SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Proofs of Lemmas in Error Estimation of Practical Convolution Discrete Gaussian Sampling with Rejection Sampling

Zhongxiang Zheng[1], Xiaoyun Wang[2,3*], Guangwu Xu[4] & Chunhuan Zhao[2]

[1]*Department of Computer Science and Technology, Tsinghua University, Beijing* 100084*, China ;*
[2]*Institute for Advanced Study, Tsinghua University, Beijing* 100084*, China ;*
[3]*Key Laboratory of Cryptologic Technology and Information Security, Ministry of Education, Shandong Universtiy, Jinan* 250100*, China;*
[4]*Department of Electrical Engineering and Computer Sciences, University of Wisconsin, Milwaukee, WI* 53201*, USA*

Appendix A Proof of Lemma 1

Lemma 1. Let s, t be positive numbers such that $ts \geqslant 1$ and $c \in [0, 1)$. We have

1.
$$\sum_{\substack{k\in\mathbb{Z}\\ |k-c|\geqslant ts}} \rho_s(k-c) \leqslant 2e^{-\pi t^2}\left(1+\frac{e^{-\frac{2\pi t}{s}}}{2}(\rho_s(\mathbb{Z})-1)\right). \tag{A1}$$

2. If $s \geqslant \eta_\varepsilon(\mathbb{Z})$, then
$$\sum_{\substack{x\in\mathbb{Z}\\ |x-c|\geqslant t\cdot s}} Pr_{x\leftarrow D_{\mathbb{Z},c,s}}(x) \leqslant 2e^{-\pi t^2}\cdot\frac{1+\varepsilon}{1-\varepsilon}\left(\frac{1+\frac{e^{-\frac{2\pi t}{s}}}{2}(\rho_s(\mathbb{Z})-1)}{\rho_s(\mathbb{Z})}\right). \tag{A2}$$

Proof. Note that

$$\begin{aligned}\sum_{\substack{k\in\mathbb{Z}\\ |k-c|\geqslant ts}} \rho_s(k-c) &= e^{-\pi t^2}\sum_{\substack{k\in\mathbb{Z}\\ |k-c|\geqslant ts}} e^{-\pi\frac{(k-c)^2-s^2t^2}{s^2}}\\ &= e^{-\pi t^2}\sum_{k\geqslant c+ts} e^{-\frac{\pi}{s^2}(|k-c|-ts)(|k-c|+ts)}\\ &\quad + e^{-\pi t^2}\sum_{k\leqslant c-ts} e^{-\frac{\pi}{s^2}(|k-c|-ts)(|k-c|+ts)}.\end{aligned}$$

Since

$$\begin{aligned}\sum_{k\geqslant c+ts} e^{-\frac{\pi}{s^2}(|k-c|-ts)(|k-c|+ts)} &= \sum_{k\geqslant\lceil c+ts\rceil} e^{-\frac{\pi}{s^2}(k-(c+ts))^2}e^{-\frac{2\pi}{s}(k-(c+ts))t}\\ &\leqslant 1+e^{-\frac{2\pi t}{s}}\sum_{k=\lceil c+ts\rceil+1}^{\infty} e^{-\frac{\pi}{s^2}(k-(c+ts))^2}\\ &\leqslant 1+e^{-\frac{2\pi t}{s}}\sum_{k=1}^{\infty} e^{-\pi\frac{k^2}{s^2}},\end{aligned}$$

and

$$\sum_{k\leqslant c-ts} e^{-\frac{\pi}{s^2}(|k-c|-ts)(|k-c|+ts)} \leqslant \sum_{k\leqslant\lfloor c-ts\rfloor} e^{-\frac{\pi}{s^2}(k-(c-ts))^2}e^{-\frac{2\pi}{s}|k-(c-ts)|t}$$

* Corresponding author (email: xiaoyunwang@mail.tsinghua.edu.cn)

$$\leqslant 1+e^{-\frac{2\pi t}{s}}\sum_{k=\lfloor c-ts\rfloor-1}^{-\infty}e^{-\frac{\pi}{s^2}(k-(c-ts))^2}$$
$$\leqslant 1+e^{-\frac{2\pi t}{s}}\sum_{k=-1}^{-\infty}e^{-\pi\frac{k^2}{s^2}}.$$

