A Capacity-Achieving Coding Scheme for the AWGN Channel with Polynomial Encoding and Decoding Complexity

Shashank Vatedka and Navin Kashyap
Department of Electrical Communication Engineering
Indian Institute of Science, Bangalore, India
email: { shashank,nkashyap }@ece.iisc.ernet.in

***Abstract*—A fundamental problem in coding theory is the design of an efficient coding scheme that achieves the capacity of the additive white Gaussian (AWGN) channel. In this article, we study a simple capacity-achieving nested lattice coding scheme whose encoding and decoding complexities are polynomial in the blocklength. Specifically, we show that by concatenating an inner nested lattice code with an outer Reed-Solomon code over an appropriate finite field, we can achieve the capacity of the AWGN channel. The main feature of this technique is that the encoding and decoding complexities grow as $O(N^2)$, while the probability of error decays exponentially in N, where N denotes the blocklength. We also show that this gives us a recipe to extend a high-complexity nested lattice code for a Gaussian channel to low-complexity concatenated code without any loss in the asymptotic rate. As examples, we describe polynomial-time coding schemes for the wiretap channel, and the compute-and-forward scheme for computing integer linear combinations of messages.**

I. Introduction

The problem of designing efficient coding schemes for the additive white Gaussian (AWGN) channel has been studied for a very long time. Shannon [15] showed that random codes can achieve the capacity of the AWGN channel. Showing that structured codes can achieve capacity remained open till it was shown by de Buda [2], [10], and later by Urbanke and Rimoldi [17] that lattice codes can achieve capacity with maximum likelihood (ML) decoding. Erez and Zamir [3] then showed that nested lattice codes can achieve capacity with closest lattice point decoding. Lattice codes have been shown to be optimal for several other problems such as dirty paper coding, Gaussian multiple access channels, quantization, and so on. They have also been used in the context of physical layer network coding [9], [13] and physical layer security [11], [18]. We refer the reader to the book by Zamir [20] for an overview of the applications of lattices for channel coding and quantization. A drawback with the proposed nested lattice schemes is that their decoding complexity grows exponentially in the blocklength N. Unlike the case of linear codes for discrete memoryless channels, the encoding complexity of lattice codes also grows exponentially with N. A notable exception is the polar lattice scheme proposed by Yan et al. [19] which can achieve the capacity of the AWGN channel with an encoding/decoding complexity of $O(N \log^2 N)$.[1] However, the probability of error is $e^{-O(\sqrt{N})}$.

Concatenated codes were introduced by Forney [4] as a technique for obtaining low-complexity codes that can achieve the capacity of discrete memoryless channels. Concatenating an inner random linear code with an outer Reed-Solomon code is a simple way of designing good codes. Using this idea, Joseph and Barron [6] proposed a capacity-achieving scheme for the AWGN channel with quadratic (in the blocklength N) encoding/decoding complexity. They used a concatenated coding scheme with an inner sparse superposition code and an outer Reed-Solomon code. The probability of decoding error goes to zero exponentially in $N/\log N$ [7].

In this article, we show that concatenating an inner nested lattice code with an outer Reed-Solomon code yields a capacity-achieving coding scheme whose encoding/decoding complexity is quadratic in the blocklength. Furthermore, the probability of error decays exponentially in N. To the best of our knowledge, this is the first capacity-achieving coding scheme for the AWGN channel whose encoding and decoding complexities are polynomial, and the probability of error decays exponentially in the blocklength. The techniques that we use are not new, and we use results from the works of Forney [4] and Erez and Zamir [3] to prove our results. An attractive feature of this technique is that it can also be used to reduce the complexity of nested lattice codes for several other Gaussian networks. It can be used as a tool to convert any nested lattice code having exponential decoding complexity to a code having quadratic decoding complexity. This comes at the expense of a minor reduction in performance (in terms of error probability) of the resulting code. As applications, we show how this can be used for the Gaussian wiretap channel and in reducing the decoding complexity of the compute-and-forward protocol for Gaussian networks.

Throughout this article, we measure complexity in terms of the number of binary operations required for decoding/encoding, and we are interested in how this complexity scales with the blocklength. We assume that arithmetic

[1] Yan et al. [19] also show that for a fixed error probability (as opposed to a probability of error that goes to zero as $N \to \infty$), the encoding/decoding complexity of polar lattices is $O(N \log N)$.

operations on real numbers are performed using floating-point arithmetic, and that each real number has a t-bit binary representation, with t being independent of the blocklength. The value of t would depend on the computer architecture used for computations (typically 32 or 64 bits). In essence, we assume that each floating-point operation has complexity $O(1)$.

The rest of the paper is organized as follows. We describe the notation used in the paper and recall some concepts related to lattices in Section II. We then describe the concatenated coding scheme for the AWGN channel in Section III, with Theorem 2 summarizing the main result. Extension of the concatenated coding scheme to the Gaussian wiretap channel and the compute-and-forward protocol are outlined in Section IV-A and Section IV-B respectively. We conclude the paper with some final remarks in Section IV-C.

