Achievable Rates for Lattice Coded Gaussian Wiretap Channels

Li-Chia Choo  
Department of Electronic and Electrical Engineering  
University College London  
London WC1E 7JE, United Kingdom  
Email: uceelcc@ee.ucl.ac.uk

Cong Ling  
Department of Electronic and Electrical Engineering  
Imperial College London  
London SW7 2AZ, United Kingdom  
Email: c.ling@ieee.org

Kai-Kit Wong  
Department of Electronic and Electrical Engineering  
University College London  
London WC1E 7JE, United Kingdom  
Email: k.wong@ee.ucl.ac.uk

Abstract—This paper uses a nested lattice chain to perform lattice coding and decoding for a Gaussian wiretap channel, in which we derive the achievable rates and the equivocation rate. We also show that it is possible to achieve the equivocation rate of the classical Gaussian wiretap channel, and meet the reliability and security criteria using the nested lattice construction.

I. INTRODUCTION

Wireless communications today is vulnerable to eavesdropping or wiretapping due to the open nature of the medium, making the characterization of transmission rates for secure and reliable communication in the physical layer important. There have been many recent studies related to the physical layer security; see the monograph [1], for example. However, the vast majority of the works used random codes, and there is a need to study practical or structured codes and their construction for the physical layer security problem.

The wiretap channel is fundamental and the basic building block to such study. Introduced first by Wyner in [2], it consists of a transmitter, a legitimate receiver and a wiretapper. The coding scheme for the wiretap channel uses coset coding. The transmitter sends one of $M$ equally likely messages from the secure codebook $C$ which consists of subcodes $\{C_1,...,C_M\}$, while the legitimate receiver can decode the codebook $C$, but the wiretapper can decode only within each subcode. The codebook $C$ is the fine code and the ensemble of subcodes $\{C_1,...,C_M\}$ is the coarse code, each of which is a coset of $C$. To send message $m\in\{1,...,M\}$, the transmitted word is chosen uniformly at random from the code $C_m$; this stochastic encoding is the main source of uncertainty for the wiretapper. Practical channel codes for the wiretap channel with coset encoding have been proposed using low-density parity-check (LDPC) codes [3]–[7], polar codes [8], [9], and explicit lattice codes [10], [11]. Lattice codes have also been proposed using an information-theoretic (non-explicit) point of view in providing security for the Gaussian interference channels [12]–[14].

In this paper, we adopt an information-theoretic approach to the lattice-based coset coding problem for the Gaussian wiretap channel. We derive achievable channel rates, equivocation rate, and error probabilities for a nested lattice code. We note that our work is very similar to [10], [11]; however, [10], [11] used decoding bit error probability as their criteria for secrecy and derived conditions for lattices to meet it, while our focus is on the equivocation rate and achievable rates. We also note that our work is different from [12]–[14], as these papers considered a jamming or interference signal at the wiretapper.

The paper is organized as follows. In Section II, we introduce lattice codes and our nested lattice code construction and decoding. In Section III, we derive achievable channel rates and equivocation rate. In Section IV, we show a construction for the nested lattices and that such a construction can achieve error probability going to zero for large dimension lattices.

II. NESTED LATTICE CODES FOR THE GAUSSIAN WIRETAP CHANNEL

A. Lattice Preliminaries

In this subsection, we introduce notation and definitions for lattices. An extensive treatment for lattices can be found in [15]. A lattice $\Lambda$ is a discrete subgroup of the Euclidean space $\mathbb{R}^n$ with ordinary vector addition. The lattice $\Lambda$ is made up of all integer linear combinations of the basis vectors, and can be specified in terms of an $n \times n$ real-valued generator matrix $G = [g_1|g_2|\cdots|g_n]$, for $g_1,...,g_n \in \mathbb{R}^n$, $\Lambda = \{ \lambda = Gx : x \in \mathbb{Z}^n \}$. (1)

The fundamental Voronoi region $V$ with volume denoted by $V$, is the set of all points in $\mathbb{R}^n$ closest to the zero vector. The nearest neighbour quantizer is ($\langle \cdot \rangle$ denotes Euclidean norm)

$$Q_V(x) = \arg \min_{\lambda \in \Lambda} \| x - \lambda \|.$$ (2)

The modulo-$\Lambda$ operation associated with $V$ is given by

$$x \mod \Lambda = x - Q_V(x) \in V, \forall x \in \mathbb{R}^n,$$ (3)

and satisfies $\| x + y \| \mod \Lambda = \| [x] \mod \Lambda + [y] \mod \Lambda$. The second moment of $\Lambda$ is the second moment per dimension of random vector $U$ uniformly distributed over $V$.

