Lattice Gaussian Coding for Capacity and Secrecy: Two Sides of One Coin

(Invited Paper)

Cong Ling
Department of Electrical and Electronic Engineering
Imperial College London
London, UK
Email: c.ling@imperial.ac.uk

Jean-Claude Belfiore
Department of Communications and Electronics
Telecom ParisTech
Paris, France
Email: belfiore@telecom-paristech.fr

***Abstract*—Based on the lattice Gaussian distribution and the associated flatness factor, we present a unified view of lattice coding for achieving the Shannon capacity of the additive white Gaussian noise (AWGN) channel and for approaching the secrecy capacity of the Gaussian wiretap channel. In the former scenario, we apply Gaussian shaping to an AWGN-good lattice; in the latter scenario, we use a secrecy-good lattice nested with an AWGN-good lattice. We show that they represent different aspects of the lattice Gaussian distribution.**

I. Introduction

The lattice Gaussian distribution is emerging as a common theme in diverse areas. In mathematics, Banaszczyk [1] firstly used it to prove the transference theorems of lattices. In cryptography, Micciancio and Regev used it to propose lattice-based cryptosystems based on the worst-case hardness assumptions [2], and recently, it has underpinned the fully-homomorphic encryption for cloud computing [3]. In communications, Forney applied the lattice Gaussian distribution to shaping of lattice codes [4] (see also [5]), and studied lattice-aliased Gaussian noise in [6].

More recently, we defined the *flatness factor* associated with the lattice Gaussian distribution and derived its many properties [7, 8]. With this new tool, we are now able to answer/address several major open questions in lattice coding. For example, Erez and Zamir [9] proposed nested lattice codes achieving the capacity of the power-constrained additive white Gaussian noise (AWGN) channel, where a quantization-good lattice serves as the shaping lattice while the AWGN-good lattice serves as the coding lattice (dithering is also required). In [8], we proposed *lattice Gaussian coding*, where the codebook has a discrete Gaussian distribution over an AWGN-good lattice. As another example, in [7] we used the lattice Gaussian distribution to achieve *semantic security* over the Gaussian wiretap channel, which led to the notion of *secrecy-good lattices*. In both cases, we do not need a shaping lattice or a dither.

In this review paper, we aim to present a unified view of lattice Gaussian coding for capacity and secrecy. In Section II, we review lattice Gaussian distributions and the flatness factor. Section III describes the lattice Gaussian coding scheme for the AWGN channel. Section IV gives the scheme for the Gaussian wiretap channel, where the fine code is a Gaussian-shaped AWGN-good lattice achieving the capacity of the legitimate channel, and the coarse code is a secrecy-good lattice which ensures the information leakage on the eavesdropper's channel is negligible. We try to shed light on the commonality of the schemes for capacity and for secrecy [7, 8].

Throughout this paper, we use the natural logarithm, denoted by $\log$, and information is measured in nats.

II. Lattice Gaussian Distribution and Flatness Factor

An n-dimensional lattice Λ in the Euclidean space $\mathbb{R}^n$ is a set defined by

$$\Lambda = \mathcal{L}(\mathbf{B}) = \{\mathbf{Bx} : \mathbf{x} \in \mathbb{Z}^n\}$$

where $\mathbf{B}$ is the n-by-n generator matrix. The dual lattice Λ^* of a lattice Λ is defined as the set of vectors $\mathbf{v} \in \mathbb{R}^n$ such that $\langle \mathbf{v}, \boldsymbol{\lambda} \rangle \in \mathbb{Z}$, for all $\boldsymbol{\lambda} \in \Lambda$.

For $\sigma > 0$ and $\mathbf{c} \in \mathbb{R}^n$, the usual Gaussian distribution of variance σ^2 centered at $\mathbf{c} \in \mathbb{R}^n$ is given by

$$f_{\sigma,\mathbf{c}}(\mathbf{x}) = \frac{1}{(\sqrt{2\pi}\sigma)^n} e^{-\frac{\|\mathbf{x}-\mathbf{c}\|^2}{2\sigma^2}},$$

for all $\mathbf{x} \in \mathbb{R}^n$. For convenience, we write $f_\sigma(\mathbf{x}) = f_{\sigma,\mathbf{0}}(\mathbf{x})$.