II. Notation and Definitions

We borrow notation from [18]. For a detailed exposition on lattices and their applications in several communication-theoretic problems, see [20]. We denote the set of integers by $\mathbb{Z}$ and real numbers by $\mathbb{R}$. For a prime number p and positive integer k, we let $\mathbb{F}_{p^k}$ denote the field of characteristic p, and containing p^k elements. If X and Y are random variables, then $I(X;Y)$ denotes the mutual information between X and Y. For $A, B \subset \mathbb{R}^n$ and $a, b \in \mathbb{R}$, we define $aA + bB$ to be the set $\{ax + by : x \in A, y \in B\}$. Given $\mathbf{x}, \mathbf{y} \in \mathbb{Z}^n$ and $p \in \mathbb{Z}$, we say that $\mathbf{x} \equiv \mathbf{y} \bmod p$ if $(\mathbf{x} - \mathbf{y}) \in p\mathbb{Z}^n$.

If G is an $n \times n$ full-rank matrix with real entries, then the set $\Lambda = G^T\mathbb{Z}^n := \{G\mathbf{z} : \mathbf{z} \in \mathbb{Z}^n\}$ is called a *lattice* in $\mathbb{R}^n$. We say that G is a *generator matrix* for Λ. It is a fact that the generator matrix of a lattice is not unique. Let $Q_\Lambda(\cdot)$ denote the lattice *quantizer* that maps a point in $\mathbb{R}^n$ to the point in Λ closest to it. For $\mathbf{x} \in \mathbb{R}^n$, we define $[\mathbf{x}] \bmod \Lambda$ to be the quantization error $\mathbf{x} - Q_\Lambda(\mathbf{x})$ when using the quantizer Q_Λ. The *fundamental Voronoi region* of Λ, $\mathcal{V}(\Lambda)$, is defined to be $\mathcal{V}(\Lambda) := \{\mathbf{x} \in \mathbb{R}^n : Q_\Lambda(\mathbf{x}) = \mathbf{0}\}$. The radius of the smallest closed ball in $\mathbb{R}^n$ centered at zero which contains $\mathcal{V}(\Lambda)$ is called the *covering radius*, and is denoted $r_{\mathrm{cov}}(\Lambda)$. Given two lattices Λ and Λ_0 in $\mathbb{R}^n$, we say that Λ_0 is *nested* in Λ if $\Lambda_0 \subset \Lambda$. We call Λ_0 the *coarse lattice* and Λ the *fine lattice*.

A. Construction A

For completeness, we describe Construction A, a technique to obtain lattices from linear codes over prime fields–see [3], [20] for a more detailed description. Let $\mathcal{C}$ be an (n, k) linear code over $\mathbb{F}_p$, i.e., it has length n and dimension k. Then, the Construction-A lattice obtained from $\mathcal{C}$, denoted $\Lambda_{\mathrm{A}}(\mathcal{C})$, is defined as the set of all points $\mathbf{x}$ in $\mathbb{Z}^n$ such that $\mathbf{x} \equiv \mathbf{y} \bmod p$ for some $\mathbf{y} \in \mathcal{C}$. Note that $p\mathbb{Z}^n$ is always a sublattice of $\Lambda_{\mathrm{A}}(\mathcal{C})$.

We will use the nested lattice construction from [3]. Let Λ_0 be a (possibly scaled) Construction-A lattice in $\mathbb{R}^n$, having a generator matrix G. Let $\Lambda_{\mathrm{A}}(\mathcal{C})$ be another Construction-A lattice obtained from an (n, k) linear code $\mathcal{C}$ over $\mathbb{F}_p$. Then, $\Lambda := \frac{1}{p}G^T\Lambda_{\mathrm{A}}(\mathcal{C}) = \{(1/p)G^T\mathbf{x} : \mathbf{x} \in \Lambda_{\mathrm{A}}(\mathcal{C})\}$ is also a lattice, and it can be verified that Λ_0 is nested in Λ. We will refer to (Λ, Λ_0) as a *nested Construction-A* lattice pair. A key feature of the nested lattice pair that will be of use to us is that $\Lambda \cap \mathcal{V}(\Lambda_0)$ (and hence the quotient group Λ/Λ_0) contains p^k elements. Furthermore, there exists a group isomorphism from the quotient group Λ/Λ_0 to $\mathbb{F}_{p^k}$ viewed as an additive group.

III. Coding Scheme for the AWGN Channel

Let us consider the point-to-point AWGN channel where the source encodes its message M to $\mathbf{u} \in \mathbb{R}^n$ and transmits this to a destination that receives

$$\mathbf{w} = \mathbf{u} + \mathbf{z},$$

where $\mathbf{z}$ is the noise vector having independent and identically distributed (iid) Gaussian entries with mean zero and variance σ^2. Erez and Zamir [3] proposed a nested lattice scheme for the AWGN channel, which we briefly describe here. The code is constructed using a pair of nested lattices $(\Lambda^{(n)}, \Lambda_0^{(n)})$, where $\Lambda_0^{(n)} \subset \Lambda^{(n)}$. The codebook consists of all the points of $\Lambda^{(n)}$ within the fundamental Voronoi region of $\Lambda_0^{(n)}$, i.e., the codebook is $\Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})$. The transmission rate is therefore $\frac{1}{n}\log_2 |\Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})|$.

