The Secrecy Gain of Formally Unimodular Lattices on the Gaussian Wiretap Channel

Author(s):
Bollauf, Maiara F.; Lin, Hsuan-Yin; Ytrehus, Øyvind

Publication date:
2022-03-02

Permanent link:
https://doi.org/10.3929/ethz-b-000535284

The Secrecy Gain of Formally Unimodular Lattices on the Gaussian Wiretap Channel

Maiara F. Bollauf, Hsuan-Yin Lin, and Øyvind Ytrehus
Simula UiB, N–5008 Bergen, Norway
Emails: {maiara, lin, oyvindy}@simula.no

***Abstract*—We consider lattice coding for the Gaussian wiretap channel, where the challenge is to ensure reliable communication between two authorized parties while preventing an eavesdropper from learning the transmitted messages. Recently, a measure called the *secrecy function* of a lattice coding scheme was proposed as a design criterion to characterize the eavesdropper's probability of correct decision. In this paper, the family of *formally unimodular lattices* is presented and shown to possess the same secrecy function behavior as unimodular and isodual lattices. Based on Construction A, we provide a universal approach to determine the *secrecy gain*, i.e., the maximum value of the secrecy function, for formally unimodular lattices obtained from formally self-dual codes. Furthermore, we show that formally unimodular lattices can achieve higher secrecy gain than the best-known unimodular lattices from the literature.**

I. Introduction

In recent years, *physical layer security* based on information theory has attracted a great deal of attention for secure applications in wireless communications in 5G and beyond (see [1] and references therein). This line of research has evolved from the classical *wiretap channel (WTC) model* introduced by Aaron Wyner in his landmark work [2], which showed that reliable and secure communication can be achieved simultaneously without the need of an additional cryptographic layer on top of the communication protocol.

Since then, substantial research efforts have been devoted to developing practical codes for reliable and secure data transmission over WTCs. Among the potential candidates are *lattices*, where in [3], [4] it was shown that a lattice-based coset encoding approach can provide secure and reliable communication on the Gaussian WTC. In particular, it was shown that for Gaussian WTC, the so-called *secrecy function* expressed in terms of the *theta series* of a lattice (see the precise definition in Section III) can be considered as a quality criterion of good wiretap lattice codes: to minimize the eavesdropper's probability of correct decision, one needs to maximize the secrecy function, and the corresponding maximum value is referred to as *(strong) secrecy gain*.

Belfiore and Solé [5] studied *unimodular* lattices and showed that their secrecy functions have a symmetry point. The value of the secrecy function at this point is called the *weak secrecy gain*. Based on this, the authors of [5] conjectured that for unimodular lattices, the secrecy gain is achieved at the symmetry point of its secrecy function. I.e., the secrecy gain of a unimodular lattice is equivalent to its weak secrecy gain. Finding good unimodular lattices that attain large secrecy gain is of practical importance. In [6], a novel technique was proposed to verify or disprove the Belfiore and Solé conjecture for a given unimodular lattice. Using this method, the conjecture is validated for all known even extremal unimodular lattices in dimensions less than 80. In another work [7], the authors use a similar method as [6] to classify the best unimodular lattices in dimensions from dimensions 8 to 23. For unimodular lattices obtained by Construction A from binary doubly even self-dual codes up to dimensions 40, their secrecy gains are also shown to be achieved at their symmetry points [8].

This work first introduces a new and wider family of lattices, referred to as *formally unimodular lattices*, that consists of lattices having the same theta series as their dual. We then prove that formally unimodular lattices have the same symmetry point as unimodular or isodual lattices. Similar to the feature of formally self-dual codes defined in coding theory, it is expected that such a broader class of lattices can achieve higher secrecy gain than the unimodular lattices. We pursue this expectation via Construction A lattices obtained from formally self-dual codes and give a universal approach to determine their secrecy gain. For formally unimodular lattices obtained by Construction A from even formally self-dual codes, we also provide a sufficient condition to verify Belfiore and Solé's conjecture on the secrecy gain. (A code is called *even* if all of its codewords have even weight, otherwise the code is *odd*.)

Furthermore, we present numerical evidence supporting the conjecture of secrecy gain also for Construction A lattices obtained from *odd* formally self-dual codes. For dimensions up to 70, we note that formally unimodular lattices have better secrecy gain than the best known unimodular lattices described in the literature, e.g., [7]. Apart from finding good formally self-dual codes from the literature, using the code construction by tailbiting the rate $1/2$ convolution codes [9, App. C], we also obtain several formally self-dual codes resulting in high secrecy gains. Due to page limitations, some proofs and detailed discussions are omitted and can be found in the extended version [9].

II. Definitions and Preliminaries

A. Notation

We denote by $\mathbb{Z}$, $\mathbb{Q}$, and $\mathbb{R}$ the set of integers, rationals, and reals, respectively. Vectors are boldfaced, e.g., $\boldsymbol{x}$. Matrices and sets are represented by capital sans serif letters and calligraphic uppercase letters, respectively, e.g., X and $\mathcal{X}$. We use the

customary code parameters $[n, k]$ or $[n, k, d]$ to denote a linear code $\mathscr{C}$ of length n, dimension k, and minimum Hamming distance d. Throughout this paper, we will focus on binary codes only.