Consider the Λ-periodic function (see Fig. 1(a))

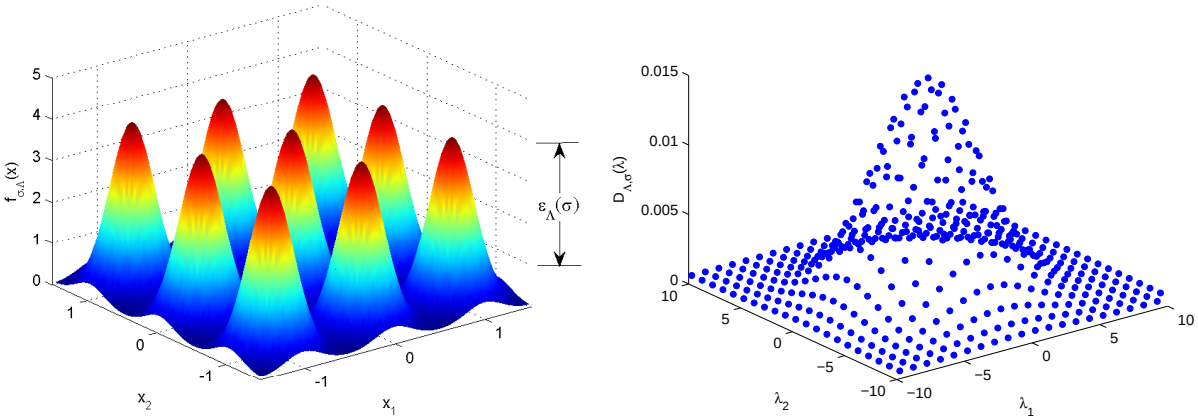
$$f_{\sigma,\Lambda}(\mathbf{x}) = \sum_{\boldsymbol{\lambda}\in\Lambda} f_{\sigma,\boldsymbol{\lambda}}(\mathbf{x}) = \frac{1}{(\sqrt{2\pi}\sigma)^n} \sum_{\boldsymbol{\lambda}\in\Lambda} e^{-\frac{\|\mathbf{x}-\boldsymbol{\lambda}\|^2}{2\sigma^2}}, \quad (1)$$

for all $\mathbf{x} \in \mathbb{R}^n$. Observe that $f_{\sigma,\Lambda}$ restricted to the fundamental region $\mathcal{R}(\Lambda)$ is a probability density.

We define the *discrete Gaussian distribution* over Λ centered at $\mathbf{c} \in \mathbb{R}^n$ as the following discrete distribution taking values in $\boldsymbol{\lambda} \in \Lambda$:

$$D_{\Lambda,\sigma,\mathbf{c}}(\boldsymbol{\lambda}) = \frac{f_{\sigma,\mathbf{c}}(\boldsymbol{\lambda})}{f_{\sigma,\mathbf{c}}(\Lambda)}, \quad \forall \boldsymbol{\lambda} \in \Lambda,$$

where $f_{\sigma,\mathbf{c}}(\Lambda) \triangleq \sum_{\boldsymbol{\lambda}\in\Lambda} f_{\sigma,\mathbf{c}}(\boldsymbol{\lambda}) = f_{\sigma,\Lambda}(\mathbf{c})$. Again for convenience, we write $D_{\Lambda,\sigma} = D_{\Lambda,\sigma,\mathbf{0}}$. Fig. 1(b) illustrates the discrete Gaussian distribution over $\mathbb{Z}^2$. As can be seen, it resembles a continuous Gaussian distribution, but is only defined over a lattice.



(a) Continuous periodic distribution $f_{\sigma,\Lambda}(\mathbf{x})$. (b) Discrete Gaussian distribution $D_{\Lambda,\sigma}(\boldsymbol{\lambda})$.

Fig. 1. Lattice Gaussian distributions.