The source also generates a random vector $\mathbf{t}$ uniformly distributed over $\mathcal{V}(\Lambda_0^{(n)})$. This vector, also called the *dither* vector, is assumed to be known to the decoder[2]. Each message M is mapped to a point $\mathbf{x}$ in the codebook $\Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})$. The encoder $\mathcal{E}^{(n)}$ takes the message M as input and outputs the vector $[\mathbf{x} - \mathbf{t}] \bmod \Lambda_0^{(n)}$, which is transmitted across the channel. This process of translating the message by $\mathbf{t}$ modulo $\Lambda_0^{(n)}$ prior to transmission is called *dithering*. The encoder satisfies a maximum transmit power constraint given by $\frac{1}{n}\max_{\mathbf{u}\in\mathcal{V}(\Lambda_0)} \|\mathbf{u}\|^2 = \frac{1}{n}{r_{\mathrm{cov}}}^2(\Lambda_0^{(n)}) < P$.

Upon receiving $\mathbf{w}$, the receiver uses a decoder $\mathcal{D}^{(n)}$ to estimate M, which does the following. It computes $\widetilde{\mathbf{w}} = [\alpha\mathbf{w} + \mathbf{t}] \bmod \Lambda_0^{(n)}$, where $\alpha = \frac{P}{P+\sigma^2}$. The estimate of M is the message that corresponds to $[Q_{\Lambda^{(n)}}(\widetilde{\mathbf{w}})] \bmod \Lambda_0^{(n)}$.

Let $C := \frac{1}{2}\log_2\left(1 + \frac{P}{\sigma^2}\right)$. Erez and Zamir [3] showed that there exist nested lattices with which we can approach the capacity of the AWGN channel. Specifically,

Lemma 1 ([3], Theorem 5)**.** *For every $\epsilon > 0$, there exists a sequence of (n, k, p) nested[3] Construction-A lattice pairs $(\Lambda^{(n)}, \Lambda_0^{(n)})$ so that for all sufficiently large n, the following hold:*

$$\frac{1}{n}{r_{\mathrm{cov}}}^2(\Lambda_0^{(n)}) \le P + \epsilon,$$

the transmission rate satisfies[4]

$$R_{\mathrm{in}}^{(n)} := \frac{1}{n}\log_2 |\Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})| \ge C - \epsilon,$$

[2]In principle, the dither vector is not necessary. However, this technique of dithered transmission simplifies the analysis of the probability of error of the decoder.

[3]Note that k, p are functions of n. We have suppressed the index n for convenience.

[4]The subscript 'in' in $R_{\mathrm{in}}^{(n)}$ indicates that we intend to use the nested lattice code as an inner code in a concatenated coding scheme, which we describe in Section III-A.

and the probability of error decays exponentially in n for all $R_{\text{in}}^{(n)} < C$, i.e., there exists a function $E : \mathbb{R}^+ \to \mathbb{R}^+$ so that for every $\mathbf{x} \in \Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})$ and all sufficiently large n, we have

$$\Pr[\mathbf{x} \neq \mathcal{D}^{(n)}(\mathcal{E}^{(n)}(\mathbf{x}) + \mathbf{z})] \leq e^{-nE(R_{\text{in}}^{(n)})}.$$

Furthermore, the quantity $E(R_{\text{in}}^{(n)})$ is positive for all $R_{\text{in}}^{(n)} < C$.

The decoding involves solving two closest lattice point problems, which are the $Q_{\Lambda^{(n)}}$ and $\bmod \Lambda_0^{(n)}$ operations. Therefore, the decoding complexity is $O(2^{nR})$. If the encoder uses a look-up table to map messages to codewords, the complexity would also be $O(2^{nR})$.

A. The Concatenated Coding Scheme for the AWGN Channel

Let us now give a brief description of the concatenated coding scheme. See [4] for a more detailed exposition and application to the discrete memoryless channel. The code has two components:

- Inner code: A nested Construction-A lattice code $(\Lambda^{(n)}, \Lambda_0^{(n)})$ with the fine lattice $\Lambda^{(n)}$ obtained from a (n, k) linear code over $\mathbb{F}_p$.
- Outer code: An $(N_{\text{out}}, K_{\text{out}}, d_{\text{out}})$ linear block code (where d_{out} is the minimum distance of the code) over $\mathbb{F}_{p^k}$.