B. On Codes and Lattices

Let $\mathscr{C}$ be an $[n, k]$ code and $\mathscr{C}^{\perp} \triangleq \{\boldsymbol{u}\colon \langle \boldsymbol{u}, \boldsymbol{v}\rangle = 0, \forall\, \boldsymbol{v} \in \mathscr{C}\}$. The *weight enumerator* of a code $\mathscr{C}$ is given by

$$W_{\mathscr{C}}(x, y) = \sum_{w=0}^{n} A_w x^{n-w} y^w,$$

where $A_w \triangleq |\{\boldsymbol{c} \in \mathscr{C}\colon w_{\mathrm{H}}(\boldsymbol{c}) = w\}|$. The relation between $W_{\mathscr{C}}(x, y)$ and $W_{\mathscr{C}^{\perp}}(x, y)$ is characterized by the well-known *MacWilliams identity* (see, e.g., [10, Th. 1, Ch. 5]):

$$W_{\mathscr{C}}(x, y) = \frac{1}{2^{n-k}} W_{\mathscr{C}^{\perp}}(x + y, x - y). \tag{1}$$

We have the following families of codes.

Definition 1 (Self-dual, isodual, formally self-dual codes):

- A code $\mathscr{C}$ is said to be *self-dual* if $\mathscr{C} = \mathscr{C}^{\perp}$.
- If there is a permutation π of coordinates such that $\mathscr{C} = \pi(\mathscr{C}^{\perp})$, $\mathscr{C}$ is called *isodual*.
- A code $\mathscr{C}$ is *formally self-dual* if $\mathscr{C}$ and $\mathscr{C}^{\perp}$ have the same weight enumerator, i.e., $W_{\mathscr{C}}(x, y) = W_{\mathscr{C}^{\perp}}(x, y)$.

Clearly, a self-dual code is also isodual, and an isodual code is formally self-dual. Any code in these classes is an $[n, n/2]$ code and, by (1), its weight enumerator $W_{\mathscr{C}}(x, y)$ satisfies [10, eq. (7), p. 599]

$$W_{\mathscr{C}}(x, y) = W_{\mathscr{C}}\left(\frac{x + y}{\sqrt{2}}, \frac{x - y}{\sqrt{2}}\right). \tag{2}$$

A (full rank) *lattice* Λ is a discrete additive subgroup of $\mathbb{R}^n$, which is generated as $\Lambda = \{\boldsymbol{\lambda} = \boldsymbol{u}\mathsf{G}_{n\times n}\colon \boldsymbol{u} = (u_1, \ldots, u_n) \in \mathbb{Z}^n\}$, where the n rows of G form a lattice basis. The *volume* of Λ is $\mathrm{vol}(\Lambda) = |\det(\mathsf{G})|$.

If a lattice Λ have generator matrix G, then the lattice $\Lambda^{\star} \subset \mathbb{R}^n$ generated by $\left(\mathsf{G}^{-1}\right)^{\mathsf{T}}$ is called the *dual lattice* of Λ.

Remark 1: $\mathrm{vol}(\Lambda^{\star}) = \mathrm{vol}(\Lambda)^{-1}$.

For lattices, the analogue of the weight enumerator of a code is the *theta series*.

Definition 2 (Theta series): Let $\Lambda \subset \mathbb{R}^n$ be a lattice, its *theta series* is given by

$$\Theta_{\Lambda}(z) = \sum_{\boldsymbol{\lambda} \in \Lambda} q^{\|\boldsymbol{\lambda}\|^2},$$

where $q \triangleq e^{i\pi z}$ and $\mathrm{Im}\{z\} > 0$.

Analogously, the spirit of the MacWilliams identity can be captured by the *Jacobi's formula* [11, eq. (19), Ch. 4]

$$\Theta_{\Lambda}(z) = \mathrm{vol}(\Lambda^{\star})\left(\frac{i}{z}\right)^{\frac{n}{2}} \Theta_{\Lambda^{\star}}\left(-\frac{1}{z}\right). \tag{3}$$

Note that sometimes the theta series of a lattice can be expressed in terms of the *Jacobi theta functions* defined as follows.

$$\vartheta_2(z) \triangleq \sum_{m\in\mathbb{Z}} q^{\left(m+\frac{1}{2}\right)^2} = \Theta_{\mathbb{Z}+\frac{1}{2}}(z),$$

$$\vartheta_3(z) \triangleq \sum_{m\in\mathbb{Z}} q^{m^2} = \Theta_{\mathbb{Z}}(z), \quad \vartheta_4(z) \triangleq \sum_{m\in\mathbb{Z}} (-q)^{m^2}.$$

In lattice theory, we have similar concepts to self-dual and isodual dual codes. Here, we also introduce *formally unimodular* lattices.

