Improving LLL algorithm for cryptanalysis

Zhenfei Zhang

School of Computer Science and Software Engineering
University of Wollongong

zz920@uowmail.edu.au

A Knapsack Problem

A Knapsack Problem

- $X_1, \ldots, X_d \in \mathbb{Z}$;
- $s_1, \ldots, s_d \in \mathbb{Z}_2$;
- $X = \sum_{i=1}^{d} s_i X_i$;
- Given $\{X_i\}$ and X, find s_i.

$$
\begin{array}{lll}
X = 1911310173 & & \\
X_1 = 437491759; & X_2 = 128552629; & X_3 = 972127522; \\
X_4 = 711069765; & X_5 = 125617110; & X_6 = 812891076; \\
X_7 = 44057509; & X_8 = 376073782; & X_9 = 340284326;
\end{array}
$$

Solving a Knapsack Problem using LLL

$X = 1911310173$
$X_1 = 437491759$; $X_2 = 128552629$; $X_3 = 972127522$;
$X_4 = 711069765$; $X_5 = 125617110$; $X_6 = 812891076$;
$X_7 = 44057509$; $X_8 = 376073782$; $X_9 = 340284326$;

$$\mathcal{B} = \begin{pmatrix} 1911310173 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 437491759 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 128552629 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 972127522 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 711069765 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 125617110 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 812891076 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 44057509 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 376073782 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 340284326 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Solving a Knapsack Problem using LLL

$X = 1911310173 \quad = X_1 + X_3 + X_5 + X_8$

$X_1 = 437491759$; $X_2 = 128552629$; $X_3 = 972127522$;

$X_4 = 711069765$; $X_5 = 125617110$; $X_6 = 812891076$;

$X_7 = 44057509$; $X_8 = 376073782$; $X_9 = 340284326$;

$$\mathrm{LLL}(\mathcal{B}) = \begin{pmatrix} 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 5 & -3 & -1 & 1 & 0 & 0 & 3 & 1 & 3 & 2 \\ -1 & -5 & 4 & 5 & -1 & 4 & 1 & 0 & -5 & 0 \\ 3 & -4 & 3 & 2 & -4 & 3 & -6 & 4 & -1 & -2 \\ 1 & 2 & -1 & 1 & 7 & 4 & 4 & 3 & -6 & -2 \\ -1 & -4 & -4 & -5 & 3 & 3 & -5 & 1 & 5 & 3 \\ -3 & 1 & -4 & 7 & 5 & -6 & 1 & 3 & -3 & -5 \\ 8 & -1 & 5 & -1 & 4 & 1 & -3 & -4 & 2 & -1 \\ 4 & 2 & 4 & 4 & 4 & -6 & -4 & 5 & 1 & 3 \\ 3 & 2 & -6 & 1 & -2 & 4 & 1 & -4 & -9 & 2 \end{pmatrix}$$

Cryptanalysis using Lattice Reduction

Problems:

- Shortest Vector problem;
- Closest Vector problem;
- Knapsack Problem;
- Factorization;
- Bounded Distance Decoding Problem;
- Learning with Error problem;
- Approximate Greatest Common Divisor Problem;
- ...

Practicality:

- Some are solvable in Poly time (Gentry-Halevi's FHE challange)
- But time consuming (45 years, small challange, Chen and Nguyen)

LLL

LLL in $\mathbb{Z}^1$ (Greatest Common Divisor)

$$\mathbf{B} = \begin{pmatrix} 18 \\ 51 \end{pmatrix}$$

- Define $\mu = \frac{b_1 \cdot b_2}{b_1 \cdot b_1} = \frac{17}{6}$;
- If $|\mu| > 0.5$, let $b_2 = b_2 - \lfloor \mu \rceil b_1 = 51 - 3 \times 18 = -3$;
- If $b_2 < b_1$, swap b_1 and b_2;
- Else, terminate.

LLL

LLL in $\mathbb{Z}^1$ (Greatest Common Divisor)

$$\mathbf{B} = \begin{pmatrix} -3 \\ 18 \end{pmatrix}$$

- Define $\mu = \frac{b_1 \cdot b_2}{b_1 \cdot b_1} = -6$;
- If $|\mu| > 0.5$, let $b_2 = b_2 - \lfloor \mu \rceil b_1 = 18 - 3 \times 6 = 0$;
- If $b_2 < b_1$, swap b_1 and b_2;
- Else, terminate.

LLL in $\mathbb{Z}^1$ (Greatest Common Divisor)

$$\mathbf{B} = \begin{pmatrix} 0 \\ -3 \end{pmatrix}$$

- Define $\mu = \frac{b_1 \cdot b_2}{b_1 \cdot b_1} = 0$;
- If $|\mu| > 0.5$, let $b_2 = b_2 - \lfloor \mu \rceil b_1 = -3$;
- If $b_2 < b_1$, swap b_1 and b_2;
- Else, terminate.

