2018 15th International ISC (Iranian Society of Cryptology) Conference on Information Security and Cryptology (ISCISC)
August 28-29, 2018; Shahid Rajaee Teacher Training University - Tehran, Iran

Modular Construction A Lattices from Cyclotomic Fields and their Applications in Information Security

Hassan Khodaiemehr
Department of Mathematics,
K. N. Toosi University of Technology,
16315-1618, Tehran, Iran
Email: ha.khodaiemehr@kntu.ac.ir
School of Mathematics,
Institute for Research in Fundamental Sciences (IPM),
19395-5746, Tehran, Iran
Email: khodaiemehr@ipm.ir

Daniel Panario
School of Mathematics and Statistics,
Carleton University,
Canada, Ottawa
Email: daniel@math.carleton.ca

Mohammad-Reza Sadeghi
Faculty of Mathematics
and Computer Science,
Amirkabir University of Technology,
Tehran, Iran
Email: msadeghi@aut.ac.ir

***Abstract*—We present an overview of recent advances in the area of information security using algebraic number fields. This overview indicates the importance of modular lattices in information security and in recently proposed methods for obtaining modular lattices using algebraic number fields. Obtaining Construction A unimodular lattices using cyclotomic number fields of prime orders have been addressed in the literature. Recently, a new lattice invariant called secrecy gain has been defined and it has been shown that it characterizes the confusion at the eavesdropper when using lattices in the Gaussian wiretap channels. There is a symmetry point, called weak secrecy gain, in the secrecy function of modular lattices. It is conjectured that the weak secrecy gain is the secrecy gain. It is known that d-modular lattices with high level d are more likely to have a large length for the shortest nonzero vector, which results in a higher weak secrecy gain. In search of such lattices, we prove that there is no modular lattices built using Construction A over cyclotomic fields of prime power order p^n, with $n > 1$. We also present a new framework based on Construction A lattices and cyclotomic number fields that gives a family of p-modular lattices with $p \equiv 1 \pmod 4$.**

***Index Terms*—Secrecy gain, modular lattices, cyclotomic fields.**

I. Introduction

In recent years, algebraic techniques have been applied to resolve security issues arising in communication networks including confidentiality, integrity and authentication. Conventional techniques for achieving confidentiality in communication networks are based on cryptographic encryption [1]. Encryption includes two principal types of algorithms: secret-key encryption algorithms and public-key encryption algorithms. As compared to public-key algorithms, secret-key algorithms are computationally efficient, and result in higher data throughput, while presenting challenges for key management, such as secure key storage and distribution [1], [2]. Public-key algorithms are simple in terms of key management, but require considerable computational resources [1], [3]. Hence, hybrid cryptosystems [4] are employed in practice in which a secret key is distributed by public-key algorithms, and encryption and decryption use secret-key algorithms. However, besides high computational cost, public-key algorithms are not provably perfectly secure and are vulnerable to the so-called man-in-the-middle attack [3]. Moreover, using public-key algorithms to distribute secret keys adds another layer of complexity in the design of networks.

In addition to these general considerations, providing secure communication over wireless networks using cryptographic approaches presents further significant challenges due to the following issues. First, the open nature of the wireless medium allows eavesdroppers and attackers to intercept information transmission or to degrade transmission quality. Second, the lack of infrastructure in decentralized networks makes key distribution difficult. Finally, the dynamic topology of mobile networks makes key management expensive. The information theoretic approach to achieve secure communication opens a promising new direction towards solving wireless networking security problems. Such an approach was initiated by Wyner [5] and by Csiszár and Körner [6].

In his seminal work, Wyner introduced the wiretap channel [5], a discrete memoryless channel where the sender Alice transmits confidential messages to a legitimate receiver Bob, in the presence of an eavesdropper Eve, who has only partial access to what Bob sees. Indeed, Eve's access is modeled as a separate channel with quality lower than the quality of the channel between Alice and Bob. Both reliable and confidential communication between Alice and Bob is shown to be achievable at the same time, by exploiting the physical difference between the channel to Bob and that to Eve, without the use of cryptographic means. Since then, many results of information theoretical nature have been found for various classes of wiretap channels ranging from Gaussian point-to-point channels to relay networks. These results capture the trade-off between reliability and secrecy while aim to determine the highest information rate that can be achieved with weak and also strong secrecy, the so-called secrecy capacity [1], [7].

In this paper, we consider the application of algebraic number theory in code design of Gaussian wiretap channels. The secrecy capacity of these channels was established in [8]. Examples of existing Gaussian wiretap codes were designed for binary inputs in [9]. A different approach was adopted in [10], where lattice codes were proposed using

The research of the first author was supported by a grant from IPM (1396-97). The second author is partially funded by NSERC of Canada.

as design criterion a new lattice invariant called secrecy gain defined as the maximum of its secrecy function. It was shown that secrecy gain characterizes the confusion at the eavesdropper. A recent study [11] generalized the result concerning semantic security of [12] to continuous channels. They also propose another new lattice design criterion called the flatness factor. They showed that a vanishing flatness factor (or equivalently an infinitely large secrecy gain) implies semantic security. This suggests the study of the secrecy gain of lattices as a way to understand how to design good Gaussian lattice wiretap codes.

Belfiore and Solé [13] discovered a symmetry point, called weak secrecy gain, in the secrecy function of unimodular lattices (generalized to all d-modular lattices in [14]). They conjectured that the weak secrecy gain is actually the secrecy gain. Ernvall-Hytönen [15] developed a method to prove or disprove the conjecture for unimodular lattices. Secrecy gains of a special class of unimodular lattices called extremal unimodular lattices and all unimodular lattices in dimensions up to 23 have been computed [14], [16]. The asymptotic behavior of the average weak secrecy gain as a function of the dimension n was investigated and an achievable lower bound on the secrecy gain of even unimodular lattices was given [14]. Numerical upper bounds on the secrecy gains of unimodular lattices in general, and unimodular lattices constructed from self-dual binary codes in particular, were given and compared to the achievable lower bound [17]. A set of infinitely many unimodular lattices satisfying the conjecture is illustrated in [18]. The proof of [15] is shortened in [19] and the conjecture is verified for more unimodular lattices. The authors of [20] discovered a 4-modular lattice that fails to satisfy the conjecture. The weak secrecy gain of 2- and 3-modular lattices is studied in [21] and [7]; it is shown that most of the known even 2- and 3-modular lattices in dimensions up to 24 have secrecy gains bigger than the best unimodular lattices.

A special family of lattices is the ones constructed from linear codes; this method of constructing lattices is usually referred to as Construction A [22]. Recent applications of Construction A lattices in communication and cryptography can be found in [23]–[27]. The original binary Construction A, due to Forney [28], can be seen as a particular case of the cyclotomic field approach proposed by Ebeling [29]. The generalization from cyclotomic fields to either complex multiplication fields (CM fields) or totally real number fields was suggested in [30]. The main interest in constructing lattices from linear codes is to take advantage of the code properties to obtain lattices with nice properties; modularity and large shortest vector (or minimal norm) are two of them. Construction and secrecy gain analysis of d-modular lattices from totally real and totally imaginary quadratic extensions, for $d = 1, 3, 5, 6, 7, 11, 14, 15, 23$, have been considered [31].

The main conclusion about the connection between the weak secrecy gain of the lattice and other lattice parameters has been reported in [31] after studying many examples. This conclusion is summarized as follows [31, Remark 4.12]:

1) When the dimension increases, the weak secrecy gain tends to increase, which has been proven for unimodular lattices [16].
2) Fixing dimension and level d, a large length for the shortest nonzero vector is more likely to induce a large weak secrecy gain.
3) Fixing dimension, level d and the length of the shortest nonzero vector, a smaller kissing number gives a larger weak secrecy gain. It was shown for unimodular lattices [16] that when the dimension n is fixed, $n \leq 23$, the secrecy gain is totally determined by the kissing number, and the lattice with the best secrecy gain is the one with the smallest kissing number.
4) Fixing dimension, the length of the shortest nonzero vector, kissing number, a smaller level d gives a bigger weak secrecy gain. However, the lattices with high level d are more likely to have a large length for the shortest nonzero vector.

The rest of this paper is organized as follows. In Section II, we provide preliminaries about lattices and algebraic number theory. Section III provides some results about cyclotomic number fields. In Section IV, we introduce Construction A lattices obtained from number fields. Section V provides our main results about the existence of modular lattices in the family of Construction A lattices obtained from cyclotomic number fields. Section VI, provides a new framework based on Construction A and cyclotomic number fields that gives a family of p-modular lattices. Section VII contains the concluding remarks.

II. Preliminaries

A. Algebraic Number Theory

Let K and L be two fields. If $K \subset L$, then L is a field extension of K denoted by L/K. The dimension of L as vector space over K is the degree of L over K, denoted by $[L : K]$. Any finite extension of $\mathbb{Q}$ is a number field. An element $\alpha \in K$ is an algebraic integer if it is a root of a monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers of K is the ring of integers of K, denoted by $\mathcal{O}_K$. If K is a number field, then $K = \mathbb{Q}(\theta)$ for an algebraic integer $\theta \in \mathcal{O}_K$ [32]. For a number field K of degree n, the ring of integers $\mathcal{O}_K$ forms a free $\mathbb{Z}$-module of rank n. Every basis $\{\omega_1, \ldots, \omega_n\}$ of the $\mathbb{Z}$-module $\mathcal{O}_K$ is an integral basis of K.