Definition 3 (Unimodular, isodual, formally unimodular lattices): A lattice $\Lambda \subset \mathbb{R}^n$ is said to be *integral* if the inner product of any two lattice vectors is an integer.

- An integral lattice such that $\Lambda = \Lambda^{\star}$ is called *unimodular* lattice.
- A lattice Λ is called *isodual* if it can be obtained from its dual $\Lambda^{\star}$ by (possibly) a rotation or reflection.
- A lattice Λ is *formally unimodular* if it has the same theta series as its dual, i.e., $\Theta_{\Lambda}(z) = \Theta_{\Lambda^{\star}}(z)$.

Remark 2: The relations among unimodular, isodual, and formally unimodular lattices are given as follows.

$$\left\{\Lambda_{\text{unimodular}}\right\} \subset \left\{\Lambda_{\text{isodual}}\right\} \subset \left\{\Lambda_{\text{formally unimodular}}\right\}.$$

Proposition 1: If Λ is formally unimodular, then $\mathrm{vol}(\Lambda) = 1$.

Consequently, unimodular, isodual, and formally unimodular lattices satisfy

$$\Theta_{\Lambda}(z) = \left(\frac{i}{z}\right)^{\frac{n}{2}} \Theta_{\Lambda}\left(-\frac{1}{z}\right). \tag{4}$$

Lattices can be constructed from linear codes through the so called *Construction A*.

Definition 4 (Construction A): Let $\mathscr{C}$ be an $[n, k]$ code, then

$$\Lambda_{\mathrm{A}}(\mathscr{C}) \triangleq \tfrac{1}{\sqrt{2}}(\phi(\mathscr{C}) + 2\mathbb{Z}^n),$$

is a lattice, where $\phi : \mathbb{F}_2^n \to \mathbb{R}^n$ is the natural embedding.

About Construction A lattices obtained from codes over $\mathbb{F}_2$, it is known from [11, p. 183] that

- The volume is $\mathrm{vol}(\Lambda_{\mathrm{A}}(\mathscr{C})) = \frac{2^{n/2}}{|\mathscr{C}|} = 2^{(n-2k)/2}$.
- $\Lambda_{\mathrm{A}}(\mathscr{C}^{\perp}) = \Lambda_{\mathrm{A}}(\mathscr{C})^{\star}$.

A connection between the weight enumerator $W_{\mathscr{C}}(x, y)$ of a code $\mathscr{C}$ and a lattice $\Lambda_{\mathrm{A}}(\mathscr{C})$ can be established.

Lemma 1 ([11, Th. 3, Ch. 7]): Consider an $[n, k]$ code $\mathscr{C}$ with $W_{\mathscr{C}}(x, y)$, then the theta series of $\Lambda_{\mathrm{A}}(\mathscr{C})$ is given by

$$\Theta_{\Lambda_{\mathrm{A}}(\mathscr{C})}(z) = W_{\mathscr{C}}(\vartheta_3(2z), \vartheta_2(2z)).$$

Remark 3: It follows immediately from Lemma 1 that if an $[n, n/2]$ code $\mathscr{C}$ is formally self-dual then $\Lambda_{\mathrm{A}}(\mathscr{C})$ is a formally unimodular lattice.

III. Secrecy Function of a Lattice

In the Gaussian WTC, the same coset encoding idea proposed in Wyner's seminal paper [2] for linear codes can be implemented in a lattice scenario, and here we follow the lattice coding scheme proposed in [4], [5].

In practice, two lattices $\Lambda_{\mathrm{e}} \subset \Lambda_{\mathrm{b}}$ are considered. Λ_{b} is designed to ensure reliability for a legitimate receiver Bob and required to have a good *Hermite parameter* (that measures the highest attainable coding gain of an n-dimensional lattice) [11]. On the other hand, Λ_{e} is aimed to increase the eavesdropper confusion, so it should be chosen such that $P_{c,\mathrm{e}}$, the eavesdropper's success probability of correctly guessing the transmitted message, is minimized. The performance of

the lattice Λ_e is measured in terms of the secrecy gain [4], [5]; to be explained next.

Denote by σ_{e}^2 the variance of the additive Gaussian noise at the eavesdropper's side. Minimizing $P_{c,\mathrm{e}}$ is equivalent to [4] minimizing

$$\sum_{\boldsymbol{r}\in\Lambda_{\mathrm{e}}} e^{-\|\boldsymbol{r}\|^2/2\sigma_e^2} = \Theta_{\Lambda_{\mathrm{e}}}\Big(z \triangleq \frac{i}{2\pi\sigma_{\mathrm{e}}^2}\Big),$$

subject to $\log_2|\Lambda_{\mathrm{b}}/\Lambda_{\mathrm{e}}| = k$. Note that $\mathrm{Im}\{i/2\pi\sigma_{\mathrm{e}}^2\} = \mathrm{Im}\{z\} > 0$, thus we consider only the positive values of $\tau \triangleq -iz = 1/2\pi\sigma_e^2 > 0$ for $\Theta_{\Lambda_{\mathrm{e}}}(z)$. Hence, the scheme is aimed at finding a lattice Λ_{e} such that $\Theta_{\Lambda_{\mathrm{e}}}(z)$ is minimized, which motivates the definition of *secrecy function* below. Note that in [12], it is also argued that minimizing the theta series of Λ_e leads to a small *flatness factor*, a criterion that directly relates to the mutual information leakage to the eavesdropper, instead of the success probability. Therefore, the optimization of $\Theta_{\Lambda_{\mathrm{e}}}(z)$ is of interest in both scenarios.

