SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Generalizing Lyubashevsky-Wichs Trapdoor Sampler for NTRU Lattices

Yang Tao[1,2], Yunfeng Ji[1,2] & Rui Zhang[1,2*]

[1]*State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093*, China;*
[2]*School of Cyber Security, University of Chinese Academy of Sciences, Beijing* 100049*, China*

Lemma 1 ([1])**.** Assume the columns of $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ generate $\mathbb{Z}_q^n$, and let $\varepsilon \in (0, \frac{1}{2})$ and $\sigma \geqslant \frac{1}{\sqrt{2\pi}}\eta_\varepsilon(\Lambda^\perp(\mathbf{A}))$. Then for $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,\sigma}$, the distribution of the syndrome $\mathbf{u} = \mathbf{A}\mathbf{e} \bmod q$ is within statistical distance 2ε of uniform over $\mathbb{Z}_q^n$. Furthermore, fix $\mathbf{u} \in \mathbb{Z}_q^n$ and let $\mathbf{x} \in \mathbb{Z}^m$ be an arbitrary solution to $\mathbf{A}\mathbf{x} = \mathbf{u} \bmod q$. Then the conditional distribution of $\mathbf{e} \leftarrow D_{\mathbb{Z}^m,\sigma}$ given $\mathbf{A}\mathbf{e} = \mathbf{u} \bmod q$ is exactly $\mathbf{x} + D_{\Lambda^\perp,\sigma,-\mathbf{x}}$.

Lemma 2 ([2])**.** Let Λ be any n-dimensional lattice. Then for any $\varepsilon \in (0,1)$, $\sigma \geqslant \frac{1}{\sqrt{2\pi}}\eta_\varepsilon(\Lambda)$, and $\mathbf{c} \in \mathbb{R}^n$, we have $\rho_{\sigma,\mathbf{c}}(\Lambda) \in [\frac{1-\varepsilon}{1+\varepsilon}, 1] \cdot \rho_\sigma(\Lambda)$.

Appendix A Proof of Theorem 1

Theorem 1. Let $\sigma \geqslant \max\{\frac{1}{\sqrt{2\pi}}\eta_\varepsilon(\Lambda^\perp(\mathbf{P})), \alpha \cdot \frac{\sqrt{2n}}{2}\|\widetilde{\mathbf{B}}\|_2\}$, where α is a constant and $\varepsilon \in (0, 2^{-\lambda}]$. Assume there exists a positive real M such that $\Pr[M \cdot \rho_{\sigma,\mathbf{s}}(\mathbf{x}) \geqslant \rho_\sigma(\mathbf{x})] \geqslant 1 - 2^{-\lambda}$ for any prescribed $\mathbf{s}$. Then, the output distribution of **GaussianSampler** is statistically close to $D_{\Lambda_\mathbf{t}^\perp(\mathbf{P}),\sigma}$.

Proof. To analyze the distribution of $\mathbf{z}$, we define an intermediate algorithm—Algorithm A1, which is statistically close to **GaussianSampler** by Lemma 1.

Algorithm A1 Gaussian Intermediate Algorithm

Require: $\mathbf{P} = [\mathbf{1}|\mathbf{h}]$, $\mathbf{t} \in \mathcal{R}_q$ and secret key $\mathbf{R} = (\mathbf{f}, \mathbf{g})$
Ensure: $\mathbf{z} \in \mathcal{R}_q^2$ satisfying $\mathbf{P}\mathbf{z} = \mathbf{t} \bmod q$
1: Generate $\mathbf{c} \leftarrow U(\mathcal{R}_q)$
2: Sample $\mathbf{y} \leftarrow D_{\mathcal{R}^2,\sigma}|\ \mathbf{P}\mathbf{y} = \mathbf{t} - \mathbf{c} \bmod q$
3: Compute $\mathbf{s} \leftarrow \mathrm{iRecover}_{\mathrm{FDH}}.\mathrm{Invert}(\mathbf{P}, \mathbf{R}, \mathbf{c})$
4: Compute $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{s}$
5: Keep $(\mathbf{z}, \mathbf{c})$ with probability $\min\{\frac{1}{M}\exp(\frac{-2\langle\mathbf{z},\mathbf{s}\rangle + \|\mathbf{s}\|_2^2}{2\sigma^2}), 1\}$
6: Output $\mathbf{z}$ and drop $\mathbf{c}$
7: If nothing was output, restart