An automorphism of L/K fixes K. In other words, an automorphism of L/K is an isomorphism τ from L to L such that $\tau(x) = x$ for each x in K. The set of all automorphisms of L/K forms a group with the operation of function composition. This group is sometimes denoted by $\mathrm{Aut}(L/K)$. If L/K is a Galois extension, then $\mathrm{Aut}(L/K))$ is the Galois group of (the extension) L over K, and is usually denoted by $\mathrm{Gal}(L/K)$.

Let $K = \mathbb{Q}(\theta)$ be a number field of degree n over $\mathbb{Q}$. There are exactly n embeddings $\sigma_1, \ldots, \sigma_n$ of K into $\mathbb{C}$ defined by $\sigma_i(\theta) = \theta_i$, for $i = 1, \ldots, n$, where the θ_i's are the distinct zeros in $\mathbb{C}$ of the minimal polynomial of θ over $\mathbb{Q}$ [32]. Let r_1 be the number of embeddings with image in $\mathbb{R}$ and $2r_2$ the number of embeddings with image in $\mathbb{C}$ so that $r_1 + 2r_2 = n$. The pair (r_1, r_2) is the signature of K. If $r_2 = 0$ we have a totally real algebraic number field. In this paper we focus on the case when K is totally real.

For a number field K of degree n and $x \in K$, the elements $\sigma_1(x), \ldots, \sigma_n(x)$ are the conjugates of x. The norm and the trace of x are

$$N_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x), \quad \mathrm{Tr}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x). \quad (1)$$

Let $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of K. The discriminant of K is defined as $d_K = \det(A)^2$, where A is the matrix $A_{i,j} = \sigma_j(\omega_i)$, for $i, j = 1, \ldots, n$. The discriminant of a number field belongs to $\mathbb{Z}$ and it is independent of the choice of a basis.

Definition 1: Let us order the σ_i's so that, for all $x \in K$, $\sigma_i(x) \in \mathbb{R}$, $1 \leq i \leq r_1$, and $\sigma_{j+r_2}(x)$ is the complex conjugate of $\sigma_j(x)$ for $r_1 + 1 \leq j \leq r_1 + r_2$. The canonical embedding (Minkowski embedding) $\sigma : K \to \mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ is the homomorphism defined by

$$\sigma(x) = (\sigma_1(x), \ldots, \sigma_{r_1}(x), \sigma_{r_1+1}(x), \ldots, \sigma_{r_1+r_2}(x)). \quad (2)$$

If we identify $\mathbb{R}^{r_1} \times \mathbb{C}^{r_2}$ with $\mathbb{R}^n$, the canonical embedding can be rewritten as $\sigma : K \to \mathbb{R}^n$

$$\begin{aligned} \sigma(x) \quad = \quad & (\sigma_1(x), \ldots, \sigma_{r_1}(x), \Re\sigma_{r_1+1}(x), \Im\sigma_{r_1+1}(x), \\ & \ldots, \Re\sigma_{r_1+r_2}(x), \Im\sigma_{r_1+r_2}(x)), \end{aligned} \quad (3)$$

where $\Re\sigma_j$ denotes the real part of σ_j and $\Im\sigma_j$ the imaginary part of σ_j, for $j = r_1 + 1, \ldots, r_1 + r_2$.

Let A be a Dedekind ring (for example the ring of algebraic integers in a number field), K its quotient field, L a finite separable extension of K, and B the integral closure of A in L [33]. If $\mathfrak{p}$ is a prime ideal of A, then $\mathfrak{p}B$ is an ideal of B with factorization $\mathfrak{p}B = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$, into primes of B, where $e_i \geq 1$. Each e_i is the ramification index of $\mathfrak{P}_i$ over $\mathfrak{p}$; it is also written as $e(\mathfrak{P}_i/\mathfrak{p})$. If $\mathfrak{P}$ lies above $\mathfrak{p}$ in B, we denote by $f(\mathfrak{P}/\mathfrak{p})$ the degree of the residue class field extension $B/\mathfrak{P}$ over $A/\mathfrak{p}$; this is the residue class degree or inertia degree.

Theorem 1: [33, p. 24] Let A be a Dedekind ring, K its quotient field, L a finite separable extension of K, and B the integral closure of A in L. Let $\mathfrak{p}$ be a prime of A. Then

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e(\mathfrak{P}/\mathfrak{p}) f(\mathfrak{P}/\mathfrak{p}). \quad (4)$$

When L/K is a Galois extension of degree n, this simplifies to $n = efg$, where g is the number primes of B above $\mathfrak{p}$. In other words, $e(\mathfrak{P}/\mathfrak{p}) = e$ and $f(\mathfrak{P}/\mathfrak{p}) = f$ for all $\mathfrak{P}|\mathfrak{p}$. If $[L : K] = e(\mathfrak{P}/\mathfrak{p})$, $\mathfrak{P}$ is totally ramified above $\mathfrak{p}$. In that case, the residue class degree is equal to 1. Since $\mathfrak{P}$ is the only prime of B lying above $\mathfrak{p}$, L is totally ramified over K.

B. Lattices

A discrete, additive, subgroup Λ of the m-dimensional real space $\mathbb{R}^m$ is a lattice [34]. Every lattice Λ has a basis $\mathcal{B} = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{R}^m$ where every $\mathbf{x} \in \Lambda$ can be represented as an integer linear combination of vectors in $\mathcal{B}$. The matrix $\mathbf{M}$ with $\mathbf{b}_1, \ldots, \mathbf{b}_n$ as its rows is a generator matrix for the lattice. The matrix $\mathbf{G} = \mathbf{M}\mathbf{M}^t$ is called a Gram matrix for the lattice. A lattice Λ in $\mathbb{R}^m$ is an integral lattice if its Gram matrix has coefficients in $\mathbb{Z}$. The determinant of the lattice $\det(\Lambda)$ is defined to be the determinant of the matrix $\mathbf{G}$ and the volume of the lattice is defined as $\mathrm{vol}(\Lambda) = \sqrt{\det(\mathbf{G})}$.

Now we present definitions in algebraic lattice theory equivalent to the above definitions.

Definition 2: An integral lattice Γ is a free $\mathbb{Z}$-module of finite rank together with a positive definite symmetric bilinear form $\langle , \rangle : \Gamma \times \Gamma \to \mathbb{Z}$.

Definition 3: The discriminant of a lattice Γ, denoted $\mathrm{disc}(\Gamma)$, is the determinant of $\mathbf{M}\mathbf{M}^t$ where $\mathbf{M}$ is a generator matrix for Γ. The volume $\mathrm{vol}(\mathbb{R}^n/\Gamma)$ of a lattice Γ is defined as $|\det(\mathbf{M})|$. The discriminant is related to the volume of a lattice by

$$\mathrm{vol}(\mathbb{R}^n/\Gamma) = \sqrt{\mathrm{disc}(\Gamma)}. \quad (5)$$

Theorem 2: [32, p. 155] Let K be a number field and $\{\omega_1, \ldots, \omega_n\}$ be an integral basis of O_K. The n vectors $\mathbf{v}_i = \sigma(\omega_i) \in \mathbb{R}^n$, $i = 1, \ldots, n$ are linearly independent, so they define a full rank lattice $\Lambda = \Lambda(\mathcal{O}_K) = \sigma(\mathcal{O}_K)$.

Theorem 3: [35] Let d_K be the discriminant of a number field K. The volume of the fundamental parallelotope of $\Lambda(\mathcal{O}_K)$ is given by

$$\mathrm{vol}(\Lambda(\mathcal{O}_K)) = 2^{-r_2}\sqrt{|d_K|}. \quad (6)$$

III. Cyclotomic Fields

Definition 4: Let K be a number field of degree n and $\mathcal{O}_K$ its ring of integers. Then, considering $\mathcal{O}_K$ as a $\mathbb{Z}$-module, if it has a basis of the form $\left\{1, \alpha, \ldots, \alpha^{n-1}\right\}$ for some $\alpha \in \mathcal{O}_K$, α is a power generator, this basis is a power basis and K is monogenic.

The most important cases among monogenic number fields are cyclotomic number fields. For any field K, an extension of the form $K(\zeta)$, where ζ is a root of unity, is a cyclotomic extension of K. When there are n different n^{th} roots of unity, we denote their group by μ_n. An n^{th} root of unity that has order n is a primitive n^{th} root of unity, denoted by ζ_n.

Lemma 1: [36, Lemma 2.1] For $\sigma \in \mathrm{Gal}(K(\zeta_n)/K)$ there is an integer a_σ that is relatively prime to n such that $\sigma(\omega) = \omega^{a_\sigma}$ for all $\omega \in \mu_n$.