The message set has size $K_{\text{out}} p^k$, and each message can be represented by a vector in $\mathbb{F}_{p^k}^{K_{\text{out}}}$. The outer code maps this vector to a codeword in $\mathbb{F}_{p^k}^{N_{\text{out}}}$. Let us call this $\mathbf{c}_{\text{out}} = [c_1\ c_2\ \cdots c_{N_{\text{out}}}]^T$, where each $c_i \in \mathbb{F}_{p^k}$. The inner code maps each $c_i \in \mathbb{F}_{p^k}$ to a point in $\Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})$. This results in a codeword of length nN_{out} having real-valued components. Each inner codeword is dithered by an independent dither vector prior to transmission. The encoding process is illustrated in Fig. 1. The receiver first uses the decoder for the inner code to estimate the components c_i, and finally uses the decoder for the outer code to recover the message. Since the outer code has minimum distance d_{out}, the message is guaranteed to be recovered correctly if not more than $(d_{\text{out}} - 1)/2$ inner codewords are in error. Furthermore, if all the inner codewords satisfy the (max) power constraint, then the concatenated code is also guaranteed to satisfy the same.

We now show that using this technique, we can achieve the capacity of the AWGN channel. Let us fix $\epsilon, \delta > 0$. Suppose we choose a sequence of nested lattice codes $(\Lambda^{(n)}, \Lambda_0^{(n)})$ that are guaranteed by Lemma 1. For every n, let us concatenate the nested lattice code with an outer $(N_{\text{out}}, K_{\text{out}}, N_{\text{out}} - K_{\text{out}} + 1)$ Reed-Solomon code over $\mathbb{F}_{p^k}$, where $N_{\text{out}} = p^k - 1$ and

$$K_{\text{out}} = N_{\text{out}}(1 - 2e^{-nE(R_{\text{in}})} - 2\delta). \tag{1}$$

Here and in the rest of this section, we drop the superscript in $R_{\text{in}}^{(n)}$ for convenience. The resulting code, which we denote $\mathcal{C}^{(N)}$, has blocklength $N = nN_{\text{out}} \approx n2^{nR_{\text{in}}}$, and rate

$$R^{(N)} = (1 - 2e^{-nE(R_{\text{in}})} - 2\delta)R_{\text{in}}. \tag{2}$$

Theorem 2. *For every $\zeta > 0$, there exists a sequence of concatenated codes $\mathcal{C}^{(N)}$ with inner nested lattice codes and outer Reed-Solomon codes that satisfies the following for all sufficiently large n:*

- *the rate, $R^{(N)} \geq C - \zeta$,*
- *the maximum transmit power,*

$$\max_{\mathbf{x} \in \mathcal{C}^{(N)}} \frac{1}{N} \|\mathbf{x}\|^2 \leq P - \zeta,$$

- *the probability of error is at most $e^{-NE(R_{\text{in}})\zeta}$, and*
- *the encoding and decoding complexities grow as $O(N^2)$.*

Proof. The construction of the concatenated codes ensures that the power constraint can be satisfied. From Lemma 1, we are assured of nested lattice codes whose rate $R_{\text{in}} \geq C - \zeta/2$. Choosing a small enough δ and a large enough n in (2) guarantees that the effective rate $R^{(N)} \geq C - \zeta$ for all sufficiently large N.

Let us now proceed to analyze the probability of error. Clearly, the probability that an inner codeword is in error is upper bounded by $e^{-nE(R_{\text{in}})}$ by Lemma 1. Since the outer Reed-Solomon code has minimum distance $N_{\text{out}} - K_{\text{out}} + 1$, the decoder makes an error only if atleast $(N_{\text{out}} - K_{\text{out}} + 1)/2 = N_{\text{out}}(e^{-nE(R_{\text{in}})} + \delta + 1/(2N_{\text{out}}))$ inner codewords are in error. For all sufficiently large N, we can upper bound the probability of decoding error as follows:

$$P_e^{(N)} \leq \binom{N_{\text{out}}}{N_{\text{out}}(e^{-nE(R_{\text{in}})} + \delta + 1/(2N_{\text{out}}))} \times \left(e^{-nE(R_{\text{in}})}\right)^{N_{\text{out}}(e^{-nE(R_{\text{in}})} + \delta + 1/(2N_{\text{out}}))} \tag{3}$$

$$\leq \binom{N_{\text{out}}}{N_{\text{out}}(e^{-nE(R_{\text{in}})} + 2\delta)} \times \left(e^{-nE(R_{\text{in}})}\right)^{N_{\text{out}}(e^{-nE(R_{\text{in}})} + \delta)} \tag{4}$$

$$\leq e^{N_{\text{out}} h(e^{-nE(R_{\text{in}})} + 2\delta)} \left(e^{-nE(R_{\text{in}})}\right)^{N_{\text{out}}(e^{-nE(R_{\text{in}})} + \delta)} \tag{5}$$

where (3) is obtained using the union bound, and the last step from Stirling's formula. In (5), $h(\cdot)$ denotes the binary entropy function. For all sufficiently large n, we have $h(e^{-nE(R_{\text{in}})} + 2\delta) < h(3\delta)$. Using this in the above and simplifying, we get

$$P_e^{(N)} \leq \exp\Big(- nN_{\text{out}}\big(E(R_{\text{in}})(e^{-nE(R_{\text{in}})} + \delta) - h(3\delta)/n\big)\Big)$$

Let us define the error exponent as

$$E_{\text{conc}} := E(R_{\text{in}})(e^{-nE(R_{\text{in}})} + \delta) - h(3\delta)/n \tag{6}$$

It is clear that $E_{\text{conc}} > E(R_{\text{in}})\delta/2$ for all sufficiently large n. This proves that the probability of error decays exponentially in N.