$$\sigma^2(V) = \frac{1}{n} \mathbb{E} \left[ \| U \|^2 \right] = \frac{1}{nV} \int_V \| x \|^2 \, dx.$$ (4)

The normalized second moment of $\Lambda$ with minimized second moment $\sigma^2(V)$ is given by

$$G(\Lambda) \triangleq \frac{\sigma^2(V)}{V \bar{z}} = \frac{1}{nV^{1+\bar{z}}} \int_V \| x \|^2 \, dx.$$ (5)
B. Goodness of Lattices

We use the following definitions of asymptotic goodness of lattices [15]. The existence of a lattice with simultaneous goodness in all the aspects defined below was shown in [16].

- **Good for quantization**: A sequence of lattices \( \Lambda(n) \) is said to be good for mean-square-error (MSE) quantization if \( G(\Lambda(n)) \rightarrow \frac{1}{2} \pi^2 \) as \( n \rightarrow \infty \).

- **Rogers-good**: Let \( R_u \) and \( R_l \) be the covering and effective radii of \( \Lambda \). Then, \( 1 \leq \left( \frac{R_u}{R_l} \right)^n < c_n (\log n)^a \) for constants \( c, a \), which implies that \( \frac{1}{n} \log (R_u/R_l) \rightarrow 0 \) as \( n \rightarrow \infty \).

- **Polytrev-good**: For the Gaussian channel \( Y = X + N \), for any \( \sigma^2 < \sigma^2(\mathcal{V}) \), with \( N \) a Gaussian vector with components i.i.d. \( \sim \mathcal{N}(0, \sigma^2) \), a sequence of lattices \( \Lambda(n) \) is Polytrev-good, if

\[
P_e = \Pr\{N \notin \mathcal{V}\} < e^{-n[E_P(\mu) - o_n(1)]},
\]

where \( o_n(1) \rightarrow 0 \) as \( n \rightarrow \infty \), \( \mu = V^2/n/(2\pi e \sigma^2) \) is the normalised volume to noise ratio (VNR), and \( E_P(\mu) \) is the Polytrev exponent [19], assuming maximum-likelihood (ML) decoding. For \( \mu > 1 \), the error probability goes to 0 exponentially in \( n \). If the sequence is simultaneously quantization good as well, \( \mu = \sigma^2(\mathcal{V})/\sigma^2 \).

- **AWGN-good**: For the same Gaussian channel and ML decoding above, the unnormalised VNR of a sequence of lattices \( \Lambda(n) \) is \( \mu^*(\Lambda(n)) = V^2/n/\sigma^2 \). The sequence is AWGN-good if \( \lim_{n \rightarrow \infty} \mu^*(\Lambda(n)) = 2\pi e, 0 < P_e < 1 \).

C. Channel model

The Gaussian wiretap channel, studied in [17], has the following input-output relationship for \( n \) channel uses:

\[
Y = X + N \quad \text{and} \quad Z = X + N_z,
\]

where \( X \) denotes the channel input, \( Y \) denotes the legitimate receiver’s received signal and \( Z \) denotes the wiretapper’s received signal, \( N \sim \mathcal{N}(0, P_N I_n) \), \( N_z \sim \mathcal{N}(0, P_{N_z} I_n) \), with \( P_N < P_N \), the noise is independent over the channel uses, and the channel input is subject to the power constraint \( \frac{1}{n} \sum_{i=1}^{n} X_i \leq P_X \). The secrecy rate for this channel is

\[
R_e = \frac{1}{2} \log(1 + \text{SNR}) - \frac{1}{2} \log(1 + \text{SNR}_z) \leq C - C_z,
\]

where SNR = \( P_X/P_N \), SNR\(_z\) = \( P_X/P_{N_z} \), \( C \) and \( C_z \) are the capacities of the main and wiretapper’s channels, respectively. The following lemma is useful for the subsequent analysis.

**Lemma 1**: "Crypto lemma" [18]: Let \( \Lambda \) be a fundamental region of \( \Lambda \). For any random variable (r.v.) \( X \in \Omega \), statistically independent of r.v. \( U \) uniformly distributed over \( \Omega \), the sum, \( Y = X + U \mod_{\Lambda} \Lambda \), is uniformly distributed over \( \Omega \) and independent of \( X \).

