ISIT'2013 1569719755

# Wiretap Encoding of Lattices from Number Fields Using Codes over $\mathbb{F}_p$

Wittawat Kositwattanarerk, Soon Sheng Ong, Frédérique Oggier
Division of Mathematical Sciences
School of Physical and Mathematical Sciences
Nanyang Technological University, Singapore
Email: ssong1@e.ntu.edu.sg and {kwittawat,frederique}@ntu.edu.sg

***Abstract*—We consider the problem of communication over a block fading wiretap channel. It is known that coding for such a channel can be done using nested lattice codes constructed over totally real number fields. In this paper, we propose a method for encoding an integral lattice over the ring of integers of a totally real number field, and study in particular the case of $\mathbb{Q}(\zeta_p+\zeta_p^{-1})$ using a linear code over $\mathbb{F}_p$. This generalizes the well-known Construction A and provides an efficient coset encoding for algebraic lattices.**

## I. Introduction

Connections between Euclidean lattices and linear codes, meaning discrete subgroups of $\mathbb{R}^N$ and linear subspaces of $\mathbb{F}_q^N$ respectively, have been classically studied (see [1] for an excellent course on the topic, or [3] for an exhaustive list of relevant results). The correspondence when the code is binary (i.e., $q = 2$) has been particularly examined, and is referred to as Construction A of lattices from binary codes. This construction considers a binary code $C$ of length $N$ and the mapping $\rho$ from $\mathbb{Z}^N$ to $\mathbb{F}_2^N$ by reduction modulo 2. Now, the preimage $\rho^{-1}(C)$ (or $\rho^{-1}(C)/\sqrt{2}$) of $C$ forms a lattice in $\mathbb{R}^N$. There is a series of dualities between theoretical properties of codes and that of the resulting lattices, such as the dual of the code and the dual of the lattice, the weight enumerator of the code and the theta series of the lattice (see e.g. [3], [4]). From a coding point of view, Construction A is also of practical interest since it provides an efficient method for encoding lattice codes. Recent works in this direction include [5] where Barnes-Wall lattices are obtained from linear codes over polynomial rings, resulting in an explicit method of bit-labeling complex Barnes-Wall lattice codes.

Construction of lattices from codes also provides a method of coset encoding for lattices in the context of wiretap lattice codes [6]. Indeed, the underlying idea of wiretap encoding is to have two nested lattices $\Lambda_e \subset \Lambda_b$ where $\Lambda_b$ is represented as a union of cosets of $\Lambda_e$. Information symbols are used to label the cosets, and random bits are introduced to pick a lattice point at random within this coset. This randomized encoding is meant to provide confidentiality between the two legitimate players, in the presence of an eavesdropper.

Encoding of wiretap codes for block fading channels is performed similarly using coset encoding [7]. However, for this channel, wiretap lattice codes are built from totally real number fields, to ensure full diversity [7], [8] and thus reliablity for the legitimate player. Therefore, constructions of lattices that generalize Construction A are needed. This is the question addressed in this paper. We propose a generalization of Construction A to lattices obtained from number fields (see [1] when the number field is the cyclotomic field $\mathbb{Q}(\zeta_p)$). We study some properties of this construction and its applications to wiretap encoding. Emphasis is given to the case where the number field is $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$, since it is totally real, and is known [8] to allow the construction of a lattice isomorphic to $\mathbb{Z}^{(p-1)/2}$.

## II. Lattices and Codes from Number Fields

We first recall the precise definition of integral lattices.

*Definition 1:* An integral lattice $\Gamma$ is a free $\mathbb{Z}$-module of finite rank $m$ together with a positive definite symmetric bilinear form $\langle\ ,\ \rangle : \Gamma \times \Gamma \to \mathbb{Z}$.

By a code $C$, we mean an $(N, k)$ linear code over the finite field $\mathbb{F}_q$ where $q$ is a prime power; that is, $C$ is a $k$-dimensional subspace of $\mathbb{F}_q^N$. The dual code of $C$, denoted $C^\perp$, is given by $C^\perp = \{y \in \mathbb{F}_q^N | y \cdot x = 0 \text{ for all } x \in C\}$ where $\cdot$ is the usual inner product of two vectors.