LLL

LLL in $\mathbb{Z}^2$ (Gauss reduction)

$$\mathbf{B} = \begin{pmatrix} 18 & 1 \\ 51 & 2 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = \frac{184}{65}$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1 = \mathbf{b}_2 - 3\mathbf{b}_1 = (-3, -1)$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

LLL in $\mathbb{Z}^2$ (Gauss reduction)

$$\mathbf{B} = \begin{pmatrix} -3 & -1 \\ 18 & 1 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = -\frac{11}{2}$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1 = \mathbf{b}_2 - (-6)\mathbf{b}_1 = (0, -5)$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

LLL

LLL in $\mathbb{Z}^2$ (Gauss reduction)

$$\mathbf{B} = \begin{pmatrix} -3 & -1 \\ 0 & -5 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = -\frac{1}{2}$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

LLL

LLL in $\mathbb{Z}^4$

$$\mathbf{B} = \begin{pmatrix} 855401 & 0 & 0 & 0 \\ 328161 & 1 & 0 & 0 \\ 211573 & 0 & 1 & 0 \\ 325714 & 0 & 0 & 1 \end{pmatrix}$$

- Gauss-reduce the first two vectors;

LLL

LLL in $\mathbb{Z}^4$

$$\mathbf{B} = \left(\begin{array}{cccc} 855401 & 0 & 0 & 0 \\ 328161 & 1 & 0 & 0 \\ \hline 211573 & 0 & 1 & 0 \\ 325714 & 0 & 0 & 1 \end{array}\right)$$

- Gauss-reduce the first two vectors;

LLL

LLL in $\mathbb{Z}^4$

$$\mathbf{B} = \left(\begin{array}{cccc} -801 & -309 & 0 & 0 \\ -260 & 941 & 0 & 0 \\ \hline 211573 & 0 & 1 & 0 \\ 325714 & 0 & 0 & 1 \end{array}\right)$$

- Gauss-reduce the first two vectors;

LLL

LLL in $\mathbb{Z}^4$

$$\mathbf{B} = \left(\begin{array}{cccc} -801 & -309 & 0 & 0 \\ -260 & 941 & 0 & 0 \\ 211573 & 0 & 1 & 0 \\ \hline 325714 & 0 & 0 & 1 \end{array}\right)$$

- Every pair of first three vectors are Gauss-reduced;

LLL

LLL in $\mathbb{Z}^4$

$$\mathbf{B} = \left(\begin{array}{cccc} -26 & -12 & 55 & 0 \\ 68 & 53 & 31 & 0 \\ 59 & -146 & -4 & 0 \\ \hline 325714 & 0 & 0 & 1 \end{array}\right)$$

- Every pair of first three vectors are Gauss-reduced;

LLL

LLL in $\mathbb{Z}^4$

$$\mathbf{B} = \begin{pmatrix} 15 & 18 & 10 & 20 \\ -20 & 15 & 18 & 10 \\ -10 & -20 & 15 & 18 \\ -18 & -10 & -20 & 15 \end{pmatrix}$$

- Finally, every pair of vectors are Gauss-reduced.

LLL

LLL in $\mathbb{Z}^4$

$$\begin{pmatrix} 855401 & 0 & 0 & 0 \\ 328161 & 1 & 0 & 0 \\ 211573 & 0 & 1 & 0 \\ 325714 & 0 & 0 & 1 \end{pmatrix} \longrightarrow \begin{pmatrix} 15 & 18 & 10 & 20 \\ -20 & 15 & 18 & 10 \\ -10 & -20 & 15 & 18 \\ -18 & -10 & -20 & 15 \end{pmatrix}$$

- Let n be the dimension, and β be maximum bit length of coefficients
- i.e., $n = 4$, $\beta = \log_2 855401 \sim 16.4$
- Requires $O(n^2)$ Gauss reduction
- Each Gauss reduction need $O(\beta^2 n^4)$ operations.
- Total cost $O(n^6 \beta^3)$