D. Lattice Coding and Decoding

Consider the nested lattices \( \Lambda_1 \subset \Lambda_2 \subset \Lambda_1 \). The encoding follows a 2-level nested coding scheme as follows: first of all, associate a message \( m \in \{1, \ldots, 2^{nR_e}\} \) with a coset via its coset leader. This is the first level nested lattice code to provide secrecy. Next, send a random member of the coset, and constrain this random member to be the set of coset leaders of the shaping lattice for the AWGN channel. Define the following codebooks (sets of coset leaders):

\[
C = \{\Lambda_1 \cap \mathcal{V}_2\} \quad \text{and} \quad C' = \{\Lambda_2 \cap \mathcal{V}_3\}.
\]

(1) **Message selection and encoding**: Associate each message with a member of the set of coset leaders \( C \). Thus, for \( c_m \in C \), \( \Lambda_{c_m} = \Lambda_m + \Lambda_2 \) is a coset of \( \Lambda_2 \) relative to \( \Lambda_1 \) and

\[
\Lambda_1 = \bigcup_{c_m \in C} \Lambda_{c_m} = \bigcup_{c_m \in C} \{\Lambda_m + \Lambda_2\},
\]

The order of the partition \( \Lambda_1/\Lambda_2 = \{\Lambda_1/\Lambda_2\} = V_2/V_1 \), and so \( \{\Lambda_1 \cap \mathcal{V}_2\} \) has \( V_2/V_1 \) cosets. The rate of the secret message is given by \( R_e = \frac{1}{2} \log |\Lambda_1/\Lambda_2| = \frac{1}{2} \log \frac{V_2}{V_1} \).

We now send a uniformly selected random member of \( \Lambda_{c_m} \). Effectively, we send a uniformly selected random member of \( \Lambda_2 \). This plays the role of random bits that the wiretapper is allowed to decode at its maximum rate, thereby protecting the actual message in \( c_m \). Write the transmitted point as

\[
b_{m,l} = c_m + a_l, \quad a_l \in \Lambda_2, \quad c_m \in \{\Lambda_1/\Lambda_2\},
\]

where \( \{\Lambda_1/\Lambda_2\} \) denotes a system of coset representatives for \( \Lambda_1/\Lambda_2 \), and \( a_l \) is a uniformly random member of \( \Lambda_2 \). For each \( c_m \), we translate it by \( a_l \in \Lambda_2 \). At this stage, \( a_l \) and hence the transmitted point is an unbounded member of \( \Lambda_2 \), which is the same as [10]. To achieve capacity over the AWGN channel, \( b_{m,l} \) has to be sent using nested lattice coding. Now as we take \( c_m \) to be an “indexing” to the particular coset \( c_m + \Lambda_2 \), the actual term in \( b_{m,l} \) to “undergo” nested lattice coding is \( a_l \). Thus, we associate each \( a_l \) with a member of the set of coset leaders \( C' \), so \( \Lambda_{a_l} = \Lambda_2 + \Lambda_3 \) is a coset of \( \Lambda_3 \) relative to \( \Lambda_2 \) and \( a_l \) is mapped to \( \{\Lambda_2/\Lambda_3\} = V_3/V_2 \) cosets. We have

\[
\Lambda_2 = \bigcup_{a_l \in C'} \Lambda_{a_l} = \bigcup_{a_l \in C'} a_l + \Lambda_3 = \bigcup_{l=1}^{\Lambda_2/\Lambda_3} a_l + \Lambda_3,
\]

\[
\Lambda_3 = \bigcup_{m=1}^{\Lambda_2/\Lambda_3} \bigcup_{l=1}^{\Lambda_2/\Lambda_3} c_m + a_l + \Lambda_3.
\]

The excess rate, or the rate over the wiretapper’s channel is \( R' = \frac{1}{n} \log |\Lambda_2/\Lambda_3| = \frac{1}{n} \log \frac{V_2}{V_3} \). The overall rate, over the main channel, is then \( R = R_e + R' = \frac{1}{n} \log \frac{V_2}{V_1} \). A point in \( \Lambda_1 \) may now be written as

\[
\lambda_1 = c_m + a_l + \lambda_3,
\]

\( \lambda_1 \in \Lambda_1, \ c_m \in \{\Lambda_1/\Lambda_2\}, \ a_l \in \{\Lambda_2/\Lambda_3\}, \ \lambda_3 \in \Lambda_3 \). We can also write \( \lambda_1 = c_m + a_l + \lambda_3 \), for \( \lambda_1 \in \Lambda_1, \ \lambda_3 \in \Lambda_3 \), the partitioning of \( \Lambda_1 \) may be written as

\[
\Lambda_1 = \{\Lambda_1/\Lambda_2\} + \{\Lambda_2/\Lambda_3\} + \Lambda_3 = \{\Lambda_1/\Lambda_3\} + \Lambda_3.
\]