### A. Some Preliminaries on Number Fields

We are interested in integral lattices built over number fields, that is, finite field extensions of $\mathbb{Q}$. Let $K$ be a number field of degree $n$. The ring of integers in $K$, denoted $\mathcal{O}_K$, is a free $\mathbb{Z}$-module of rank $n$. There exists an integral basis $\{\nu_1, \ldots, \nu_n\}$ of $\mathcal{O}_K$ such that every element $x$ of $\mathcal{O}_K$ can be written as $x = \sum_{i=1}^n x_i\nu_i$ where $x_i \in \mathbb{Z}$. Every ideal of $\mathcal{O}_K$ has a unique decomposition as a product of prime ideals. Let $p$ be a prime in $\mathbb{Z}$, then $p\mathcal{O}_K = \prod_{i=1}^g \mathfrak{p}_i^{e_i}$ where $\mathfrak{p}_i$ are prime ideals. The number $g$ of prime ideals above $p$ and the ramification indices $e_i$ are related to the degree $n$ of the number field $K$ by the formula $n = \sum_{i=1}^g e_i f_i$ where $f_i$ is the inertial degree, i.e., the degree of the finite field $\mathcal{O}_K/\mathfrak{p}_i$ over $\mathbb{F}_p$. When $K$ is a Galois extension, this simplifies to $n = efg$. In other words, $e_i = e$ and $f_i = f$ for all $i$.

### B. General Constructions

Given a number field $K$ and a prime $\mathfrak{p} \in \mathcal{O}_K$ where $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_{p^f}$, let $C$ be a linear code of length $N$ and dimension $k$ over $\mathbb{F}_{p^f}$. We define $\Gamma_C$ to be the "preimage" of $C$ in $\mathcal{O}_K^N$. The precise definition is given as follows.

*Definition 2:* Let $\rho : \mathcal{O}_K^N \to \mathbb{F}_{p^f}^N$ be the mapping defined by the reduction modulo the ideal $\mathfrak{p}$ in each of the $N$ coordinates. Define

$$\Gamma_C := \rho^{-1}(C) \subset \mathcal{O}_K^N.$$

We first note that $\rho^{-1}(C)$ is a subgroup of $\mathcal{O}_K^N$ since $C$ is a subgroup of $\mathbb{F}_{p^f}^N$. Furthermore, $\mathcal{O}_K^N$ is a free $\mathbb{Z}$-module of rank $nN$, and so it follows that $\rho^{-1}(C)$ is also a free $\mathbb{Z}$-module. Now, since $|\mathcal{O}_K^N/\mathfrak{p}^N| < \infty$, $\rho^{-1}(C)$ and $\mathcal{O}_K^N$ must have the same rank as a $\mathbb{Z}$-module. We conclude that $\rho^{-1}(C)$ is a $\mathbb{Z}$-module of rank $nN$.

Let $\sigma_1, \ldots, \sigma_n$ be the $n$ embeddings of $K$ into $\mathbb{C}$. Recall that the signature $(r_1, r_2)$ of a number field $K$ of degree $n$ is the pair of the number $r_1$ of real embeddings of $K$, and the number $r_2$ of pairs of complex embeddings of $K$, where $n = r_1 + 2r_2$. Let $K$ be a totally real number field of degree $n$ (that is, $r_1 = n$ and $r_2 = 0$), and let $x = (x_1, \ldots, x_N)$ and $y = (y_1, \ldots, y_N)$ be vectors in $\mathcal{O}_K^N$. Then, $\rho^{-1}(C)$ forms a lattice with the symmetric bilinear form

$$\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i), \tag{1}$$

where the twisting element $\alpha \in K$ is totally positive, meaning that $\sigma_i(\alpha) > 0$ for all $i$ [2]. This condition ensures that the trace form is positive definite; by the definition of trace,

$$\begin{aligned}\langle x, x \rangle &= \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i x_i) \\ &= \sum_{i=1}^{N} \sum_{j=1}^{n} \sigma_j(\alpha) \sigma_j(x_i)^2 > 0\end{aligned}$$

given that $\sigma_i(\alpha) > 0$ for all $i$ and $x$ is not the zero vector. Note that since $x_i^2 \in \mathcal{O}_K$, its trace also belongs to $\mathbb{Z}$. Now, we need to have $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i^2) \in \mathbb{Z}$ to ensure that $\rho^{-1}(C)$ is an integral lattice. As a matter of fact, this depends on the choice of $\alpha$. While it is sufficient to have $\alpha \in \mathcal{O}_K$, depending on the code $C$, other choices of $\alpha$ might be possible. We will see later why doing so could be preferable.