Definition 5 (Secrecy function and secrecy gain [4, Def. 1 and 2]): Let Λ be a lattice with volume $\mathrm{vol}(\Lambda) = \nu^n$. The secrecy function of Λ is defined by

$$\Xi_\Lambda(\tau) \triangleq \frac{\Theta_{\nu\mathbb{Z}^n}(i\tau)}{\Theta_\Lambda(i\tau)},$$

for $\tau \triangleq -iz > 0$. As maximizing $\Xi_\Lambda(\tau)$ is equivalent to minimizing $\Theta_\Lambda(z)$, the *(strong) secrecy gain* of a lattice is given by $\xi_\Lambda \triangleq \sup_{\tau>0}\Xi_\Lambda(\tau)$.

Ideally, the goal is to determine ξ_Λ. However, since the global maximum of a secrecy function is in general not always easy to calculate, a weaker definition is useful. We start by defining the *symmetry point*.

Definition 6 (Symmetry point): A point $\tau_0 \in \mathbb{R}$ is said to be a *symmetry point* if for all $\tau > 0$,

$$\Xi(\tau_0 \cdot \tau) = \Xi\Big(\frac{\tau_0}{\tau}\Big). \tag{5}$$

Definition 7 (Weak secrecy gain [4, Def. 3]): If the secrecy function of a lattice Λ has a symmetry point τ_0, then the weak secrecy gain χ_Λ is defined as $\chi_\Lambda = \Xi_\Lambda(\tau_0)$.

IV. Weak Secrecy Gain of Formally Unimodular Lattices

This section shows that formally unimodular lattices also hold the same secrecy function properties as unimodular and isodual lattices [4].

Lemma 2: Consider a lattice Λ and its dual $\Lambda^\star$. Then,

$$\Xi_\Lambda(\tau) = \Xi_{\Lambda^\star}\Big(\frac{1}{\tau}\Big). \tag{6}$$

A necessary and sufficient condition for a lattice Λ to achieve the weak secrecy gain at $\tau = 1$ is given as follows.

Theorem 1: Consider a lattice Λ with $\mathrm{vol}(\Lambda) = 1$ and its dual $\Lambda^\star$. Then, Λ achieves the weak secrecy gain at $\tau = 1$, if and only if Λ is formally unimodular.

Proof: By definition, we have

$$\Xi_\Lambda(\tau) = \Xi_\Lambda\Big(\frac{1}{\tau}\Big). \tag{7}$$

Using Lemma 2, it follows from (7) and (6) that

$$\Xi_\Lambda\Big(\frac{1}{\tau}\Big) = \Xi_\Lambda(\tau) = \Xi_{\Lambda^\star}\Big(\frac{1}{\tau}\Big).$$

By Def. 5, this implies that $\Theta_\Lambda(z) = \Theta_{\Lambda^\star}(z)$ for $\mathrm{vol}(\Lambda) = 1$. Conversely, from Def. 3, we see that (6) implies (7). ∎

Note that Theorem 1 holds for isodual lattices as well, which yields to [4, Prop. 1].

Corollary 1: Consider a lattice Λ with $\mathrm{vol}(\Lambda) = \nu^n$ and its dual $\Lambda^\star$. Then, Λ achieves the weak secrecy gain at $\tau = \nu^{-2}$, if and only if $\nu^{-1}\Lambda$ is a formally unimodular lattice.

Equation (5) with $\tau_0 = \nu^{-2}$ holds for a lattice equivalent to its dual. See [4, Prop. 2].

V. Secrecy Gain of Formally Unimodular Lattices

Our goal in this section is to investigate the following conjecture.

Conjecture 1: The secrecy function of a formally unimodular lattice Λ achieves its maximum at $\tau = 1$, i.e., $\xi_\Lambda = \Xi_\Lambda(1)$.

Although we cannot completely prove Conjecture 1, we proceed to study the secrecy gain for formally unimodular lattices obtained from formally self-dual codes via Construction A (see Remark 3). Note that for linear codes, it is known that formally self-dual codes that are not self-dual can outperform self-dual codes in some cases, as they comprise a wider class and hence may allow a better minimum Hamming distance or an overall more favorable weight enumerator. This leads us to look for improved results on the secrecy gain compared to unimodular lattices [6]–[8].

