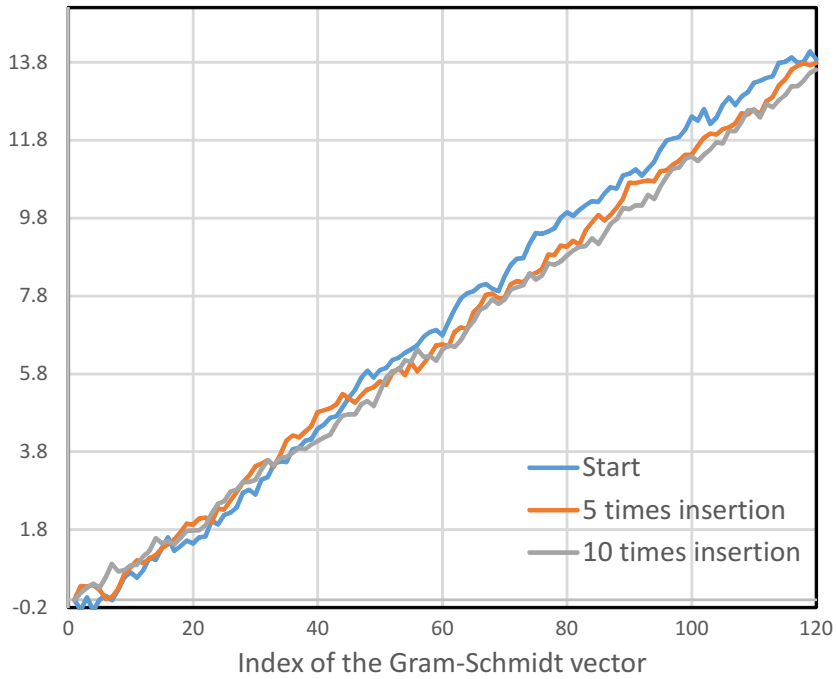




Figure: Same as Figure 1, but the lattice dimension $n = 120$

# Conclusion and Future Work

- This Work
  - We gave a heuristic but practical condition of $\mathbf{v} \in L$ (which we call a mutant vector) that $\sum_{i=1}^{n} \|\mathbf{b}_i^*\|^2$ is strictly decreased
- Future Work
  - Search and sample mutant vectors efficiently
  - Our analysis for LLL could be applied to analyze the behavior of BKZ in more details

# References


M. Ajtai, R. Kumar and D. Sivakumar,
"A sieve algorithm for the shortest lattice vector problem",
*Proceedings of the 33rd annual ACM symposium on Theory of computing–STOC 2001*, ACM, pp. 601–610, 2001.

J. Buchmann and C. Ludwig,
"Practical lattice basis sampling reduction",
*Algorithmic Number Theory–ANTS 2006*, Springer LNCS 4076, pp. 222–237, 2006.

M. Fukase and K. Kashiwabara,
An accelerated algorithm for solving SVP based on statistical analysis,
Journal of Information Processing, vol. **23**, no. 1, 1–15, 2015.

S.D. Galbraith,
Mathematics of public key cryptography,
Cambridge University Press, 2012.

N. Gama, P.Q. Nguyen and O. Regev,
"Lattice enumeration using extreme pruning",
*Advances in Cryptology–EUROCRYPT 2010*, Springer LNCS 6110, pp. 257–278, 2010.

A.K. Lenstra, H.W. Lenstra and L. Lovász,
Factoring polynomials with rational coefficients,
Mathematische Annalen, vol. **261**, no. 4, pp. 515–534, 1982.

C.P. Schnorr,
"Lattice reduction by random sampling and birthday methods",
STACS 2003, Springer LNCS 2606, pp. 145–156, 2003.

C.P. Schnorr and M. Euchner,
Lattice basis reduction: improved practical algorithms and solving subset sum problems,
Mathematical programming, vol. **66**, pp. 181–199, 1994.