Let us now inspect the encoding and decoding complexity. As remarked in the introduction, we assume that each floating-point operation requires a constant number of binary operations (i.e., independent of N) and has a complexity of

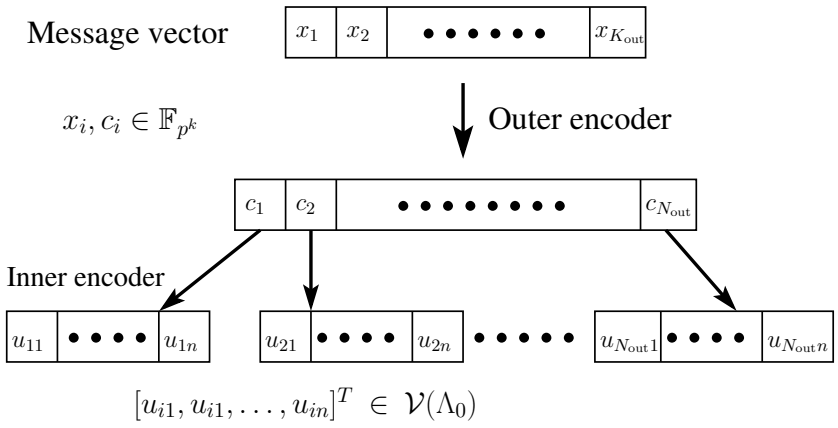

Fig. 1. Illustration of the concatenated nested lattice coding scheme.

$O(1)$. Encoding/decoding each inner (nested lattice) codeword requires $O(2^{nR_{\text{in}}})$ floating-point operations, and there are N_{out} many codewords, leading to a total complexity of $O(N^2)$. Furthermore, encoding/decoding a Reed-Solomon codeword requires $O(N_{\text{out}}^2)$ operations in $\mathbb{F}_{p^k}$ [14, Chapter 6]. Multiplication and inversion are the most computationally intensive operations in $\mathbb{F}_{p^k}$, and they can be performed using $O((k \log_2 p)^2) = O(n^2)$ binary operations [5, Chapter 2]. Therefore, the outer code has an encoding/decoding complexity of $O(N_{\text{out}}^2) \times O(n^2) = O(N^2)$. We can therefore conclude that encoding and decoding the concatenated code requires a complexity of $O(N^2)$. □

B. Complexity

Let us denote x to be the decoding complexity. From Theorem 2, we can conclude that for a fixed gap to capacity ($\Delta := C - R$), the probability of error for the concatenated coding scheme scales as $e^{-a\sqrt{x}}$ for some constant $a > 0$. As argued in [4, Section 5.1], this is a much stronger statement than saying that the decoding complexity is polynomial in the blocklength.

Previously, Joseph and Barron [6], [7] proposed a concatenated coding scheme with inner sparse superposition codes and outer Reed-Solomon codes. They showed that their scheme achieves the capacity of the AWGN channel with polynomial (in the blocklength N) time encoding/decoding. The decoding complexity is $x = O(N^2)$. However, the probability of error decays exponentially in $N/\log N$ for a fixed gap to capacity Δ. Therefore, the probability of error is exponentially decaying in $\sqrt{x}/\log x$. More recently, Yan et al. [19] proposed a lattice-based scheme using polar codes that achieves capacity with an encoding/decoding complexity of $O(N \log N)$ for a fixed error probability, and $x = O(N \log^2 N)$ with a probability of error (for a fixed Δ) which was exponential in N^β, for some $0 < \beta < 0.5$. The probability of error is therefore $O(e^{-a(x/\log x)^\beta})$. The concatenated scheme we have studied here outperforms these works in the sense that the probability of error decays exponentially in the square root of x for a fixed Δ. However, we have not been able to show that for a fixed probability of error, the decoding complexity is polynomial in the gap to capacity. The only such result that we are aware of is by Yan et al. [19], where they showed that polar lattices have a decoding complexity that is polynomial in the gap to the Poltyrev capacity (for the AWGN channel without restrictions/power constraint). Finding a capacity-achieving coding scheme for the power-constrained AWGN channel with a decoding complexity that scales polynomially in the gap to capacity for a fixed probability of error still remains an open problem.