Example of an LLL reduction

$$\begin{pmatrix} 83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 73193167 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of an LLL reduction

$$\begin{pmatrix} 83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 73193167 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc} 83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -9897250 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\
-18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\
-18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\
67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\begin{pmatrix} 587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\ -18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1643 & -690 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\
195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\
-440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\
\hline
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\
195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\
-440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hline
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\
195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\
-440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\
75 & -202 & 48 & 1 & 0 & 0 & 0 & 0 \\
\hline
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc} -89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\ -83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\ -42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\ -3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\ \hline 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Example of an LLL reduction

$$\begin{pmatrix} -89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\ -83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\ -42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\ -3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ \hline 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
-89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\
-83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\
-42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\
-3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\
-2 & 26 & -34 & 7 & 1 & 0 & 0 & 0 \\
\hline
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
-24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\
23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\
-26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\
9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\
5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\
\hline
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
-24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\
23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\
-26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\
9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\
5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
-24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\
23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\
-26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\
9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\
5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\
1 & 6 & 10 & -25 & -19 & 1 & 0 & 0 \\
\hline
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$
\left(\begin{array}{cccccccc}
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\
-2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\
5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\
7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\
5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\
\hline
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Example of an LLL reduction

$$
\left(\begin{array}{cccccccc}
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\
-2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\
5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\
7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\
5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
\hline
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc} 6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\ -12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\ -2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\ 5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\ 7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\ 5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\ 3 & 2 & -5 & -1 & 1 & -13 & 1 & 0 \\ \hline 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Example of an LLL reduction

$$\left(\begin{array}{cccccccc}
-6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\
-6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\
-6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\
-2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\
4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\
\hline
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of an LLL reduction

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\ -3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\ -6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\ -6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\ -2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\ 4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of an LLL reduction

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\ -3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\ -6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\ -6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\ -2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\ 4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\ 7 & 2 & 1 & -4 & 0 & -6 & 3 & 1 \end{pmatrix}$$

Example of an LLL reduction

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 4 & 0 & 6 & -3 & -1 & 7 & 2 & 1 \\ -7 & -2 & -1 & 4 & 0 & 6 & -3 & -1 \\ -1 & 4 & 0 & 6 & -3 & -1 & 7 & 2 \\ 7 & 5 & -9 & -1 & 1 & -1 & -7 & -2 \\ 4 & 4 & -2 & 1 & 2 & -5 & -7 & -8 \\ 1 & 6 & 0 & 6 & 3 & 8 & -2 & 7 \\ 0 & 6 & -3 & -1 & 7 & 2 & 1 & -4 \end{pmatrix}$$

Improving floating point precisions

LLL using floating point

LLL using floating point

$$\mathbf{B} = \begin{pmatrix} 18 & 1 \\ 51 & 2 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = \frac{184}{65} \sim 2.8$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1 = \mathbf{b}_2 - 3\mathbf{b}_1 = (-3, -1)$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

LLL using floating point

LLL using floating point

$$\mathbf{B} = \begin{pmatrix} 18 & 1 \\ 51 & 2 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = \frac{184}{65} = \frac{1011\ 1000}{0100\ 0001} \sim 2.8$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1 = \mathbf{b}_2 - 3\mathbf{b}_1 = (-3, -1)$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

The error in the *fp* will not effect μ if the precision is $\mathcal{O}(1.6d) \sim 4$

LLL using floating point

$$\mathbf{B} = \begin{pmatrix} 18 & 1 \\ 51 & 2 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = \frac{184}{65} \sim \frac{1011\ 0000}{0100\ 0000} = 2.75$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1 = \mathbf{b}_2 - 3\mathbf{b}_1 = (-3, -1)$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

The error in the *fp* will not effect μ if the precision is $\mathcal{O}(1.6d) \sim 4$

LLL using floating point

$$\mathbf{B} = \begin{pmatrix} -3 & -1 \\ 18 & 1 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = -\frac{11}{2} = -5.5$;
- If $|\mu| > 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1 = \mathbf{b}_2 - (-6)\mathbf{b}_1 = (0, -5)$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

LLL using floating point

LLL using floating point

$$\mathbf{B} = \begin{pmatrix} -3 & -1 \\ 0 & -5 \end{pmatrix}$$

- Define $\mu = \frac{\mathbf{b}_1 \cdot \mathbf{b}_2}{\mathbf{b}_1 \cdot \mathbf{b}_1} = -\frac{1}{2} = -0.5$;
- If $|\mu| \leq 0.5$, let $\mathbf{b}_2 = \mathbf{b}_2 - \lfloor \mu \rceil \mathbf{b}_1$;
- If $|\mathbf{b}_2| < |\mathbf{b}_1|$, swap $\mathbf{b}_1$ and $\mathbf{b}_2$;
- Else, terminate.

$$\mathcal{B} = \begin{pmatrix} 1911310173 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 437491759 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 128552629 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 972127522 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 711069765 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 125617110 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 812891076 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 44057509 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 376073782 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 340284326 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- To process first two vectors;
- Precision used $1.6d = 16$;
- Required precision $1.6 * 2 \sim 4$

$$\mathcal{B} = \begin{pmatrix} -14345 & 40372 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -36529 & -30433 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 128552629 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 972127522 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 711069765 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 125617110 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 812891076 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 44057509 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 376073782 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 340284326 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- To process first two vectors;
- Precision used $1.6d = 16$;
- Required precision $1.6 * 2 \sim 4$

$$\mathcal{B} = \begin{pmatrix} -521 & 289 & 34 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ -399 & -551 & 105 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 781 & 594 & 4594 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 972127522 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 711069765 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 125617110 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 812891076 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 44057509 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 376073782 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 340284326 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- To process first three vectors;
- Precision used $1.6d = 16$;
- Required precision $1.6 * 4 \sim 5$