Based on Lemma 1, for any field K, the mapping $\tau : \mathrm{Gal}(K(\zeta_n)/K) \to (\mathbb{Z}/n\mathbb{Z})^\times = \{1 \leq m \leq n | (m, n) = 1\}$, that sends σ to a_σ, is an injective group homomorphism. When $K = \mathbb{Q}$, this embedding is an isomorphism. For $n > 2$, $K = \mathbb{Q}(\zeta_n)$ is totally imaginary and by using the previous result, we can determine $\phi(n)/2$ pairs of embeddings from K into $\mathbb{C}$, where $\phi(\cdot)$ is Euler's ϕ-function. It should be noted that $(\mathbb{Z}/n\mathbb{Z})^\times$ is Abelian but not necessarily cyclic. For example, $(\mathbb{Z}/8\mathbb{Z})^\times$ is not cyclic. It is proved in [37, Theorem 2.6] that $\mathbb{Z}[\zeta_n]$ is the ring of algebraic integers of $\mathbb{Q}(\zeta_n)$, i.e., $\mathbb{Q}(\zeta_n)$ is a monogenic number field. Using the following theorem, we can compute the discriminant of $\mathbb{Q}(\zeta_n)$.

Theorem 2: [37, Proposition 2.7] Let $K = \mathbb{Q}(\zeta_n)$, then

$$d_K = (-1)^{\phi(n)/2} \frac{n^{\phi(n)}}{\prod_{p|n} p^{\phi(n)/(p-1)}}. \quad (7)$$

When $n = p^k$, for p a prime number, the discriminant of $K = \mathbb{Q}(\zeta_{p^k})$ is

$$d_K = \pm p^{p^{k-1}(pk-k-1)}, \quad (8)$$

where we have a negative sign if $p^k = 4$ or if $p \equiv 3 \pmod 4$ and we have a positive sign otherwise [37, Proposition 2.1]. The expression of the discriminant of the cyclotomic number

field $\mathbb{Q}(\zeta_{2^r})$, where $r > 2$, is given by $d_{\mathbb{Q}(\zeta_{2^r})} = 2^{2^{r-1}(r-1)}$ and for $r = 2$, the discriminant is equal to -4 [38].

There are differences between the prime-power case and the case of general n. For example, if n has at least two distinct prime factors. Then $1-\zeta_n$ is a unit of $\mathbb{Z}[\zeta_n]$ and $(1-\zeta_n)^{-1} = \prod_{\substack{1<j<n \\ (j,n)=1}} (1-\zeta_n^j)$ [37, Proposition 2.8]. If n is prime, $1-\zeta_n$ is not unit and $\mathfrak{P} = (1-\zeta_n)$ is a prime ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_n]$; in this case, n is totally ramified in $\mathbb{Q}(\zeta_n)$, because $nO_K = \mathfrak{P}^{n-1}$ [37, Lemma 1.4].

In addition to cyclotomic fields, we discuss subfields of $\mathbb{Q}(\zeta_n)$. The most important subfield for our purposes is the maximal real subfield $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ denoted $\mathbb{Q}(\zeta_n)^+$. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}(\zeta_n)^+$ is of degree 2, because ζ_n is a root of $X^2 - (\zeta_n + \zeta_n^{-1}) + 1$. Thus, $\mathbb{Q}(\zeta_n)$ is a CM field, that is, a totally imaginary quadratic extension of a totally real number field. Due to the following theorem, $\mathbb{Q}(\zeta_n)^+$ is also monogenic.

Theorem 3: [37, Proposition 2.16] $\mathbb{Z}[\zeta_n + \zeta_n^{-1}]$ is the ring of integers of $\mathbb{Q}(\zeta_n)^+$.

If $n = p^r$, the degree of $K = \mathbb{Q}(\zeta_{p^r})$ over $\mathbb{Q}$ is $p^{r-1}(p-1)$ and the prime p totally ramifies in K as $pO_K = \mathfrak{P}^{p^{r-1}(p-1)}$, where $\mathfrak{P}$ is a prime principal ideal with generator $1-\zeta_{p^r}$ and residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_p$. The degree of $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$ over $\mathbb{Q}$ is $\frac{p^{r-1}(p-1)}{2}$. It can be proved that the prime p also totally ramifies in K^+ as $pO_{K^+} = \mathfrak{p}^{\frac{p^{r-1}(p-1)}{2}}$, with $\mathfrak{p} = \mathfrak{P} \cap \mathcal{O}_{K^+} = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1})\mathcal{O}_{K^+}$ [30]. By using the Hasse Theorem that states the conductor-discriminant relation, a formula has been obtained to compute the discriminant of any subfield of $\mathbb{Q}(\zeta_{p^r})$ where p is an odd prime and r is a positive integer [39]. Let p be an odd prime number, r a positive integer, and $L = \mathbb{Q}(\zeta_{p^r})$. Since L is a Galois extension of $\mathbb{Q}$ and its Galois group is a cyclic group isomorphic to $(\mathbb{Z}/p^r\mathbb{Z})^\times$, there is a one-to-one correspondence between the subfields of L and the divisors of $[L:\mathbb{Q}] = (p-1)p^{r-1}$. The discriminant of any subfield K of L can be obtained as a function of p and its degree only. Since the degree of K is a divisor of $(p-1)p^{r-1}$, we write $[K:\mathbb{Q}] = up^j$, where u is a divisor of $p-1$ and $j \leq r-1$.

Theorem 4: [39, Theorem 4.1] Let K be a subfield of $\mathbb{Q}(\zeta_{p^r})$ with $[K:\mathbb{Q}] = up^j$, where $p \nmid u$. Then, $d_K = p^{u\left[(j+2)p^j - \frac{p^{j+1}-1}{p-1}\right]-1}$.

IV. Construction of Lattices from Codes

There exist many ways to construct lattices based on codes [22]. Here we mention a lattice construction from totally real and complex multiplication (CM) fields [30], which naturally generalizes Construction A of lattices from p-ary codes obtained from the cyclotomic field $\mathbb{Q}(\zeta_p)$ [29], p a prime. Let K be a Galois number field of degree n which is either totally real or a CM field. Let $\mathcal{O}_K$ be the ring of integers of K and $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_K$ above the prime p. We have $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_{p^f}$, where f is the inertia degree of p. Define ρ to be the map of reduction modulo $\mathfrak{p}$ componentwise as follows

$$\begin{array}{rcl} \rho : \mathcal{O}_K^N & \to & \mathbb{F}_{p^f}^N, \\ (x_1, \ldots, x_N) & \mapsto & (x_1 \bmod \mathfrak{p}, \ldots, x_N \bmod \mathfrak{p}) \end{array} \tag{9}$$

for some positive integer N. Let $\mathcal{C} \subset \mathbb{F}_{p^f}^N$ be a linear code over $\mathbb{F}_{p^f}$, that is a k-dimensional subspace of $\mathbb{F}_{p^f}^N$. As ρ is a $\mathbb{Z}$-module homomorphism, $\rho^{-1}(\mathcal{C})$ is a submodule of $\mathcal{O}_K^N$. Since $\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank n, $\rho^{-1}(\mathcal{C})$ is a free $\mathbb{Z}$-module of rank nN. Let $b_\alpha : \mathcal{O}_K^N \times \mathcal{O}_K^N \to \mathbb{R}$ be the symmetric bilinear form defined by

$$b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \overline{y}_i), \tag{10}$$

where $\alpha \in K \cap \mathbb{R}$, $\mathrm{Tr}_{K/\mathbb{Q}}$ is the trace function in (1), $\overline{y}_i$ denotes the complex conjugate of y_i if K is a CM field, and $\overline{y}_i = y_i$ if K is totally real. If α is furthermore totally positive, i.e., $\sigma_i(\alpha) > 0$, for σ_1 (the identity), $\sigma_2, \ldots, \sigma_n$ all elements of the Galois group of K over $\mathbb{Q}$, then b_α is positive definite, i.e., $b_\alpha(\mathbf{x}, \mathbf{x}) > 0$ for all nonzero $\mathbf{x} \in \mathcal{O}_K^N$ [31]. If we take α in the codifferent of K which is the set $\mathcal{D}_K^{-1} = \{x \in K : \mathrm{Tr}(xy) \in \mathbb{Z} \text{ for all } y \in \mathcal{O}_K\}$, then $\mathrm{Tr}(\alpha x_i \overline{y}_i) \in \mathbb{Z}$ [31]. The pair $(\rho^{-1}(\mathcal{C}), b_\alpha)$ thus forms a lattice of rank nN, which is integral when $\alpha \in \mathcal{D}_K^{-1}$ but also in other cases, depending on the choice of $\mathcal{C}$, as we will see in the following. It should be noted that $\rho^{-1}(\mathcal{C}) \subset \mathcal{O}_K^N$ and by using the canonical embedding (See Definition 1) σ we can map $x \in K$ into $\sigma(x) \in \mathbb{R}^n$, where $n = [K:\mathbb{Q}]$. Let σ^N be the componentwise extension of σ, that is

$$\begin{array}{rcl} \sigma^N : K^N & \to & \mathbb{R}^{nN}, \\ (x_1, \ldots, x_N) & \mapsto & (\sigma(x_1), \ldots, \sigma(x_N)). \end{array} \tag{11}$$

Thus, $\sigma^N(\rho^{-1}(\mathcal{C})) \subset \mathbb{R}^{nN}$ is a real lattice of dimension nN. This method of constructing lattices from linear codes is usually referred to as Construction A [22], [30], [31]. To simplify the notation, we show above Construction A lattices using $(\rho^{-1}(\mathcal{C}), b_\alpha)$ without mentioning the operation of σ^N. The original binary Construction A, proposed by Forney [28], can be seen as a particular case of the cyclotomic field approach proposed by Ebeling [29], which in turn is a particular case of the above construction. For p a prime, take for K the cyclotomic field $\mathbb{Q}(\zeta_p)$, where ζ_p is a primitive p^{th} root of unity and $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Take $\mathfrak{p} = (1-\zeta_p)$ the prime ideal above p, and $\alpha = 1/p$. Since $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, this construction involves linear codes over $\mathbb{F}_p$. The case $p = 2$ is the binary Construction A. The generalization from cyclotomic fields to either CM fields or totally real number fields is suggested in [30] for the case where $\mathfrak{p}$ is totally ramified.

