The Semantic Secrecy Rate of the Lattice Gaussian Coding for the Gaussian Wiretap Channel

Hamed Mirghasemi and Jean-Claude Belfiore

***Abstract*—In this paper, we investigate the achievable semantic secrecy rate of existing lattice coding schemes, proposed in [6], for both the mod-Λ Gaussian wiretap and the Gaussian wiretap channels. For both channels, we propose new upper bounds on the amount of leaked information which provide milder sufficient conditions to achieve semantic secrecy. These upper bounds show that the lattice coding schemes in [6] can achieve the secrecy capacity to within $\frac{1}{2}\ln e/2$ nat for the mod-Λ Gaussian and to within $\frac{1}{2}(1-\ln(1+\frac{SNR_e}{SNR_e+1}))$ nat for the Gaussian wiretap channels where SNR_e is the signal-to-noise ratio of Eve.**

I. Introduction

In [9], Wyner introduced the Wiretap channel, where Alice wishes to communicate a message to the legitimate receiver (Bob) over a channel (denoted by $(\mathcal{X},\mathcal{Y},p_{Y^n|X^n}(\mathbf{y}|\mathbf{x}))$), while it's messages are being eavesdropper by Eve through another channel (denoted by $(\mathcal{X},\mathcal{Z},p_{Z^n|X^n}(\mathbf{z}|\mathbf{x}))$). A wiretap code for the wiretap channel $(\mathcal{X},\mathcal{Y},\mathcal{Z},p_{Y^n|X^n},p_{Z^n|X^n})$ consists of the following

- a message set $\mathcal{M}_n$ from which a message is chosen randomly according to a distribution p_M;
- a stochastic encoding function $\phi_n : \mathcal{M}_n \to \mathcal{X}^n$;
- a decoding function $\psi_n : \mathcal{Y}_n \to \mathcal{M}_n$.

Any wiretap coding scheme should satisfy simultaneously two conditions, namely reliability and security. The reliability condition is that Bob can decode the message correctly as the code length n goes to infinity. The security condition is characterized by the mutual information between the message M and Eve's channel output Z^n. The weak security condition is defined by $\lim_{n\to\infty}\frac{I(M,Z^n)}{n}\to 0$. Motivated by the fact that the weak secrecy condition is not appropriate for some applications, Csiszar in [3] introduced the strong secrecy condition, given by $\lim_{n\to\infty} I(M,Z^n)=0$. In the notation of strong secrecy, uniform distribution of the message is often assumed. Since assuming that messages are a priori uniform is completely unacceptable in cryptography, the notation of semantic security has been proposed which requires that it is asymptotically impossible to guess any function of message better than to guess it without considering Z^n at all [2], and it is shown that strong secrecy for any message distribution implies semantic security. The maximum amount of information that Alice can transmit to Bob while satisfying both of reliability and security conditions is called the secrecy capacity. While the secrecy capacity of many channels has been extensively studied, the problem of wiretap code design for semantic secrecy has assumed interest in recent years ([7] and [1] for the case of discrete memoryless channels, and [10] for the case of modulo lattice channel). For the Gaussian wiretap channel, to best of our knowledge, a coding scheme which can achieve the semantic secrecy capacity has not been yet proposed. In [8], it is shown that the coding scheme of [1] can achieve the strong secrecy capacity of Gaussian wiretap channel, and in [6], the proposed lattice coding scheme can achieves rates within $1/2$ nats of secrecy capacity under semantic security criterion. In this work, we consider the lattice coding scheme proposed in [6], and we provide tighter upper bounds on the amount of leaked information (Theorem 1 for the case of modulo lattice channel and Theorem 3 for the case of Gaussian channel). Using these bounds, we show that the lattice coding scheme in [6] can achieve rates within $\frac{1}{2}\ln(e/2)$ of the secrecy capacity of the mod-Λ Gaussian wiretap channel and within $\frac{1}{2}(1-\ln(1+\frac{SNR_e}{1+SNR_e}))$ of the secrecy capacity of the Gaussian wiretap channel under the semantic security criterion.

This work was supported in part by FP7 project PHYLAWS (EU FP7-ICT 317562). H. Mirghasemi and J-C. Belfiore are with the Communications and Electronics Department, Telecom ParisTech, 75634 Paris Cedex 13. Emails: {mirghasemi,belfiore@telecom-paristech.fr}.

A. The wiretap channel

The achievable semantic secrecy rate for a continuous channel is defined as follows.

Definition 1. A rate $R \overset{\text{def}}{=} \frac{1}{n}\ln|\mathcal{M}_n|$ is an achievable semantic secrecy rate if there exists a sequence of (ϕ_n,ψ_n) encoders and decoders such that

- Reliability: $\lim_{n\to\infty}\Pr(M\neq\psi_n(Y^n))=0$, where M is the random variable denoting the transmitted message;
- Semantic secrecy: $\lim_{n\to\infty} I(M,Z^n)=0$ for all message distributions;
- Power constraint: $\forall m\in\mathcal{M}_n\,,\ \frac{1}{n}E[\|\phi_n(m)\|^2]\leq P\,.$

The following lemma is essential to satisfy the semantic secrecy condition. This lemma states that if the conditional distributions of the channel output signals for different messages are very close to a given distribution, the amount of leaked information would be negligible.