So we get an improved Banaszczyk bound

$$\sum_{|k-c|\geqslant ts}\rho_s(k-c)\leqslant 2e^{-\pi t^2}\left(1+\frac{e^{-\frac{2\pi t}{s}}}{2}(\rho_s(\mathbb{Z})-1)\right).$$

Appendix B Proof of Lemma 2

Lemma 2. Let Λ be an n-dimensional lattice, $\mathbf{z}\in\mathbb{Z}^m$ a nonzero integer vector, $\mathbf{s}\in\mathbb{R}^m$ with $s_i\geqslant\sqrt{z_{\max}^2+z_{\min}^2}\eta_\varepsilon(\mathbb{Z})$ for all $i\leqslant m$ and $\mathbf{c_i}+\mathbf{\Lambda}$ arbitrary cosets. Let $\mathbf{y}_i$ be independent samples from $D_{\mathbf{c_i}+\Lambda,s_i}$, respectively. Let $Y=\sum_i z_i\mathbf{c_i}+\gcd(\mathbf{z})\Lambda$ and $s=\sqrt{\sum_i(z_is_i)^2}$. Then $\tilde{D}_{Y,s}$, the distribution of $\mathbf{y}=\sum z_i\mathbf{y_i}$, is close to $D_{Y,s}$. More precisely,

$$\delta_{RE}(Pr_{\tilde{D}_{Y,s}}[x=\bar{x}],Pr_{D_{Y,s}}[x=\bar{x}])\leqslant\frac{1+\varepsilon}{1-\varepsilon}-1.$$

Proof.

We just include the modification part here. Readers are referred to the proof Theorem 3.2 of [1] for necessary notations. Our goal is to show that the result holds for a larger scope of s_i where $s_i\geqslant\sqrt{z_{max}^2+z_{min}^2}\eta_\varepsilon(\mathbb{Z})$.

When bounding the smoothing parameter of L in [1]

$$\eta(L)\leqslant\eta((S')^{-1}\cdot(Z\otimes\Lambda))\leqslant\eta_\varepsilon(\mathbb{Z})\cdot\tilde{bl}(Z)/\min(s_i)$$

where $Z=\mathbb{Z}^m\cap ker(\mathbf{z}^T)=\{\mathbf{v}\in\mathbb{Z}^m:\langle\mathbf{z},\mathbf{v}\rangle=0\}$ and $\tilde{bl}(\Lambda)$ represents the Gram-Schmidt minimum of a lattice Λ where $\tilde{bl}(\Lambda)=\min_{\mathbf{B}}\|\tilde{\mathbf{B}}\|$, $\|\tilde{\mathbf{B}}\|=\max_i\|\tilde{\mathbf{b}_i}\|$ and the minimum is taken over all bases $\mathbf{B}$ of Λ.

Micciancio and Peikert bound $\tilde{bl}(Z)\leqslant\min(\|\mathbf{z}\|,\sqrt{2}\|\mathbf{z}\|_\infty)$ because there exist a full-rank set of vectors $z_i\cdot\mathbf{e_j}-z_j\cdot\mathbf{e_i}\in Z$ where z_i has the minimal $|z_i|\neq 0$ and $j\neq i\in[1,..,m]$. Among this set of vectors, we have $\max_i\|\tilde{\mathbf{b}_i}\|=\sqrt{z_{max}^2+z_{min}^2}$ where $\sqrt{z_{max}^2+z_{min}^2}\leqslant\|\mathbf{z}\|$ when $m=2$ it takes equality and $\sqrt{z_{max}^2+z_{min}^2}\leqslant\sqrt{2}\|\mathbf{z}\|_\infty$ when $z_{max}=z_{min}$ it takes equality.

And by bounding $\tilde{bl}(Z)\leqslant\sqrt{z_{max}^2+z_{min}^2}$, we have $\eta(L)\leqslant\eta_\varepsilon(\mathbb{Z})\cdot\tilde{bl}(Z)/\min(s_i)\leqslant\eta_\varepsilon(\mathbb{Z})\cdot\sqrt{z_{max}^2+z_{min}^2}/\min(s_i)$. And for $s_i\geqslant\sqrt{z_{max}^2+z_{min}^2}\eta_\varepsilon(\Lambda)$, it is seen that $\eta_\varepsilon(\mathbb{Z})\cdot\sqrt{z_{max}^2+z_{min}^2}/\min(s_i)\leqslant 1$.