Definition 5: Given an arbitrary lattice (L, b) where L is a $\mathbb{Z}$-module and b is a symmetric bilinear form which is positive definite, the dual lattice of (L, b) is the pair (L^*, b), where

$$L^* = \{\mathbf{x} \in L \otimes_{\mathbb{Z}} \mathbb{R} \,|\, b(\mathbf{x}, \mathbf{y}) \in \mathbb{Z} \text{ for all } \mathbf{y} \in L\}, \tag{12}$$

in which $\otimes_{\mathbb{Z}}$ denotes the tensor product over $\mathbb{Z}$. If $L \subset L^*$, (L, b) is integral. If $(L, b) \cong (L^*, b)$, i.e., there exists a $\mathbb{Z}$-module homomorphism $\tau : L \to L^*$ such that $b(\tau(\mathbf{x}), \tau(\mathbf{y})) = b(\mathbf{x}, \mathbf{y})$ for all $\mathbf{x}, \mathbf{y} \in L$, then (L, b) is unimodular. If (L, b) is integral and $(L, b) \cong (L^*, db)$ for some positive integer d, (L, b) is d-modular (or modular of level d). An integral lattice (Λ, b) is called even if $b(\mathbf{x}, \mathbf{x}) \in 2\mathbb{Z}$ for all $\mathbf{x} \in \Lambda$ and odd otherwise.

Let $\mathcal{C} \subset \mathbb{F}_q^N$ be a linear code of dimension k, and q a prime power. Its dual code is $C^\perp = \left\{\mathbf{x} \in \mathbb{F}_q^N \,|\, \mathbf{x} \cdot \mathbf{y} = \sum_{i=1}^N x_i y_i = 0 \text{ for all } \mathbf{y} \in \mathcal{C}\right\}$; $\mathcal{C}$ is self-orthogonal if $\mathcal{C} \subset \mathcal{C}^\perp$, and is self-dual if $\mathcal{C} = \mathcal{C}^\perp$. It is well

known for the binary Construction A that $\mathcal{C} \subset \mathbb{F}_2^N$ is self-dual if and only if $(\rho^{-1}(\mathcal{C}), b_{\frac{1}{2}})$ is unimodular [22], [29]. More generally, for $K = \mathbb{Q}(\zeta_p)$, if $\mathcal{C} \subset \mathbb{F}_p^N$ is self-dual, then $(\rho^{-1}(\mathcal{C}), b_{\frac{1}{p}})$ is unimodular [29]. The converse of this statement is proved in [31] for totally real number fields and CM fields with a totally ramified prime. Self-dual codes thus provide a systematic way to obtain modular lattices. This was used for example in [40], where $K = \mathbb{Q}(\sqrt{-2})$, $\mathfrak{p} = (3)$ and self-dual codes over the ring $\mathcal{O}_K/\mathfrak{p}$ were used to construct 2-modular lattices. Similarly, in [41], it was shown that by taking $K = \mathbb{Q}(\zeta_3)$, $\mathfrak{p} = (4)$, and self-dual codes over the ring $\mathcal{O}_K/\mathfrak{p}$, 3-modular lattices can be constructed.

As above, we consider the nN-dimensional lattice $(\rho^{-1}(\mathcal{C}), b_\alpha)$. Let $\Delta = |d_K|$ be the absolute value of the discriminant of K.

Proposition 1: [31] Using the previous notation, the following results hold:

1) The lattice $(\rho^{-1}(\mathcal{C}), b_\alpha)$ has discriminant $\Delta^N p^{2f(N-k)} N(\alpha)^N$ and volume $\Delta^{\frac{N}{2}} p^{f(N-k)} N(\alpha)^{\frac{N}{2}}$.
2) The dual lattice $(\rho^{-1}(\mathcal{C})^*, b_\alpha)$ has discriminant $\Delta^{-N} p^{-2f(N-k)} N(\alpha)^{-N}$ and volume $\Delta^{\frac{-N}{2}} p^{-f(N-k)} N(\alpha)^{\frac{-N}{2}}$.
3) The lattice $(\rho^{-1}(\mathcal{C}^\perp), b_\alpha)$ has discriminant $\Delta^N p^{2fk} N(\alpha)^N$ and volume $\Delta^{\frac{N}{2}} p^{fk} N(\alpha)^{\frac{N}{2}}$.

Two particular cases of the above construction method, when $\alpha = 1/p$ or $\alpha = 1/2p$ for K a real quadratic field with $\mathfrak{p}$ inert and K an imaginary quadratic field with $\mathfrak{p}$ totally ramified, have been discussed in [31]. The following proposition justifies why we consider self-orthogonal codes in the construction of modular lattices which are of great interest in information security.

Proposition 2: [31, Proposition 2.9] If $\mathcal{C}$ is not self-orthogonal, i.e. if $\mathcal{C} \not\subset \mathcal{C}^\perp$, then $(\rho^{-1}(\mathcal{C}), b_\alpha)$ is not an integral lattice for any $\alpha \in \mathfrak{p}^{-1} \cap \mathbb{Q}$ when K is totally real or when K is a CM field and $\mathfrak{p}$ is totally ramified.

V. Construction A Modular Lattices Using Cyclotomic Fields

In this section, we present the construction of modular lattices using the provided algebraic tools in the previous sections. We consider $K = \mathbb{Q}(\zeta_n)$ and its maximal totally real subfield K^+, when n is a prime power. In other cases, that is when $K = \mathbb{Q}(\zeta_n)$ and $n \neq p^r$ for an odd prime number p, making a general decision is not easy. Due to the lack of space, we can not provide more details. Here, we concentrate on generalizing the following results to obtain d-modular lattices using cyclotomic number fields.

Proposition 3: [29, Section 5.2] Let p be an odd prime, and let ζ_p be a primitive p^{th} root of unity. Consider the cyclotomic field $K = \mathbb{Q}(\zeta_p)$, which is a CM field, 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 $\mathcal{O}_K/\mathfrak{p} \cong \mathbb{F}_p$, and the bilinear form $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^N \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i/p)$. Given a code $\mathcal{C}$ over $\mathbb{F}_p$, if $\mathcal{C} \subset \mathcal{C}^\perp$ then $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is an even integral lattice of rank $N(p-1)$. In addition, if $\mathcal{C}$ is self-dual, then $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is an even unimodular lattice.

Proposition 4: [30, Corollary 2] Let $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and let $\mathcal{C} \subset \mathbb{F}_p^N$ be a k-dimensional code such that $\mathcal{C} \subset \mathcal{C}^\perp$. Then the lattice $(\rho^{-1}(\mathcal{C}), b_\alpha)$ given in the previous section, together with the bilinear form $b_\alpha(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^N \mathrm{Tr}_{K^+/\mathbb{Q}}(\alpha x_i y_i)$, where $\alpha = 1/p$, is an integral lattice of rank $N(p-1)/2$. In addition, if $\mathcal{C}$ is self-dual, then $(\rho^{-1}(\mathcal{C}), b_\alpha)$ is an odd unimodular lattice.

As far as we know, the generalizations of the above results to $K = \mathbb{Q}(\zeta_{p^r})$ and $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$, or generalization to the cases that $K = \mathbb{Q}(\zeta_n)$, with $n \neq p^r$ for a prime number p, have not been addressed in the literature. In the following theorems, we consider all of these cases.

Theorem 5: Let $K = \mathbb{Q}(\zeta_{p^r})$, with $r > 1$ and p an odd prime number, be the cyclotomic field with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_{p^r}]$. We have that K is a CM field and the prime p totally ramifies in K as $pO_K = \mathfrak{P}^{p^{r-1}(p-1)}$, with residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_p$, where $\mathfrak{P} = (1-\zeta_{p^r})$. Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N,k) self-dual code over $\mathbb{F}_p$. Then, $(\rho^{-1}(\mathcal{C}), b_{1/p})$ with $b_{1/p}(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^N \mathrm{Tr}_{K/\mathbb{Q}}(x_i \bar{y}_i/p)$, is d-modular if and only if $d = 1$ and $r = 1$.