Lemma 1 ([6, Lemma 2])**.** *Assume that for any n, there exists a density function q_{Z^n} in $\mathbb{R}^n$ such that $D_{TV}(p_{Z^n|M=m},q_{Z^n})\leq$*

978-1-4799-5999-0/14/$31.00 ©2014 IEEE

ϵ_n[1] *for all* $m \in \mathcal{M}_n$. *Then we have*

$$I(M, Z^n) \leq 2n\epsilon_n R - 2\epsilon_n \ln(2\epsilon_n)\,. \tag{1}$$

B. Preliminaries on Lattices

A n-dimensional lattice Λ is a discrete subgroup of $\mathbb{R}^n$, and can be characterized by a set of linearly independent generators $\mathbf{B} = \{\mathbf{b}_j, 1 \leq j \leq n\}$ such that Λ is the set of all integer linear combinations of the generators: $\Lambda = \{\mathbf{Bx} | \, \mathbf{x} \in \mathbb{Z}^n\}$. The dual lattice Λ^* of a lattice Λ is defined by: $\Lambda^* = \{\mathbf{u} \in \mathbb{R}^n | < \mathbf{u}, \lambda > \in \mathbb{Z}, \forall \lambda \in \Lambda\}$. A bounded region $\mathcal{R}(\Lambda) \in \mathbb{R}^n$ is called a fundamental region of Λ if every element of $\mathbb{R}^n$ can be written uniquely as the sum of a lattice point from Λ and an element from $\mathcal{R}$. The nearest-neighbor quantizer and the modulo lattice operators are defined as

$$Q_\Lambda(\mathbf{x}) \stackrel{\text{def}}{=} \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \lambda\|\,,$$
$$\mathbf{x} \bmod \Lambda \stackrel{\text{def}}{=} \mathbf{x} - Q_\Lambda(\mathbf{x})\,,$$

respectively. The Voronoi cell of Λ, one fundamental region of lattice Λ, is defined by $\mathcal{V}(\Lambda) = \{\mathbf{x} \in \mathbb{R}^n | \, Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$, and it's volume is denoted by $V(\Lambda)$. For any $\sigma > 0$ and any lattice Λ, the volume-to-noise ratio (VNR) is defined as $\gamma_\Lambda(\sigma) \stackrel{\text{def}}{=} \frac{V(\Lambda)^{2/n}}{\sigma^2}$. For any $\tau > 0$, the Theta series of lattice Λ is defined as: $\Theta_\Lambda(\tau) \stackrel{\text{def}}{=} \sum_{\lambda \in \Lambda} e^{-\pi\tau\|\lambda\|^2}$.
A sequence of lattices Λ^n are good for Quantizaion if $\lim_{n\to\infty} \frac{\int_{\mathcal{V}} \|\mathbf{x}\|^2 \mathrm{d}\mathbf{x}}{nV^{1+2/n}} = \frac{1}{2\pi e}$. Also, a sequence of lattices Λ^n is AWGN-good if the probability that an iid Gaussian vector with variance σ^2 falls outside $\mathcal{R}(\Lambda)$ vanishes as long as $\gamma_\Lambda(\sigma) < 2\pi$.

C. Lattice Gaussian Distribution

For any positive σ and $\mathbf{c} \in \mathbb{R}^n$, we denote the continuous Gaussian distribution of variance σ^2 centered at $\mathbf{c}$ by $f_{\sigma,\mathbf{c}}(\mathbf{x}) = \frac{1}{(2\pi\sigma^2)^{n/2}} e^{-\frac{\|\mathbf{x}-\mathbf{c}\|^2}{2\sigma^2}}$. Another continuous distribution, called Λ-folded Gaussian distribution, is given by

$$f_{\sigma,\Lambda}(\mathbf{x}) = \sum_{\lambda \in \Lambda} f_{\sigma,\lambda}(\mathbf{x})\,.$$

Also, we consider the Lattice Gaussian distribution

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

where $f_{\sigma,\mathbf{c}}(\Lambda) \stackrel{\text{def}}{=} \sum_\lambda f_{\sigma,\mathbf{c}}(\lambda)$.