Adaptive Precision Floating Point LLL

LLL using Adaptive floating point

- The cost of *fplll* depends largely on the precision (ℓ);
  - $(d^3\beta^2 + d^4\beta)\mathcal{M}(\ell)$
  - $\mathcal{M}(\cdot)$ is the multiplication cost of two integers
  - $\|\mathbf{b}_i\| \leq 2^\beta$
- The original *fplll* uses a fixed precision $\ell \sim 1.6d$;
- One needs $1.6k$ for $(\mathbf{b}_1, \ldots, \mathbf{b}_k)$ for k from 2 to d;
- Increase the precision with regards to #vectors;
- The reduction is accelerated.

Adaptive Precision Floating Point LLL

Complexity

- The cost of *Adp-fplll*:
  - $\sum_{i=2}^{d} d^2\beta(1+\frac{\beta}{i})\mathcal{M}(i) = \frac{1}{2}d^4\beta^2 + \frac{1}{6}d^5\beta$;
  - Compared with $d^4\beta^2 + d^5\beta$ for *fplll*;
- One need to re-generate μ (a.k.a. GSO) due to the change of precision;
  - Incur a cost of $\mathcal{O}(d^5\beta)$ in worst-cases;
- In theory, the advantage is $0 \sim 50\%$.

Adaptive Precision Floating Point LLL

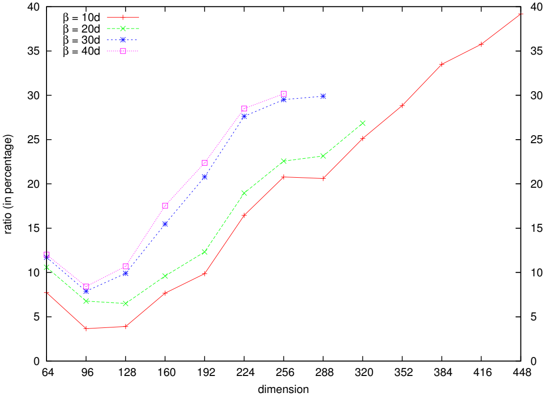


Figure: Apt-fplll vs fplll

Recursive Reduction

Recursive Reduction

$$\mathcal{B} = \begin{pmatrix} 69069346 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 23286381 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 21463395 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 57272001 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 17637855 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 21407089 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 7776123 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 29209763 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

- Recall that the complexity depends on d and β
- $d = 8$
- $\beta = \log_2 69069346 \sim 26$

Recursive Reduction

$$\mathcal{B} = \left(\begin{array}{cccccccc}
69069346 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
23286381 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
21463395 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
57272001 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
\hline
17637855 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
21407089 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
\hline
7776123 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
29209763 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

- Recursive reduction step 1
- $d = 2$
- $\beta = \log_2 69069346 \sim 26$

Recursive Reduction

$$\mathcal{B} = \left(\begin{array}{cccccccc}
-2711 & 3353 & 0 & 0 & 0 & 0 & 0 & 0 \\
-13730 & -8496 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
-741 & 0 & 2631 & -986 & 0 & 0 & 0 & 0 \\
-20583 & 0 & -4208 & 1577 & 0 & 0 & 0 & 0 \\
\hline
-843 & 0 & 0 & 0 & -1187 & 978 & 0 & 0 \\
13505 & 0 & 0 & 0 & -6378 & 5255 & 0 & 0 \\
\hline
-3980 & 0 & 0 & 0 & 0 & 0 & 3407 & -907 \\
3729 & 0 & 0 & 0 & 0 & 0 & 4147 & -1104
\end{array}\right)$$

- Recursive reduction step 1
- $d = 2$
- $\beta = \log_2 69069346 \sim 26$

Recursive Reduction

$$\mathcal{B} = \left(\begin{array}{cccccccc} -2711 & 3353 & 0 & 0 & 0 & 0 & 0 & 0 \\ -13730 & -8496 & 0 & 0 & 0 & 0 & 0 & 0 \\ -741 & 0 & 2631 & -986 & 0 & 0 & 0 & 0 \\ -20583 & 0 & -4208 & 1577 & 0 & 0 & 0 & 0 \\ \hline -843 & 0 & 0 & 0 & -1187 & 978 & 0 & 0 \\ 13505 & 0 & 0 & 0 & -6378 & 5255 & 0 & 0 \\ -3980 & 0 & 0 & 0 & 0 & 0 & 3407 & -907 \\ 3729 & 0 & 0 & 0 & 0 & 0 & 4147 & -1104 \end{array}\right)$$