Proof: If $r = 1$ and $d = 1$, then $K = \mathbb{Q}(\zeta_p)$ and the result follows from Proposition 3. Now assume that $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is a d-modular lattice. Then, due to the definition of modular lattices, we have $\frac{1}{\sqrt{d}}\rho^{-1}(\mathcal{C}) = (\rho^{-1}(\mathcal{C}))^*$. Consequently, $\mathrm{vol}\left(\frac{1}{\sqrt{d}}\rho^{-1}(\mathcal{C})\right) = \mathrm{vol}((\rho^{-1}(\mathcal{C}))^*)$. We have $\mathrm{vol}((\rho^{-1}(\mathcal{C}))^*) = 1/\mathrm{vol}(\rho^{-1}(\mathcal{C}))$ that implies $d^{\frac{-nN}{2}}(\mathrm{vol}(\rho^{-1}(\mathcal{C})))^2 = 1$. It is enough to compute $\mathrm{vol}(\rho^{-1}(\mathcal{C}))$. To this end, we have $\mathrm{vol}(\rho^{-1}(\mathcal{C})) = \sqrt{|\mathrm{disc}(\rho^{-1}(\mathcal{C}))|} = \sqrt{\Delta^N p^{2N-2k-nN}}$, where $\Delta = |d_K| = p^{p^{r-1}(pr-r-1)}$. Thus, we have

$$d^{\frac{-nN}{2}} p^{2N-2k-nN} p^{Np^{r-1}(pr-r-1)} = 1. \quad (13)$$

We conclude that d is 1 or p. Let $d = p$ and apply $n = p^{r-1}(p-1)$ in (13). We have

$$\frac{-p^{r-1}(p-1)N}{2} + 2N - 2k - p^{r-1}(p-1)N + Np^{r-1}(pr-r-1) = 0.$$

Simplifying the above equation gives the following relation

$$N\left[3(1-p)p^{r-1} + 2p^{r-1}(pr-r-1) + 4\right] = 4k.$$

Since $\mathcal{C}$ is a self-dual code, $k = N/2$ and we have

$$\begin{aligned} 2 &= 3(1-p)p^{r-1} + 2p^{r-1}(pr-r-1) + 4 \\ &= p^{r-1}(1-3p+2pr-2r) + 4. \end{aligned}$$

Finally, we have $p^{r-1}(1-3p+2pr-2r) = -2$ which implies $r = 2$ and $p = 2$ or $r = 1$ and $p = 1$ and both of these cases are contradictions. Thus, $d = 1$ and it is enough to show that $r = 1$. In this case, $\rho^{-1}(\mathcal{C})$ is unimodular and we have $\rho^{-1}(\mathcal{C}^\perp) = (\rho^{-1}(\mathcal{C}))^*$ and consequently $\mathrm{vol}(\rho^{-1}(\mathcal{C}^\perp)) = \mathrm{vol}((\rho^{-1}(\mathcal{C}))^*)$, which implies

$$k - \frac{N}{2}\left[p^{r-1}(rp-r-p)+2\right] = k + \frac{N}{2}\left[p^{r-1}(rp-r-p)\right].$$

We conclude that $p^{r-1}(rp-r-p) = -1$ which is possible if and only if $r = 1$. ∎

Theorem 6: Let $K^+ = \mathbb{Q}(\zeta_{p^r} + \zeta_{p^r}^{-1})$, with $r > 1$ and p an odd prime number, be the totally real maximal subfield of a cyclotomic field with the ring of integers $\mathcal{O}_{K^+} = \mathbb{Z}[\zeta_{p^r} + \zeta_{p^r}^{-1}]$. We have that K^+ is a totally real number field and the prime p totally ramifies in K^+ as $pO_{K^+} = \mathfrak{p}^{\frac{p^{r-1}(p-1)}{2}}$, with residue field $\mathcal{O}_{K^+}/\mathfrak{p} \cong \mathbb{F}_p$, where $\mathfrak{p} = (2 - \zeta_{p^r} - \zeta_{p^r}^{-1})$. Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N,k) self-dual code over $\mathbb{F}_p$. Then,

$(\rho^{-1}(\mathcal{C}), b_{1/p})$ with $b_{1/p}(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(x_i y_i/p)$, is d-modular if and only if $d = 1$ and $r = 1$.

Proof: If $r = 1$ and $d = 1$, then $K^+ = \mathbb{Q}(\zeta_p + \zeta_p^{-1})$ and the result follows from Proposition 4. Now, assume that $(\rho^{-1}(\mathcal{C}), b_{1/p})$ is a d-modular lattice. Then, due to the definition of modular lattices, we have $\frac{1}{\sqrt{d}}\rho^{-1}(\mathcal{C}) = (\rho^{-1}(\mathcal{C}))^*$. Consequently, $\mathrm{vol}\left(\frac{1}{\sqrt{d}}\rho^{-1}(\mathcal{C})\right) = \mathrm{vol}((\rho^{-1}(\mathcal{C}))^*)$. We have $\mathrm{vol}((\rho^{-1}(\mathcal{C}))^*) = 1/\mathrm{vol}(\rho^{-1}(\mathcal{C}))$ that implies $d^{\frac{-nN}{2}}(\mathrm{vol}(\rho^{-1}(\mathcal{C})))^2 = 1$. It is enough to compute $\mathrm{vol}(\rho^{-1}(\mathcal{C}))$. Similarly as before, we have $\mathrm{vol}(\rho^{-1}(\mathcal{C})) = \sqrt{|\mathrm{disc}(\rho^{-1}(\mathcal{C}))|} = \sqrt{\Delta^N p^{2N-2k-nN}}$, where $\Delta = |d_{K^+}| = p^{\frac{p-1}{2}\left((r+1)p^{r-1} - \frac{p^r-1}{p-1}\right)-1}$. Thus, we have

$$d^{\frac{-nN}{2}} p^{2N-2k-nN} p^{N\left[\frac{p-1}{2}\left((r+1)p^{r-1} - \frac{p^r-1}{p-1}\right)-1\right]} = 1. \quad (14)$$

We conclude that d is 1 or p. Let $d = p$, and apply $n = \frac{p^{r-1}(p-1)}{2}$ in (14). We have

$$\frac{p^{r-1}(1-p)N}{4} + N + \frac{p^{r-1}(1-p)N + N(p-1)\left((r+1)p^{r-1} - \frac{p^r-1}{p-1}\right)}{2} = 2k.$$

Since $\mathcal{C}$ is a self-dual code, $k = N/2$ and we have

$$\begin{aligned} 0 &= \frac{N(p-1)}{4}\left[-3p^{r-1} + 2(r+1)p^{r-1} - \frac{2(p^r-1)}{p-1}\right] \\ &= \frac{N}{4}\left[-3(p-1)p^{r-1} + 2(r+1)(p-1)p^{r-1} - 2(p^r-1)\right] \\ &= \frac{N}{4}\left[p^r(2r-3) + p^{r-1}(1-2r) + 2\right] \\ &= \frac{N}{4}\left[p^{r-1}(2pr - 3p + 1 - 2r) + 2\right]. \end{aligned}$$

Thus, we have $p^{r-1}(1-3p+2pr-2r) = -2$ which implies $r = 2$ and $p = 2$ or $r = 1$ and $p = 1$ and both of these cases are contradictions. Thus, $d = 1$ and it is enough to show that $r = 1$. In this case, $\rho^{-1}(\mathcal{C})$ is unimodular and we have $\rho^{-1}(\mathcal{C}^\perp) = (\rho^{-1}(\mathcal{C}))^*$ and consequently $\mathrm{vol}(\rho^{-1}(\mathcal{C}^\perp)) = \mathrm{vol}((\rho^{-1}(\mathcal{C}))^*)$, which implies

$$k + \frac{N}{4}\left[p^{r-1}(rp - r - p) - 1\right] = k - \frac{N}{4}\left[p^{r-1}(rp - r - p) + 3\right].$$

We conclude that $p^{r-1}(rp - r - p) = -1$ which is possible if and only if $r = 1$. ∎

VI. A New Family of p-modular Construction A Lattices Based on Cyclotomic Fields

In the applications of d-modular lattices in information security, only special values of d are accepted, more precisely, $d = 1, 2, 3, 5, 6, 7, 11, 14, 15$ and 23 [31]. We could not find any modular lattice in our trials using cyclotomic number fields (with non-prime orders) and Construction A that fulfil these conditions. Thus, these remain open problems.

In the sequel, we present a new framework based on Construction A and cyclotomic number fields giving us a family of p-modular lattices, with $p \equiv 1 \pmod 4$.

According to Kronecker-Weber theorem [42], [43], every algebraic integer in a number field, whose Galois group is Abelian, can be expressed as a sum of roots of unity with rational coefficients. Let $\mathbb{Q}_m = \mathbb{Q}(e^{2\pi i/m})$. We can assume that $m \not\equiv 2 \pmod 4$, because if $m \equiv 2 \pmod 4$ with $m = 2m_0$, then it is easy to check that $e^{-2\pi i/m_0}$ is a primitive m^{th} root of unity, and hence $\mathbb{Q}_m = \mathbb{Q}_{m_0}$.