D. Flatness Factor

For any lattice Λ and any σ, the flatness factor is defined by

$$\epsilon_\Lambda(\sigma) \stackrel{\text{def}}{=} (\frac{\gamma_\Lambda(\sigma)}{2\pi})^{n/2} \Theta_\Lambda(\frac{1}{2\pi\sigma^2}) - 1\,, \tag{2}$$

[1]For any two distributions f and g defined on a common domain $\mathcal{R}$, the total variation distance is defined by $D_{\text{TV}}(f,g) = \int_{\mathcal{R}} |f(\mathbf{z}) - g(\mathbf{z})| \, \mathrm{d}\mathbf{z}$.

and quantifies the maximum difference between the Λ-folded Gaussian distribution and the Uniform distribution over $\mathcal{R}(\Lambda)$, i.e.,

$$\epsilon_\Lambda(\sigma) = \max_{\mathbf{x} \in \mathcal{R}} |\frac{f_{\sigma,\Lambda}(\mathbf{x})}{1/V(\Lambda)} - 1|\,. \tag{3}$$

In the rest of paper, we provide upper bounds on $I(M, Z^n)$ in terms of the flatness factor. The following lemma guarantees the existence of lattices in $\mathbb{R}^n$ whose flatness factors vanish exponentially as $n \to \infty$.

Lemma 2 ([6, Theorem 1])**.** *For any σ, there exists a sequence of lattices Λ such that $\epsilon_\Lambda(\sigma) \to 0$ exponentially provided that $\frac{V(\Lambda)^{2/n}}{\sigma^2} < 2\pi$.*

II. Mod-Λ Gaussian Wiretap Channel

In this section, we consider the mod-Λ Gaussian wiretap channel where both legitimate and eavesdropper channels are mod-Λ channels. For a given nested chain of n-dimensional lattices $\Lambda_s \subset \Lambda_e \subset \Lambda_b$, the channel input X^n is restricted to the $\mathcal{V}(\Lambda_s)$, and the outputs Y^n and Z^n of legitimate and eavesdropper are given by

$$Y^n = [X^n + N_b^n] \bmod \Lambda_s\,,$$
$$Z^n = [X^n + N_e^n] \bmod \Lambda_s\,,$$

where N_b and N_e are n-dimensional Gaussian vectors with zero mean and variance σ_b^2 and σ_e^2 respectively. We denote $R = \frac{1}{n}\ln(V(\Lambda_e)/V(\Lambda_b))$ and $R^{'} = \frac{1}{n}\ln(V(\Lambda_s)/V(\Lambda_e))$. The nested lattice encoding for the mod$-\Lambda$ Gaussian wiretap channel is as follows. For the given message set $\mathcal{M}_n = \{1, \cdots, e^{nR}\}$, let $\phi : \mathcal{M} \to \Lambda_b/\Lambda_e$ be a one-to-one function which associates each message $m \in \mathcal{M}_n$ to a coset representative $\lambda_m \in \Lambda_b \cap \mathcal{R}(\Lambda_e)$. To encode the message m, Alice samples a lattice point $\lambda \in \Lambda_e \cap \mathcal{V}(\Lambda_s)$ according to the uniform distribution and transmits $\lambda + \lambda_m$. We set $\sigma^2(\Lambda_s) = P$ to asymptotically satisfy the power constraint.

A. Secrecy

To derive an upper bound on the amount of leaked information to Eve, we need an upper bound on D_{TV} between $p_{Z^n|M}(.|m)$ and a fixed distribution $q_{Z^n}(.)$ for all $m \in \mathcal{M}_n$. First, we note that

$$P_{Z^n|M=m}(\mathbf{z}) = \frac{1}{e^{nR'}} \sum_{\bar{\lambda} \in \Lambda_e/\Lambda_s} \bar{f}_{\bar{\lambda}}(\mathbf{z})\,,$$

where $\bar{f}_{\bar{\lambda}}(\mathbf{z}) \stackrel{\text{def}}{=} \sum_{\lambda \in \Lambda_e} f_{\sigma_e,\lambda_m}(\mathbf{z} - \lambda)\mathbf{1}_{\mathcal{R}(\bar{\lambda})}(\mathbf{z})$. In the following theorem, we provide an upper bound on $D_{\text{TV}}(\bar{f}_{\bar{\lambda}}, U_{\mathcal{R}(\Lambda_s)})$, where $U_{\mathcal{R}(\Lambda_s)}$ is the uniform distribution on $\mathcal{R}(\Lambda_s)$.

Theorem 1. *For any $\mathbf{c} \in \mathbb{R}^n$ and any n-dimensional lattice Λ, let $\bar{f}$ be the PDF of the distribution over $\mathcal{R}(\Lambda)$ defined by $f_{\sigma,\mathbf{c}} \bmod \mathcal{R}(\Lambda)$. Then we have*

$$D_{TV}(\bar{f}, U_{\mathcal{R}}(\Lambda)) \leq \sqrt{\epsilon_\Lambda(\sqrt{2}\sigma)} \tag{4}$$

Proof.

