SCIENCE CHINA
Information Sciences

• LETTER •

March 2021, Vol. 64 139104:1–139104:3
https://doi.org/10.1007/s11432-019-9919-7

Error estimation of practical convolution discrete Gaussian sampling with rejection sampling

Zhongxiang ZHENG[1], Xiaoyun WANG[2,3*], Guangwu XU[3,4] & 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 Science, University of Wisconsin-Milwaukee, Milwaukee* WI 53211*, USA*

Received 21 February 2019/Accepted 10 June 2019/Published online 4 February 2021

Citation Zheng Z X, Wang X Y, Xu G W, et al. Error estimation of practical convolution discrete Gaussian sampling with rejection sampling. Sci China Inf Sci, 2021, 64(3): 139104, https://doi.org/10.1007/s11432-019-9919-7

Dear editor,

Discrete Gaussian sampling is a fundamental tool in lattice cryptography which has been used in digital signatures, identify-based encryption, attribute-based encryption, zero-knowledge proof, and fully homomorphic cryptosystem. As a subroutine of lattice-based scheme, a high precision sampling usually leads to a high security level and also brings large time and space complexity. In order to optimize security and efficiency, how to achieve a higher security level with a lower precision becomes a widely studied open question [1–4]. A popular method for addressing this question is to use different metrics other than statistical distance to measure errors. The proposed metrics include KL-divergence, Rényi-divergence, and Max-log distance, and these techniques are supposed to achieve 2^p security with $\frac{p}{2}$ precision or even less [1–3]. However, we note that error bounds are not universal but depend on specific sampling methods. For example, if one uses the popular rejection sampling, there will be large gaps between some existing results and practical experiments in terms of error bounds. We discuss these issues by making two novel observations about practical errors. As an application of these observations, we consider convolution theorem [5, 6] of discrete Gaussian sampling by using rejection method and reformulate it into a practical one with much more accurate error bounds. We describe a rigorous proof of it in Appendixes A–C and demonstrate that the bounds are tightly matched by our experiments. Our bounds under the statistical distance (Δ_{SD}), relative difference (Δ_{RE}), KL-divergence (Δ_{KL}), Rényi-divergence ($\Delta_{\mathrm{RD}_\alpha}$) and Max-log distance ($\Delta_{\mathrm{ML}}$) using rejection sampling may have no influence on estimating security level, but this successful application reveals the proposed observations are very effective in analyzing practical probabilities. Moreover, some technical tools including several improved inequalities for discrete Gaussian measure are developed.

Two propositions. Here we make two novel observations about practical errors which are the keys to more precisely determine the dominant term of practical errors in discrete Gaussian sampling. We first define two bounds for practical errors: $\varepsilon_t = \rho_{1/t}(\mathbb{Z}) - 1$ and $\mu = 2^{-p}$. Note that for $t > 1, \varepsilon_t = 2\sum_{i=1}^{+\infty} \mathrm{e}^{-\pi t^2 i^2} \in (2\mathrm{e}^{-\pi t^2}, \frac{2\mathrm{e}^{-\pi t^2}}{1-\mathrm{e}^{-3\pi t^2}})$. We will use ε_t to control the truncation error with respect to t, and μ to control float-point errors.

Our first observation indicates that, in general, the sum of the stored probabilities cannot be close to 1 by the order of μ^2.

Proposition 1. Let $P_1, \ldots, P_n$ be a finite probability distribution and $\bar{P}_1, \ldots, \bar{P}_n$ be the corresponding p-bits approximations (i.e., $\bar{P}_i = \mathrm{Rd}_p(P_i)$). We have $|1 - \sum_{i=1}^{n} \bar{P}_i| \leqslant \mu$. Moreover, this bound is sharp in the sense that it cannot be improved to $< \frac{\mu}{2}$.

We would like to make the following remarks.

(1) There are more cases for which $|1 - \sum_{i=1}^{n} \bar{P}_i| \geqslant \frac{\mu}{4}$. However, the probability for $|1 - \sum_{i=1}^{n} \bar{P}_i| \leqslant \mu^2$ is extremely small.