Example 6.1: [44] Let $L = \mathbb{Q}(\zeta_m + \zeta_m^{-1})$ be the maximal real subfield of $\mathbb{Q}_m$. The conductor of a number field L is the smallest integer m such that $L \subset \mathbb{Q}_m$ which is denoted by $\mathfrak{f}_L$. For $m \geq 5$, $\mathfrak{f}_L = m$. If $m = 3, 4$, then $L = \mathbb{Q}$ and $\mathfrak{f}_L = 1$. As another case, consider $L = \mathbb{Q}(\sqrt{d})$, where d is an squarefree integer, $|d| > 1$. Then

$$\mathfrak{f}_L = |d_L| = \begin{cases} |d|, & \text{if } d \equiv 1 \pmod 4, \\ |4d|, & \text{if } d \equiv 2, 3 \pmod 4. \end{cases} \quad (15)$$

If $L = \mathbb{Q}_p$ (p an odd prime), then by using (8), $d_L = (-1)^{\frac{p-1}{2}} p^{p-2}$ is the square of an integer in $\mathcal{O}_L$, thus $\mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right) \subset \mathbb{Q}_p$. It follows that for a prime p

$$\mathbb{Q}(\sqrt{p}) \subset \begin{cases} \mathbb{Q}_p, & \text{if } p \equiv 1 \pmod 4, \\ \mathbb{Q}_{4p}, & \text{if } p \equiv 3 \pmod 4, \\ \mathbb{Q}_8, & \text{if } p = 2. \end{cases} \quad (16)$$

Moreover, if $d = \pm 2^\nu p_1 p_2 \cdots p_r$ is squarefree, then $\mathbb{Q}(\sqrt{d}) \subset \mathbb{Q}_{4d}$. □

Theorem 7: Let $K = \mathbb{Q}(\zeta_p)$, where p is an odd prime and $p \equiv 1 \pmod 4$, with the ring of integers $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$. Then, K is a CM field and the prime p totally ramifies in K as $pO_K = \mathfrak{P}^{p-1}$, with residue field $\mathcal{O}_K/\mathfrak{P} \cong \mathbb{F}_p$, where $\mathfrak{P} = pO_K + (1-\zeta_p)\mathcal{O}_K$. Let $\mathcal{C} \subset \mathbb{F}_p^N$ be an (N, k) self-dual code over $\mathbb{F}_p$. Then, $(\rho^{-1}(\mathcal{C}), b_\alpha)$ with $b_\alpha(\mathbf{x},\mathbf{y}) = \sum_{i=1}^{N} \mathrm{Tr}_{K/\mathbb{Q}}(\alpha x_i \bar{y}_i)$ and $\alpha = \frac{1}{\sqrt{p}}$, is a p-modular lattice.

Proof: The proof is omitted due to lack of space. ∎

Remark 1: For $K = \mathbb{Q}(\zeta_p)$, the $p-1$ embeddings $\sigma_1, \ldots, \sigma_{p-1} : K \to \mathbb{C}$ are given by

$$\sigma_r(\zeta_p) = \zeta^r, \quad r = 1, \ldots, p-1. \quad (17)$$

Then, the trace of an element $\gamma \in K$, $\gamma = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, $a_i \in \mathbb{Q}$, is easily computed to be [29, p. 122]

$$\mathrm{Tr}_{K/\mathbb{Q}}(\gamma) = (p-1)a_0 - a_1 - a_2 - \cdots - a_{p-2}. \quad (18)$$

Let $\mathfrak{P} = (1-\zeta_p)$ be the principal ideal of $\mathcal{O}_K = \mathbb{Z}[\zeta_p]$ generated by the element $1-\zeta_p$ in $\mathcal{O}_K$. Then, $\mathfrak{P} \cap \mathbb{Z} = p\mathbb{Z}$ and for any $x \in \mathfrak{P}$, $\mathrm{Tr}_{K/\mathbb{Q}}(x) \in p\mathbb{Z}$ [29, p. 122]. The mapping $\rho : \mathcal{O}_K \to \mathbb{F}_p$ sending $\gamma = a_0 + a_1\zeta_p + \cdots + a_{p-2}\zeta_p^{p-2}$, $a_i \in \mathbb{Z}$, to $\rho(\gamma) = a_0 + a_1 + \cdots + a_{p-2} \pmod p$ is an additive homomorphism and the kernel of this homomorphism is equal to $\mathfrak{P}$. This shows that the mapping ρ can be considered as the reduction $\bmod \mathfrak{P}$ [29, p. 123]. The vectors

$$1-\zeta_p, \zeta_p - \zeta_p^2, \zeta_p^2 - \zeta_p^3, \ldots, \zeta^{p-2} - \zeta^{p-1} \quad (19)$$

form a $\mathbb{Z}$-basis for $\mathfrak{P}$ [29, p. 126].

Remark 2: In order to use Theorem 7, we need to express $\sqrt{p}$ in terms of the $\mathbb{Z}$-basis of $\mathbb{Z}[\zeta_p]$. To this end, we use *quadratic Gauss sums*. We also have the following useful result [45, pp. 75]

$$\sum_{n=0}^{p-1} e^{2\pi i n^2/p} = \begin{cases} \sqrt{p} & p \equiv 1 \pmod 4, \\ i\sqrt{p} & p \equiv 3 \pmod 4. \end{cases} \quad (20)$$

The main reason for applying the canonical embedding on algebraic lattices is the embedding of their corresponding lattices into the real space $\mathbb{R}^n$ for some n. Theorem 7 does not guarantee that its introduced lattice is embedded

in $\mathbb{R}^{N(p-1)}$, because the element α is not necessarily totally positive and some of $\sqrt{\sigma_i(\alpha)}$'s may be purely imaginary numbers. In the next theorem, we explain this issue for $p = 5$.

Proposition 5: Let $p = 5$ and $\rho^{-1}(\mathcal{C})$ be the obtained lattice in Theorem 7. Define $\Gamma_{\mathcal{C}} = \sigma^N(\rho^{-1}(\mathcal{C}))$, where σ^N is the canonical embedding which has been applied componentwise over $\mathcal{O}_K^N$, that is, $\sigma^N(x_1, \ldots, x_N) = (\sigma(x_1), \ldots, \sigma(x_N))$, for $(x_1, \ldots, x_N) \in \mathcal{O}_K^N$ and $\sigma = (\sigma_1, \ldots, \sigma_4)$. Then, $\Gamma_{\mathcal{C}}$ is a $\mathbb{Z}$-lattice in $\mathbb{R}^{2N} \times \mathbb{R}^{*2N}$, where $\mathbb{R}^*$ is the set of purely imaginary numbers.

Proof: The proof is omitted due to lack of space. ■

Using Theorem 7, we find a new family of 5-modular lattices which is applicable in information security. We need a family of self dual codes over $\mathbb{F}_5$, which is provided in [46]. Self-dual codes over $\mathbb{F}_5$ exist if and only if the length is even. If a codeword $\mathbf{u}$ in a self-orthogonal code $\mathcal{C}$ contains i 0's, j $\{\pm 1\}$'s and k $\{\pm 2\}$'s (so that the weight of $\mathbf{u}$ is $j + k$), then $\mathbf{u} \cdot \mathbf{u} = 0$ implies $j \equiv k \pmod 5$. This equation also implies that a codeword in a self-orthogonal code cannot have weight 1 or 3, although all other weights can occur [46]. The first obtained 5-ary self-dual code in [46] is the $[2, 1, 2]$ code $\mathcal{C}_2$, consisting of the codewords $\{(0, 0), (1, 2), (2, -1), (-2, 1), (-1, -2)\}$. It has generator matrix $\left[\begin{array}{cc} 1 & 2 \end{array}\right]$.

Example 6.2: Let $p = 5$ and $K = \mathbb{Q}(\zeta_5)$, with $\rho : \mathbb{Z}[\zeta_5]^2 \to \mathbb{F}_5^2$ given in Remark 1. The degree of $K/\mathbb{Q}$ is 4, and the four embeddings of K are σ_1, which is the identity, σ_2, which is the conjugate of σ_1 and maps ζ_5 to ζ_5^4, σ_3, which maps ζ_5 to ζ_5^2, and σ_4, which is the conjugate of σ_3 and maps ζ_5 to ζ_5^3. Consider the self dual code $\mathcal{C} = \mathcal{C}_2$ of length 2 over $\mathbb{F}_5$ as in the above, with generator matrix $\left[\begin{array}{cc} \mathbf{I} & \mathbf{A} \end{array} \pmod 5\right]$ and $\mathbf{A} \pmod 5 = \left[\begin{array}{c} 2 \end{array}\right]$. Using the mapping ρ in Remark 1, we can take 2 to be the preimage of 2 and we have $\mathbf{A} = \left[\begin{array}{c} 2 \end{array}\right]$. We next compute a generator matrix for the lattice $\rho^{-1}(\mathcal{C})$ explicitly by using the discussion from Section IV. We choose the basis $\{v_1 = 1, v_2 = \zeta_5, v_3 = \zeta_5^2, v_4 = \zeta_5^3\}$ for $\mathcal{O}_K$, and it follows that the generator matrix for the lattice $\mathcal{O}_K$ together with the trace form $\langle x, y\rangle = \mathrm{Tr}_{K/\mathbb{Q}}(x\bar{y})$, $x, y \in \mathcal{O}_K$, is

$$\mathbf{M} = \sqrt{2}\begin{bmatrix} \Re\sigma_1(1) & \Im\sigma_2(1) & \Re\sigma_3(1) & \Im\sigma_4(1) \\ \Re\sigma_1(\zeta_5) & \Im\sigma_2(\zeta_5) & \Re\sigma_3(\zeta_5) & \Im\sigma_4(\zeta_5) \\ \Re\sigma_1(\zeta_5^2) & \Im\sigma_2(\zeta_5^2) & \Re\sigma_3(\zeta_5^2) & \Im\sigma_4(\zeta_5^2) \\ \Re\sigma_1(\zeta_5^3) & \Im\sigma_2(\zeta_5^3) & \Re\sigma_3(\zeta_5^3) & \Im\sigma_4(\zeta_5^3) \end{bmatrix}$$
$$= \sqrt{2}\begin{bmatrix} 1 & 0 & 1 & 0 \\ \Re\zeta_5 & \Im\zeta_5^4 & \Re\zeta_5^2 & \Im\zeta_5^3 \\ \Re\zeta_5^2 & \Im\zeta_5^3 & \Re\zeta_5^4 & \Im\zeta_5 \\ \Re\zeta_5^3 & \Im\zeta_5^2 & \Re\zeta_5 & \Im\zeta_5^4 \end{bmatrix}.$$