$$D_{\text{TV}}(\bar{f}(\mathbf{z}),1/V) \overset{(a)}{\leq} [\int_{\mathcal{R}(\Lambda)} \frac{|\bar{f}(\mathbf{z})-1/V|^2}{1/V}\,\mathrm{d}\mathbf{z}]^{1/2} = \sqrt{V\int_{\mathcal{R}(\Lambda)} \bar{f}^2(\mathbf{z})\,\mathrm{d}\mathbf{z} - 2\int_{\mathcal{R}(\Lambda)} \bar{f}(\mathbf{z})\,\mathrm{d}\mathbf{z} + 1}\,, \tag{5}$$

where (a) follows from the Cauchy-Schwarz inequality. In the rest of proof, we calculate the two above integrals $\int_{\mathcal{R}(\Lambda)} \bar{f}(\mathbf{z})$ and $\int_{\mathcal{R}(\Lambda)} \bar{f}^2(\mathbf{z})$. We note that

$$\begin{aligned}\bar{f}(\mathbf{z}) &= \sum_{\lambda} f_{\sigma,\lambda}(\mathbf{z}-\mathbf{c})\mathbf{1}_{\mathcal{R}(\Lambda)}(\mathbf{z}) \\ &= f_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c})\mathbf{1}_{\mathcal{R}(\Lambda)}(\mathbf{z})\end{aligned}$$

The Fourier expansion of $f_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c})$ gives us [5]

$$f_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c}) = \frac{1}{V}\sum_{\lambda^*\in\Lambda^*} e^{-2\pi^2\sigma^2\|\lambda^*\|^2} e^{-2\pi i<\mathbf{c},\lambda^*>} e^{-2\pi i<\mathbf{z},\lambda^*>} \tag{6}$$

We have

$$\begin{aligned}&\int_{\mathcal{R}(\Lambda)} \bar{f}(\mathbf{z})\,\mathrm{d}\mathbf{z} = \int_{\mathcal{R}(\Lambda)} f_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c})\mathbf{1}_{\mathcal{R}(\Lambda)}\,\mathrm{d}\mathbf{z} \\ &= \frac{1}{V}\sum_{\lambda^*\in\Lambda^*} e^{-2\pi^2\sigma^2\|\lambda^*\|^2} e^{-2\pi i<\mathbf{c},\lambda^*>} \int_{\mathcal{R}(\Lambda)} e^{-2\pi i<\mathbf{z},\lambda^*>}\,\mathrm{d}\mathbf{z} \\ &\overset{(a)}{=} 1\end{aligned} \tag{7}$$

where (a) follows from

$$\frac{1}{V}\int_{\mathcal{R}(\Lambda)} e^{-2\pi i<\mathbf{z},\lambda^*>}\,\mathrm{d}\mathbf{z} = \delta_{\lambda^*}\,, \tag{8}$$

where δ_{λ^*} is the delta function $\delta_{\lambda^*} = \{1, \text{if}\,\lambda^* = \mathbf{0}, 0, \text{otherwise}\}$. Now, we turn to $\int \bar{f}^2(\mathbf{z})\,\mathrm{d}\mathbf{z}$. We have

$$\int_{\mathcal{R}(\Lambda)} \bar{f}^2(\mathbf{z})\,\mathrm{d}\mathbf{z} = \int_{\mathcal{R}(\Lambda)} f^2_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c})\,\mathrm{d}\mathbf{z}\,.$$

Expansion of $f^2_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c})$ gives us

$$\begin{aligned}&\int_{\mathcal{R}(\Lambda)} f^2_{\sigma,\Lambda}(\mathbf{z}-\mathbf{c})\,\mathrm{d}\mathbf{z} = 1/V + 2/V^2 \\ &\times (\sum_{\lambda^*\neq\mathbf{0}} e^{-2\pi^2\sigma^2\|\lambda^*\|^2} e^{-2\pi i<\mathbf{c},\lambda^*>} \int_{\mathcal{R}(\Lambda)} e^{-2\pi i<\lambda^*,\mathbf{z}>}\,\mathrm{d}\mathbf{z}) \\ &+ 1/V^2(\sum_{\lambda_1^*,\lambda_2^*\neq\mathbf{0}} e^{-2\pi^2\sigma^2(\|\lambda_1^*\|^2+\|\lambda_2^*\|^2)} e^{-2\pi i<\lambda_1^*+\lambda_2^*,\mathbf{c}>} \\ &\qquad \int_{\mathcal{R}(\Lambda)} e^{-2\pi i<\lambda_1^*+\lambda_2^*,\mathbf{z}>}\,\mathrm{d}\mathbf{z}) \\ &\overset{(a)}{=} \frac{1}{V}(1+\sum_{\lambda^*\in\Lambda^*\setminus\{\mathbf{0}\}} e^{-4\pi^2\sigma^2\|\lambda^*\|^2}) \\ &= \frac{1}{V}(1+\epsilon_\Lambda(\sqrt{2}\sigma))\end{aligned} \tag{9}$$

where (a) follows from eqs. (7) and (8). Combination of eqs. (5), (7) and (9) completes the proof. □

Remark 1. The proposed upper bound on $I(M,Z^n)$ in [6, Theorem 2] guarantees $I(M,Z^n)\to 0$ if $\epsilon_\Lambda(\sigma)\to 0$. Since the flatness factor $\epsilon_\Lambda(\sigma)$ is a monotonically decreasing function of σ, our proposed upper bound provides a milder condition to have $I(M,Z^n)\to 0$.