(2) **Transmission**: We add dither, defined as \( U \sim \text{Unif}(\mathcal{V}_3) \), and apply the mod-\( \Lambda_3 \) map. Then, the encoder sends

\[
X = [\lambda_1 - U] \mod \Lambda_3 = [c_m + a_l - U] \mod \Lambda_3.
\]

The lattice is scaled so that \( \sigma^2(\mathcal{V}_3) = P_X \) so that by the crypto lemma, we have \( \frac{1}{n} \mathbb{E} \|X\|^2 = P_X \).
(3) Decoding: Signals Y and Z are multiplied by α and α_z, dither is added and the mod-A_3 map is applied. We have $Y' = [\alpha Y + U] \mod A_3$, $Y_z' = [\alpha_z Z + U] \mod A_3$. (17)

By the inflated lattice lemma and modulo-lattice channel transformation [19], the channels from the transmitted codeword b_m to just before the decoders are

Main channel: $Y' = [c_m + a_2 + N'] \mod A_3$, (18)

Wiretapper’s channel: $Y_z' = [c_m + a_3 + N'_z] \mod A_3$, (19)

where $N' = N'' \mod A_3$, $N'' = \{(1 - \alpha)U + \alpha N\}$, $N'_z = N''_z \mod A_3$, and $N''_z = \{(1 - \alpha)U + \alpha N_z\}$. The decoders at the receivers use Euclidean lattice decoding.

- **Legitimate receiver:** We assume that the decoder jointly decodes $(c_m, a_1)$ together.\(^\text{1}\) To determine the decision region, note that $c_m \in V_1$ is translated by $a_1 \in V_2$. This can be seen as an arbitrary $V_1$ being moved into the larger region $V_2$, giving an overall decision region $V_1 \cap V_2 = V_1$. The $c_m + a_1$ is enclosed by $V_2$. The decoder is $(c_m, a_1) = Q_{V_1 \cap V_2}(Y') \mod A_3$, (20)

and the joint decoding error probability is then $P_{e,c,m} = \Pr\{N' \notin V_1 \cap V_2 = \Pr\{N' \notin V_1\}$. (21)

- **Wiretapper:** Assume that $c_m$ is known, and its decoder then attempts to decode $a_1 \in V_2$. The decoder is $a_1 = Q_{V_2}(Y_z') \mod A_3$, (22)

with decoding error probability $P_{e,c,z} = \Pr\{N'_z \notin V_2\}$. (23)

In the next two sections, we show our main result, which is formally stated by the following theorem.

**Theorem 1:** For our nested lattice coding scheme described above, $P_{e,c,m}P_{e,c,z} \to 0$, as $n \to \infty$ for rates $R$ and $R'$ approaching $C$ and $C_z$, while the construction achieves $C$ and $C_z$ on the main and wiretapper’s channels, respectively. The equivocation rate $\lim_{n \to \infty} R_e = \frac{1}{2} \log H(M|Z) - C - C_z$ satisfies the secrecy rate for the Gaussian wiretap channel and the secrecy constraint $\lim_{n \to \infty} \frac{1}{n} I(M; Z) = 0$ is achieved.

### III. Rates and Equivocation

Let C, A be the r.v.’s uniformly distributed over codebooks C, C’ by construction, of which the realizations are $c_m$ and $a_1$, respectively. The equivalent channels are (18) and (19) with $c_m$ and $a_1$ replaced by C and A. For notational convenience, we write $[C + A] \mod A_3$ as $C \oplus A$.

**A. Channel Rates**

The main channel input $C \oplus A \in [A_1/A_3]$, and has rate $R = \frac{1}{n} \log \frac{V_3}{V_1} = \frac{1}{2} \log \frac{V_3^2}{2\pi e} - \frac{1}{2} \log \frac{V_1^2}{2\pi e}$

\[(a) \frac{1}{2} \log \frac{P_x}{2\pi e G(A_3)} - \frac{1}{2} \log \frac{V_1}{2\pi e} \]

\[= \frac{1}{2} \log P_x - \frac{1}{2} \log 2\pi e G(A_3) - \frac{1}{2} \log \frac{V_1}{2\pi e}, \quad (24)\]