Appendix C Proof of Lemma 3

Lemma 3. If $s_1t\geqslant\frac{\sqrt{a^2+b^2}}{\psi}$,

$$b(x_c)=\frac{\beta(x_c)}{\alpha(x_c)}\leqslant C_3e^{-\pi\omega^2\psi^2t^2}.$$

Proof.

Recall that we use the following notations: $\eta=\frac{\sqrt{a^2+b^2}}{s_1},\psi=\frac{\sqrt{a^2+b^2}-a}{b}$ and $\omega=1-\frac{\eta}{\psi t}$. Our goal is to show that under the condition of $s_1=s_2$ and $s_1t\geqslant\frac{\sqrt{a^2+b^2}}{\psi}$, we have

$$b(x_c)=\frac{\beta(x_c)}{\alpha(x_c)}\leqslant Ce^{-\pi\omega^2\psi^2t^2}.$$

where $C=\frac{2}{\left(1-e^{-\pi(2\omega\psi\eta t+\eta^2)}\right)\left(1+e^{-2\pi\eta^2}(1+e^{-4\pi\eta^2})\right)}$.

We first analyse $\alpha(x_c)$

$$\alpha(x_c)=\frac{1}{\rho_{s_1}^2(\mathbb{Z})}\sum_{(x_1,x_2)\in S_{x_c}}e^{-\pi\frac{x_1^2+x_2^2}{s_1^2}}.$$

Note that $\xi=-\frac{ub+va}{a^2+b^2}x_c$. By (**??**), we know that

$$\sum_{k=\lceil\xi\rceil+1}^{\infty}e^{-\pi\frac{(x_cu+kb)^2+(x_cv+ka)^2}{s_1^2}}=e^{-\pi\frac{\|P_1\|^2}{s_1^2}}\sum_{i=1}^{\infty}e^{-\pi\eta^2(i^2+2i(\lceil\xi\rceil-\xi))},$$

and

$$\sum_{k=\lfloor\xi\rfloor-1}^{-\infty} e^{-\pi\frac{(x_c u+kb)^2+(x_c v+ka)^2}{s_1^2}} = e^{-\pi\frac{\|P_0\|^2}{s_1^2}} \sum_{i=1}^{\infty} e^{-\pi\eta^2(i^2+2i(\xi-\lfloor\xi\rfloor))}.$$

Thus

$$\alpha(x_c) = \begin{cases} \frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_1\|^2}{s_1^2}} \sum_{i=0}^{\infty} e^{-\pi\eta^2(i^2+2i(\lceil\xi\rceil-\xi))} + e^{-\pi\frac{\|P_0\|^2}{s_1^2}} \sum_{i=0}^{\infty} e^{-\pi\eta^2(i^2+2i(\xi-\lfloor\xi\rfloor))}\right), & \text{if } \xi\notin\mathbb{Z}, \\ \frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_0\|^2}{s_1^2}} + 2e^{-\pi\frac{\|P_0\|^2}{s_1^2}} \sum_{i=1}^{\infty} e^{-\pi\eta^2 i^2}\right), & \text{if } \xi\in\mathbb{Z}. \end{cases}$$

Let

$$\begin{aligned} d_0 &= e^{-\pi\eta^2(1+2(\xi-\lfloor\xi\rfloor))}(1+e^{-\pi\eta^2(3+2(\xi-\lfloor\xi\rfloor))}), \\ d_1 &= e^{-\pi\eta^2(1+2(\lceil\xi\rceil-\xi))}(1+e^{-\pi\eta^2(3+2(\lceil\xi\rceil-\xi))}). \end{aligned}$$

We have

$$\begin{aligned} 1+d_0 &\leqslant \sum_{i=0}^{\infty} e^{-\pi\eta^2(i^2+2i(\xi-\lfloor\xi\rfloor))}, \\ 1+d_1 &\leqslant \sum_{i=0}^{\infty} e^{-\pi\eta^2(i^2+2i(\lceil\xi\rceil-\xi))}. \end{aligned}$$