- Recursive reduction step 2
- $d = 4$
- $\beta = \log_2 20583 \sim 14$

Recursive Reduction

$$\mathcal{B} = \left(\begin{array}{cccccccc} -8 & -47 & -10 & -29 & 0 & 0 & 0 & 0 \\ 59 & 52 & 51 & -4 & 0 & 0 & 0 & 0 \\ 22 & -50 & -17 & 87 & 0 & 0 & 0 & 0 \\ 75 & 40 & -120 & 7 & 0 & 0 & 0 & 0 \\ \hline -52 & 0 & 0 & 0 & -20 & -13 & -9 & 24 \\ 19 & 0 & 0 & 0 & -17 & -36 & 40 & 26 \\ 9 & 0 & 0 & 0 & -26 & -19 & -54 & 44 \\ 26 & 0 & 0 & 0 & -112 & 88 & -7 & 5 \end{array}\right)$$

- Recursive reduction step 2
- $d = 4$
- $\beta = \log_2 20583 \sim 14$

Recursive Reduction

$$\mathcal{B} = \begin{pmatrix} -8 & -47 & -10 & -29 & 0 & 0 & 0 & 0 \\ 59 & 52 & 51 & -4 & 0 & 0 & 0 & 0 \\ 22 & -50 & -17 & 87 & 0 & 0 & 0 & 0 \\ 75 & 40 & -120 & 7 & 0 & 0 & 0 & 0 \\ -52 & 0 & 0 & 0 & -20 & -13 & -9 & 24 \\ 19 & 0 & 0 & 0 & -17 & -36 & 40 & 26 \\ 9 & 0 & 0 & 0 & -26 & -19 & -54 & 44 \\ 26 & 0 & 0 & 0 & -112 & 88 & -7 & 5 \end{pmatrix}$$

- Recursive reduction step 3
- $d = 8$
- $\beta = \log_2 120 \sim 7$

Recursive Reduction

Complexity

- New complexity: $O(d^4\beta + d^2\beta^2)$
- Compare with L^2: $O(d^4\beta + d^3\beta^2)$

Analyze Gentry-Halevi's Fully homomorphic encryption scheme

- $d = 2^{11}$, $\beta \sim 2^{19.5}$
- Complexity for L^2: $(2^{11})^4(2^{19.5}) + (2^{11})^3(2^{19.5})^2 \sim 2^{72}$
- Our complexity: $(2^{11})^4(2^{19.5}) + (2^{11})^2(2^{19.5})^2 \sim 2^{63.5}$

Adaptive Precision Floating Point LLL

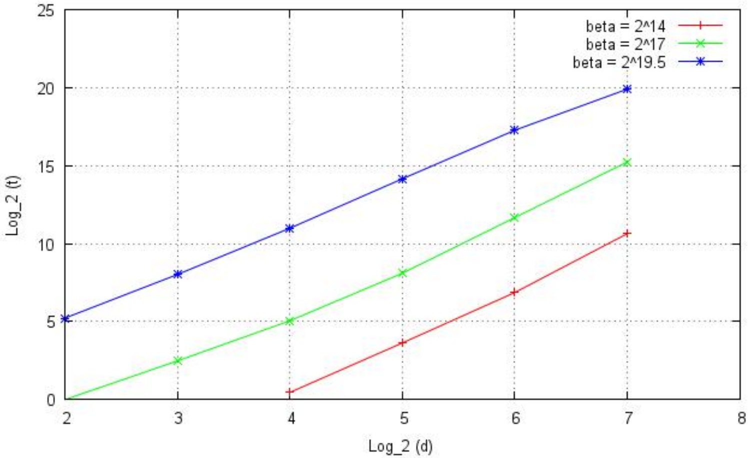


Figure: Implementation results

Recursive Reduction

Ideal Lattice

A basis of ideal lattice

$$\begin{pmatrix} v_1 & v_2 & v_3 & \dots & v_d \\ -v_d & v_1 & v_2 & \dots & v_{d-1} \\ -v_{d-1} & -v_n & v_1 & \dots & v_{d-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -v_2 & -v_3 & -v_4 & \dots & v_1 \end{pmatrix} \quad \begin{pmatrix} 15 & 18 & 10 & 20 \\ -20 & 15 & 18 & 10 \\ -10 & -20 & 15 & 18 \\ -18 & -10 & -20 & 15 \end{pmatrix}$$