If $K$ is a CM-field; that is, if $K$ is a totally imaginary quadratic extension of a totally real number field, then $\rho^{-1}(C)$ forms a lattice with the symmetric bilinear form

$$\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i), \tag{2}$$

where $\bar{y}_i$ denotes the complex conjugate of $y_i$. Similar to the earlier case, the element $\alpha \in K \cap \mathbb{R}$ is chosen to be totally positive to make sure that the form is positive definite. Again, since $\alpha x_i \bar{x}_i \in \mathcal{O}_K$, whether $\mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{x}_i) \in \mathbb{Z}$ depends on the choice of $\alpha$, and $\alpha \in \mathcal{O}_K$ is a sufficient condition.

*Remark 1:* We note that instead of considering the lattice $\rho^{-1}(C)$ with $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i/p)$ (respectively $\sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i/p)$), we can alternatively consider the lattice $\rho^{-1}(C)/\sqrt{p}$ with $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i)$ (respectively $\sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i)$).

### C. Some Examples

Several particular cases of the above constructions have been considered in the literature.

*Example 1:* The following construction is discussed in Section 5.2 of [1]. Let $p$ be an odd prime, and let $\zeta_p$ be the primitive $p$th root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$ with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. The degree of $K$ over $\mathbb{Q}$ is $p-1$. Take the prime ideal $\mathfrak{p} = (1-\zeta_p)$ with the residue field $\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$, and the bilinear form $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i/p)$. Since $\mathbb{Q}(\zeta_p)$ is a CM-field, this bilinear form corresponds to (2) with $\alpha = 1/p$. Now, given a code $C$ over $\mathbb{F}_p$, if $C \subset C^\perp$ then $\rho^{-1}(C)$ is an even integral lattice of rank $N(p-1)$. In addition, if $C$ is self-dual, then $\Gamma_C$ is unimodular.

*Example 2:* When $p = 2$ in the above example, $\zeta_p = -1$, $\mathcal{O}_K = \mathbb{Z}$, and $\mathfrak{p} = 2\mathbb{Z}$, which yields the so-called Construction A (see Section 1.3 of [1]). To obtain lattices of rank $N$ from binary linear codes of length $N$, we consider

$$\Gamma_C = \frac{1}{\sqrt{2}} \rho^{-1}(C),$$

with $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}(x_i y_i)$ (see Remark 1). Given $x = (x_1, \ldots, x_N)/\sqrt{2}$, $y = (y_1, \ldots, y_N)/\sqrt{2} \in \Gamma_C$, $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}(x_i y_i/2) = \sum_{i=1}^{N} x_i y_i/2$ is the regular inner product of two vectors.

## III. The case of $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$

Let $p$ be an odd prime, and let $\zeta_p$ be a primitive $p$th root of unity. Let $K = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ be the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$, with ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p + \zeta_p^{-1}]$. The degree of $K$ over $\mathbb{Q}$ is $(p-1)/2$. The prime $p$ totally ramifies in $K$:

$$p\mathcal{O}_K = \mathfrak{p}^{(p-1)/2},$$

where $\mathfrak{p}$ is a prime principal ideal with generator $2 - \zeta_p - \zeta_p^{-1}$ and residue field

$$\mathcal{O}_K/\mathfrak{p} \simeq \mathbb{F}_p$$

where $\mathbb{F}_p$ denote the finite field with $p$ elements. Let $C \subset \mathbb{F}_p^n$ be a linear code over $\mathbb{F}_p$ of length $n$.

*Definition 3:* Let $\rho : \mathcal{O}_K^N \to \mathbb{F}_p^N$ be the mapping defined by the reduction modulo the principal ideal $\mathfrak{p} = (2 - \zeta_p - \zeta_p^{-1})$ on every coordinate. Then define

$$\Gamma_C := \rho^{-1}(C) \subset \mathcal{O}_K^N.$$

We know from the previous section that $\Gamma_C$ is an integral lattice of rank $N\frac{p-1}{2}$, with respect to the bilinear form $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i)$ for a totally positive element $\alpha \in \mathcal{O}_K$.

Let $C$ be a linear $(n, k)$ code over $\mathbb{F}_p$. We will show next that if $C \subset C^\perp$, then we can take $\alpha$ to be $1/p$.

*Lemma 1:* Let $C \subset \mathbb{F}_p^n$ be a $k$-dimensional code with $C \subset C^\perp$. Then $\Gamma_C$ is an odd integral lattice with respect to the bilinear form $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i/p)$.