These yield an estimation of $\alpha(x)$, if $\xi\notin\mathbb{Z}$

$$\frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_1\|^2}{s_1^2}}(1+d_1)+e^{-\pi\frac{\|P_0\|^2}{s_1^2}}(1+d_0)\right) \leqslant \alpha(x);$$

if $\xi\in\mathbb{Z}$

$$\frac{(1+2d_0)e^{-\pi\frac{\|P_0\|^2}{s_1^2}}}{\rho^2_{s_1}(\mathbb{Z})} \leqslant \alpha(x).$$

And as for $\beta(x_c)$, we have

$$\beta(x_c) = \frac{1}{\rho^2_{s_1}(\mathbb{Z})} \sum_{\substack{(x_1,x_2)\in S_{x_c} \\ |x_1|\geqslant s_1 t \text{ or } |x_2|\geqslant s_1 t}} e^{-\pi\frac{x_1^2+x_2^2}{s_1^2}}.$$

where $|x_c| \leqslant \sqrt{a^2+b^2}s_1 t$.

Three cases shall be discussed separately

1. $(a-b)s_1 t \leqslant x_c \leqslant \sqrt{a^2+b^2}s_1 t$;
2. $-(a-b)s_1 t < x_c < (a-b)s_1 t$;
3. and $-\sqrt{a^2+b^2}s_1 t \leqslant x_c \leqslant -(a-b)s_1 t$.

Case I: $(a-b)s_1 t \leqslant x_c \leqslant \sqrt{a^2+b^2}s_1 t$.

In this case, condition $|x_1| \geqslant s_1 t$ or $|x_2| \geqslant s_1 t$ corresponds to $k \leqslant \left\lfloor\frac{-s_1 t - xv}{a}\right\rfloor$ or $k \geqslant \left\lceil\frac{s_1 t - xu}{b}\right\rceil$. So by (**??**),

$$\beta(x_c) = \frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(\sum_{k=\left\lceil\frac{s_1 t - x_c u}{b}\right\rceil}^{\infty} e^{-\pi\frac{(x_c u+kb)^2+(x_c v+ka)^2}{s_1^2}} + \sum_{k=\left\lfloor\frac{-s_1 t - xv}{a}\right\rfloor}^{-\infty} e^{-\pi\frac{(xu+kb)^2+(xv+ka)^2}{s_1^2}}\right)$$

$$= \frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_1\|^2}{s_1^2}}\sum_{i=\left\lceil\frac{s_1t-x_cu}{b}\right\rceil-\lceil\xi\rceil}^{\infty}e^{-\pi\eta^2(i^2+2i(\lceil\xi\rceil-\xi))}\right)+$$
$$\frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_0\|^2}{s_1^2}}\sum_{i=\left\lfloor\frac{-s_1t-x_cv}{a}\right\rfloor-\lfloor\xi\rfloor}^{-\infty}e^{-\pi\eta^2(i^2-2i(\xi-\lfloor\xi\rfloor))}\right)$$

Note that $(a-b)s_1t \leqslant x_c \leqslant \sqrt{a^2+b^2}s_1t$, we see that

$$\left\lceil\frac{s_1t-x_cu}{b}\right\rceil-\lceil\xi\rceil \geqslant \frac{s_1t-x_cu}{b}-\xi-1 \geqslant \frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}s_1t-1$$

Obviously, $\frac{\sqrt{a^2+b^2}-b}{a\sqrt{a^2+b^2}} \geqslant \frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}$ as $a>b>0$, we get

$$\left\lfloor\frac{-s_1t-x_cv}{a}\right\rfloor-\lfloor\xi\rfloor \leqslant \frac{-s_1t-x_cv}{a}-\xi+1 \leqslant -\frac{\sqrt{a^2+b^2}-b}{a\sqrt{a^2+b^2}}s_1t+1 \leqslant -(\frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}s_1t-1).$$

Case III: $-\sqrt{a^2+b^2}s_1t \leqslant x_c \leqslant -(a-b)s_1t$.