Principal Ideal Lattice

A principal ideal lattice

$\mathcal{L}$ is generated by only one element and a determinant

$$\begin{pmatrix} p & 0 & 0 & \dots & 0 & 0 \\ -\alpha & 1 & 0 & \dots & 0 & 0 \\ -\alpha^2 & & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ -\alpha^{\deg g - 1} & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 855401 & 0 & 0 & 0 \\ 328161 & 1 & 0 & 0 \\ 211573 & 0 & 1 & 0 \\ 325714 & 0 & 0 & 1 \end{pmatrix}$$

Example of iLLL

$$\begin{pmatrix} 83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 73193167 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of iLLL

$$
\begin{pmatrix}
\begin{array}{cccccccc}
83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
73193167 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}
\end{pmatrix}
$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-9897250 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
67400468 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$
\left(\begin{array}{cccccccc}
83090417 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
-9897250 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & -9897250 & 1 & 0 & 0 & 0 & 0 & 0 \\
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Example of iLLL

$$\left(\begin{array}{cccccccc} 587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\ -18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\ \hline 0 & -9897250 & 1 & 0 & 0 & 0 & 0 & 0 \\ 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\
-18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & -9897250 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\begin{pmatrix} 587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\ -18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\ -1643 & -690 & 1 & 0 & 0 & 0 & 0 & 0 \\ \hline 229382 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
587 & 4290 & 0 & 0 & 0 & 0 & 0 & 0 \\
-18732 & 4651 & 0 & 0 & 0 & 0 & 0 & 0 \\
-1643 & -690 & 1 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & -1643 & -690 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\
195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\
-440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\
\hline
0 & -1643 & -690 & 1 & 0 & 0 & 0 & 0 \\
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\
195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\
-440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\
0 & -1643 & -690 & 1 & 0 & 0 & 0 & 0 \\
\hline
54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc} 142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\ 195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\ -440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\ 75 & -202 & 48 & 1 & 0 & 0 & 0 & 0 \\ \hline 54626226 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
142 & 230 & 125 & 0 & 0 & 0 & 0 & 0 \\
195 & -352 & 275 & 0 & 0 & 0 & 0 & 0 \\
-440 & -61 & 388 & 0 & 0 & 0 & 0 & 0 \\
75 & -202 & 48 & 1 & 0 & 0 & 0 & 0 \\
\hline
0 & 75 & -202 & 48 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
-89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\
-83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\
-42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\
-3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\
\hline
0 & 75 & -202 & 48 & 1 & 0 & 0 & 0 \\
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
-89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\
-83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\
-42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\
-3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\
0 & 75 & -202 & 48 & 1 & 0 & 0 & 0 \\
\hline
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
-89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\
-83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\
-42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\
-3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\
-2 & 26 & -34 & 7 & 1 & 0 & 0 & 0 \\
\hline
13559580 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
-89 & -35 & -36 & 12 & 0 & 0 & 0 & 0 \\
-83 & 59 & 42 & -15 & 0 & 0 & 0 & 0 \\
-42 & 66 & -25 & 51 & 0 & 0 & 0 & 0 \\
-3 & 24 & 76 & 76 & 0 & 0 & 0 & 0 \\
-2 & 26 & -34 & 7 & 1 & 0 & 0 & 0 \\
\hline
0 & -2 & 26 & -34 & 7 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
-24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\
23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\
-26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\
9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\
5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\
\hline
0 & -2 & 26 & -34 & 7 & 1 & 0 & 0 \\
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$
\left(\begin{array}{cccccccc}
-24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\
23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\
-26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\
9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\
5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\
0 & -2 & 26 & -34 & 7 & 1 & 0 & 0 \\
\hline
63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)
$$

Example of iLLL

$$\begin{pmatrix} -24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\ 23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\ -26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\ 9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\ 5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\ 1 & 6 & 10 & -25 & -19 & 1 & 0 & 0 \\ \hline 63222454 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
-24 & -10 & 20 & -6 & 7 & 0 & 0 & 0 \\
23 & 2 & -4 & -3 & 19 & 0 & 0 & 0 \\
-26 & 16 & -14 & 1 & 8 & 0 & 0 & 0 \\
9 & 26 & 19 & 40 & 10 & 0 & 0 & 0 \\
5 & 39 & -7 & -47 & -13 & 0 & 0 & 0 \\
1 & 6 & 10 & -25 & -19 & 1 & 0 & 0 \\
\hline
0 & 1 & 6 & 10 & -25 & -19 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\
-2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\
5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\
7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\
5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\
\hline
0 & 1 & 6 & 10 & -25 & -19 & 1 & 0 \\
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\
-2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\
5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\
7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\
5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\
0 & 1 & 6 & 10 & -25 & -19 & 1 & 0 \\
\hline
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\
-2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\
5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\
7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\
5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\
3 & 2 & -5 & -1 & 1 & -13 & 1 & 0 \\
\hline
11182519 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{array}\right)$$