where (a) is due to the fact that $G(A_3) = \sigma^2(V_3)/V_3^2$ and $\sigma^2(V_3) = P_X$. Consider the sequence of lattices $A_3^{(n)}$, good for quantization so that $\lim_{n \to \infty} G(A_3^{(n)}) = \frac{1}{2\pi e}$, and the AWGN good lattices $A_1^{(n)}$. As such, from [18, Section 2.4], we have $\log \frac{V_3^2}{2\pi e} - \log \frac{1}{n} \mathbb{E}||N'||^2 = n \to \infty$. Using the minimum MSE (MMSE) scaling $\alpha = \frac{P_X}{2\pi e}$, we get

\[\frac{1}{2} \mathbb{E}||N'||^2 = \frac{1}{2} \mathbb{E}||((1 - \alpha)U + \alpha N||^2 = \alpha N. \quad (25)\]

Then, from (24), we have

\[R = \frac{1}{2} \log (1 + \text{SNR}) = C, \quad (26)\]

as $n \to \infty$. For the wiretapper’s channel, the input $c_m \oplus A \in [A_2/A_3]$, and using a similar calculation the rate is

\[R' = \frac{1}{2} \log (1 + \text{SNR}_z) = C_z, \quad (27)\]

as $n \to \infty$. This time we use the sequence of AWGN good lattices $A_2^{(n)}$, and $\alpha_z = \frac{P_x}{2\pi e + P_x N}$. In summary, we need the sequences $A_1^{(n)}, A_2^{(n)}$ to be AWGN good, and the sequence $A_3^{(n)}$ good for quantization.

**B. Calculation of the Equivocation Rate**

For the equivocation of the message M,

\[H(M|Z) = H(M) - I(M; Z). \quad (28)\]

We now use the expansions $I(M, X; Z) = I(M; Z) + I(X; Z|M) = I(X; Z) + I(M; Z|X)$, to give $I(M; Z) = I(X; Z) - I(M; X|Z)$. Since $I(M; X|Z) = 0$ as $M \to X \to Z$ forms a Markov chain. Substituting this into (28), we obtain

\[H(M|Z) = H(M) - I(X; Z) + I(X; Z|M) \]

\[\geq H(M) - C_z + H(C, A|M) - H(C, A|Z, M) \]

\[= \log \frac{V_3}{V_1} - C_z + \log \frac{V_3}{V_1} - H(C, A|Z, M), \quad (29)\]

where (a) is by $I(X; Z) \leq C_z$, since $C_z$ is the maximum possible rate of the wiretapper’s channel, and due to the one-to-one correspondence between $(C, A)$ and X so that $I(X; Z|M) = I(C, A; Z|M) = H(C, A|M) - H(C, A|Z, M)$, and (b) is due to $H(M) = \log (V_2/V_1)$, $H(C, A|M) = \log (V_3/V_2)$. The last term in (29) is the entropy of the codeword conditioned on the cost $C + A_2$ and the wiretapper’s observation. This is related to the wiretapper’s decoding error probability $P_{e,c,z}$. Following a proof similar to that for Fano’s inequality, we have $H(C, A|M, Z) \leq 1 + P_{e,c,z} \log \frac{V_3}{V_2} \leq n\epsilon$, where while $n \to \infty$, $\epsilon \to 0$ as long as $P_{e,c,z} \to 0$. Substituting this into (29) and dividing by n, we get the equivocation rate

\[R_e = \lim_{n \to \infty} \frac{1}{n} H(M|Z) = \frac{1}{n} \log (V_2/V_1) = C - C_z, \quad (30)\]

which is the equivocation rate of the Gaussian wiretap channel in [17]. Finally, it is easy to see that

\[\lim_{n \to \infty} \frac{1}{n} I(M; Z) = \lim_{n \to \infty} \left[ H(M) - \frac{1}{n} H(M|Z) \right] \]

\[= \lim_{n \to \infty} \frac{1}{n} \log (V_2/V_1) - (C - C_z) = 0, \quad (31)\]

and the secrecy constraint can be achieved.
Calculations in this section have used codewords from the codebooks $C$ and $C'$. Later, we will see that a nested lattice construction exists with small decoding error probabilities as $n \to \infty$ for the main and wiretapper’s channels at rates $R \to C$ and $R' \to C_2$, respectively. We then conclude that using our coding scheme, we can achieve the capacities for the main and wiretapper’s channels, the equivocation rate of the Gaussian wiretap channel (8), and satisfy the security constraint.