*Proof:* Take $x, y \in \Gamma_c = \rho^{-1}(C)$. Then, by definition, $\rho(x), \rho(y) \in C$, and since $C \subset C^\perp$,

$$\rho(x) \cdot \rho(y) = \sum_{i=1}^{n} \rho(x_i)\rho(y_i) = 0,$$

implying that

$$x \cdot y = \sum_{i=1}^{n} x_i y_i \equiv 0 \pmod{\mathfrak{p}}.$$

Now, by the linearity property of the trace,

$$\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i/p) = \frac{1}{p}\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{N} x_i y_i\right).$$

It now suffices to show that $\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{N} x_i y_i\right) \in p\mathbb{Z}$. Since $K$ is a Galois extension, the Galois group acts transitively on the ideals above $p$. We know that $\sum_{i=1}^{n} x_i y_i \in \mathfrak{p}$ and $\mathfrak{p}$ is the only prime above $p$. Therefore, all the conjugates of $\sum_{i=1}^{n} x_i y_i$ lie in $\mathfrak{p}$, and so does its trace. This concludes the proof that $\Gamma_C$ is integral, since $\mathrm{Tr}_{K/\mathbb{Q}}\left(\sum_{i=1}^{N} x_i y_i\right) \in \mathfrak{p} \cap \mathbb{Z} = p\mathbb{Z}$.

We are left to show that $\Gamma_C$ is odd. For that, it is sufficient to find an $x \in \Gamma_C$ such that $\langle x, x \rangle$ is odd. Take $x = (2 - \zeta_p - \zeta_p^{-1}, 0, \ldots, 0)$. Then

$$\begin{aligned}\langle x, x \rangle &= \mathrm{Tr}_{K/\mathbb{Q}}((2 - \zeta_p - \zeta_p^{-1})^2/p) \\ &= \frac{1}{p}\mathrm{Tr}_{K/\mathbb{Q}}(6 - 4(\zeta_p + \zeta_p^{-1}) + (\zeta_p^2 + \zeta_p^{-2})) \\ &= \frac{1}{p}(3(p-1) + 3) = 3\end{aligned}$$

where the last equality follows from the transitivity of the trace, namely

$$\begin{aligned}\mathrm{Tr}_{K/\mathbb{Q}}(\zeta_p + \zeta_p^{-1}) &= \mathrm{Tr}_{K/\mathbb{Q}}(\mathrm{Tr}_{\mathbb{Q}(\zeta_p)/K}(\zeta_p)) \\ &= \mathrm{Tr}_{\mathbb{Q}(\zeta_p)/\mathbb{Q}}(\zeta_p) \\ &= -1.\end{aligned}$$

■

We note that the property of being integral for this particular trace form does not depend on the particular choice of the field, but rather on the fact that the prime $p$ considered has only one prime $\mathfrak{p}$ above (in other words, $g = 1$).

Let $\Gamma_C^*$ be the dual lattice of $\Gamma_C$, that is

$$\Gamma_C^* = \{x \in \mathbb{R}^n \mid x \cdot y \in \mathbb{Z} \text{ for all } y \in \Gamma\}.$$

*Lemma 2:* Let $C \subset \mathbb{F}_p^n$ be a $k$-dimensional code such that $C \subset C^\perp$. Then

$$\Gamma_C^* = \Gamma_{C^\perp}.$$

*Proof:* Let $x \in \Gamma_C$, $y \in \Gamma_{C^\perp}$. Then by definition of these lattices, $\rho(x) \in C$ and $\rho(y) \in C^\perp$, and it follows by definition of $C^\perp$ that $\rho(x) \cdot \rho(y) \equiv 0 \pmod{p}$. By redoing the argument in the proof of Lemma 1, we deduce that $\langle x, y \rangle \in \mathbb{Z}$, and thus $\Gamma_{C^\perp} \subset \Gamma_C^*$.

Now, since the dimension of $C$ is $k$, it follows that

$$\mathrm{vol}(\mathbb{R}^{N\frac{p-1}{2}}/\Gamma_C) = p^{\frac{N}{2}-k}$$

and

$$\mathrm{vol}(\mathbb{R}^{N\frac{p-1}{2}}/\Gamma_C^*) = p^{k-\frac{N}{2}}$$

On the other hand, the dimension of $C^\perp$ is $N - k$, and so

$$disc(\Gamma_{C^\perp}) = p^{N-2(N-k)} = p^{2k-N},$$

implying that

$$\mathrm{vol}(\mathbb{R}^{N\frac{p-1}{2}}/\Gamma_{C^\perp}) = p^{k-\frac{N}{2}}.$$

We may now conclude that $\Gamma_C^* = \Gamma_{C^\perp}$. ■

Combining the lemmas given in this section, we obtain the following proposition.