Theorem 2. *Let $\Lambda_s\subset\Lambda_e\subset\Lambda_b$ be a chain of n-dimensional nested lattices such that as $n\to\infty$ such that:*

- *Λ_s is quantization and AWGN-good;*
- *Λ_e is secrecy-good, i.e.*[2]

$$\epsilon_{\Lambda_e}(\sigma) = e^{-\Omega(n)}\,,\ \forall \gamma_{\Lambda_e}(\sigma) < 2\pi\,; \tag{10}$$

- *Λ_b is AWGN-good.*

Then as $n\to\infty$, the semantic secrecy rate of the nested lattice coding satisfies

$$R < \frac{1}{2}\ln(\frac{\sigma_e^2}{\sigma_b^2}) - \frac{1}{2}\ln(\frac{e}{2})\,.$$

Proof. From the results of [4], we know that without random dither at the transmitter and an MMSE filter at the receiver,

$$R + R^{'} < \frac{1}{2}\ln(SNR_b) \tag{11}$$

is achievable. From lemma 1, lemma 2 and theorem 1, in order to satisfy $I(M,Z^n)\to 0$, lattice Λ_e should satisfy

$$\gamma_{\Lambda_e}(\sqrt{2}\sigma_e) = \frac{V(\Lambda_s)^{2/n}}{(e^{nR^{'}})^{2/n}2\sigma_e^2} \to \frac{P2\pi e}{e^{2R^{'}}2\sigma_e^2} < 2\pi\,,$$

and therefore,

$$R^{'} > \frac{1}{2}\ln SNR_e + \frac{1}{2}\ln(e/2)\,. \tag{12}$$

The combination of eqs. (11) and (12) implies

$$R < \frac{1}{2}\ln(\frac{\sigma_e^2}{\sigma_b^2}) - \frac{1}{2}\ln(\frac{e}{2})\,.$$

□

Remark 2. The secrecy capacity of mod-Λ Gaussian wiretap channel is upper bounded by $\frac{1}{2}\ln(\frac{\sigma_e^2}{\sigma_b^2})$. Theorem 2 suggests that lattice nested coding can achieve the semantic capacity to within $\frac{1}{2}\ln(e/2)$ nat which improves the established maximum achievable semantic secrecy rate in [6, Theorem 3] up to $\frac{1}{2}\ln 2$ nat.

III. Gaussian Wiretap Channel

Consider the Gaussian Wiretap channel where both legitimate and eavesdropper channels are modeled by AWGN channels;

$$\begin{aligned}Y^n &= X^n + N_b^n\,, \\ Z^n &= X^n + N_e^n\,,\end{aligned} \tag{13}$$

where X^n is the transmitted signal, Y^n and Z^n are outputs at the legitimate and the eavesdropper, and N_b^n and N_e^n are n-dimensional Gaussian vectors with zero mean and variance σ_b^2 and σ_e^2 respectively.

[2]We say $f(x)=\Omega(g(x))$ when $\limsup_{x\to\infty}|g(x)/f(x)|<\infty$.

A. Coding Scheme

Now we describe the coding scheme in [6] which employs lattice Gaussian coding. Let $\Lambda_e \subset \Lambda_b$ be n-dimensional lattices in $\mathbb{R}^n$ such that

$$\frac{1}{n}\ln\frac{V(\Lambda_e)}{V(\Lambda_b)} = R\,.$$

To transmit a given message m, Alice samples λ from the discrete Gaussian distribution $D_{\Lambda_e,\sigma_0,-\lambda_m}$ and transmits $X^n = \lambda + \lambda_m$. In [6], it is shown that as $n \to \infty$, if

$$\epsilon_{\Lambda_e}(\frac{\sigma_0^2}{\sqrt{\frac{\pi}{\pi-1}}}) \to 0\,, \tag{14}$$

we have $\frac{1}{n}\mathbb{E}[\|X^n\|^2] \to \sigma_0^2$. Therefore, we can choose $\sigma_0^2 = P$ to satisfy the power constraint asymptotically. Decoding of the confidential message is done by using MMSE lattice decoding, i.e. after receiving $\mathbf{y} = \mathbf{x}+\mathbf{n}_b$, bob computes $\tilde{\lambda}_m = [Q_{\Lambda_b}(a\mathbf{y})] \bmod \mathcal{R}(\Lambda_e)$ where $\alpha = \frac{\sigma_0^2}{\sigma_0^2+\sigma_b^2}$.

B. Secrecy

We note that the Eve's channel transition probability is given by

$$p_{Z^n|X^n}(\mathbf{z}|\lambda_m+\lambda) = f_{\sigma_e,\lambda_m+\lambda}(\mathbf{z})\,,$$

Since λ is sampled from $D_{\Lambda_e,\sigma_0,-\lambda_m}$, $P_{Z^n|M}$ is given by

$$p_{Z^n|M=m}(\mathbf{z}) = \frac{1}{f_{\sigma_0}(\Lambda_e+\lambda_m)}\sum_{\lambda\in\Lambda_e+\lambda_m} f_{\sigma_0}(\lambda)f_{\sigma_e}(\mathbf{z}-\lambda)\,. \tag{15}$$

In the following lemma, we derive an upper bound on the KL distance between $p_{Z^n|M=m}$ and a continuous iid Gaussian distribution with variance $\sigma_0^2+\sigma_e^2$.