Example of iLLL

$$\left(\begin{array}{cccccccc}
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-12 & 8 & 2 & 4 & 3 & -4 & 0 & 0 \\
-2 & 0 & -18 & -7 & 2 & 8 & 0 & 0 \\
5 & 1 & 7 & -4 & 24 & -2 & 0 & 0 \\
7 & 15 & 1 & -20 & -21 & -1 & 0 & 0 \\
5 & 0 & -1 & 12 & 15 & 24 & 0 & 0 \\
3 & 2 & -5 & -1 & 1 & -13 & 1 & 0 \\
\hline
0 & 3 & 2 & -5 & -1 & 1 & -13 & 1
\end{array}\right)$$

Example of iLLL

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\ -3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\ -6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\ -6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\ -2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\ 4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\ \hline 0 & 3 & 2 & -5 & -1 & 1 & -13 & 1 \end{pmatrix}$$

Example of iLLL

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\ -3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\ -6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\ -6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\ -2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\ 4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\ 0 & 3 & 2 & -5 & -1 & 1 & -13 & 1 \end{pmatrix}$$

Example of iLLL

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\ -3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\ -6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\ -6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\ -2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\ 4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\ 7 & 2 & 1 & -4 & 0 & -6 & 3 & 1 \end{pmatrix}$$

Example of iLLL

$$\begin{pmatrix}
-6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\
6 & 9 & -9 & 5 & -2 & -2 & 0 & 0 \\
-3 & -2 & 5 & 1 & -1 & 13 & -1 & 0 \\
-6 & 5 & 1 & 11 & 5 & -3 & -4 & 0 \\
-6 & -3 & -8 & 2 & -7 & 1 & 6 & 0 \\
-2 & -12 & -10 & -5 & 6 & 11 & -4 & 0 \\
4 & -3 & 4 & 2 & 0 & 6 & 15 & 0 \\
7 & 2 & 1 & -4 & 0 & -6 & 3 & 1
\end{pmatrix}$$

Example of iLLL

$$\begin{pmatrix} -6 & 3 & 1 & -7 & -2 & -1 & 4 & 0 \\ 4 & 0 & 6 & -3 & -1 & 7 & 2 & 1 \\ -7 & -2 & -1 & 4 & 0 & 6 & -3 & -1 \\ -1 & 4 & 0 & 6 & -3 & -1 & 7 & 2 \\ 7 & 5 & -9 & -1 & 1 & -1 & -7 & -2 \\ 4 & 4 & -2 & 1 & 2 & -5 & -7 & -8 \\ 1 & 6 & 0 & 6 & 3 & 8 & -2 & 7 \\ 0 & 6 & -3 & -1 & 7 & 2 & 1 & -4 \end{pmatrix}$$

Why Better?

At least not worth

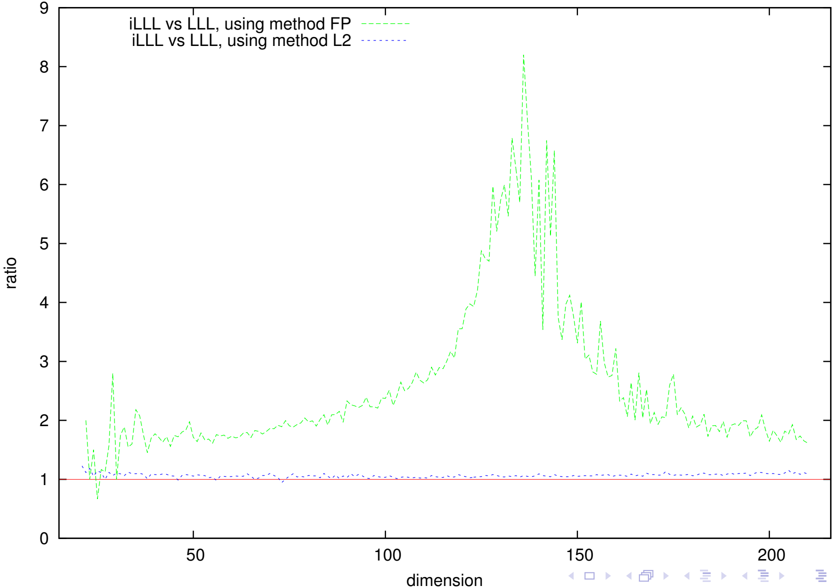
- iLLL has the same time complexity.
- iLLL returns same basis that LLL with an overwhelming probability