*Proposition 1:* Let $C \subset \mathbb{F}_p^N$ be a $k$-dimensional code such that $C \subset C^\perp$. Then the lattice $\Gamma_C$ given in Definition 3 together with the bilinear form $\langle x, y \rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i y_i)$ is an odd integral lattice of rank $N\frac{p-1}{2}$. In addition, if $C$ is self-dual, then $\Gamma_C$ is unimodular.

*Example 3:* Consider the self-dual code of length 2 over $\mathbb{F}_5$ given by a generator matrix

$$\begin{pmatrix} 1 & 2 \end{pmatrix}.$$

That is, $C = \{(0,0), (1,2), (2,4), (3,1), (4,3)\}$. Then, $\Gamma_C$ is an odd unimodular lattice of rank 4, and the only such lattice is $\mathbb{Z}^4$.

*Example 4:* Consider now the Cartesian product of the code $C$ given in the previous example by itself. That is, we consider the code $C_2$ over $\mathbb{F}_5$ given by a generator matrix

$$\begin{pmatrix} 1 & 2 & 0 & 0 \\ 0 & 0 & 1 & 2 \end{pmatrix}.$$

Then, $\Gamma_{C_2}$ is an odd unimodular lattice of rank 8, which is $\mathbb{Z}^8$.

For practical applications, having a generator matrix of lattices $\Gamma_C = \rho^{-1}(C)/\sqrt{p}$ is of interest. Recall that $\Gamma_C \subset \mathcal{O}_K^N$, thus a lattice point $x = (x_1, \ldots, x_N) \in \Gamma_C$ has its $N$ components living in $\mathcal{O}_K$. Since $\Gamma_C$ has rank $N(p-1)/2$ as a free $\mathbb{Z}$-module, we are interested in a $\mathbb{Z}$-basis of $\Gamma_C$. Let $\{\nu_1, \ldots, \nu_n\}$ be a $\mathbb{Z}$-basis of $\mathcal{O}_K$. Then a generator matrix $M$ for the lattice formed by $\mathcal{O}_K$ together by the trace form $\langle x, y \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$ is

$$\begin{pmatrix} \sigma_1(\nu_1) & \sigma_2(\nu_1) & \ldots & \sigma_n(\nu_1) \\ \vdots & & & \vdots \\ \sigma_1(\nu_n) & \sigma_2(\nu_n) & \ldots & \sigma_n(\nu_n) \end{pmatrix}$$

since $MM^T = \mathrm{Tr}_{K/\mathbb{Q}}(\nu_i \nu_j)$. A vector $x$ in this lattice is thus a linear combination of the rows of $M$: $x = (\sigma_1(\sum_{j=1}^{n} u_j \nu_j), \ldots, \sigma_n(\sum_{i=j}^{n} u_j \nu_j))$, and

$$\langle x, y \rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy)$$

as it should be (this is the bilinear form (1) when $N = 1$ and $\alpha = 1$). Now for $x = (x_1, \ldots, x_N) \in \mathcal{O}_K^N$, we have that $x_i = \sum_{j=1}^{n} u_{ij} \nu_j$ for $i = 1, \ldots, N$, and $x$ is embedded into $\mathbb{R}^{N(p-1)/2}$ as

$$x = (\sigma_1(x_1), \ldots, \sigma_n(x_1), \ldots, \sigma_1(x_N), \ldots, \sigma_n(x_N)). \quad (3)$$

Then

$$\langle x, y\rangle = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i).$$

*Example 5:* Consider again the code $C$ from Example 3. That is, $C$ is a code of length 2 over $\mathbb{F}_5$ given by a generator matrix

$$\begin{pmatrix} 1 & 2 \end{pmatrix}.$$

We will now compute a generator matrix for the lattice $\Gamma_C$ explicitly.

Let $\xi = \zeta_5 + \zeta_5^{-1}$ and $K = \mathbb{Q}(\xi)$. It is easy to see that the degree of extension $K/\mathbb{Q}$ is 2 and $\zeta_5^2 + \zeta_5^{-2} = -1 - \xi$.