In some sense, the continuous distribution $f_{\sigma,\Lambda}$ and the discrete distribution $D_{\Lambda,\sigma}$ are the Fourier dual of each other. To see this, note that since $f_{\sigma,\Lambda}(\mathbf{x})$ is Λ-periodic, it has the Fourier expansion on the dual lattice Λ^*

$$f_{\sigma,\Lambda}(\mathbf{x}) = \frac{1}{V(\Lambda)} \sum_{\boldsymbol{\lambda}^* \in \Lambda^*} \hat{f}_\sigma(\boldsymbol{\lambda}^*) e^{j2\pi\langle \boldsymbol{\lambda}^*, \mathbf{x}\rangle}$$

where

$$\hat{f}_\sigma(\mathbf{y}) = \int f_\sigma(\mathbf{x}) e^{-j2\pi\langle \mathbf{x},\mathbf{y}\rangle} d\mathbf{x} = e^{-2\pi^2\sigma^2\|\mathbf{y}\|^2} \tag{2}$$

is the Fourier transform. Thus, the Fourier coefficients $\hat{f}_\sigma(\boldsymbol{\lambda}^*)$ have a discrete Gaussian distribution over the dual lattice Λ^* (upon normalization).

The flatness factor of a lattice Λ quantifies the maximum variation of $f_{\sigma,\Lambda}(\mathbf{x})$ for $\mathbf{x} \in \mathbb{R}^n$.

Definition 1 (Flatness factor [7]). *For a lattice Λ and for a parameter σ, the flatness factor is defined by:*

$$\epsilon_\Lambda(\sigma) \triangleq \max_{\mathbf{x}\in\mathcal{R}(\Lambda)} \left| V(\Lambda) f_{\sigma,\Lambda}(\mathbf{x}) - 1 \right|.$$

In other words, $\frac{f_{\sigma,\Lambda}(\mathbf{x})}{1/V(\Lambda)}$, the ratio between $f_{\sigma,\Lambda}(\mathbf{x})$ and the uniform distribution over $\mathcal{R}(\Lambda)$, is within the range $[1-\epsilon_\Lambda(\sigma), 1+\epsilon_\Lambda(\sigma)]$.

Proposition 1 (Expression of $\epsilon_\Lambda(\sigma)$ [7]). *We have:*

$$\epsilon_\Lambda(\sigma) = \left(\frac{\gamma_\Lambda(\sigma)}{2\pi}\right)^{\frac{n}{2}} \Theta_\Lambda\left(\frac{1}{2\pi\sigma^2}\right) - 1$$

where $\gamma_\Lambda(\sigma) = \frac{V(\Lambda)^{\frac{2}{n}}}{\sigma^2}$ is the volume-to-noise ratio (VNR).

The following result guarantees the existence of sequences of mod-p lattices whose flatness factors can vanish as $n \to \infty$.

Theorem 1 ([7]). *$\forall \sigma > 0$ and $\forall \delta > 0$, there exists a sequence of mod-p lattices $\Lambda^{(n)}$ such that*

$$\epsilon_{\Lambda^{(n)}}(\sigma) \le (1+\delta) \cdot \left(\frac{\gamma_{\Lambda^{(n)}}(\sigma)}{2\pi}\right)^{\frac{n}{2}}, \tag{3}$$

i.e., the flatness factor can go to zero exponentially for any fixed VNR $\gamma_{\Lambda^{(n)}}(\sigma) < 2\pi$.

The importance of a small flatness factor is two-fold. Firstly, it assures the "folded" distribution $f_{\sigma,\Lambda}(\mathbf{x})$ is flat; secondly, it implies the discrete Gaussian distribution $D_{\Lambda,\sigma,\mathbf{c}}$ is "smooth". In the following, we collect properties of lattice Gaussian distributions.

Lemma 1 ([7]). *Let $\Lambda' \subset \Lambda$ be a pair of nested lattices such that $\epsilon_{\Lambda'}(\sigma) < \frac{1}{2}$. If $\mathbf{a}$ is uniformly distributed in Λ/Λ' and $\mathbf{b}$ is sampled from $D_{\Lambda',\sigma,\mathbf{c}-\mathbf{a}}$, then the distribution $D_{\mathbf{a}+\mathbf{b}}$ of $\mathbf{a}+\mathbf{b}$ satisfies*

$$\mathbb{V}(D_{\mathbf{a}+\mathbf{b}}, D_{\Lambda,\sigma,\mathbf{c}}) \le \frac{2\epsilon_{\Lambda'}(\sigma)}{1-\epsilon_{\Lambda'}(\sigma)}.$$