Theorem 3. *Consider the continuous distribution $q(\mathbf{x}) \in \mathbb{R}^n$ obtained by adding a continuous Gaussian distribution $f_s(\mathbf{x})$ and a discrete Gaussian $D_{\Lambda+\mathbf{c},r}$. We define $t \overset{def}{=} \sqrt{s^2+r^2}$, and $\ell \overset{def}{=} \sqrt{\frac{r^2s^2(2r^2+s^2)}{t^4}}$. We have*

$$D_{KL}(f_t(\mathbf{x}),q(\mathbf{x})) \le \ln(1+\epsilon_\Lambda(r)) + \epsilon_\Lambda(r) + \frac{1}{2}\epsilon_\Lambda(r)\epsilon_\Lambda(\ell)\,. \tag{16}$$

Proof. The continuous distribution q on $\mathbb{R}^n$ obtained by adding f_s and $D_{\Lambda+\mathbf{c},r}$ is given by

$$\begin{aligned}
&q(\mathbf{x})\\
&= \frac{1}{f_r(\Lambda+\mathbf{c})}\sum_{\mathbf{y}\in\Lambda+c} f_r(\mathbf{y})f_s(\mathbf{x}-\mathbf{y})\\
&= \frac{1}{(4\pi^2r^2s^2)^{n/2}}\frac{1}{f_r(\Lambda+\mathbf{c})}\sum_{\mathbf{y}\in\Lambda+\mathbf{c}} e^{-(\|\mathbf{y}\|^2/2r^2+\|\mathbf{x}-\mathbf{y}\|^2/2s^2)}\\
&= \frac{1}{(4\pi^2r^2s^2)^{n/2}}\frac{1}{f_r(\Lambda+\mathbf{c})}\\
&\qquad\times\sum_{\mathbf{y}\in\Lambda+\mathbf{c}} e^{-(\frac{r^2+s^2}{2r^2s^2}\|\mathbf{y}-\frac{r^2}{r^2+s^2}\mathbf{x}\|^2+\frac{\|\mathbf{x}\|^2}{2(r^2+s^2)})}\\
&= f_t(\mathbf{x})\frac{f_{rs/t,(r/t)^2\mathbf{x}}(\Lambda+\mathbf{c})}{f_r(\Lambda+\mathbf{c})}
\end{aligned}$$

From the definition of KL-distance, we have

$$\begin{aligned}
&D_{\mathrm{KL}}(f_t(\mathbf{x}),q(\mathbf{x})) = \int_{\mathbb{R}^n} f_t(\mathbf{x})\ln\frac{f_t(\mathbf{x})}{q(\mathbf{x})}\,\mathrm{d}\mathbf{x}\\
&= -\int_{\mathbb{R}^n} f_t(\mathbf{x})\ln\frac{q(\mathbf{x})}{f_t(\mathbf{x})}\,\mathrm{d}\mathbf{x}\\
&\overset{(a)}{=} -\int_{\mathbb{R}^n} f_t(\mathbf{x})\\
&\qquad\ln\frac{\sum_{\mathbf{u}\in\Lambda^*} e^{-2\pi i<(r/t)^2\mathbf{x}-\mathbf{c},\mathbf{u}>}e^{-2\pi^2(rs/t)^2\|\mathbf{u}\|^2}}{\sum_{\mathbf{u}\in\Lambda^*} e^{2\pi i<\mathbf{c},\mathbf{u}>}e^{-2\pi^2r^2\|\mathbf{u}\|^2}}\,\mathrm{d}\mathbf{x}\\
&= \ln\sum_{\mathbf{u}\in\Lambda^*} e^{2\pi i<\mathbf{u},\mathbf{c}>}e^{-2\pi^2r^2\|\mathbf{u}\|^2} + \mathrm{I}\,,
\end{aligned} \tag{17}$$

where (a) follows from the Poisson Summation formula, and

$$\begin{aligned}
\mathrm{I} &= -\int_{\mathbb{R}^n} f_t(\mathbf{x})\ln\sum_{\mathbf{u}\in\Lambda^*} e^{-2\pi i<(r/t)^2\mathbf{x}-\mathbf{c}>}e^{-2\pi^2(rs/t)^2\|\mathbf{u}\|^2}\\
&\overset{(a)}{\le} -\int_{\mathbb{R}^n} f_t(\mathbf{x})\sum_{\mathbf{u}\neq 0} e^{-2\pi i<(r/t)^2\mathbf{x}-\mathbf{c}>}e^{-2\pi^2(rs/t)^2\|\mathbf{u}\|^2}\,\mathrm{d}\mathbf{x}\\
&\quad+\frac{1}{2}\int_{\mathbb{R}^n} f_t(\mathbf{x})\times\\
&\quad(\sum_{\mathbf{u}_1}\sum_{\mathbf{u}_2} e^{-2\pi i<(r/t)^2\mathbf{x}-\mathbf{c},\mathbf{u}_1+\mathbf{u}_2>}e^{-2\pi^2(rs/t)^2(\mathbf{u}_1^2+\mathbf{u}_2^2)})\,\mathrm{d}\mathbf{x}\\
&= \mathrm{I}_1+\mathrm{I}_2\,,
\end{aligned} \tag{18}$$