IV. CONSTRUCTION AND ERROR ANALYSIS

A. Construction of Nested Lattices

The construction follows from the method in [20], which uses a coarse lattice and forms finer lattices successively from it. We begin with a coarse lattice $\Lambda_3$, simultaneously covering, quantization, Rogers and Poltyrev good (existence shown in [16]). Let $\Lambda_3$ have the generator matrix $G'$, so that $\Lambda_3 = G'Z^n$. The fine lattices are constructed in the order of $\Lambda_1$ first, then $\Lambda_2$.

Let $k_1, k_2, n, p$ be integers such that $k_2 < k_1 \leq n$, and $p$ is a prime. To construct $\Lambda_1$, we perform the following:

1) Let $G_1$ be a $k_1 \times n$ generator matrix with elements $\sim \text{Unif}(0, 1, \ldots, p^{-1})$, that is, uniform over $Z_p$.
2) Define discrete codebook $C_1 = \{x = yG_1 : y \in Z_p^{k_1}\}$.
3) Lift $C_1$ to $\mathbb{R}^n$ to form the lattice $\Lambda_1' = p^{-1}C_1 + Z^n$.
4) The fine lattice is given by $\Lambda_1 = G'\Lambda_1'$.

To construct $\Lambda_2$, we do the following:

1) Let $G_2$ be the $k_2 \times n$ generator matrix which is the first $k_2$ rows of $G_1$.
2) Define discrete codebook $C_2 = \{x = yG_2 : y \in Z_p^{k_2}\}$.
3) Lift $C_2$ to $\mathbb{R}^n$ to form the lattice $\Lambda_2' = p^{-1}C_2 + Z^n$.
4) The fine lattice is given by $\Lambda_2 = G_2\Lambda_2'$.

In $C_1, C_2, x \in Z_p^n$. By construction, $Z^n \subset \Lambda_1'$ and $Z^n \subset \Lambda_2'$. We have $C_2 \subset C_1$ since all elements of $C_2$ can be found in $C_1$ as $G_2 \subset G_1$. This means that we have $\Lambda_3 \subset \Lambda_2 \subset \Lambda_1$. If $G_1, G_2$ are of full rank, then the number of fine lattice points in the Voronoi region of the coarse lattice is $|\Lambda_i \cap V_3| = p^{k_i}, i = 1, 2$. The probability that $G_1, G_2$ are of full rank is given by the union bound $Pr\{\bigcup_{j=1}^{k_2} \{\text{rank}(G_j) < k_1\}\} \leq \sum_{j=1}^{k_2} \sum_{x \neq 0, x \in Z_p^{k_2}} Pr\{|yG_j - 0| \leq p^{-n}(p^{k_j} + p^{k_2} - 2)\}$, which $\to 0$ as $n \to k_1$ and $n \to k_2$. The restriction on $n$ and $p, \frac{n}{p} \to 0$, is seen later in the error probability analysis.

The construction described above gives nested lattices $\Lambda_3 \subset \Lambda_2 \subset \Lambda_1$ all Rogers and Poltyrev good [21]. Furthermore, the points of the lattices $\Lambda_1, \Lambda_2$ contained in $V_3$, denoted $\Lambda_i(j), j = 0, 1, \ldots, p^{k_i} - 1, i = 1, 2$ satisfy

1) $\Lambda_i(j)$ is equally likely to be any of the points in $\{p^{-1}\Lambda_3 \cap V_3\}$.
2) For any $j \neq k$, $\Lambda_i(j) - \Lambda_i(k)$ mod $\Lambda_3$ is uniformly distributed over $\{p^{-1}\Lambda_3 \cap V_3\}$.

B. Error Analysis

Here, we show that the probabilities of error are small for both channels at rates $R \to C$ and $R' \to C_2$, using Euclidean lattice decoding. The legitimate receiver performs joint decoding of $(c_m, a_l)$, while the wiretapper decodes $a_l$, given $c_m$. The lattice $\Lambda_3$ is Rogers, Poltyrev, quantization good. Following [19], we make some necessary definitions.

- $\sigma^2 > P_X$ is the second moment of a ball containing $V_3$.
- Let $Z_1 \sim \mathcal{N}(0, \sigma^2 I_n)$; for the main channel $Z = \mathcal{N}(0, \alpha P_N)$, $Z^* = (1 - \alpha)Z_1 + \alpha N$; for wiretapper’s channel, $Z_2 = \mathcal{N}(0, \alpha P_{N_2})$, $Z_2^* = (1 - \alpha)Z_1 + \alpha z N_2$.
- $G_n^*$ denotes the normalized second moment of an $n$-dimensional sphere, $G_n^* \to \frac{\pi e}{2n}$ as $n \to \infty$.
- $\epsilon_1(\Lambda_3) \triangleq \log \left(\frac{R_n}{R_1}\right) + \frac{1}{2} \log 2\pi e G_n^* + \frac{1}{n}, \epsilon_2(\Lambda_3) \triangleq \log \left(\frac{R_n}{R_1}\right) + \frac{1}{2} \log 2\pi e G_1^*$ for $\Lambda_3$.