Lemma 2 (Variance of lattice Gaussian [7]). *Let $\mathbf{x} \sim D_{\Lambda,\sigma,\mathbf{c}}$. If $\varepsilon = \epsilon_\Lambda\left(\sigma/\sqrt{\frac{\pi}{\pi-t}}\right) < 1$ for $0 < t < \pi$, then*

$$\left| \mathbb{E}\left[\|\mathbf{x}-\mathbf{c}\|^2\right] - n\sigma^2 \right| \le \frac{2\pi\varepsilon_t}{1-\varepsilon}\sigma^2$$

where

$$\varepsilon_t \triangleq \begin{cases} \varepsilon, & t \ge 1/e; \\ (t^{-4}+1)\varepsilon, & 0 < t < 1/e. \end{cases}$$

Lemma 3 (Entropy of lattice Gaussian [7]). *Let $\mathbf{x} \sim D_{\Lambda,\sigma,\mathbf{c}}$. If $\varepsilon = \epsilon_\Lambda\left(\sigma/\sqrt{\frac{\pi}{\pi-t}}\right) < 1$ for $0 < t < \pi$, then the entropy rate of $\mathbf{x}$ satisfies*

$$\left| \frac{1}{n}\mathbb{H}(\mathbf{x}) - \left[\log(\sqrt{2\pi e}\sigma) - \frac{1}{n}\log V(\Lambda)\right] \right| \le \varepsilon',$$

where $\varepsilon' = -\frac{\log(1-\varepsilon)}{n} + \frac{\pi\varepsilon_t}{n(1-\varepsilon)}$.

Lemma 4 ([10]). *Given any vector $\mathbf{c} \in \mathbb{R}^n$, and $\sigma_s, \sigma > 0$. Let $\tilde{\sigma} \triangleq \frac{\sigma_s\sigma}{\sqrt{\sigma_s^2+\sigma^2}}$ and let $\sigma_s' = \sqrt{\sigma_s^2+\sigma^2}$. Consider the continuous distribution g on $\mathbb{R}^n$ obtained by adding a continuous Gaussian of variance σ^2 to a discrete Gaussian $D_{\Lambda-\mathbf{c},\sigma_s}$:*

$$g(\mathbf{x}) = \frac{1}{f_{\sigma_s}(\Lambda-\mathbf{c})} \sum_{\mathbf{t}\in\Lambda-\mathbf{c}} f_{\sigma_s}(\mathbf{t}) f_\sigma(\mathbf{x}-\mathbf{t}), \quad \mathbf{x} \in \mathbb{R}^n.$$

If $\varepsilon = \epsilon_\Lambda(\tilde{\sigma}) < \frac{1}{2}$*, then* $\frac{g(\mathbf{x})}{f_{\sigma_s'}(\mathbf{x})}$ *is uniformly close to* 1*:*

$$\forall \mathbf{x} \in \mathbb{R}^n, \quad \left| \frac{g(\mathbf{x})}{f_{\sigma_s'}(\mathbf{x})} - 1 \right| \leq 4\varepsilon. \tag{4}$$

Regev's lemma leads to an important property, namely, the discrete Gaussian distribution over a lattice is almost capacity-achieving if the flatness factor is small [8].

III. Achieving Channel Capacity

Consider the classic AWGN channel

$$\mathsf{Y}^n = \mathsf{X}^n + \mathsf{W}^n$$

where W^n is an n-dimensional Gaussian noise vector with zero mean and variance σ_w^2.

In [8], we proposed a new coding scheme based on the lattice Gaussian distribution with power constraint P. The SNR is defined by $\mathsf{SNR} = P/\sigma_w^2$. Let Λ be an AWGN-good lattice of dimension n. The encoder maps the information bits to points in Λ, which obey the lattice Gaussian distribution (cf. Fig. 1(b))

$$\mathbf{x} \sim D_{\Lambda,\sigma_s}.$$

Since the continuous Gaussian distribution is capacity-achieving, we want the lattice Gaussian distribution to behave like the continuous Gaussian distribution (in particular $P \approx \sigma_s^2$). This can be assured by a small flatness factor $\epsilon_\Lambda\left(\sigma_s/\sqrt{\frac{\pi}{\pi - t}}\right)$ for $0 < t < \pi$. For $t \to 0$, this condition is essentially $\epsilon_\Lambda(\sigma_s) \to 0$. Thus, while we are concerned with the discrete distribution D_{Λ,σ_s}, we in fact require the associated periodic distribution $f_{\sigma_s,\Lambda}$ to be flat.