We choose the basis $\{1, \xi\}$ for $\mathcal{O}_K$, and it follows that the generator matrix for the lattice $\mathcal{O}_K$ together with the trace form $\langle x, y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(xy/5)$, $x, y \in \mathcal{O}_K$, is

$$\begin{pmatrix} 1 & 1 \\ \xi & -1-\xi \end{pmatrix}.$$

Now, $\rho^{-1}(C)$ is a $\mathbb{Z}$-lattice in $\mathcal{O}_K^2$ of rank 4 generated by $(2-\xi, 0)$, $(0, 2-\xi)$, $(1, 2)$, and $(\xi, 2\xi)$ with the trace form $\langle x, y\rangle = \sum_{i=1}^{2} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i/5)$, $x_i, y_i \in \mathcal{O}_K^2$. It follows that the generator matrix for $\Gamma_C$ as a free $\mathbb{Z}$-module of rank 4 is

$$\begin{pmatrix} 2-\xi & 2-(-1-\xi) & 0 & 0 \\ 0 & 0 & 2-\xi & 2-(-1-\xi) \\ 1 & 1 & 2 & 2 \\ \xi & -1-\xi & 2\xi & 2(-1-\xi) \end{pmatrix}.$$

The theory presented in the previous section is general and might be applied to different fields. We chose to focus on $\mathbb{Q}(\zeta_p + \zeta_p^{-1})$ because it is a totally real field, which is known to allow the construction of a lattice isomorphic to $\mathbb{Z}^{(p-1)/2}$, which makes it suitable for coding applications to fading channels, as discussed next.

## IV. Applications to Wiretap Coding

A wiretap channel, as introduced by Wyner [9], is a broadcast channel where Alice, a legitimate sender, communicates to Bob in the presence of an eavesdropper Eve. The underlying assumption is that the channel between Alice and Bob is different from that between Alice and Eve. A wiretap code has the purpose of exploiting this difference in channels and providing reliability and confidentiality for the communication between Alice and Bob. When the channel is real (or complex), wiretap codes are designed from lattices [6].

### A. Wiretap Encoding for Lattices

The idea behind wiretap coding is that, instead of having a one-to-one correspondence between a vector of information and a lattice point, this vector of information is mapped to a set of codewords, after which the codeword to be actually transmitted is chosen randomly from this set.

Let $\mathbf{s} \in \mathbb{F}_q^k$ be the information vector. Consider two nested lattices $\Lambda_e \subset \Lambda_b \subset \mathbb{R}^N$. We partition the lattice $\Lambda_b$ into a union of disjoint cosets of the form $\Lambda_e + \mathbf{c}$, where $\mathbf{c}$ is an $N$-dimensional vector. We need $q^k$ cosets to be labeled by the information vector $\mathbf{s} \in \mathbb{F}_q^k$:

$$\Lambda_b = \bigcup_{j=1}^{q^k} (\Lambda_e + \mathbf{c}_j).$$

Once the mapping

$$\mathbf{s} \mapsto \Lambda_e + \mathbf{c}_{j(\mathbf{s})}$$

is done, Alice randomly chooses a point $\mathbf{x} \in \Lambda_e + \mathbf{c}_{j(\mathbf{s})}$ and sends it over the wiretap channel. This is equivalent to choosing a random vector $\mathbf{r} \in \Lambda_e$. Finally, the transmitted lattice point $\mathbf{x} \in \Lambda_b$ is of the form

$$\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c}. \tag{4}$$

Construction A from Example 2 can be used for wiretap lattice encoder as follows. Let $C$ be an $(N, k)$ linear binary code. If $\Lambda_b = \rho^{-1}(C)/\sqrt{2}$ and $\Lambda_e = (2\mathbb{Z})^N/\sqrt{2}$, we can partition $\Lambda_b$ as

$$\Lambda_b = \frac{1}{\sqrt{2}}\left((2\mathbb{Z})^N + C\right) = \frac{1}{\sqrt{2}} \bigcup_{\mathbf{c}_i \in C} ((2\mathbb{Z})^N + \mathbf{c}_i).$$

*Example 6:* Consider the 2-dimensional repetition code $C = \{(0,0), (1,1)\}$. Then

$$\rho^{-1}(C) = (2\mathbb{Z})^2 + C = ((2\mathbb{Z}^2) + (0,0)) \cup ((2\mathbb{Z})^2 + (1,1)).$$

Since $C = C^{\perp}$, the lattice

$$\frac{\rho^{-1}(C)}{\sqrt{2}}$$

is a 2-dimensional unimodular lattice, thus equivalent to $\mathbb{Z}^2$. In a wiretap encoder, Alice has $k = 1$ secret bit that she uses to choose either the coset $(2\mathbb{Z}^2) + (0,0)$ or $(2\mathbb{Z}^2) + (1,1)$. Then, depending on how many bits of randomness she is using, she will pick one point at random within the chosen coset.