Lemma 3: Consider a Construction A lattice $\Lambda_{\mathrm{A}}(\mathscr{C})$ obtained from a formally self-dual code $\mathscr{C}$. Then, its theta series is equal to

$$\Theta_{\Lambda_{\mathrm{A}}(\mathscr{C})} = \frac{W_{\mathscr{C}}\Big(\sqrt{\vartheta_3^2(z)+\vartheta_4^2(z)}, \sqrt{\vartheta_3^2(z)-\vartheta_4^2(z)}\Big)}{2^{\frac{n}{2}}}.$$

Proof: Using Lemma 1 and the useful identities given in [11, eq. (26), Ch. 4], the theta series $\Theta_{\Lambda_{\mathrm{A}}(\mathscr{C})}$ becomes

$$\begin{aligned}
&\Theta_{\Lambda_{\mathrm{A}}(\mathscr{C})}(z)\\
&\quad= W_{\mathscr{C}}(\vartheta_3(2z), \vartheta_2(2z))\\
&\quad\overset{(a)}{=} W_{\mathscr{C}}\Big(\frac{\vartheta_3(2z)+\vartheta_2(2z)}{\sqrt{2}}, \frac{\vartheta_3(2z)-\vartheta_2(2z)}{\sqrt{2}}\Big)\\
&\quad= W_{\mathscr{C}}\Bigg(\frac{\sqrt{\vartheta_3^2(z)+\vartheta_4^2(z)}+\sqrt{\vartheta_3^2(z)-\vartheta_4^2(z)}}{\sqrt{2}\sqrt{2}},\\
&\qquad\qquad \frac{\sqrt{\vartheta_3^2(z)+\vartheta_4^2(z)}-\sqrt{\vartheta_3^2(z)-\vartheta_4^2(z)}}{\sqrt{2}\sqrt{2}}\Bigg)\\
&\quad= \frac{1}{2^{\frac{n}{2}}} W_{\mathscr{C}}\Bigg(\frac{\sqrt{\vartheta_3^2(z)+\vartheta_4^2(z)}+\sqrt{\vartheta_3^2(z)-\vartheta_4^2(z)}}{\sqrt{2}},\\
&\qquad\qquad \frac{\sqrt{\vartheta_3^2(z)+\vartheta_4^2(z)}-\sqrt{\vartheta_3^2(z)-\vartheta_4^2(z)}}{\sqrt{2}}\Bigg)\\
&\quad\overset{(b)}{=} \frac{1}{2^{\frac{n}{2}}} W_{\mathscr{C}}\Big(\sqrt{\vartheta_3^2(z)+\vartheta_4^2(z)}, \sqrt{\vartheta_3^2(z)-\vartheta_4^2(z)}\Big).
\end{aligned}$$

where (a) and (b) follow from (2). ∎

Lemma 4: Let $s(\tau) \triangleq \vartheta_4(i\tau)/\vartheta_3(i\tau)$. Then, $s(\tau)$ is an increasing function for $\tau > 0$, and $0 < s(\tau) < 1$.

Remark 4: Let $t(\tau) \triangleq s(\tau)^2$. Then, $0 < t(\tau) < 1$ and $t(\tau)$ is also an increasing function for $\tau > 0$. Hence, according to Lemma 4, given any $t \in (0,1)$, there always exists a unique $\tau > 0$ such that $t(\tau) = \vartheta_4^2(i\tau)/\vartheta_3^2(i\tau)$. Moreover, we have $t(1) = 1/\sqrt{2}$ by using the identity of $\vartheta_3(i) = 2^{1/4}\vartheta_4(i)$ from [13].

Due to Remark 4, Lemma 3, and the fact that $\Theta_{\mathbb{Z}^n}(z) = \vartheta_3^n(z)$, now we are able to give a new universal approach to derive the strong secrecy gain of a Construction A lattice obtained from formally self-dual codes.

Theorem 2: Let $\mathscr{C}$ be a formally self-dual code. Then

$$\big[\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)\big]^{-1} = \frac{W_{\mathscr{C}}\big(\sqrt{1+t(\tau)}, \sqrt{1-t(\tau)}\big)}{2^{\frac{n}{2}}},$$

where $0 < t(\tau) = \vartheta_4^2(i\tau)/\vartheta_3^2(i\tau) < 1$. Moreover, define $f_{\mathscr{C}}(t) \triangleq W_{\mathscr{C}}(\sqrt{1+t}, \sqrt{1-t})$ for $0 < t < 1$. Then, maximizing the secrecy function $\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$ is equivalent to determining the minimum of $f_{\mathscr{C}}(t)$ on $t \in (0,1)$.