It should be noted that

$$\Re\zeta_5 = \Re\zeta_5^4 = \cos(\tfrac{2\pi}{5}) = \tfrac{-1+\sqrt{5}}{4},$$
$$\Re\zeta_5^2 = \Re\zeta_5^3 = \cos(\tfrac{4\pi}{5}) = \tfrac{-1-\sqrt{5}}{4},$$

$$\Im\zeta_5 = \tfrac{1}{4}\sqrt{10+2\sqrt{5}}, \qquad \Im\zeta_5^4 = \tfrac{-1}{4}\sqrt{10+2\sqrt{5}},$$
$$\Im\zeta_5^2 = \tfrac{1}{4}\sqrt{10-2\sqrt{5}} \qquad \Im\zeta_5^3 = \tfrac{-1}{4}\sqrt{10-2\sqrt{5}}.$$

Using Proposition 2.6 in [31], a generator matrix for $(\rho^{-1}(\mathcal{C}), b_\alpha)$, with $\alpha = 1/\sqrt{5}$, is

$$\mathbf{M}_{\mathcal{C}} = \begin{bmatrix} \mathbf{M} & \mathbf{A} \otimes \mathbf{M} \\ \mathbf{0}_{4\times 4} & \mathbf{M}_p \end{bmatrix} (\mathbf{I}_2 \otimes \mathbf{D}_\alpha), \qquad (21)$$

where $\mathbf{M}_p$ is obtained using the $\mathbb{Z}$-basis $\{\omega_1 = 1-\zeta_5, \omega_2 = \zeta_5 - \zeta_5^2, \omega_3 = \zeta_5^2 - \zeta_5^3, \omega_4 = \zeta_5^3 - \zeta_5^4\}$ for $\mathfrak{P}$ as follows

$$\mathbf{M}_p = \sqrt{2}\begin{bmatrix} \Re\sigma_1(\omega_1) & \Im\sigma_2(\omega_1) & \Re\sigma_3(\omega_1) & \Im\sigma_4(\omega_1) \\ \Re\sigma_1(\omega_2) & \Im\sigma_2(\omega_2) & \Re\sigma_3(\omega_2) & \Im\sigma_4(\omega_2) \\ \Re\sigma_1(\omega_3) & \Im\sigma_2(\omega_3) & \Re\sigma_3(\omega_3) & \Im\sigma_4(\omega_3) \\ \Re\sigma_1(\omega_4) & \Im\sigma_2(\omega_4) & \Re\sigma_3(\omega_4) & \Im\sigma_4(\omega_4) \end{bmatrix}.$$

The matrix $\mathbf{D}_\alpha$ is the diagonal matrix $\mathrm{diag}\left(\sqrt{\sigma_1(\alpha)}, \sqrt{\sigma_2(\alpha)}, \sqrt{\sigma_3(\alpha)}, \sqrt{\sigma_4(\alpha)}\right)$.

In order to show that $(\rho^{-1}(\mathcal{C}), b_\alpha)$ is integral, we compute the Gram matrix as follows [31]. Define $\mathbf{v} = (v_1, v_2, v_3, v_4)^t = (1, \zeta_5, \zeta_5^2, \zeta_5^3)^t$, $\mathbf{v}^\dagger = \left(1, \zeta_5^4, \zeta_5^3, \zeta_5^2\right)$ and $\boldsymbol{\omega} = (\omega_1, \omega_2, \omega_3, \omega_4)^t = (1-\zeta_5)\mathbf{v}$, then

$$\mathbf{G}_{\mathcal{C}} = \begin{bmatrix} \mathrm{Tr}_{K/\mathbb{Q}}\left(5\alpha\mathbf{v}\mathbf{v}^\dagger\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(2\alpha\mathbf{v}\boldsymbol{\omega}^\dagger\right) \\ \mathrm{Tr}_{K/\mathbb{Q}}\left(2\alpha\bar{\boldsymbol{\omega}}\mathbf{v}^t\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\alpha\boldsymbol{\omega}\boldsymbol{\omega}^\dagger\right) \end{bmatrix},$$

in which

$$\mathbf{v}\mathbf{v}^\dagger = \begin{bmatrix} 1 & \zeta_5^4 & \zeta_5^3 & \zeta_5^2 \\ \zeta_5 & 1 & \zeta_5^4 & \zeta_5^3 \\ \zeta_5^2 & \zeta_5 & 1 & \zeta_5^4 \\ \zeta_5^3 & \zeta_5^2 & \zeta_5 & 1 \end{bmatrix},$$

$$\mathbf{v}\boldsymbol{\omega}^\dagger = \mathbf{v}(\overline{1-\zeta_5})\mathbf{v}^\dagger = (1-\zeta_5^4)\mathbf{v}\mathbf{v}^\dagger, \qquad (22)$$

$$\bar{\boldsymbol{\omega}}\mathbf{v}^t = (\overline{1-\zeta_5})\bar{\mathbf{v}}\mathbf{v}^t = (1-\zeta_5^4)(\mathbf{v}\mathbf{v}^\dagger)^t, \qquad (23)$$

$$\boldsymbol{\omega}\boldsymbol{\omega}^\dagger = (1-\zeta_5)(1-\zeta_5^4)(\mathbf{v}\mathbf{v}^\dagger) = (3+\zeta_5^2+\zeta_5^3)\mathbf{v}\mathbf{v}^\dagger. \qquad (24)$$

Using the additive property of the trace function, it is enough to find $\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{5}\zeta_5^i)$, for $i = 0, 1, \ldots, 4$. We have

$$\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{5}\zeta_5^0) = \mathrm{Tr}_{K/\mathbb{Q}}(-1-2\zeta_5^2-2\zeta_5^3) = -4+2+2 = 0,$$
$$\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{5}\zeta_5) = \mathrm{Tr}_{K/\mathbb{Q}}(2+\zeta_5+2\zeta_5^2) = 8-1-2 = 5,$$
$$\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{5}\zeta_5^2) = \mathrm{Tr}_{K/\mathbb{Q}}(2\zeta_5+\zeta_5^2+2\zeta_5^3) = -2-1-2 = -5,$$
$$\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{5}\zeta_5^3) = \mathrm{Tr}_{K/\mathbb{Q}}(-2-2\zeta_5-\zeta_5^3) = -8+2+1 = -5,$$
$$\mathrm{Tr}_{K/\mathbb{Q}}(\sqrt{5}\zeta_5^4) = \mathrm{Tr}_{K/\mathbb{Q}}(1-\zeta_5-\zeta_5^2+\zeta_5^3) = 4+1+0 = 5.$$

For example, we have computed the upper left component of $\mathbf{G}_{\mathcal{C}}$ in (26). Other components can be computed similarly and we have

$$\mathbf{G}_{\mathcal{C}} = \begin{bmatrix} 0 & 5 & -5 & -5 & -2 & 4 & 0 & -4 \\ 5 & 0 & 5 & -5 & 2 & -2 & 4 & 0 \\ -5 & 5 & 0 & 5 & -4 & 2 & -2 & 4 \\ -5 & -5 & 5 & 0 & 0 & -4 & 2 & -2 \\ -2 & 2 & -4 & 0 & -2 & 3 & -2 & -2 \\ 4 & -2 & 2 & -4 & 3 & -2 & 3 & -2 \\ 0 & 4 & -2 & 2 & -2 & 3 & -2 & 3 \\ -4 & 0 & 4 & -2 & -2 & -2 & 3 & -2 \end{bmatrix}. \qquad (25)$$

Thus, $(\rho^{-1}(\mathcal{C}), b_\alpha)$ is an integral lattice and it can be checked that $\det(\mathbf{G}_{\mathcal{C}}) = 5^4$, that is a necessary condition for being 5-modular. □

VII. Conclusions

In this paper, we have presented the importance of modular lattices in information security and recently proposed methods for obtaining modular lattices using algebraic number fields. There is a symmetry point, called weak secrecy gain, in the secrecy function of modular lattices conjectured to be the secrecy gain. It characterizes the confusion at the eavesdropper in the case of using lattices in the Gaussian wiretap channels. In order to increase the weak secrecy gain, we can use d-modular lattices with high level d since

$$\mathrm{Tr}_{K/\mathbb{Q}}\left(5\alpha\mathbf{v}\mathbf{v}^{\dagger}\right)=\begin{bmatrix}\mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^4\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^3\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^2\right)\\ \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^4\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^3\right)\\ \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^2\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^4\right)\\ \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^3\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5^2\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\zeta_5\right) & \mathrm{Tr}_{K/\mathbb{Q}}\left(\sqrt{5}\right)\end{bmatrix}=\begin{bmatrix}0 & 5 & -5 & -5\\ 5 & 0 & 5 & -5\\ -5 & 5 & 0 & 5\\ -5 & -5 & 5 & 0\end{bmatrix}. \tag{26}$$

they are more likely to have a large length for the shortest nonzero vector. In search of such lattices, we have proved that there is no modular lattices built using Construction A over cyclotomic fields of prime power order p^n, with $n > 1$. We have also presented a new framework based on Construction A and cyclotomic number fields giving us a family of p-modular lattices with $p \equiv 1 \pmod 4$.