IV. Discussion

The approach used in the previous section can be used as a recipe for reducing the decoding complexity of optimal coding schemes for Gaussian channels. A nested lattice scheme that achieves a rate R over a Gaussian channel can be concatenated with a high-rate outer Reed-Solomon code to achieve any rate arbitrarily close to R. The only requirement is that the nested lattice code has a probability of error which decays exponentially in its blocklength. This procedure helps us bring down the decoding complexity to a quadratic function of the blocklength while ensuring that the probability of error continues to be an exponential function of the blocklength. As examples, we discuss two important applications: a scheme that achieves the secrecy capacity of the wiretap channel, and the compute-and-forward protocol for computing linear combinations of several messages over a Gaussian channel. Since our objective is only to suggest potential applications, we will keep the details to a minimum.

A. The Gaussian Wiretap Channel

The Gaussian wiretap channel [8] consists of three parties: a source, a destination and an eavesdropper. The source has a message M which is intended only for the destination but not the eavesdropper. The source encodes M to a real n-dimensional vector $\mathbf{u}$ and transmits it across to the destination. The destination receives $\mathbf{w}_{\text{D}}$, which is modeled as

$$\mathbf{w}_{\text{D}} = \mathbf{u} + \mathbf{z}_{\text{D}},$$

where $\mathbf{z}_{\mathrm{D}}$ is AWGN with mean zero and variance σ^2. On the other hand, the eavesdropper observes

$$\mathbf{w}_{\mathrm{E}} = \mathbf{u} + \mathbf{z}_{\mathrm{E}},$$

where $\mathbf{z}_{\mathrm{E}}$ is AWGN with mean zero and variance $\sigma_{\mathrm{E}}^2 > \sigma^2$. We want to ensure that the destination recovers M with negligible probability of error, while the eavesdropper gets very little information about M. Specifically, we require $I(M; \mathbf{w}_{\mathrm{E}}) \to 0$ as $n \to \infty$. This is also called the *strong secrecy* constraint. A more detailed exposition of the wiretap and related channels studied in information-theoretic security can be found in [1]. We define the secrecy capacity of the wiretap channel as the supremum over all achievable rates while satisfying the strong secrecy constraint. If we define $C_{\mathrm{M}} := \frac{1}{2}\log_2(1 + P/\sigma^2)$ and $C_{\mathrm{E}} := \frac{1}{2}\log_2(1 + P/\sigma_{\mathrm{E}}^2)$ to be the capacities of the main and eavesdropper channels respectively, then the secrecy capacity of this wiretap channel is $C_{\mathrm{M}} - C_{\mathrm{E}}$.

Tyagi and Vardy [16] gave an explicit scheme using 2-universal hash functions that converts any coding scheme of rate R over the point-to-point AWGN (main) channel to a coding scheme that achieves a rate $R - C_{\mathrm{E}}$ over the wiretap channel while satisfying the strong secrecy constraint. This "conversion" adds an additional decoding complexity which is polynomial in the blocklength. We can therefore use this result with Theorem 2 to conclude that we can achieve the secrecy capacity of the Gaussian wiretap channel with polynomial time decoding/encoding.

B. Compute-and-forward

The compute-and-forward protocol was proposed by Nazer and Gastpar [13] for communication over Gaussian networks. Let us begin by describing the setup. We have L source nodes $\mathtt{S}_1, \mathtt{S}_2, \ldots, \mathtt{S}_L$, having independent messages $X_1, X_2, \ldots, X_L$ respectively. The messages are chosen from $\mathbb{F}_{p^k}^K$ for some prime number p and positive integers k, K. Let $\oplus$ denote the addition operator in $\mathbb{F}_{p^k}^K$. These messages are mapped to N-dimensional real vectors $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_L$ respectively and transmitted across a Gaussian channel to a destination $\mathtt{D}$ which observes

$$\mathbf{w} = \sum_{l=1}^{L} h_l \mathbf{u}_l + \mathbf{z}, \tag{7}$$

where $h_1, h_2, \ldots, h_L$ are real-valued channel coefficients and $\mathbf{z}$ is AWGN with mean zero and variance σ^2. The destination must compute $a_1 X_1 \oplus a_2 X_2 \oplus \cdots \oplus a_L X_L$, where $a_1, a_2, \ldots, a_L$ are integers. We assume that each source node must satisfy a maximum power constraint of P. We only consider symmetric rates here, i.e., all sources have identical message sets. The rate of the code is $\frac{kK}{N}\log_2 p$. This problem is relevant in many applications such as exchange of messages in bidirectional relay networks, decoding messages over the Gaussian multiple access channel [13], and designing good receivers for MIMO channels [21] to name a few. The basic idea is that instead of decoding the messages one at a time and using successive cancellation, it may be more efficient to decode multiple linear combinations of the messages. If we have L linearly independent such combinations, then we can recover all the individual messages.