Example 1: Consider a $[6,3,3]$ odd formally self-dual code $\mathscr{C}$ with $W_{\mathscr{C}}(x,y) = x^6 + 4x^3y^3 + 3x^2y^4$ [14]. Thus $f_{\mathscr{C}}(t) = W_{\mathscr{C}}(\sqrt{1+t}, \sqrt{1-t}) = 4[1 + t^3 + (1-t^2)^{3/2}]$ and $f'_{\mathscr{C}}(t) = 12t(t - \sqrt{1-t^2})$. Observe that for $0 < t < 1/\sqrt{2}$, we have $\sqrt{1-t^2} > 1/\sqrt{2}$. Then, $t - \sqrt{1-t^2} < 1/\sqrt{2} - 1/\sqrt{2} = 0$. This indicates that the derivative $f'_{\mathscr{C}}(t) < 0$ on $t \in (0, 1/\sqrt{2})$. Similarly, one can also show that $f'_{\mathscr{C}}(t) > 0$ on $t \in (1/\sqrt{2}, 1)$, and $t = 1/\sqrt{2}$ is the minimum of $f_{\mathscr{C}}(t)$. Hence, Remark 4 and Theorem 2 indicate that the maximum of $\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$ is achieved at $\tau = 1$. Also, one can get $\xi_{\Lambda_{\mathrm{A}}(\mathscr{C})} \approx 1.172$. $\Diamond$

Using Gleason's Theorem [15, Th. 9.2.1], an expression of $f_{\mathscr{C}}(t)$ can be shown if $\mathscr{C}$ is an even formally self-dual code.

Lemma 5: If $\mathscr{C}$ is an $[n, n/2]$ even formally self-dual codes, then we have

$$f_{\mathscr{C}}(t) = 2^{\frac{n}{2}} \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r (t^4 - t^2 + 1)^r, \tag{8}$$

where $a_r \in \mathbb{Q}$ and $\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r = 1$.

Next, we provide a sufficient condition for a Construction A formally unimodular lattice obtained from even formally self-dual codes to achieve the strong secrecy gain at $\tau = 1$, or, equivalently, $t = 1/\sqrt{2}$.

Theorem 3: Consider $n \geq 8$ and an $[n, n/2]$ even formally self-dual code $\mathscr{C}$. If the coefficients a_r of $f_{\mathscr{C}}(t)$ expressed in terms of (8) satisfy

$$\sum_{r=1}^{\lfloor \frac{n}{8} \rfloor} r a_r \Big(\frac{3}{4}\Big)^{r-1} > 0, \tag{9}$$

then the secrecy gain of $\Lambda_{\mathrm{A}}(\mathscr{C})$ is achieved at $\tau = 1$.

To prove this theorem, it is sufficient to show that the function $f_{\mathscr{C}}(t)$ as in (8) defined for $0 < t < 1$ achieves its minimum at $t = 1/\sqrt{2}$. The detailed proof is given in [9].

Example 2: Consider an $[18, 9, 6]$ even formally self-dual code $\mathscr{C}$ with

$$W_{\mathscr{C}}(x,y) = x^{18} + 102x^{12}y^6 + 153x^{10}y^8 + 153x^8y^{10} + 102x^6y^{12} + y^{18}.$$

By solving $f_{\mathscr{C}}(t) = W_{\mathscr{C}}(\sqrt{1+t}, \sqrt{1-t})$ with (8) (see the details of derivation provided in [9, App. B]), we find that $a_0 = -29/16, a_1 = 27/8$ and $a_2 = -9/16$. The condition (9) in Theorem 3 for those coefficients is satisfied since $27/8 - 27/32 = 81/32 > 0$. Thus, the secrecy gain conjecture is true for the formally unimodular lattice $\Lambda_{\mathrm{A}}(\mathscr{C})$. $\Diamond$

VI. Numerical Results

Even though the result of Theorem 3 is restricted to formally unimodular lattices obtained from even formally self-dual codes, we have numerical evidence showing that Conjecture 1 also holds for formally unimodular lattices obtained from odd formally self-dual codes. The secrecy gains of some formally unimodular Construction A lattices obtained from (even and odd) formally self-dual codes are summarized in Table I. Note that all codes have the parameters $[n, n/2]$ and the superscript "(d)" refers to the minimum Hamming distance d of the code. Their exact weight enumerators can be found in [9, App. D]. The highlighted values represent the best values found in the respective dimensions, when comparing self-dual (sd), even and odd formally self-dual (efsd and ofsd) codes.

Remark 5: We remark the following about Table I:

- "[·]" indicates the reference number.
- We use the sufficient condition (9) in Theorem 3 for the even codes and the numerical derivative analysis with Wolfram Mathematica [25] for the odd codes to confirm the strong secrecy gain in Table I.
- For most dimensions $n > 8$, the secrecy gain of formally unimodular lattices that are not unimodular outperform the unimodular lattices (obtained from self-dual codes), presented in [7, Tables I and II]. In some cases (*e.g.* [12,6], [22,11]) we were unable to find good efsd codes with different secrecy gains form the sd codes. Also, to highlight the comparison with unimodular lattices, the second column refers to the upper bound on the secrecy gain of unimodular lattices obtained from Construction A in [16, Tab. III] and not all of the values are known to be achieved. Gains can be observed in dimensions $10, 12, 14, 20$, and 22.
- It is known that the well-known Barnes-Wall lattice BW_{32} achieves the secrecy gain of $64/9 \approx 7.11$ [4, Sec. IV-C], which is better than all the tabulated values in dimension 32. However, because BW_{32} is not obtained via Construction A, we did not address the details here.
- Observe that for codes of length 40, the self-dual code in the table is a Type I (weights divisible by two), as it presents a higher secrecy gain ($\xi_{\Lambda_{\mathrm{A}}(\mathscr{C}_{\mathrm{sd}})} \approx 12.191$) compared to the Type II (weights divisible by four) ($\xi_{\Lambda_{\mathrm{A}}(\mathscr{C}_{\mathrm{sd}})} \approx 11.977$). The same happens with codes of length 32 and this confirms the advantage of this approach as to the results in [8].
- Formally self-dual (isodual) codes without references in Table I are constructed by tailbiting the rate $1/2$ convolutional codes. Details can be found in [9, App. C].

TABLE I
COMPARISON OF (STRONG) SECRECY GAINS FOR SEVERAL VALUES OF EVEN DIMENSIONS n. CODES WITHOUT REFERENCES ARE OBTAINED BY TAILBITING THE RATE $1/2$ CONVOLUTIONAL CODES.

n	Upper bound [16]	$\mathscr{C}_{\text{sd}}^{(d)}$	$\xi_{\Lambda_{\text{A}}(\mathscr{C}_{\text{sd}})}$	$\mathscr{C}_{\text{efsd}}^{(d)}$	$\xi_{\Lambda_{\text{A}}(\mathscr{C}_{\text{efsd}})}$	$\mathscr{C}_{\text{ofsd}}^{(d)}$	$\xi_{\Lambda_{\text{A}}(\mathscr{C}_{\text{ofsd}})}$
6	1	–	–	$\mathscr{C}_{\text{efsd}}^{(2)}$ [15]	1	$\mathscr{C}_{\text{ofsd}}^{(3)}$ [14]	$\mathbf{1.172}$
8	1.33	$\mathscr{C}_{\text{sd}}^{(4)}$ [15]	$\mathbf{1.333}$	–	–	$\mathscr{C}_{\text{ofsd}}^{(3)}$ [14]	1.282
10	1.45	–	–	$\mathscr{C}_{\text{efsd}}^{(4)}$ [17]	1.455	$\mathscr{C}_{\text{ofsd}}^{4}$ [14]	$\mathbf{1.478}$
12	1.6	$\mathscr{C}_{\text{sd}}^{(4)}$ [7]	1.6	$\mathscr{C}_{\text{efsd}}^{(4)}$ [18]	1.6	$\mathscr{C}_{\text{ofsd}}^{(4)}$ [14]	$\mathbf{1.657}$
14	1.78	$\mathscr{C}_{\text{sd}}^{(4)}$ [7]	1.778	$\mathscr{C}_{\text{efsd}}^{(4)}$ [18]	1.825	$\mathscr{C}_{\text{ofsd}}^{(4)}$ [14]	$\mathbf{1.875}$
16	2.21	$\mathscr{C}_{\text{sd}}^{(4)}$ [7]	2	$\mathscr{C}_{\text{efsd}}^{(4)}$ [19]	2.133	$\mathscr{C}_{\text{ofsd}}^{(5)}$ [14]	$\mathbf{2.141}$
18	2.49	$\mathscr{C}_{\text{sd}}^{(4)}$ [7]	2.286	$\mathscr{C}_{\text{efsd}}^{(6)}$ [20]	$\mathbf{2.485}$	$\mathscr{C}_{\text{ofsd}}^{(5)}$	2.427
20	2.81	$\mathscr{C}_{\text{sd}}^{(4)}$ [7]	2.667	$\mathscr{C}_{\text{efsd}}^{(6)}$ [21]	2.813	$\mathscr{C}_{\text{ofsd}}^{(6)}$ [18]	$\mathbf{2.868}$
22	3.2	$\mathscr{C}_{\text{sd}}^{(6)}$ [7]	3.2	$\mathscr{C}_{\text{efsd}}^{(6)}$	3.2	$\mathscr{C}_{\text{ofsd}}^{(7)}$ [14]	$\mathbf{3.335}$
30	5.84	$\mathscr{C}_{\text{sd}}^{(6)}$ [22]	5.697	$\mathscr{C}_{\text{efsd}}^{(8)}$ [23]	$\mathbf{5.843}$	$\mathscr{C}_{\text{ofsd}}^{(7)}$	5.785
32	7.00	$\mathscr{C}_{\text{sd}}^{(8)}$ [22]	6.737	$\mathscr{C}_{\text{efsd}}^{(8)}$	$\mathbf{6.748}$	$\mathscr{C}_{\text{ofsd}}^{(7)}$	6.628
40	12.81	$\mathscr{C}_{\text{sd}}^{(8)}$ [22]	12.191	$\mathscr{C}_{\text{efsd}}^{(8)}$	12.134	$\mathscr{C}_{\text{ofsd}}^{(9)}$	$\mathbf{12.364}$
70	130.15	$\mathscr{C}_{\text{sd}}^{(12)}$ [24]	127.712	$\mathscr{C}_{\text{efsd}}^{(12)}$	128.073	$\mathscr{C}_{\text{ofsd}}^{(13)}$	$\mathbf{128.368}$