(2) Let $P'_i = \frac{\bar{P}_i}{\sum_{i=1}^{n} \bar{P}_i}$, then $\frac{\bar{P}_i}{1+2^{-p}} \leqslant P'_i \leqslant \frac{\bar{P}_i}{1-2^{-p}}$. We observe that in most cases, $\mathrm{Rd}_p(P'_i) = \bar{P}_i$ for all $i = 1, 2, \ldots, n$, so normalizing the stored probabilities achieves nothing in terms of storage. We shall call this anti-intuitive phenomena the Distribution Precision Paradox.

(3) We also have $\sum_{i=1}^{n} \mathrm{Rd}_p(P'_i) = 1 + O(\mu)$. This can be seen from the fact that $\left|\mathrm{Rd}_p(P'_i) - \bar{P}_i\right| \leqslant 2^{-p+1}\bar{P}_i$.

(4) The proposition naturally leads to a conclusion that floating-point errors are mostly around $O(\mu)$ rather than $O(\mu^2)$ for methods such as rejection sampling.

(5) When adding truncation errors into consideration, we can get a similar result that normalization process will not efficiently remove the influence of truncation errors on the sum of probabilities because of the limitation of the storage space. As a result, in a base sampler of discrete Gaussian sampling, we always have $\sum_{i=1}^{n} \mathrm{Rd}_p(P'_i) = 1 + O(\mu) + O(\varepsilon_t)$.

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

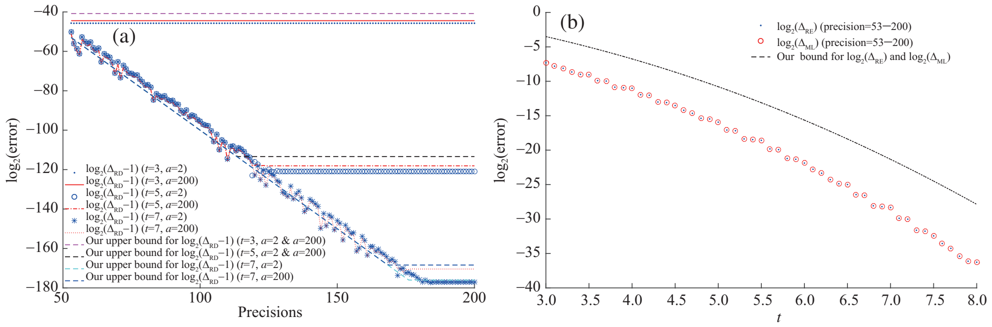

Figure 1 (Color online) Experiments results of practical errors of discrete gaussian convolution. (a) For $\Delta_{\rm SD}$, $\Delta_{\rm KL}$ and $\Delta_{\rm RD}$; (b) for $\Delta_{\rm ML}$ and $\Delta_{\rm RE}$.

Our second observation reveals a contrary result for the case of convolution of two discrete Gaussian variables. We actually show that during the process of convolution, the ignored part of truncation error according to the tail bound lemma proposed in [7] may contribute significantly and become the main term with respect to several metrics.

Let x_1, x_2 be sampled from D_s independently and be restricted on the truncation ranges $S_1 = [-ts, ts]$. Let a, b be positive integers with $\gcd(a,b) = 1$ and $x = ax_1 + bx_2$. The probability of x is computed by the convolution, denoted by $P'(x)$. We also restrict the support of x to $S = [-t\sqrt{a^2+b^2}s, t\sqrt{a^2+b^2}s]$. Setting $\eta = \frac{\sqrt{a^2+b^2}}{s}$, $\psi = \min\{\frac{\sqrt{a^2+b^2}-a}{b}, \frac{\sqrt{a^2+b^2}-b}{a}\}$ and $\omega = 1 - \frac{\eta}{\psi t}$, we can state our observation as follows.

Proposition 2. Let $P(x)$ be the probability of x for the ideal discrete Gaussian distribution $D_{\sqrt{a^2+b^2}s}$. If $st \geqslant \frac{\sqrt{a^2+b^2}}{\psi}$, then

$$\Delta_{\rm RE}(P', P) \leqslant \varepsilon_t^{\omega^2\psi^2}.$$

Moreover, this bound is sharp in the sense that it cannot be improved to $< \varepsilon_t^{(\sqrt{2}-1)^2}$.

We have several remarks.

(1) Our following experiments show that our bound is sharp and $\Delta_{\rm RE}(P', P) \leqslant \varepsilon_t^{(\sqrt{2}-1)^2}$ is false. However, the inequality $\Delta_{\rm ML}(P', P) \leqslant O(\varepsilon_t)$ ($\Delta_{\rm RE}(P', P) \leqslant O(\varepsilon_t)$) was assumed previously [1].