The distribution of $(\mathbf{z}, \mathbf{c})$ in Algorithm A1 is $\Pr[(\mathbf{z}, \mathbf{c})] = \Pr[\mathbf{c}] \cdot \Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{c}] = \frac{1}{|\mathcal{R}_q|} \times \Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{c}]$. Since the conditional distribution of $\mathbf{y}$ is $[(\mathbf{t} - \mathbf{c})|\mathbf{0}]^t + D_{\Lambda^\perp(\mathbf{P}),\sigma,-[(\mathbf{t}-\mathbf{c})|\mathbf{0}]^t}$ (Lemma 1), we have

$$\Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{c}] = D_{\Lambda^\perp(\mathbf{P}),\sigma,-[(\mathbf{t}-\mathbf{c})|\mathbf{0}]^t}(\mathbf{z} - \mathbf{s} - [(\mathbf{t} - \mathbf{c})|\mathbf{0}]^t) \tag{A1}$$

$$= \frac{\rho_{\sigma,-[(\mathbf{t}-\mathbf{c})|\mathbf{0}]^t}(\mathbf{z} - \mathbf{s} - [(\mathbf{t} - \mathbf{c})|\mathbf{0}]^t)}{\rho_{\sigma,-[(\mathbf{t}-\mathbf{c})|\mathbf{0}]^t}(\Lambda^\perp(\mathbf{P}))} \tag{A2}$$

$$= \frac{\rho_{\sigma,\mathbf{s}}(\mathbf{z})}{\rho_{\sigma,\mathbf{s}}(\Lambda^\perp(\mathbf{P}) + [(\mathbf{t} - \mathbf{c})|\mathbf{0}]^t + \mathbf{s})} = \frac{\rho_{\sigma,\mathbf{s}}(\mathbf{z})}{\rho_{\sigma,\mathbf{s}}(\Lambda_\mathbf{t}^\perp(\mathbf{P}))} = D_{\Lambda_\mathbf{t}^\perp(\mathbf{P}),\sigma,\mathbf{s}} \tag{A3}$$

* Corresponding author (email: r-zhang@iie.ac.cn)

Hence, the distribution of $(\mathbf{z}, \mathbf{c})$ before rejection sampling in Algorithm A1 is $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma,\mathbf{s}} \times U(\mathcal{R}_q)$. On the other hand, the ideal distribution we want is $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma} \times U(\mathcal{R}_q)$. Therefore,

$$\frac{D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma}(\mathbf{x})}{D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma,\mathbf{s}}(\mathbf{x})} = \frac{\rho_{\sigma}(\mathbf{x})}{\rho_{\sigma,\mathbf{s}}(\mathbf{x})} \cdot \frac{\rho_{\sigma}(\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) - \mathbf{s})}{\rho_{\sigma}(\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}))} \in [\frac{1-\varepsilon}{1+\varepsilon}, \frac{1+\varepsilon}{1-\varepsilon}] \cdot \frac{\rho_{\sigma}(\mathbf{x})}{\rho_{\sigma,\mathbf{s}}(\mathbf{x})} = \frac{\rho_{\sigma}(\mathbf{x})}{\rho_{\sigma,\mathbf{s}}(\mathbf{x})}(1+\delta),$$

where $\delta \in [\frac{-2\varepsilon}{1+\varepsilon}, \frac{2\varepsilon}{1-\varepsilon}]$ by Lemma 2. For $\varepsilon \in (0, 2^{-\lambda}]$, we have $-2 \cdot 2^{-\lambda} \leqslant \delta \leqslant 4 \cdot 2^{-\lambda}$.