We can extend the scheme of [13] to a concatenated coding scheme that achieves the rates guaranteed by [13], but now with encoders and decoders that operate in polynomial time. Recall that the messages are chosen from $\mathbb{F}_{p^k}^K$. We say that a rate $\mathcal{R}$ is achievable if for every $\epsilon > 0$, there exists a sequence of encoders and decoders so that for all sufficiently large blocklengths N, we have the transmission rate $R^{(N)} := \frac{kK}{N}\log_2 p > \mathcal{R} - \epsilon$, and the probability of error is less than ϵ. We can show the following:

Lemma 3. *Consider the problem of computing $a_1 X_1 \oplus a_2 X_2 \oplus \cdots \oplus a_L X_L$ from (7). Any rate*

$$\mathcal{R} < \frac{1}{2}\log_2\left(\frac{P}{\alpha^2 + P\sum_{l=1}^{L}(\alpha h_l - a_l)^2}\right), \tag{8}$$

where

$$\alpha := \frac{P\sum_{l=1}^{L} h_l a_l}{\sigma^2 + P\sum_{l=1}^{L} h_l^2}, \tag{9}$$

is achievable with encoders and decoders whose complexities grow as $O(N^2)$. For transmission rates less than $\mathcal{R}$, the probability that the decoder makes an error goes to zero exponentially in N.

Proof. The technique used to justify this claim is a simple extension of the coding scheme of [13] using the methods described in Section III. For completeness, we will briefly describe the scheme. For more details regarding the compute-and-forward protocol, see [13]. We use the concatenated coding scheme of Section III-A. The inner code is obtained from nested Construction-A lattices $(\Lambda^{(n)}, \Lambda_0^{(n)})$. Suppose that $\Lambda^{(n)}$ is constructed using a (n, k) linear code over $\mathbb{F}_p$. The outer code is an $(N_{\mathrm{out}}, K_{\mathrm{out}}, N_{\mathrm{out}} - K_{\mathrm{out}} + 1)$ Reed-Solomon code, with $N_{\mathrm{out}} = p^k - 1$ and K_{out} to be specified later. The transmission rate is $R^{(n)} = \frac{kK_{\mathrm{out}}}{nN_{\mathrm{out}}}\log_2 p$.

The messages are chosen from $\mathbb{F}_{p^k}^{K_{\mathrm{out}}}$. Let the message at the lth user be $M_l = [m_1^{(l)}, m_2^{(l)}, \ldots, m_{K_{\mathrm{out}}}^{(l)}]^T$, where $m_i^{(l)} \in \mathbb{F}_{p^k}$. The messages are mapped to an N_{out}-length codeword over $\mathbb{F}_{p^k}$ using the outer code. Let the resulting codeword be $\mathbf{y}^{(l)} = [y_1^{(l)}, y_2^{(l)}, \ldots, y_{N_{\mathrm{out}}}^{(l)}]^T$.

Each $y_i^{(l)}$ is then encoded to $\mathbf{u}_i^{(l)}$ using the inner code and then transmitted. Recall that there exists a group isomorphism from $\Lambda^{(n)}/\Lambda_0^{(n)}$ to $\mathbb{F}_{p^k}$. For $1 \le l \le L$ and $1 \le i \le N_{\mathrm{out}}$, let $\mathbf{x}_i^{(l)}$ be the representative of $y_i^{(l)}$ in $\Lambda^{(n)} \cap \mathcal{V}(\Lambda_0^{(n)})$. Independent dither vectors $\mathbf{t}_1^{(l)}, \mathbf{t}_2^{(l)}, \ldots, \mathbf{t}_{N_{\mathrm{out}}}^{(l)}$ are generated at the L sources. Transmitter l successively sends $\mathbf{u}_i^{(l)} = [\mathbf{x}_i^{(l)} - \mathbf{t}_i^{(l)}] \bmod \Lambda_0^{(n)}$ for $1 \le i \le N_{\mathrm{out}}$ to the receiver.

The decoder, upon receiving $\mathbf{w}_i = \sum_{l=1}^{L} \mathbf{u}_i^{(l)} + \mathbf{z}$, computes $\widetilde{\mathbf{w}}_i = \left[\alpha \mathbf{w}_i + \sum_{l=1}^{L} a_l \mathbf{t}_i^{(l)}\right] \bmod \Lambda_0^{(n)}$. The estimate of $[\sum_{l=1}^{L} a_i \mathbf{x}_i^{(l)}] \bmod \Lambda_0^{(n)}$, is $[Q_{\Lambda^{(n)}}(\widetilde{\mathbf{w}}_i)] \bmod \Lambda_0^{(n)}$. Recall the definition of $\mathcal{R}$ in (8). Nazer and Gastpar showed in [13] that there exists a sequence of nested Construction-A lattices with $R_{\mathrm{in}}^{(n)} = \frac{k}{n}\log_2 p$ for which the probability that the decoder