where (a) follows from the inequality: $\ln 1+x \ge x - x^2/2$. We have

$$\begin{aligned}
\mathrm{I}_1 &= -\sum_{\mathbf{u}\neq 0} e^{2\pi i<\mathbf{u},\mathbf{c}>}e^{-2\pi^2(rs/t)^2\|\mathbf{u}\|^2}\times\\
&\qquad\int_{\mathbb{R}^n} f_t(\mathbf{x})e^{-2\pi i<(r/t)^2\mathbf{x},\mathbf{u}>}\,\mathrm{d}\mathbf{x}\\
&\overset{(a)}{=} -\sum_{\mathbf{u}\neq 0} e^{-2\pi^2(rs/t)^2\|\mathbf{u}\|^2}e^{-2\pi^2(r^4/t^2)\|\mathbf{u}\|^2}e^{2\pi i<\mathbf{u},\mathbf{c}>}\\
&\le \sum_{\mathbf{u}\neq 0} e^{2\pi i<\mathbf{u},\mathbf{c}>}e^{-2\pi^2r^2\|\mathbf{u}\|^2}\,,
\end{aligned} \tag{19}$$

where a follows from the fact that $\int_{\mathbb{R}^n} e^{-\frac{1}{2}\mathbf{x}A\mathbf{x}+iB\cdot\mathbf{x}} = \sqrt{\frac{(2\pi)^n}{\det A}}e^{-\frac{1}{2}B\cdot A^{-1}\cdot B}$. For the second therm, we have

$$\begin{aligned}
\mathrm{I}_2 &= \frac{1}{2}\sum_{\mathbf{u}_1\neq 0}\sum_{\mathbf{u}_2\neq 0} e^{2\pi i<\mathbf{u}_1+\mathbf{u}_2,\mathbf{c}>}e^{-2\pi^2(rs/t)^2(\mathbf{u}_1^2+\mathbf{u}_2^2)}\times\\
&\qquad\int_{\mathbb{R}^n} f_t(\mathbf{x})e^{-2\pi i<(r/t)^2\mathbf{x},\mathbf{u}_1+\mathbf{u}_2>}\,\mathrm{d}\mathbf{x}\\
&= \frac{1}{2}\sum_{\mathbf{u}_1\neq 0} e^{-2\pi^2r^2(1-(r/t)^4)\|\mathbf{u}_1\|^2}\sum_{\mathbf{u}_2\neq 0} e^{-2\pi^2r^2(\mathbf{u}_2-(r/t)^2\mathbf{u}_1)^2}\\
&\overset{(a)}{\le} \frac{1}{2}\sum_{\mathbf{u}_1\neq 0} e^{-2\pi^2r^2(1-(r/t)^4)\|\mathbf{u}_1\|^2}\sum_{\mathbf{u}_2\neq 0} e^{-2\pi^2r^2\|\mathbf{u}_2\|^2}\,,
\end{aligned} \tag{20}$$

where (a) follows from the fact that the maximum of $f_{\sigma,\Lambda}(\mathbf{x})$ are reached when $\mathbf{x}\in\Lambda$. Combination of eqs. (17) to (20) completes the proof. □

Theorem theorem 3 provides an upper bound on the KL-distance between $P_{Z^n|M}(.|m)$ and $f_{\sqrt{\sigma_0^2+\sigma_e^2}}$ as follows

$$D_{\mathrm{KL}}(P_{Z^n|M}(.|m), f_{\sqrt{\sigma_0^2+\sigma_e^2}}) \leq \ln(1+\epsilon_{\Lambda_e}(\sigma_0)) + \epsilon_{\Lambda_e}(\sigma_0) + \frac{1}{2}\epsilon_{\Lambda_e}(\sigma_0)\epsilon_{\Lambda_e}(\bar{\sigma}_e)\,, \tag{21}$$

where $\bar{\sigma}_e^2 \stackrel{\text{def}}{=} \frac{\sigma_0^2\sigma_e^2(2\sigma_0^2+\sigma_e^2)}{(\sigma_0^2+\sigma_e^2)^2}$. We note that since $\bar{\sigma}_e$ is smaller than σ_0, and $\epsilon_\Lambda(\sigma)$ is a monotonically decreasing of σ, we have $D_{\mathrm{KL}}(P_{Z^n|M}(.|m), g_{\sqrt{\sigma_0^2+\sigma_e^2}}) \to 0$ if

