Comment on "On Gaussian sampling, smoothing parameter and application to lattice signatures"

Cong Ling

Imperial College London, London SW7 2AZ, United Kingdom
c.ling@imperial.ac.uk

We show the key ideas of the above-referenced work for lattice Gaussian sampling [1], which won the best paper award of Asiacrypt 2023, are not new; the same ideas have been proposed by Ling *et al.* in 2014 [2, 3], which are not cited in [1] however.

Next, let us compare the main technical contributions of [1] with [2, 3].

1 "Algebraic Extensions and Sampling" [1, Section 3]

The authors of [1] consider lattice Λ and its sublattices Λ', and show that if one can sample efficiently in Λ' and Λ/Λ', then one has a sampler for Λ', for sampling width above the smoothing parameter of Λ'.

However, the same problem has been studied in [3]. The second part of the following lemma gives such a sampler:

Lemma 1. *([3, Lemma 5]) Let $\Lambda' \subset \Lambda$ be a pair of nested lattices such that $\epsilon_{\Lambda'}(\sigma) < \frac{1}{2}$. Then*

$$\mathbb{V}(D_{\Lambda,\sigma,\mathbf{c}} \mod \Lambda', U(\Lambda/\Lambda')) \leq 4\epsilon_{\Lambda'}(\sigma),$$

where $U(\Lambda/\Lambda')$ denotes the uniform distribution over the finite set Λ/Λ'. Conversely, if L is uniformly distributed in $[\Lambda/\Lambda']$ and L' is sampled from $D_{\Lambda',\sigma,\mathbf{c}-\mathsf{L}}$, then the distribution $D_{\mathsf{L}+\mathsf{L}'}$ satisfies

$$\mathbb{V}(D_{\mathsf{L}+\mathsf{L}'}, D_{\Lambda,\sigma,\mathbf{c}}) \leq \frac{2\epsilon_{\Lambda'}(\sigma)}{1-\epsilon_{\Lambda'}(\sigma)}.$$

This lemma has been used to construct a Gaussian sampler in [3, Section V], with the following details given [3, p.6410]:

"We note that the distribution of Alice's signal can be approximated by D_{Λ_b,σ_s}, when the confidential message is uniformly distributed. More precisely, since Alice transmits $\mathbf{x} \sim D_{\Lambda_e+\lambda_m,\sigma_s}$, by Lemma 1, the density p_{X^n} of $\mathbf{x}$ is close to the discrete Gaussian distribution over Λ_b, if $\lambda_m \in \Lambda_b/\Lambda_e$ is uniformly distributed. In fact, we have $\mathbb{V}(p_{X^n}, D_{\Lambda_b,\sigma_s}) \leq \frac{2\varepsilon}{1-\varepsilon}$ when $\varepsilon \triangleq \epsilon_{\Lambda_e}(\sigma_s) < \frac{1}{2}$."

The sampler in [1, Section 3] follows the same approach. It is more general, allows a slightly non-uniform distribution on $[\Lambda/\Lambda']$, and refers to a short exact sequence

$$0 \to \Lambda' \to \Lambda \to \Lambda/\Lambda' \to 0$$

which is just another way to say $\Lambda' \subset \Lambda$. In fact, [1, Lemma 3] and its proof are almost the same as [3, Lemma 5, p.6405] and its proof [3, p.6414], despite being more general. The bound $\frac{\varepsilon}{1-\varepsilon}$ on the total variational distance of [1, Lemma 3] differs from the $\frac{2\epsilon_{\Lambda'}(\sigma)}{1-\epsilon_{\Lambda'}(\sigma)}$ of [3, Lemma 5, p.6405] by a factor of 2, only due to a slight difference in the definitions of the total variantial distance.

Moreover, the sampler of [1, Corollary 3] assumes a uniform distribution over $[\Lambda/\Lambda']$, which is exactly the setting of [3, Lemma 5].

2 "Sampling in Remarkable Lattices" [1, Section 6]

The authors of [1] build efficient samplers for the $\mathrm{A}_n, \mathrm{D}_n,$, E_n and other lattices.

However, [2, Section IV] has already presented a sampler for Construction A in which codewords are sampled uniformly at random and proved that the resultant distribution is close to a lattice Gaussian if s exceeds the smoothing parameter of $q\mathbb{Z}$.

It further exemplified the method by considering the checkerboard lattice D_n and Gosset lattice E_8.

3 "A Filtration Sampler" [1, Section 4.2]

A 'filtration sampler' is given in [1, Section 4.2], where $\Lambda_0 \subset \Lambda_1 \subset \Lambda_2 \subset \cdots$. It is stated that "the smoothing parameter is dominated by the biggest term appearing in the splitting."

However, the same problem has been considered in [2, Section IV]:

"*Remark 7:* It is straightforward to extend the encoding procedure to multi-level lattices [19]. In this case, the variational distance bound (27) is determined by the flatness factor of the bottom lattice."

4 "An Exact Calculation of the Smoothing Parameter" [1, p.84]

A method is given in [1, p.84] to find the smoothing parameter using the relation between the lattice Gaussian distribution and the theta series. It is stated that "determining the smoothing parameter of a lattice amounts to find q such that $\Theta_{\Lambda^\vee}(q) - 1 = \epsilon$", where $\Lambda^\vee$ denotes the dual lattice.

However, such a method has already been proposed in [3]:

Corollary 1. *([3, Corollary 1]) Alternatively, the flatness factor can be expressed on the dual lattice Λ^* as*

$$\epsilon_\Lambda(\sigma) = \Theta_{\Lambda^*}\left(2\pi\sigma^2\right) - 1. \tag{1}$$

After a change of variables, (1) is identical to $\Theta_{\Lambda^\vee}(q) - 1 = \epsilon$ in [1, p.84].

5 Conclusion

Reference [1] makes many extensions, but the key ideas are the same as [2, 3] published in IEEE Transactions on Information Theory 9 years before.

References

1. Espitau, T., Wallet, A., Yu, Y.: On Gaussian sampling, smoothing parameter and application to lattice signatures. In: Guo, J., Steinfeld, R. (eds.) Advances in Cryptology – ASIACRYPT 2023. pp. 65–97. Springer Nature, Singapore (2023)
2. Ling, C., Belfiore, J.C.: Achieving AWGN channel capacity with lattice Gaussian coding. IEEE Transactions on Information Theory **60**(10), 5918–5929 (2014)
3. Ling, C., Luzzi, L., Belfiore, J.C., Stehlé, D.: Semantically secure lattice codes for the Gaussian wiretap channel. IEEE Transactions on Information Theory **60**(10), 6399–6416 (2014)