Since the lattice points are not equally probable a priori in the lattice Gaussian coding, we will use maximum-a-posteriori (MAP) decoding. In [7], it was shown that MAP decoding is equivalent to Euclidean lattice decoding of Λ using a scaling coefficient $\alpha = \frac{\sigma_s^2}{\sigma_s^2 + \sigma_w^2}$, which is asymptotically equal to the MMSE coefficient $\frac{P}{P+\sigma_w^2}$. In fact, the error probability of the proposed scheme under MMSE lattice decoding admits almost the same expression as that of Poltyrev [11], with σ_w replaced by $\tilde{\sigma}_w = \frac{\sigma_s \sigma_w}{\sqrt{\sigma_s^2 + \sigma_w^2}}$. To satisfy the sphere bound, we choose the fundamental volume $V(\Lambda)$ such that

$$V(\Lambda)^{2/n} > 2\pi e \tilde{\sigma}_w^2. \tag{5}$$

Meanwhile, the rate of the scheme is given by the entropy of the lattice Gaussian distribution. By Lemma 3, we have

$$\begin{aligned} R &\to \log(\sqrt{2\pi e}\sigma_s) - \frac{1}{n}\log V(\Lambda) \\ &< \log(\sqrt{2\pi e}\sigma_s) - \frac{1}{2}\log\left(2\pi e \frac{\sigma_s^2 \sigma_w^2}{\sigma_s^2 + \sigma_w^2}\right) \\ &= \frac{1}{2}\log\left(1 + \frac{\sigma_s^2}{\sigma_w^2}\right) \\ &\to \frac{1}{2}\log(1 + \mathsf{SNR}). \end{aligned}$$

In fact, the rate can be arbitrarily close to the channel capacity. A more careful analysis also shows that the condition $\mathsf{SNR} > e$ is needed.

Theorem 2 (Coding theorem for lattice Gaussian coding [8])**.** *Consider a lattice code whose codewords are drawn from the discrete Gaussian distribution* D_{Λ,σ_s} *for an AWGN-good lattice* Λ*. If* $\mathsf{SNR} > e$*, then any rate up to the channel capacity* $\frac{1}{2}\log(1 + \mathsf{SNR})$ *is achievable, while the error probability of MMSE lattice decoding vanishes exponentially fast.*

IV. Approaching Secrecy Capacity

Now consider the Gaussian wiretap channel where Alice and Bob are the legitimate users, while Eve is an eavesdropper. The outputs Y^n and Z^n at Bob and Eve's ends respectively are given by

$$\begin{cases} \mathsf{Y}^n = \mathsf{X}^n + \mathsf{W}_b^n, \\ \mathsf{Z}^n = \mathsf{X}^n + \mathsf{W}_e^n, \end{cases} \tag{6}$$

where W_b^n, W_e^n are n-dimensional Gaussian noise vectors with zero mean and variance σ_b^2, σ_e^2 respectively.

For secrecy rate R, we use coset coding induced by a lattice partition $\Lambda_e \subset \Lambda_b$ such that

$$\frac{1}{n}\log|\Lambda_b/\Lambda_e| = R.$$

The fine lattice Λ_b is the usual coding lattice for Bob, i.e., it is an AWGN-good lattice. The coarse lattice Λ_e is new, and turns out to be a secrecy-good lattice. To encode, Alice uses the secret bits to select one coset of Λ_e and transmits a random point inside this coset.

Let us discuss intuitively why this scheme is secure. Informally, given message m, Alice samples a lattice point uniformly at random from a coset $\Lambda_e + \boldsymbol{\lambda}_m$ (this corresponds to Poltyrev's setting of infinite lattice coding [11]). Due to the channel noise, Eve observes the periodic distribution

$$\frac{1}{(\sqrt{2\pi}\sigma_e)^n} \sum_{\boldsymbol{\lambda} \in \Lambda + \boldsymbol{\lambda}_m} e^{-\frac{\|\mathbf{z} - \boldsymbol{\lambda}\|^2}{2\sigma_e^2}}.$$

If the flatness factor $\epsilon_{\Lambda_e}(\sigma_e)$ is small, it will be close to a uniform distribution, regardless of message m. Then Eve would not be able to distinguish which message Alice has sent. With a careful design of Λ_e, this is possible, because Eve's channel is noisier. Of course, the technical difficulty here is that one cannot really sample a lattice point uniformly from a lattice or its coset.