Set $\delta^{+} = 4 \cdot 2^{-\lambda}$. Notice that $\Pr[M(1+\delta^{+})D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma,\mathbf{s}}(\mathbf{x}) \geqslant D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma}(\mathbf{x})] \geqslant \Pr[M \cdot \rho_{\sigma,\mathbf{s}}(\mathbf{x}) \geqslant \rho_{\sigma}(\mathbf{x})] \geqslant 1 - 2^{-\lambda}$. Then, the rejection sampling probability should be $\gamma_{\text{ideal}} = \min\{\frac{D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma}(\mathbf{x})}{M(1+\delta^{+})D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma,\mathbf{s}}(\mathbf{x})}, 1\} = \min\{\frac{(1+\delta)\rho_{\sigma}(\mathbf{x})}{M(1+\delta^{+})\rho_{\sigma,\mathbf{s}}(\mathbf{x})}, 1\}$. Due to rejection sampling, Algorithm A1 with γ_{ideal} is $\frac{2^{-\lambda}}{M(1+\delta^{+})}$-close to the ideal distribution $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma} \times U(\mathcal{R}_q)$ with $\frac{1}{M(1+\delta^{+})}$ probability and the iterations occur at most λM times with probability $1 - (1 - \frac{1}{(1+\delta^{+})M})^{\lambda M} \geqslant 1 - 2^{-\lambda}$. Thus, the statistical distance between Algorithm A1 with γ_{ideal} and ideal distribution $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma} \times U(\mathcal{R}_q)$ with $\frac{1}{M(1+\delta^{+})}$ probability is at most $O(\lambda) \cdot 2^{-\lambda}$. However, we don't know the exact value of γ_{ideal}. Thus, we use $\gamma_{\text{real}} = \min\{\frac{\rho_{\sigma}(\mathbf{x})}{M\rho_{\sigma,\mathbf{s}}(\mathbf{x})}, 1\}$ $= \min\{\frac{1}{M}\exp(\frac{-2\langle\mathbf{x},\mathbf{s}\rangle + \|\mathbf{s}\|_2^2}{2\sigma^2}), 1\}$ as an approximation and $|\gamma_{\text{real}} - \gamma_{\text{ideal}}| = \frac{\rho_{\sigma}(\mathbf{x})}{M\rho_{\sigma,\mathbf{s}}(\mathbf{x})} \cdot \frac{\delta^{+}-\delta}{1+\delta^{+}} \leqslant 6 \cdot 2^{-\lambda}$. Therefore, the statistical distance between Algorithm A1 (with γ_{real} as probability) and output distribution of Algorithm A1 with γ_{ideal} probability is at most $O(\lambda M) \cdot 2^{-\lambda}$. Furthermore, the distribution of $(\mathbf{z}, \mathbf{c})$ in Step 5 of Algorithm A1 is statistically close to the ideal distribution $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma} \times U(\mathcal{R}_q)$ and the marginal distribution $\mathbf{z}$ of Algorithm A1 is statistically close to $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma}$.

To conclude, the output distribution of **GaussianSampler** is statistically indistinguishable to $D_{\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}),\sigma}$.

Appendix B Proof of Theorem 2

Theorem 2. Assume $\Delta((\mathbf{P}, \mathbf{Py}), (\mathbf{P}, U(\mathcal{R}_q))) \leqslant \epsilon_1$ for $\mathbf{y} \leftarrow U(\mathcal{R}_{q,\tau}^2)$, where $\epsilon_1 \leqslant 2^{-n\log q - \lambda}$. Then the output distribution of **UniformSampler** is statistically close to uniform distribution over $\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2$.

Proof. (Sketch) To analyze the distribution of $\mathbf{z}$, we also introduce an intermediate algorithm—Algorithm B1, whose

Algorithm B1 Uniform Intermediate Algorithm

Require: $\mathbf{P} = [\mathbf{1}|\mathbf{h}]$, $\mathbf{t} \in \mathcal{R}_q$ and secret key $\mathbf{R} = (\mathbf{f}, \mathbf{g})$
Ensure: $\mathbf{z} \in \mathcal{R}_q^2$ satisfying $\mathbf{Pz} = \mathbf{t} \bmod q$