In this case, condition $|x_1| \geqslant s_1t$ or $|x_2| \geqslant s_1t$ corresponds to $k \leqslant \left\lfloor\frac{-s_1t-x_cu}{b}\right\rfloor$ or $k \geqslant \left\lceil\frac{s_1t-x_cv}{a}\right\rceil$. So similarly with Case I, we see that

$$\left\lceil\frac{s_1t-x_cv}{a}\right\rceil-\lceil\xi\rceil \geqslant \frac{s_1t-x_cv}{a}-\xi-1 \geqslant \frac{\sqrt{a^2+b^2}-b}{a\sqrt{a^2+b^2}}s_1t-1 \geqslant \frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}s_1t-1.$$

Also

$$\left\lfloor\frac{-s_1t-x_cu}{b}\right\rfloor-\lfloor\xi\rfloor \leqslant \frac{-s_1t-x_cu}{b}-\xi+1 \leqslant -(\frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}s_1t-1).$$

Case II: $-(a-b)s_1t < x_c < (a-b)s_1t$.

In this case, condition $|x_1| \geqslant s_1t$ or $|x_2| \geqslant s_1t$ corresponds to $k \leqslant \left\lfloor\frac{-s_1t-x_cv}{a}\right\rfloor$ or $k \geqslant \left\lceil\frac{s_1t-x_cv}{a}\right\rceil$. So by (**??**),

$$\beta(x) = \frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(\sum_{k=\left\lceil\frac{s_1t-x_cv}{a}\right\rceil}^{\infty}e^{-\pi\frac{(x_cu+kb)^2+(xv+ka)^2}{s_1^2}}+\sum_{k=\left\lfloor\frac{-s_1t-x_cv}{a}\right\rfloor}^{-\infty}e^{-\pi\frac{(x_cu+kb)^2+(x_cv+ka)^2}{s_1^2}}\right)$$
$$= \frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_1\|^2}{s_1^2}}\sum_{i=\left\lceil\frac{s_1t-x_cv}{a}\right\rceil-\lceil\xi\rceil}^{\infty}e^{-\pi\eta^2(i^2+2i(\lceil\xi\rceil-\xi))}\right)+$$
$$\frac{1}{\rho^2_{s_1}(\mathbb{Z})}\left(e^{-\pi\frac{\|P_0\|^2}{s_1^2}}\sum_{i=\left\lfloor\frac{-s_1t-x_cv}{a}\right\rfloor-\lfloor\xi\rfloor}^{-\infty}e^{-\pi\eta^2(i^2-2i(\xi-\lfloor\xi\rfloor))}\right)$$

Obviously, $\frac{a^2+2b^2-ab}{a(a^2+b^2)} \geqslant \frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}$ as $a>b>0$, we have

$$\left\lceil\frac{s_1t-x_cv}{a}\right\rceil-\lceil\xi\rceil \geqslant \frac{s_1t-x_cv}{a}-\xi-1 \geqslant \frac{a^2+2b^2-ab}{a(a^2+b^2)}s_1t-1 \geqslant \frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}s_1t-1.$$

and

$$\left\lfloor\frac{-s_1t-x_cv}{a}\right\rfloor-\lfloor\xi\rfloor \leqslant \frac{-s_1t-x_cv}{a}-\xi+1 \leqslant -\frac{a^2+2b^2-ab}{a(a^2+b^2)}s_1t+1 \leqslant -(\frac{\sqrt{a^2+b^2}-a}{b\sqrt{a^2+b^2}}s_1t-1).$$

When $s_1 t \geqslant \frac{\sqrt{a^2+b^2}}{\psi}$, we have $\omega \geqslant 0$ and $\frac{\psi}{\eta}t - 1 \geqslant \frac{\omega\psi}{\eta}t$. As a result, for all $x_c \in [-\sqrt{a^2+b^2}s_1 t, \sqrt{a^2+b^2}s_1 t]$, we have

$$\sum_{i=\left\lfloor \frac{-s_1 t - x_c v}{a} \right\rfloor - \lfloor \xi \rfloor}^{-\infty} e^{-\pi\eta^2(i^2 - 2i(\xi - \lfloor \xi \rfloor))} \leqslant D_0, \text{ and } \sum_{i=\left\lceil \frac{s_1 t - x_c v}{a} \right\rceil - \lceil \xi \rceil}^{\infty} e^{-\pi\eta^2(i^2 + 2i(\lceil \xi \rceil - \xi))} \leqslant D_0.$$

where $D_0 = \frac{e^{-\pi\omega^2\psi^2 t^2}}{1 - e^{-\pi(2\omega\psi\eta t + \eta^2)}}$.