Now we describe the wiretap coding scheme more formally. Consider a message set $\mathcal{M}_n = \{1, \ldots, e^{nR}\}$, and a one-to-one function $\phi : \mathcal{M}_n \to \Lambda_b/\Lambda_e$ which associates each message $m \in \mathcal{M}_n$ to a coset $\widetilde{\boldsymbol{\lambda}}_m \in \Lambda_b/\Lambda_e$. One could choose the coset representative $\boldsymbol{\lambda}_m \in \Lambda_b \cap \mathcal{R}(\Lambda_e)$ for any fundamental region $\mathcal{R}(\Lambda_e)$. In order to encode the message $m \in \mathcal{M}_n$, Alice actually samples X_m^n from lattice Gaussian distribution

$$\mathsf{X}_m^n \sim D_{\Lambda_e + \boldsymbol{\lambda}_m, \sigma_s}.$$

equivalently, Alice transmits $\boldsymbol{\lambda}+\boldsymbol{\lambda}_m$ where $\boldsymbol{\lambda} \sim D_{\Lambda_e,\sigma_s,-\boldsymbol{\lambda}_m}$. Let $\tilde{\sigma}_e = \frac{\sigma_s\sigma_e}{\sqrt{\sigma_s^2+\sigma_e^2}}$ and $\sigma_s' = \sqrt{\sigma_s^2+\sigma_e^2}$. Regev's Lemma 4 implies that if $\epsilon_{\Lambda_e}(\tilde{\sigma}_e) < \frac{1}{2}$, then:

$$\mathbb{V}\left(p_{\mathsf{Z}^n|\mathsf{M}}(\cdot|m), f_{\sigma_s'}\right) \leq 4\epsilon_{\Lambda_e}(\tilde{\sigma}_e).$$

We see that the received signals converge to the same Gaussian distribution $f_{\sigma_s'}$. This already gives *distinguishing security*, which means that, asymptotically, the channel outputs are indistinguishable for different input messages.

An upper bound on the amount of leaked information then follows.

Theorem 3 (Information leakage [7])**.** *Suppose that the wiretap coding scheme described above is employed on the Gaussian wiretap channel (6), and let $\varepsilon_n = \epsilon_{\Lambda_e}(\tilde{\sigma}_e)$. Assume that $\varepsilon_n < \frac{1}{2}$ for all n. Then the mutual information between the confidential message and the eavesdropper's signal is bounded as follows:*

$$\mathbb{I}(\mathsf{M};\mathsf{Z}^n) \leq 8\varepsilon_n nR - 8\varepsilon_n \log 8\varepsilon_n. \tag{7}$$

A wiretap coding scheme is secure in the sense of *strong secrecy* if $\lim_{n\to\infty}\mathbb{I}(\mathsf{M};\mathsf{Z}^n) = 0$. From (7), a flatness factor $\varepsilon_n = o(\frac{1}{n})$ would be enough. In practice, an exponential decay of the information leakage is desired, and this motivates the notion of secrecy-good lattices:

Definition 2 (Secrecy-good lattices)**.** *A sequence of lattices $\Lambda^{(n)}$ is* secrecy-good *if*

$$\epsilon_{\Lambda^{(n)}}(\sigma) = e^{-\Omega(n)}, \quad \forall \gamma_{\Lambda^{(n)}}(\sigma) < 2\pi. \tag{8}$$

In the notion of strong secrecy, plaintext messages are often assumed to be random and uniformly distributed in $\mathcal{M}$. This assumption is deemed problematic from the cryptographic perspective, since in many setups plaintext messages are not random. This issue can be resolved by using the standard notion of *semantic security* [12] which means that, asymptotically, it is impossible to estimate any function of the message better than to guess it without considering Z^n at all. The relation between strong secrecy and semantic security was recently revealed in [7, 13], namely, achieving strong secrecy for all distributions of the plaintext messages is equivalent to achieving semantic security. Since in our scheme we make no *a priori* assumption on the distribution of m, it achieves semantic security.