(2) It is also interesting to note if $st < \frac{\sqrt{a^2+b^2}}{\psi}$, $\Delta_{\rm RE}(P', P)$ can be close to 1.

(3) Because practical distribution usually has a bounded support, the analysis about max-like metrics is discussed according to the support of practical distribution unless specifically otherwise, says $S = [-t\sqrt{a^2+b^2}s, t\sqrt{a^2+b^2}s]$ in this case.

Refinement of practical convolution theorem. We will use the two observations to consider practical issues of convolution of discrete Gaussian samplings using rejection sampling, which mainly devotes to a derivation of convolution theorem with more accurate bounds.

Recall that for a real number $t > 1$, we use $\varepsilon_t = \rho_{1/t}(\mathbb{Z}) - 1$ to control the truncation error with respect to t. For positive integers a, b and real number s_1, η, ψ and ω are defined as above.

Now, we state our version of convolution theorem.

Theorem 1. Let $a > b \in \mathbb{Z}$ be nonzero integers with $\gcd(a,b) = 1$ and $\boldsymbol{s} \in \mathbb{R}^2$ with $s_1 = s_2 \geqslant \sqrt{a^2+b^2}\eta_\varepsilon(\mathbb{Z})$ (the discussion can be extended to the case of $s_1 \neq s_2$). Let $x_i \in [-ts_i, ts_i]$ be independent samples from $D_{\mathbb{Z},s_i}$, respectively, with floating-point error $\mu_i \leqslant \mu$ for $i = 1, 2$. Let $\tilde{D}_{\mathbb{Z},s}$ be the distribution of $x = ax_1 + bx_2 \in S = [-ts, ts]$ where $s = \sqrt{a^2s_1^2 + b^2s_2^2}$. Then

$$\Delta_{\rm SD}(\tilde{D}_{\mathbb{Z},s}, D_{\mathbb{Z},s}) \leqslant C_1\varepsilon_t + \mu + \varepsilon,$$
$$\Delta_{\rm RE}(\tilde{D}_{\mathbb{Z},s}, D_{\mathbb{Z},s}) \leqslant C_3\varepsilon_t^{\omega^2\psi^2} + 2\mu + 2\varepsilon,$$
$$\Delta_{\rm ML}(\tilde{D}_{\mathbb{Z},s}, D_{\mathbb{Z},s}) \leqslant C_3\varepsilon_t^{\omega^2\psi^2} + 2\mu + 2\varepsilon,$$
$$\Delta_{\rm KL}(\tilde{D}_{\mathbb{Z},s} \| D_{\mathbb{Z},s}) \leqslant (2C_1 + C_4)\varepsilon_t + 2\mu + 2\varepsilon^2,$$
$$\Delta_{{\rm RD}_\alpha}(\tilde{D}_{\mathbb{Z},s} \| D_{\mathbb{Z},s}) \leqslant 1 + (2C_1 + C_4)\varepsilon_t + 2\mu + \frac{\alpha}{2}\varepsilon^2,$$

where $C_1 = \frac{1-\frac{1}{2}{\rm e}^{-\frac{2\pi t}{s_1}}}{s_1} + \frac{1}{2}{\rm e}^{\frac{-2\pi t}{s_1}}$, $C_3 = \frac{2}{(1-{\rm e}^{-\pi(2\omega\psi\eta t+\eta^2)})(1+{\rm e}^{-2\pi\eta^2}(1+{\rm e}^{-4\pi\eta^2}))}$, and $C_4 = \frac{1-\frac{1}{2}{\rm e}^{-\frac{2\pi t}{s}}}{s} + \frac{1}{2}{\rm e}^{\frac{-2\pi t}{s}}$.