$$\left(1-2\left(\frac{\eta-0.5}{\eta}\right)^2\right)^{\frac{(d-1)d}{2}}.$$

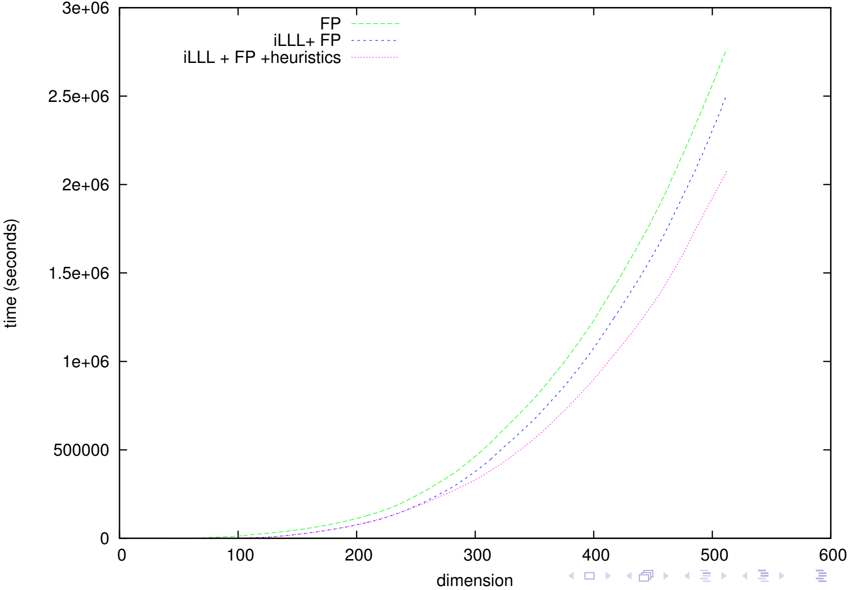
In average better

- From $O(d^{4+\epsilon}\beta+d^{3+\epsilon}\beta^2)$ to $O(d^{4+\epsilon}\beta+d^{2+\epsilon}\beta^2)$.
- In average Gauss-reduction uses less floating point precision.

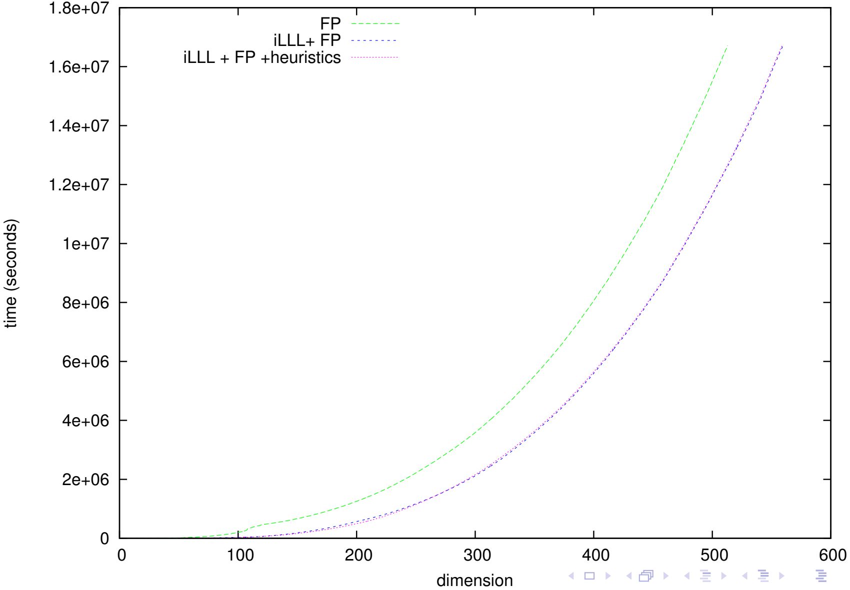
Practical Test: $det = 2^{10d}$.



Practical Test: Gentry-Halevi's Toy Challenge.



Practical Test: Gentry-Halevi's Small Challenge.



conclusion

Theoretical Results

Algorithms	Time Complexity	
LLL	$O(d^{5+\varepsilon}\beta^{2+\varepsilon})$	Classic Result
L^2	$O(d^{3+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$	Best in Practice
Ap-fplll	$O(d^{3+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$	Better Practical Result
Rec-Red	$O(d^{2+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$	Better Theoretical Bound
iLLL	$O(d^{2+\varepsilon}\beta^2 + d^{4+\varepsilon}\beta)$	Theory and Practice

Table: Comparison of time complexity

conclusion

Practical Results

Gentry-Halevi's Challenge	dim 512	dim 2048
Previous Best Results/Prediction	30 days	45 years
LLL implementation @2.66GHz	32 days	25.8 years
iLLL implementation @2.66GHz	24 days	23.6 years
iLLL prediction @4.0GHz	16 days	15.7 years

Table: Practical Result on Gentry Halevi's Challenge

Papers

- **Adaptive Precision Floating Point LLL**
- **Lattice Reduction for Modular Knapsack**
- **LLL for Ideal Lattice**