makes an error in estimating the desired linear combination decays as $e^{-nE_c(R_{\text{in}}^{(n)})}$, where $E_c(\cdot)$ is some function which is positive for all $R_{\text{in}}^{(n)} < \mathcal{R}$. As we did before for the AWGN channel, we choose $K_{\text{out}} = N_{\text{out}}(1 - 2e^{-nE_c(R_{\text{in}}^{(n)})} - \epsilon)$. Assuming that fewer than $(N_{\text{out}} - K_{\text{out}})/2$ inner codewords are in error, the decoder can recover $\widehat{\mathbf{x}}_c = \left[\left[\sum_l a_l \mathbf{x}_1^{(l)} \right] \bmod \Lambda_0^{(n)}, \ldots, \left[\sum_l a_l \mathbf{x}_{N_{\text{out}}}^{(l)} \right] \bmod \Lambda_0^{(n)} \right]^T$ without error. Due to the existence of a group isomorphism between $\mathbb{F}_{p^k}$ and $\Lambda^{(n)}/\Lambda_0^{(n)}$, this implies that the decoder can recover $a_1\mathbf{y}^{(1)} \oplus \cdots \oplus a_L\mathbf{y}^{(L)}$, and hence, $a_1M_1 \oplus \cdots \oplus a_LM_L$. Arguing as in Section III, the probability that the decoder makes an error goes to zero exponentially in N, and the decoding/encoding complexities grow as $O(N^2)$. □

C. Concluding Remarks

We have seen that concatenation can be a very powerful tool in reducing the asymptotic decoding complexity of nested lattice codes. However, it must be noted that achieving good performance using this scheme would require very large blocklengths. Although the probability of error decays exponentially in N, and the decoding/encoding complexities are $O(N^2)$, this is true only for very large values of N. The fact that N is exponential in the blocklength of the inner code is a major reason for this. The concatenated coding approach shows that it is easy to obtain polynomial-time encoders and decoders for which the probability of error decays exponentially in the blocklength. The exponential decay is under the assumption that the gap between the transmission rate and capacity $\Delta = C - R$ is kept fixed. For a fixed error probability P_e, the blocklength required by the concatenated coding scheme to achieve rate $R = C - \Delta$ and error probability P_e does not scale polynomially with $1/\Delta$. For a fixed error probability, we would like the complexity to not grow too fast as the rate approaches C. Ideally, we want the gap to capacity Δ going to zero polynomially in $1/N$. It has been recently shown that polar codes have this property for binary memoryless symmetric channels [12]. Designing codes for the Gaussian channel whose decoding/encoding complexities are also polynomial in $1/\Delta$ for a fixed probability of error still remains an open problem.

V. Acknowledgements

The authors would like to thank Prof. Sidharth Jaggi for a discussion that led to this work. The work of the first author was supported by the TCS Research Scholarship Program.

References

[1] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering,* Cambridge University Press, 2011.

[2] R. de Buda, "Some optimal codes have structure," *IEEE J. Sel. Areas in Communications*, vol. 7, no. 6, pp. 893–899, 1989.

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

[4] G.D. Forney, *Concatenated Codes,* Cambridge: MIT press, 1966.

[5] D. Hankerson, A.J. Menezes, S. Vanstone, *Guide to Elliptic Curve Cryptography,* Springer Science & Business Media, 2006.

[6] A. Joseph and A.R. Barron, "Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2541–2557, May. 2012.

[7] A. Joseph and A.R. Barron, "Fast sparse superposition codes have near exponential error probability for $R < C$," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 919–942, Feb. 2014.

[8] S. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[9] S.C. Liew, S. Zhang, L. Lu, "Physical-layer network coding: tutorial, survey, and beyond," *Physical Communication,* vol. 6, pp. 4–42, Mar. 2013.

[10] T. Linder, C. Schlegel, K. Zeger, "Corrected proof of de Buda's theorem [lattice channel codes]," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1735–1737, Sep. 1993.

[11] C. Ling, L. Luzzi, J.-C. Belfiore, D. Stehle, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[12] M. Mondelli, S.H. Hassani, R. Urbanke, "Unified scaling of polar codes: Error exponent, scaling exponent, moderate deviations, and error floors," *arXiv preprint,* arXiv:1501.02444, 2015.

[13] B. Nazer and M. Gastpar, "Compute-and-forward: harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[14] R. Roth, *Introduction to Coding Theory,* Cambridge University Press, 2006.

[15] C.E. Shannon, "A mathematical theory of communication," *Bell Syst. Tech. Journal,* vol. 27, no. 3, pp. 379–423, July 1948.

[16] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," *in proc. 2014 IEEE Int. Symp. Information Theory (ISIT),* Honolulu, HI, 2014, pp.956-960.

[17] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 273–278, Jan. 1998.

[18] S. Vatedka, N. Kashyap, A. Thangaraj, "Secure compute-and-forward in a bidirectional relay", *IEEE Trans. Inf. Theory*, vol. 51, no. 5, pp 2531–2556, May 2015.

[19] Y. Yan, L. Liu, C. Ling, X. Wu, "Construction of capacity-achieving lattice codes: Polar lattices," *arXiv preprint* arXiv:1411.0187, 2014.

[20] R. Zamir, *Lattice Coding for Signals and Networks: A Structured Coding Approach to Quantization, Modulation, and Multiuser Information Theory,* Cambridge University Press, 2014.

[21] J. Zhan, B. Nazer, U. Erez, M. Gastpar, "Integer-forcing linear receivers," *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7661–7685, Dec. 2014.