$$\epsilon_{\Lambda_e}(\bar{\sigma}_e) \to 0\,. \tag{22}$$

Remark 3. In [6, Theorem 4], the proposed upper bound on $I(M, Z^n)$ suggests that if $\epsilon_{\Lambda_e}(\tilde{\sigma}_e) \to 0$, then $I(M, Z^n) \to 0$ where $\tilde{\sigma}_e \stackrel{\text{def}}{=} \frac{\sigma_0\sigma_e}{\sqrt{\sigma_0^2+\sigma_e^2}}$. Since $\bar{\sigma}_e$ is larger than $\tilde{\sigma}_e$, our proposed upper bound provides a milder condition to have $I(M, Z^n) \to 0$.

Theorem 4. *Suppose that $SNR_b \cdot SNR_e > 1$. Then if Λ_b is a sequence of AWGN-good lattices and Λ_e is a sequence of secrecy-good lattice, any achievable semantic secrecy rate satisfies*

$$R < \frac{1}{2}\ln(1+SNR_b) - \frac{1}{2}\ln(1+SNR_e) - \frac{1}{2} + \frac{1}{2}\ln(1+\frac{SNR_e}{1+SNR_e})\,. \tag{23}$$

Proof. Bob's error probability is upper bounded by

$$P_e(m) \leq (1+\epsilon^{'})P(\tilde{\mathbf{w}}_b(m) \notin \mathcal{V}(\Lambda_b))\,,$$

where $\epsilon^{'} \stackrel{\text{def}}{=} \epsilon_e(\frac{P}{\sqrt{1+\sigma_b^2/P}})$ and $\tilde{\mathbf{w}}_b(m) \stackrel{\text{def}}{=} (\alpha-1)\mathbf{x} + \alpha\mathbf{n}_b$. Therefore, if Λ_b is a AWGN-good lattice, the error probability $P_e(m)$ vanishes exponentially if

$$\gamma_{\Lambda_b}(\tilde{\sigma}_b) = \frac{V(\Lambda_b)^{2/n}}{\tilde{\sigma}_b^2} > 2\pi e\,, \tag{24}$$

where $\tilde{\sigma}_b \stackrel{\text{def}}{=} \frac{\sigma_0\sigma_b}{\sqrt{\sigma_0^2+\sigma_b^2}}$, and if

$$\epsilon_{\Lambda_e}(\frac{\sigma_0^2}{\sqrt{1+\sigma_b^2/\sigma_0^2}}) \to 0\,. \tag{25}$$

Combination of eqs. (14), (22), (24) and (25) completes the proof. □

Remark 4. The secrecy capacity of Gaussian wiretap channel is $\frac{1}{2}\ln(\frac{1+SNR_e}{1+SNR_b})$. Our theorem suggests that the lattice Gaussian signaling and MMSE lattice decoding can achieve rates within $\frac{1}{2}(1-\ln(1+\frac{SNR_e}{1+SNR_e}))$ of the secrecy capacity. It is worthy to mention that we could improve the established secrecy rate in [6] up to $\frac{1}{2}\ln(1+\frac{SNR_e}{1+SNR_e})$ nat.

REFERENCES

[1] M. Bellare and S. Tessaro. Polynomial-time, semantically-secure encryption achieving the secrecy capacity. *CoRR*, abs/1201.3160, 2012.

[2] M. Bellare, S. Tessaro, and A. Vardy. Semantic security for the wiretap channel. In *CRYPTO*, pages 294–311, 2012.

[3] I. Csiszar. Almost independence and secrecy capacity. *Problmes of Information Transmission*, 32:40–47, 1996.

[4] U. Erez and R. Zamir. Achieving 1/2 log (1+snr) on the awgn channel with lattice encoding and decoding. *Information Theory, IEEE Transactions on*, 50(10):2293–2314, Oct 2004.

[5] Jr. Forney, G.D., M.D. Trott, and S.-Y. Chung. Sphere-bound-achieving coset codes and multilevel coset codes. *Information Theory, IEEE Transactions on*, 46(3):820 – 850, may 2000.

[6] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé. Semantically secure lattice codes for the gaussian wiretap channel. *CoRR*, abs/1210.6673, 2012.

[7] H. Mahdavifar and A. Vardy. Achieving the secrecy capacity of wiretap channels using polar codes. *IEEE Transactions on Information Theory*, 57(10):6428–6443, 2011.

[8] H. Tyagi and A. Vardy. Explicit capacity-achieving coding scheme for the gaussian wiretap channel. *Proc. IEEE International Symposium on Information Theory*, 2014.

[9] A. D. Wyner. The Wire-tap Channel. *Bell Systems Technical Journal*, 54(8):1355–1387, January 1975.

[10] Y. Yan, L. Liu, and C . Ling. Polar lattices for strong secrecy over the mod-λ gaussian wiretap channel. *CoRR*, abs/1401.4532, 2014.