Experiment results. We describe two experiments about the practical errors of convolution discrete Gaussian sampling to validate our results. The first experiment is to exhibit the influences of convolution errors, truncation errors and floating-point errors, respectively. More specifically, we choose $s_1 = s_2$ and compute the probability distributions for $x_1 \leftarrow D_{\mathbb{Z},s_1}$ and $x_2 \leftarrow D_{\mathbb{Z},s_2}$ under different precisions where $x_1 \in [-ts_1, ts_1], x_2 \in [-ts_2, ts_2]$. Then we compute the probability distribution of the variable $\tilde{x} = ax_1 + bx_2$, denoted as $\tilde{D}_{\mathbb{Z},s=\sqrt{a^2s_1^2+b^2s_2^2}}$, and compare it with a precomputed and much more accurate probability distribution for $x \leftarrow D_{\mathbb{Z},s=\sqrt{a^2s_1^2+b^2s_2^2}}$ to get a result of output errors. And it is clear that the approach fits well with the practical situations such as rejection sampling.

The detailed parameters are selected as $s_1 = s_2 = 19.53\sqrt{2\pi}$, $a = 11, b = 1$, $s = \sqrt{a^2s_1^2 + b^2s_2^2}$, $x_1 \in [-ts_1, ts_1], x_2 \in [-ts_2, ts_2]$, t varying from 3 to 8 and the precision varying from 53 to 200. For the contrast probability distribution, the precision is selected as 500 and $t = 10$. These parameters are chosen according to the instantiation in [2].

According to Theorem 1, errors under $\Delta_{\rm SD}$, $\Delta_{\rm RD}$ and $\Delta_{\rm KL}$ are combinations of truncation errors, floating-point errors and convolution errors. The parameters of our experiments are chosen with fixed s, separated $t = 3, 5, 7$ and varying precisions. It is interesting to find that practical errors will eventually stay unchanged with large enough precisions, where the practical error is mainly influenced by truncation errors and convolution errors. It can be seen that the results shown in Figure 1(a) are consist with that in Theorem 1.

As for $\Delta_{\rm RE}$ and $\Delta_{\rm ML}$, we select following parameters to conduct experiments: $s_1 = s_2 = 34$, $a = 4, b = 3$,

$s = \sqrt{a^2 s_1^2 + b^2 s_2^2}$, $x_1 \in [-ts_1, ts_1], x_2 \in [-ts_2, ts_2]$, with t varying from 3 to 8 and precisions varying from 53 to 200. For the contrast probability distribution, the precision is selected as 500 and $t = 10$ which make truncation errors and floating-point errors as small as possible. These parameters are chosen according to the instantiation in [1].

The results about errors under Δ_{ML} and Δ_{RE} can be found in Figure 1(b). What is interesting is that as $C_3 \varepsilon_t^{\omega^2 \psi^2} \gg \max(2\mu, 2\varepsilon)$, our estimation indicates that the practical errors may not change when the precisions varies from 53 to 200 which seems to be well supported by the experiment.

Conclusion. We make two critical observations about practical errors and take the practical error estimation for convolution theorem with respect to discrete Gaussian sampling (using rejection method) as an example to show how to use these observations to more precisely determine the dominate term of practical errors. Extensive experiments have been conducted and the results highly agree with our derived bound. Our result shows that error estimations of a convolution theorem under KL-divergence, Max-log distance and Rényi-divergence depend on the use of sampling methods; in particular, finer error bounds do not hold when using rejection sampling.

Acknowledgements This work was supported by National Key Research and Development Program of China (Grant No. 2017YFA0303903), National Cryptography Development Fund (Grant No. MMJJ20170121), and Zhejiang Province Key R&D Project (Grant No. 2017C01062).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Micciancio D, Walter M. Gaussian sampling over the integers: efficient, generic, constant-time. In: Proceedings of CRYPTO 2017, 2017. 455–485

2 Pöppelmann T, Ducas L, Güneysu T. Enhanced lattice-based signatures on reconfigurable hardware. In: Proceedings of International Workshop on Cryptographic Hardware and Embedded Systems. Berlin: Springer, 2014. 353–370

3 Prest T. Sharper bounds in lattice-based cryptography using the Rényi divergence. In: Proceedings of ASIACRYPTO 2017, 2017. 347–374

4 Du Y S, Wei B D, Zhang H. A rejection sampling algorithm for off-centered discrete Gaussian distributions over the integers. Sci China Inf Sci, 2019, 62: 039103

5 Peikert C. An efficient and parallel Gaussian sampler for lattices. In: Proceedings of Annual Cryptology Conference. Berlin: Springer, 2010. 80–97

6 Micciancio D, Peikert C. Hardness of SIS and LWE with small parameters. In: Proceedings of Advances in Cryptology-CRYPTO 2013. Berlin: Springer, 2013. 21–39

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