1: Generate $\mathbf{c} \leftarrow U(\mathcal{R}_q)$
2: Sample $\mathbf{y} \leftarrow U(\mathcal{R}_{q,\tau}^2)|\ \mathbf{Py} = \mathbf{t} - \mathbf{c} \bmod q$
3: Compute $\mathbf{s} \leftarrow \text{iRecover}_{\text{FDH}}.\text{Invert}(\mathbf{P}, \mathbf{R}, \mathbf{c})$
4: Compute $\mathbf{z} \leftarrow \mathbf{y} + \mathbf{s}$
5: Keep $(\mathbf{z}, \mathbf{c})$ when $\|\mathbf{z}\|_{\infty} \leqslant \tau - \beta$
6: Output $\mathbf{z}$ and drop $\mathbf{c}$
7: If nothing was output, restart

output distribution is statistically close to **UniformSampler**. Thus, it suffices to calculate the output distribution of Algorithm B1. The distribution of $(\mathbf{z}, \mathbf{c})$ in Algorithm B1 is $P_{(\mathbf{z},\mathbf{c})} = \Pr[\mathbf{c}] \cdot \Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{c}] = \frac{1}{|\mathcal{R}_q|} \times \Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{c}]$. Since $\|\mathbf{z}\|_{\infty} \leqslant \tau - \beta$ and the distribution of $\mathbf{Py}$ is statistically close to $U(\mathcal{R}_q)$, we have $\Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{c}] = \Pr[\mathbf{y} = \mathbf{z} - \mathbf{s}|\mathbf{Py} = \mathbf{t} - \mathbf{c} \bmod q] = \frac{\Pr[\mathbf{Py} = \mathbf{t} - \mathbf{c} \bmod q|\mathbf{y} = \mathbf{z} - \mathbf{c}]\Pr[\mathbf{y} = \mathbf{z} - \mathbf{c}]}{\Pr[\mathbf{Py} = \mathbf{t} - \mathbf{c} \bmod q]} = \frac{|\mathcal{R}_q|}{(1+\epsilon_1 \cdot |\mathcal{R}_q|)(2\tau+1)^{2n}}$, where $\epsilon_1 \leqslant 2^{-n\log q - \lambda}$. The ideal distribution P_{ideal} of $(\mathbf{z}, \mathbf{c})$ is $U(\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2) \times U(\mathcal{R}_q)$. Assume M is a constant satisfying $\Pr[M(1+\delta)P_{(\mathbf{z},\mathbf{c})} \geqslant P_{\text{ideal}}(\mathbf{z}, \mathbf{c})] \geqslant 1 - 2^{-\lambda}$, where $\delta = 2^{-\lambda}$. Hence, rejection sampling probability should be $\gamma_{\text{ideal}} = \min\{\frac{P_{\text{ideal}}(\mathbf{z},\mathbf{c})}{M(1+\delta)P_{(\mathbf{z},\mathbf{c})}}, 1\} = \min\{\frac{(1+\epsilon_1 \cdot |\mathcal{R}_q|)(2\tau+1)^{2n}}{M(1+\delta)|\mathcal{R}_q||\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2|}, 1\}$. However, we don't know the exact value of γ_{ideal}. We use $\gamma_{\text{real}} = \min\{\frac{(2\tau+1)^{2n}}{M|\mathcal{R}_q||\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2|}, 1\}$ as an approximation. By Gaussian heuristic, the expectation of $|\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2| = \frac{(2\tau-2\beta+1)^{2n}}{q^n}$. We set M as $\frac{(2\tau+1)^{2n}}{(2\tau-2\beta+1)^{2n}}$. Therefore, the rejection sampling is equivalent to check $\|\mathbf{z}\|_{\infty} \leqslant \tau - \beta$. The output distribution of Algorithm B1 is a uniform distribution over $\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2$. Furthermore, the output distribution of **UniformSampler** is statistically close to uniform distribution over $\Lambda_{\mathbf{t}}^{\perp}(\mathbf{P}) \cap \mathcal{R}_{q,\tau-\beta}^2$.

References

1 Gentry C, Peikert C, Vaikuntanathan V. Trapdoors for hard lattices and new cryptographic constructions. In: Dwork C, eds. Proceedings of the 40th Annual ACM Symposium on Theory of Computing, STOC 2008, Victoria, 2008. 197-206

2 Micciancio D, Regev O. Worst-case to average-case reductions based on Gaussian measures. Proceedings of 45th Symposium on Foundations of Computer Science, FOCS 2004, Rome, 2004. 372-381