The error probability for the pair $(m, l)$ can be bounded as

$$P_{e,l,m} = Pr\{N' \notin V_1\} \leq Pr\{N'' \notin V_1\} \leq e^{\epsilon_1(\Lambda_3)n} \text{Pr}\{Z^* \notin V_3\}. \tag{32}$$

Now, truncate $Z^*$ to $V_3$ to give $Z_{V3}$. Since $V_1 \subset V_3$, we can follow the argument in [19, Eqns. (84)-(88)] to have

$$Pr\{Z^* \notin V_1\} \leq Pr\{Z_{V3} \notin V_1\} + Pr\{Z^* \notin V_3\}. \tag{34}$$

If we view $\Lambda_3$ as a channel code with respect to the Gaussian $Z^*$, Euclidean decoding is ML for such a channel. So we use (6) to bound $Pr\{Z^* \notin V_1\}$ with the equivalent VNR of $\Lambda_3$ viewed as a channel code with respect to $Z^*$ given by $\mu = \frac{P_X}{\tau_{Z^*}} \geq 1 + \frac{P_X}{\tau_{Z^*}} - o_1(1) = e^{2C} - o_1(1)$, thus giving

$$Pr\{Z^* \notin V_3\} \leq e^{-n[EP(e^{2C}) - o_1(1)]}. \tag{35}$$

To bound the first term in (34), consider the $(\Lambda_3, Z_{V3})$ channel $Y = [X + Z_{V3}] \mod \Lambda_3$, the modulo additive channel with $Z^*$ restricted to $V_3$, for which Euclidean decoding is ML with $Z_{V3}$ Gaussian in $V_3$. The random coding error exponent is

$$E_{\Lambda_3}(R; Z_{V3}) = \max_{0 \leq p \leq 1} \rho \left[\frac{1}{n} \log \frac{V_3}{n} - h_\rho(Z_{V3}) - R\right], \tag{36}$$

where $\rho \triangleq 1/(1 + p)$, and the Renyi entropy of order $\rho$ is $h_\rho(Z_{V3}) \triangleq \frac{1}{1 - \rho} \log \left(\int f_{Z_{V3}}(x)^\rho dx\right)^{\frac{1}{\rho}}$. By [19, Eqn. (208)], we have $\rho h_\rho(Z_{V3}) \leq \rho h_\rho(Z^*)$ and therefore

$$E_{\Lambda_3}(R; Z_{V3}) \geq \max_{0 \leq p \leq 1} \rho \left[\frac{1}{n} \log V_3 - h_\rho(Z^*) - R\right] - \epsilon_1(\Lambda_3) \geq E_P\left(e^{2(C - R - \epsilon_2(\Lambda_3))}\right) - \epsilon_1(\Lambda_3), \tag{37}$$

where $E_P(\cdot)$ is the Poltyrev random coding exponent [19, Eqn. (56)], (a) is by following the steps in [19, Eqns. (126)-(131)], and $\epsilon_1(\Lambda_3), \epsilon_2(\Lambda_3)$ are small as $n$ is large. This shows that the $(\Lambda_3, Z_{V3})$ channel’s random coding exponent is asymptotically close to the random coding Poltyrev exponent at $E_P\left(e^{2(C - R)}\right)$ as $n$ is large, assuming the input $c_m \oplus a_l$ is randomly uniform.

$^2$The proofs for [19, Lemmas 6 & 11] go through unchanged because they are derived based on the coarse lattice $\Lambda_3$ only.
over $V_3$. Next consider the input taken from the random code ensemble taken from a uniform distribution over $\{p^{-1}\Lambda_3 \cap V_3\}$. Then, the random code error exponent for this code ensemble over the $(\Lambda_3, Z_{V_3})$ channel is, as proved in [19, Appendix C],

$$E_{\Lambda_3}(R, Z_{V_3}, p) > E_{\Lambda_3}(R, Z_{V_3}) - o_n(1).$$

(38)

The proof for [19, Appendix C] is unchanged as it is performed only for $\{p^{-1}\Lambda_3 \cap V_3\}$, and not our nested lattices. However, we modify it slightly, noticing that [19, Eqn. (224) in Appendix C] is also obtained using our construction with $n/p \to 0$ as $n$ grows. Using this condition, our nested lattices can have $p^n$, $i = 1, 2$, points intersecting with $V_3$.