It was shown in [7] that, under mild conditions, the secrecy rate

$$R < \frac{1}{2}\log(1+\mathsf{SNR}_b) - \frac{1}{2}\log(1+\mathsf{SNR}_e) - \frac{1}{2} \tag{9}$$

is achievable, which is within a half nat from the secrecy capacity.

Lastly, let us scrutinize the distribution of Alice's constellation. For this purpose only, we assume the confidential message $\boldsymbol{\lambda}_m \in [\Lambda_b/\Lambda_e]$ is uniformly distributed (or the secrecy rate will be smaller). By Lemma 1, if $\epsilon_{\Lambda_e}(\sigma_s) \leq \varepsilon$ (which we trivially have, since even $\epsilon_{\Lambda_e}(\tilde{\sigma}_e) \to 0$), then

$$\mathbb{V}(p_{\mathsf{X}^n}, D_{\Lambda_b,\sigma_s}) \leq \frac{2\varepsilon}{1-\varepsilon}.$$

Namely, the density p_{X^n} is close to the discrete Gaussian distribution over Λ_b. This shows that in fact, the fine code is capacity-achieving for Bob's channel. In contrast, from (9), we know that the coarse code has a rate $> \frac{1}{2}\log(1+\mathsf{SNR}_e)+\frac{1}{2}$, i.e., above the capacity of Eve's channel.

V. Discussion

In this paper, we have demonstrated the applications of the lattice Gaussian distribution to coding problems for the AWGN channel and the Gaussian wiretap channel. For capacity it is desired that the discrete Gaussian distribution of the lattice codebook behaves like the continuous Gaussian distribution, while for secrecy it is required that the aliased Gaussian distribution of the noise becomes flat. Both scenarios demand a vanishing flatness factor and thus can be viewed as two sides of one coin.

Acknowledgment

This work was supported in part by FP7 project PHYLAWS (EU FP7-ICT 317562).

References

[1] W. Banaszczyk, "New bounds in some transference theorems in the geometry of numbers," *Math. Ann.*, vol. 296, pp. 625–635, 1993.

[2] D. Micciancio and O. Regev, "Worst-case to average-case reductions based on Gaussian measures," in *Proc. Ann. Symp. Found. Computer Science*, Rome, Italy, Oct. 2004, pp. 372–381.

[3] C. Gentry, "Fully homomorphic encryption using ideal lattices," in *Proc. STOC*, 2009.

[4] G. Forney and L.-F. Wei, "Multidimensional constellations–Part II: Voronoi constellations," *IEEE J. Sel. Areas Commun.*, vol. 7, no. 6, pp. 941–958, Aug 1989.

[5] F. R. Kschischang and S. Pasupathy, "Optimal nonuniform signaling for Gaussian channels," *IEEE Trans. Inform. Theory*, vol. 39, pp. 913–929, May 1993.

[6] G. Forney, M. Trott, and S.-Y. Chung, "Sphere-bound-achieving coset codes and multilevel coset codes," *IEEE Trans. Inform. Theory*, vol. 46, no. 3, pp. 820–850, May 2000.

[7] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," submitted to IEEE Trans. Inform. Theory, Oct. 2012, revised, Oct. 2013. [Online]. Available: http://arxiv.org/abs/1210.6673

[8] C. Ling and J.-C. Belfiore, "Achieiving the AWGN channel capacity with lattice Gaussian coding," submitted to IEEE Trans. Inform. Theory, Mar. 2012, revised, Nov. 2013. [Online]. Available: http://arxiv.org/abs/1302.5906

[9] U. Erez and R. Zamir, "Achieving $\frac{1}{2}$ log(1+SNR) on the AWGN channel with lattice encoding and decoding," *IEEE Trans. Inform. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[10] O. Regev, "On lattices, learning with errors, random linear codes, and cryptography," *J. ACM*, vol. 56, no. 6, pp. 34:1–34:40, 2009.

[11] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inform. Theory*, vol. 40, pp. 409–417, Mar. 1994.

[12] S. Goldwasser and S. Micali, "Probabilistic encryption," *J. Comput. Syst. Sci.*, vol. 28, no. 2, pp. 270–299, 1984.

[13] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Proc. CRYPTO 2012*, ser. Lecture Notes in Computer Science, vol. 7417. Springer-Verlag, pp. 294–311.