VII. CONCLUSION

This paper introduced the *formally unimodular lattices*, a new class consisting of lattices having the same theta series as their dual. We showed some properties of formally unimodular lattices and their secrecy function behavior in the Gaussian WTC. Furthermore, we investigated Construction A lattices obtained from formally self-dual codes and gave a universal approach to determine their secrecy gain. We found formally unimodular lattices of better secrecy gain than the best known unimodular lattices from the literature.

REFERENCES

[1] Y. Wu, A. Khisti, C. Xiao, G. Caire, K.-K. Wong, and X. Gao, "A survey of physical layer security techniques for 5G wireless networks and challenges ahead," *IEEE J. Sel. Areas Commun.*, vol. 36, no. 4, pp. 679–695, Apr. 2018.

[2] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.

[3] J.-C. Belfiore and F. Oggier, "Secrecy gain: A wiretap lattice code design," in *Proc. IEEE Int. Symp. Inf. Theory Appl. (ISITA)*, Taichung, Taiwan, Oct. 17–20, 2010.

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

[5] J.-C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian wiretap channel," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Dublin, Ireland, Aug. 30 – Sep. 3, 2010.

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

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

[8] J. Pinchak, "Wiretap codes: Families of lattices satisfying the Belfiore-Solé secrecy function conjecture," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Istanbul, Turkey, Jul. 7–12, 2013, pp. 2617–2620.

[9] M. F. Bollauf, H.-Y. Lin, and Ø. Ytrehus, "The secrecy gain of formally unimodular lattices on the Gaussian wiretap channel," Oct. 2021, arXiv:2111.01439v1 [cs.IT]. [Online]. Available: https://arxiv.org/abs/2111.01439

[10] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-Correcting Codes*. Amsterdam, The Netherlands: North-Holland, 1977.

[11] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer, 1999.

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

[13] E. W. Weisstein, "Jacobi theta functions," From MathWorld—A Wolfram Web Resource. [Online]. Available: https://mathworld.wolfram.com/JacobiThetaFunctions.html

[14] K. Betsumiya and M. Harada, "Binary optimal odd formally self-dual codes," *Des., Codes Cryptography*, vol. 23, no. 1, pp. 11–21, 2001.

[15] W. C. Huffman and V. Pless, *Fundamentals of Error-Correcting Codes*. Cambridge, U.K.: Cambridge University Press, jun 2003.

[16] F. Lin and F. Oggier, "Gaussian wiretap lattice codes from binary self-dual codes," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Lausanne, Switzerland, Sep. 3–7, 2012.

[17] G. T. Kennedy and V. Pless, "On designs and formally self-dual codes," *Des., Codes Cryptography*, vol. 4, no. 1, pp. 43–55, 1994.

[18] K. Betsumiya, T. A. Gulliver, and M. Harada, "Binary optimal linear rate $1/2$ codes," in *Proc. Appl. Algebra, Algebr. Algorithms Error-Correcting Codes (AAECC)*, Honolulu, HI, USA, Nov. 15–19, 1999, pp. 462–471.

[19] K. Betsumiya and M. Harada, "Classification of formally self-dual even codes of lengths up to 16," *Des., Codes Cryptography*, vol. 23, no. 3, pp. 325–332, 2001.

[20] N. J. A. Sloane and N. Heninger, *The On-Line Encyclopedia of Integer Sequences*, OEIS Foundation Inc., Jun. 2006. [Online]. Available: http://oeis.org/A123456

[21] J. E. Fields, P. Gaborit, W. C. Huffman, and V. Pless, "On the classification of extremal even formally self-dual codes of lengths 20 and 22," *Discrete Appl. Math.*, vol. 111, no. 1-2, pp. 75–86, Jul. 2001.

[22] J. H. Conway and N. J. A. Sloane, "A new upper bound on the minimal distance of self-dual codes," *IEEE Trans. Inf. Theory*, vol. 36, no. 6, pp. 1319–1333, Nov. 1990.

[23] S. Bouyuklieva and I. Bouyukliev, "Classification of the extremal formally self-dual even codes of length 30," *Adv. Math. Commun.*, vol. 4, no. 3, pp. 433–439, 2010.

[24] M. Harada, "The existence of a self-dual $[70, 35, 12]$ code and formally self-dual codes," *Finite Fields Th. App.*, vol. 3, no. 2, pp. 131–139, Apr. 1997.

[25] Wolfram Research, Inc., "Mathematica, Version 12.3.1," champaign, IL, 2021. [Online]. Available: https://www.wolfram.com/mathematica