REFERENCES

[1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," *Found. Trends Commun. Inf. Theory*, vol. 5, no. 4, pp. 355–580, Apr. 2009.

[2] N. Asokan and P. Ginzboorg, "Key-agreement in ad-hoc networks," *Computer Communications*, vol. 23, no. 17, pp. 1627–1637, 2000.

[3] A. J. Menezes and P. C. van Oorschot and S. A. Vanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[4] R. Cramer and V. Shoup, "Design and analysis of practical public-key encryption schemes secure against adaptive chosen ciphertext attack," *SIAM J. on Computing*, vol. 33, no. 1, pp. 167–226, 2004.

[5] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.

[6] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. on Inform. Theory*, vol. 24, no. 3, pp. 339–348, 1978.

[7] F. Lin, F. Oggier, and P. Solé, "2- and 3-modular lattice wiretap codes in small dimensions," *AAECC*, vol. 26, no. 6, pp. 571–590, 2015.

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

[9] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE Trans. on Inform. Foren. Secur.*, vol. 6, no. 3, pp. 532–540, 2011.

[10] J. C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *International Symposium On Inf. Theory Its Applications (ISITA)*, Oct. 2010, pp. 174–178.

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

[12] M. Bellare, S. Tessaro, and A. Vardy, "Semantic security for the wiretap channel," in *Advances in Cryptology – CRYPTO 2012*. Springer Berlin Heidelberg, 2012, pp. 294–311.

[13] J. C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian wiretap channel," in *IEEE Inf. Theory Workshop (ITW)*, Aug. 2010, pp. 1–5.

[14] F. Oggier, J. C. Belfiore, and P. Solé, "Lattice codes for the wiretap Gaussian channel: construction and analysis," *IEEE Trans. on Inf. Theory*, vol. 62, no. 10, pp. 5690–5708, 2016.

[15] A.-M. Ernvall-Hytönen, "On a conjecture by Belfiore and Solé on some lattices," *IEEE Trans. on Inform. Theory*, vol. 58, no. 9, pp. 5950–5955, 2012.

[16] F. Lin and F. Oggier, "A classification of unimodular lattice wiretap codes in small dimensions," *IEEE Trans. on Inf. Theory*, vol. 59, no. 6, pp. 3295–3303, 2013.

[17] ——, "Gaussian wiretap lattice codes from binary self-dual codes," in *IEEE Inf. Theory Workshop (ITW)*, Sept 2012, pp. 662–666.

[18] J. Pinchak, "Wiretap codes: families of lattices satisfying the Belfiore-Solé secrecy function conjecture," in *2013 IEEE International Symposium on Inf. Theory (ISIT)*, Jul. 2013, pp. 2617–2620.

[19] J. Pinchak and B. A. Sethuraman, "The Belfiore-Solé conjecture and a certain technique for verifying it for a given lattice," in *Inf. Theory and Applications Workshop (ITA)*, Feb. 2014, pp. 1–3.

[20] A.-M. Ernvall-Hytönen and B. A. Sethuraman, "Counterexample to the generalized Belfiore-Solé secrecy function conjecture for ℓ-modular lattices," in *IEEE International Symposium on Inf. Theory (ISIT)*, Jun. 2015, pp. 2466–2469.

[21] F. Lin and F. Oggier, "Secrecy gain of Gaussian wiretap codes from 2-and 3-modular lattices," in *IEEE International Symposium on Inf. Theory (ISIT)*, Jul. 2012, pp. 1747–1751.

[22] J. H. Conway and N. J. A. Sloane, *Sphere Packing, Lattices and Groups*. New York: Springer, 1998.

[23] H. Khodaiemehr, D. Kiani, and M.-R. Sadeghi, "LDPC lattice codes for full-duplex relay channels," *IEEE Trans. on Commun.*, vol. 65, no. 2, pp. 536–548, Feb. 2017.

[24] H. Khodaiemehr, M.-R. Sadeghi, and A. Sakzad, "Practical encoder and decoder for power constrained QC LDPC-lattice codes," *IEEE Trans. on Commun.*, vol. 65, no. 2, pp. 486–500, Feb. 2017.

[25] H. Khodaiemehr, M.-R. Sadeghi, and D. Panario, "Construction of full-diversity 1-level LDPC lattices for block-fading channels," in *2016 IEEE International Symposium on Inf. Theory (ISIT)*, Jul. 2016, pp. 2714–2718.

[26] K. Bagheri, M.-R. Sadeghi, T. Eghlidos, and D. Panario, "A secret key encryption scheme based on 1-level QC-LDPC lattices," in *2016 13th International Iranian Society of Cryptology Conference on Information Security and Cryptology (ISCISC)*, Sept. 2016, pp. 20–25.

[27] K. Bagheri, M.-R. Sadeghi, and T. Eghlidos, "An efficient public key encryption scheme based on qc-mdpc lattices," *IEEE Access*, vol. 5, pp. 25 527–25 541, 2017.

[28] G. D. Forney, "Coset codes-part I: introduction and geometrical classification," *IEEE Trans. on Inform. Theory*, vol. 34, no. 5, pp. 1123–1151, 1988.

[29] W. Ebeling, *Lattices and Codes: A Course Partially Based on Lecturers by* F. H*irzebruch*, ser. Advanced Lectures in Mathematics. Springer, Germany, 2013.

[30] W. Kositwattanarerk, S. S. Ong, and F. Oggier, "Construction A of lattices over number fields and block fading wiretap coding," *IEEE Trans. on Inf. Theory*, vol. 61, no. 5, pp. 2273–2282, 2015.

[31] X. Hou and F. Oggier, "Modular lattices from a variation of Construction A over number fields," *Advances in Mathematics of Communications*, vol. 11, no. 4, pp. 719–745, 2017.

[32] I. N. Stewart and D. O. Tall, *Algebraic Number Theory*. Chapman and Hall, 1979.

[33] S. Lang, *Algebraic Number Theory*. Springer-Verlag, 1994.

[34] M. Aliasgari and M.-R. Sadeghi, "An algebraic method for decoding q-ary codes via submodules of $\mathbb{Z}^n$," *IEEE Commun. Letters*, vol. 18, no. 5, pp. 857–860, May 2014.

[35] F. Oggier and E. Viterbo, "Algebraic number theory and code design for Rayleigh fading channels," *Found. Trends Commun. Inf. Theory*, vol. 1, no. 3, pp. 333–415, 2004.

[36] K. Conrad, "Cyclotomic fields," http://www.math.uconn.edu/~kconrad/blurbs/galoistheory/cyclotomic.pdf, [Online; accessed 22-Jan.-2018].

[37] L. C. Washington, *Introduction to Cyclotomic Fields, Volume* 83 *of Graduate Texts in Mathematics*. Springer Science & Business Media, 1997.

[38] J. O. D. Lopes, "The discriminant of subfields of $\mathbb{Q}(\zeta_{2^r})$," *J. of Algebra and Its Applications*, vol. 2, no. 4, pp. 463–469, 2003.

[39] T. P. da Nóbrega Neto, J. C. Interlando, and J. O. D. Lopes, "On computing discriminants of subfields of $\mathbb{Q}(\zeta_{p^r})$," *J. of Number Theory*, vol. 96, no. 2, pp. 319–325, 2002.

[40] R. Chapman, S. T. Dougherty, P. Gaborit, and P. Solé, "2-modular lattices from ternary codes," *J. De Théorie Des Nombres De Bordeaux*, vol. 14, no. 1, pp. 73–85, 2002.

[41] K. S. Chua and P. Solé, "Eisenstein lattices, Galois rings, and theta series," *European J. of Combinatorics*, vol. 25, no. 2, pp. 179–185, 2004.

[42] K. Conrad, "History of class field theory," www.math.uconn.edu/~kconrad/blurbs/gradnumthy/cfthistory.pdf, [Online; accessed 22-Jan.-2018].

[43] J. Milne, "Class field theory, version 4.02," http://www.jmilne.org/math/CourseNotes/cft.html, 2013, [Online; accessed 22-Jan.-2018].

[44] T. R. Shemanske, "An overview of class field theory," https://math.dartmouth.edu/~trs/expository-papers/tex/CFT.pdf, 2000, [Online; accessed 22-Jan.-2018].

[45] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, second edition ed. Springer-Verlag, 1990.

[46] J. S. Leon, V. Pless, and N. J. A. Sloane, "Self-dual codes over $\mathrm{GF}(5)$," *J. of Combinatorial Theory, Series A*, vol. 32, no. 2, pp. 178–194, 1982.