### B. Wiretap Codes for Block Fading Channels

We now focus on the case where the wiretap channel is a block fading channel, namely, Alice wants to send data to Bob on a wiretap block fading channel where an eavesdropper Eve is trying to intercept the data through another block fading channel. Perfect Channel State Information (CSI) is assumed at both receivers. With the aid of an in-phase/quadrature component interleaver, it is possible to remove the phase of the complex fading coefficients to obtain a real fading which is Rayleigh distributed and guarantee that the fading coefficients are independent from one real symbol to the next [8, sec 2.1]. Let $L$ be the coherence time of the block fading. This is modeled by

$$\begin{array}{rcl} Y & = & \mathsf{diag}(\mathbf{h}_b)X + V_b, \text{ and} \\ Z & = & \mathsf{diag}(\mathbf{h}_e)X + V_e \end{array} \tag{5}$$

where the transmitted signal $X$ is an $n \times L$ matrix, and the $n \times L$ matrices $V_b$ and $V_e$ are the Gaussian noise at Bob and Eve respectively. By channel assumption, $V_b$ and $V_e$ have zero

mean and variance $\sigma_b^2$ and $\sigma_e^2$ respectively. The fading matrices can be given explicitly by

$$\mathsf{diag}(\mathbf{h}_b) = \mathsf{diag}(|h_{b,1}|, \ldots, |h_{b,n}|) \text{ and}$$
$$\mathsf{diag}(\mathbf{h}_e) = \mathsf{diag}(|h_{e,1}|, \ldots, |h_{e,n}|)$$

where the fading coefficients $h_{b,i}, h_{e,i}$ are complex Gaussian random variables with variance $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$, so that $|h_{b,i}|, |h_{e,i}|$ are Rayleigh distributed with parameter $\sigma_{h,b}^2$, resp. $\sigma_{h,e}^2$, for all $i = 1, \ldots, n$.

One may vectorize the received channel model (5) and obtain an $Ln-$dimensional lattice structure from the transmitted signal. That is,

$$\begin{aligned}
\mathsf{vec}\,(Y) &= \mathsf{vec}\,(\mathsf{diag}\,(\mathbf{h}_b)\,X) + \mathsf{vec}\,(V_b) \\
&= \begin{pmatrix} \mathsf{diag}(\mathbf{h}_b) & & \\ & \ddots & \\ & & \mathsf{diag}(\mathbf{h}_b) \end{pmatrix} \mathsf{vec}(X) + \mathsf{vec}(V_b), \\
\mathsf{vec}\,(Z) &= \mathsf{vec}\,(\mathsf{diag}\,(\mathbf{h}_e)\,X) + \mathsf{vec}\,(V_e) \\
&= \begin{pmatrix} \mathsf{diag}(\mathbf{h}_e) & & \\ & \ddots & \\ & & \mathsf{diag}(\mathbf{h}_e) \end{pmatrix} \mathsf{vec}(X) + \mathsf{vec}(V_e).
\end{aligned}$$

We now interpret the $n \times L$ codeword $X$ as coming from a lattice by writing

$$\mathsf{vec}(X) = M\mathbf{u}$$

where $\mathbf{u} \in \mathbb{Z}^{Ln}$ and $M$ denotes the $Ln \times Ln$ generator matrix of the lattice $\Lambda_b$. This representation allows us to consider the transmitted signals as real lattice points, and wiretap coding simplifies to coset encoding, which is discussed in Subsection IV-A.

It was shown in [7] that the code design criterion to increase Eve's confusion is to choose $\Lambda_e \subset \Lambda_b$ such that

$$\sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^{n} \frac{1}{\|\mathbf{x}_i\|^{L+2}} \tag{6}$$

is minimized, where $\mathbf{x}_i$ is the $i$th row of some $n \times L$ matrix $X'$ such that $\mathbf{x} = \mathsf{vec}(X')$ is a point in $\Lambda_e$. We note here a few remarks concerning this infinite sum. First, depending on the lattice $\Lambda_e$, the sum might not converge, in which case we consider instead a finite number of points in $\Lambda_e$. Also, it is assumed that $||\mathbf{x}_i|| \neq 0$ for all $\mathbf{x} \in \Lambda_e$ and $i = 1 \ldots n$. We will now discuss how this can be done using number fields.