Now, referring back to the construction, the jointly decoded codeword $c_n \oplus a_l$ can be treated as a combined codeword from $\{\Lambda_1 \cap V_3\}$. From the properties of the construction, codewords from $\{\Lambda_1 \cap V_3\}$ are uniformly distributed over $\{p^{-1}\Lambda_3 \cap V_3\}$, and the difference between two codewords mod $\Lambda_3$ from $\{\Lambda_1 \cap V_3\}$ is also uniformly distributed over $\{p^{-1}\Lambda_3 \cap V_3\}$. Applying the union bound, we have that codewords from $\{\Lambda_1 \cap V_3\}$ have the same performance as random codewords drawn uniformly from $\{p^{-1}\Lambda_3 \cap V_3\}$ in terms of error exponent [20]. Thus, codewords from $\{\Lambda_1 \cap V_3\}$ over the $(\Lambda_3, Z_{V_3})$ channel have error probability

$$Pr\{Z_{V_3} \notin V_3\} = e^{-nE_{\Lambda_3}(R, Z_{V_3}, p)} \leq e^{-n(E_{\Lambda_3}(R, Z_{V_3}) - o_n(1))}.$$

(39)

Combining the results in (33)–(35), (37), (39) and following [19, Eqns. (95)–(96)], we obtain

$$P_{e,l,m} = Pr\{N_i' \notin V_3\} \leq e^{-n(E_{P}(e^{2(C - R)} - o_n(1))}.$$

(40)

At rates $R$ approaching $C$, the argument in $E_{P}(\cdot)$ approaches 1 from above, so $E_{P}$ is small but as $n$ gets large, $P_{e,l,m}$ approaches 0.

2) Decoding error probability for the wiretapper’s channel:

For the wiretapper’s channel, the proof is similar. In the final step, the codeword $a_l \mod \Lambda_3$ is uniformly distributed over $\{\Lambda_2 \cap V_3\}$. Codewords from $\{\Lambda_2 \cap V_3\}$ have the same performance as codewords from $\{p^{-1}\Lambda_3 \cap V_3\}$. The wiretapper’s channel counterpart of (38) can be met, using the construction for $\Lambda_2 \cap V_3$ with $n/p \to 0$ as $n \to \infty$, as before. Thus, we have

$$P_{e,l} = Pr\{N_i' \notin V_2\} \leq e^{-n(E_{P}(e^{2(C - R)} - o_n(1))}.$$

(41)

which is small for $R^{'}$ approaching $C_2$ and $n$ large. Now (40), (41) show that the decoding error probability at the main and wiretapper’s channels are small for $n$ large and the error exponents achieved the random coding Poltyrev exponent at $E_{P}(e^{2(C - R)})$ and $E_{P}(e^{2(C - R)})$, with coding rates $R$ and $R^{'}$ that approach $C$ and $C_2$, respectively. The constructed nested lattices that achieve the above, $\Lambda_3 \subset \Lambda_2 \subset \Lambda_1$, are all Rogers and Poltyrev good; $\Lambda_3$ is also quantization good.

V. CONCLUSION

We showed that using a chain of nested lattices $\Lambda_3 \subset \Lambda_2 \subset \Lambda_1$, lattice coding and decoding can achieve the secrecy rate of the Gaussian wiretap channel; we need the sequence of lattices $\Lambda_1^{(n)}$ and $\Lambda_2^{(n)}$ to be AWGN good, and the sequence $\Lambda_3^{(n)}$ to be good for quantization. We considered a decoder at the legitimate receiver which jointly decoded the transmitted codeword made up of the message bits and random bits, and a lattice construction $\Lambda_3 \subset \Lambda_2 \subset \Lambda_1$ with all lattices Rogers good and Poltyrev good, $\Lambda_3$ is also quantization good, and $k_1, k_2, p$ growing appropriately with $n$. We could then show the achievability of probability of decoding error going to zero at rates approaching the capacities of the main and wiretapper’s channels. In the future, we are interested in considering other explicit constructions. A staged decoder decoding message and random bits separately may be considered, which will give us more insight on the requirements of $\Lambda_1$ and $\Lambda_2$.

REFERENCES