So

$$\begin{aligned}
\beta(x) &\leqslant \frac{1}{\rho_{s_1}^2(\mathbb{Z})} \left(e^{-\pi \frac{\|P_1\|^2}{s_1^2}} \sum_{i=\left\lceil \frac{s_1 t - x_c v}{a} \right\rceil - \lceil \xi \rceil}^{\infty} e^{-\pi\eta^2(i^2 + 2i(\lceil \xi \rceil - \xi))} \right) + \\
&\quad \frac{1}{\rho_{s_1}^2(\mathbb{Z})} \left(e^{-\pi \frac{\|P_0\|^2}{s_1^2}} \sum_{i=\left\lfloor \frac{-s_1 t - x_c v}{a} \right\rfloor - \lfloor \xi \rfloor}^{-\infty} e^{-\pi\eta^2(i^2 - 2i(\xi - \lfloor \xi \rfloor))} \right) \\
&\leqslant \frac{1}{\rho_{s_1}^2(\mathbb{Z})} D_0 \left(e^{-\pi \frac{\|P_1\|^2}{s_1^2}} + e^{-\pi \frac{\|P_0\|^2}{s_1^2}} \right)
\end{aligned}$$

Thus when $\xi \in \mathbb{Z}$

$$\begin{aligned}
b(x_c) &= \frac{\beta(x_c)}{\alpha(x_c)} \leqslant \frac{D_0 \left(e^{-\pi \frac{\|P_1\|^2}{s_1^2}} + e^{-\pi \frac{\|P_0\|^2}{s_1^2}} \right)}{e^{-\pi \frac{\|P_0\|^2}{s_1^2}} (1 + 2d_0)} \\
&= \frac{(1 + e^{-\pi/s_1^2}) e^{-\pi\psi^2\omega^2 t^2}}{(1 - e^{-\pi(2\omega\psi\eta t + \eta^2)})(1 + 2e^{-\pi\eta^2}(1 + e^{-3\pi\eta^2}))} \\
&\leqslant D_1 e^{-\pi\omega^2\psi^2 t^2}
\end{aligned}$$

where $D_1 = \frac{1 + e^{-\pi/s_1^2}}{(1 - e^{-\pi(2\omega\psi\eta t + \eta^2)})(1 + 2e^{-\pi\eta^2}(1 + e^{-3\pi\eta^2}))}$.

And when $\xi \notin \mathbb{Z}$, assume $\|P_1\|^2 \geqslant \|P_0\|^2$ without loss of generality, we have

$$\begin{aligned}
b(x_c) &= \frac{\beta(x_c)}{\alpha(x_c)} \leqslant \frac{D_0 e^{-\pi \frac{\|P_1\|^2}{s_1^2}} + D_0 e^{-\pi \frac{\|P_0\|^2}{s_1^2}}}{e^{-\pi \frac{\|P_1\|^2}{s_1^2}} (1 + d_1) + e^{-\pi \frac{\|P_0\|^2}{s_1^2}} (1 + d_0)} \leqslant \frac{2D_0 e^{-\pi \frac{\|P_0\|^2}{s_1^2}}}{e^{-\pi \frac{\|P_0\|^2}{s_1^2}} (1 + d_0)} \\
&\leqslant \frac{2e^{-\pi\omega^2\psi^2 t^2}}{(1 - e^{-\pi(2\omega\psi\eta t + \eta^2)})(1 + 2e^{-2\pi\eta^2}(1 + e^{-4\pi\eta^2}))} \\
&\leqslant D_2 e^{-\pi\omega^2\psi^2 t^2}
\end{aligned}$$

where $D_2 = \frac{2}{(1 - e^{-\pi(2\omega\psi\eta t + \eta^2)})(1 + 2e^{-2\pi\eta^2}(1 + e^{-4\pi\eta^2}))}$.

Let $C = D_2 > D_1$, for all ξ, we have

$$b(x_c) \leqslant C e^{-\pi\omega^2\psi^2 t^2}$$

References

1 Micciancio D, Peikert C. Hardness of SIS and LWE with small parameters[M]. Advances in Cryptology-CRYPTO 2013. Springer, Berlin, Heidelberg, 2013: 21-39.