Let $K$ be a totally real number field of degree $n$ with $n$ embeddings $\sigma_1, \sigma_2, \ldots, \sigma_n$ of $K$ into $\mathbb{C}$ and ring of integers $\mathcal{O}_K$. The first row of $X'$ is denoted $\mathbf{x}_1$. Let $\mathbf{x}_i = \sigma_i(\mathbf{x}_1)$ so that each row of $X'$ can be obtained by conjugating $\mathbf{x}_1$:

$$X' = \begin{pmatrix} \mathbf{x}_1 \\ \vdots \\ \mathbf{x}_n \end{pmatrix} = \begin{pmatrix} x_1 & \ldots & x_L \\ \sigma_2(x_1) & \ldots & \sigma_2(x_L) \\ \vdots & & \vdots \\ \sigma_n(x_1) & \ldots & \sigma_n(x_L) \end{pmatrix}. \tag{7}$$

Alternatively, the $j$th column of $X'$, $j = 1, \ldots, L$, can be seen as a lattice point

$$(\sigma_1(x_j), \ldots, \sigma_n(x_j)) \tag{8}$$

in the lattice $\mathcal{O}_K$ with the bilinear form given in (1). In this case, since $K$ is chosen to be totally real, $||\mathbf{x}_i|| \neq 0$ for all $i$ [8]. In fact, for every non-zero coefficient of the first row $\mathbf{x}_1$, all the corresponding columns will also have non-zero coefficients. Conversely, each zero coefficient on the first row gives a column of zeros, and to have $||\mathbf{x}_i|| = 0$ for some $i$ means that $||\mathbf{x}_i|| = 0$ for all $i$, and so $X'$ can only contain zeros. Furthermore, it was shown in [7] that (6) then becomes

$$\sum_{\mathbf{x} \in \Lambda_e} \prod_{i=1}^{n} \frac{1}{\|\sigma_i(\mathbf{x}_1)\|^{L+2}} = \sum_{\mathbf{x} \in \Lambda_e} \frac{1}{N_{K/\mathbb{Q}}\left(\|\mathbf{x}_1\|^2\right)^{\frac{L}{2}+1}}.$$

### C. Wiretap Encoding of Algebraic Lattices

We have seen in the previous subsection that lattice codes from totally real number fields have desirable properties for block fading wiretap channels. Furthermore, (7) and (8) suggest that it is advantageous if the lattice $\Lambda_e$ is chosen so that an element $x \in \Lambda_e$ is of the form (3). Now, let $\Lambda_b = \rho^{-1}(C)/\sqrt{p}$ and $\Lambda_e = \mathfrak{p}^L/\sqrt{p}$. This choice of lattices allows us to carry out wiretap encoding using the fact that

$$\frac{\rho^{-1}(C)}{\sqrt{p}} = \frac{1}{\sqrt{p}}\left(\mathfrak{p}^L + C\right) = \frac{1}{\sqrt{p}} \bigcup_{c_i \in C} \left(\mathfrak{p}^L + c_i\right).$$

## V. Conclusion

We proposed a construction of lattices over number fields using linear codes over finite fields, mimicking Construction A from binary codes. We studied into details the maximal totally real subfield of the cyclotomic field $\mathbb{Q}(\zeta_p)$. Applications to coset encoding for block fading wiretap channels were presented. Future work involves determining parameters of the resulting lattices and studying wiretap channel coding applications, including code design and simulations.


## Acknowledgment

The research of W. Kositwattanarerk, S.S. Ong and F. Oggier is supported by the Singapore National Research Foundation under Research Grant NRF-RF2009-07.


## References


[1] W. Ebeling, "Lattices and Codes: A Course Partially Based on Lectures by F. Hirzebruch", originally published by *Vieweg*, reedited by *Springer*.

[2] E. Bayer-Fluckiger, "Lattices and Number Fields", *Contemporary Mathematics*, 241:69–84, 1999.

[3] J. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", *Springer*.

[4] E. Bannai, S. T. Dougherty, M. Harada, and M. Oura, "Type II Codes, Even Unimodular Lattices, and Invariant Rings", IEEE Trans. Inform. Theory **45** (1999), no. 4, 1194–1205.

[5] J. Harshan, E. Viterbo, J.-C. Belfiore, "Practical Encoders and Decoders for Euclidean Codes from Barnes-Wall Lattices", preprint, http://arxiv.org/abs/1203.3282.

[6] F. Oggier, P. Solé, J.-C. Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis", preprint, http://arxiv.org/abs/1103.4086.

[7] J.-C. Belfiore, F. Oggier, "Lattice Code Design for the Rayleigh Fading Wiretap Channel," *International Conference on Communications (ICC 2011)*.

[8] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," in *Foundations and Trends in Communications and Information Theory*, 2004, vol. 1, no. 3, pp. 333–415.

[9] A. Wyner, "The wire-tap channel," *Bell. Syst. Tech. Journal*, vol. 54, October 1975.