On the Secrecy Gain of Isodual Lattices from Tail-Biting Convolutional Codes

Palma Persson, Maiara F. Bollauf, Hsuan-Yin Lin, and Øyvind Ytrehus
Simula UiB, N–5006 Bergen, Norway
Emails: palma.rud.persson@gmail.com, {maiara, lin, oyvindy}@simula.no

***Abstract*—The secrecy gain of Construction A isodual lattices obtained from rate 1/2 binary tail-biting convolutional codes is considered. The secrecy gain criterion has been proposed in lattice coding for the Gaussian wiretap channel to characterize the secrecy-goodness performance. The higher the secrecy gain, the smaller the eavesdropper's success probability of correctly guessing the transmitted message. This work performs exhaustive code searches for even lengths up to 108 to find the best isodual codes obtained from rate 1/2 binary tail-biting convolutional codes of certain memory constraints in terms of secrecy gain and investigates the corresponding isodual lattices. Numerical results indicate that the best results found via this tail-biting technique perform similarly to the best-known isodual codes from the conventional pure double-circulant code construction up to length 40. This approach offers two advantages: (1) it provides reasonably good codes of "any" even lengths, and (2) practical maximal-likelihood decoding is available for these codes.**

I. Introduction

In the communication model of a wiretap channel [1], a single party named Alice wants to communicate with another party named Bob while keeping the transmitted messages secure from an unauthorized eavesdropper, Eve. For the Gaussian wiretap channel, it was shown that a lattice-based coset coding approach could provide secure and reliable communication [2], [3]. In particular, given a lattice Λ_b designed for Bob, to achieve security, one needs to design a lattice wiretap code ($\Lambda_\mathrm{e} \subseteq \Lambda_\mathrm{b}$) such that Eve's success probability of correctly guessing the transmitted message, $P_{\mathrm{c,e}}$, is minimized. A design criterion called *secrecy gain* [2] has been proposed and shown to be inversely proportional to the upper bound on $P_{\mathrm{c,e}}$.

The secrecy gain is the maximum attainable value of a *secrecy function*, which is determined by the lattice Λ_e's *theta series* and volume. The secrecy gain study has recently been extended to the so-called *formally unimodular lattices*, or lattices with the same theta series as their duals [4], [5]. It was shown that formally unimodular lattices share the same secrecy function property with *unimodular* and *isodual* lattices, i.e., they all have *symmetry points* in their secrecy functions. Thus, formally unimodular, isodual, and unimodular lattices are all conjectured to achieve the secrecy gain at the symmetry points of their secrecy functions [2]–[5]. Moreover, it is shown that Construction A lattices obtained from the *formally self-dual codes* (which have the same weight enumerator as their duals, including isodual codes) can achieve a higher secrecy gain than the unimodular lattices. The secrecy gain of Construction A_4 formally unimodular lattices obtained from codes over the integers modulo 4 has also been studied in [6], [7].

In [5], a systematic approach by *tail-biting (TB)* the rate $1/2$ binary convolutional codes of a given memory to construct isodual codes was proposed. Such binary codes are referred to as *TB isodual codes*. To obtain the secrecy gain of Construction A lattices obtained from isodual codes, the calculation of the codes' weight enumerators is necessary, and long-length good isodual codes in terms of secrecy gain may be hard to determine via classical algebraic approaches. TB isodual codes were considered, and their weight enumerators can be obtained with low-complexity trellis computation even for large code lengths. High secrecy gains of the Construction A lattices obtained from TB isodual codes were demonstrated. This paper further investigates the *best* TB isodual codes and presents the following contributions:

- We have performed exhaustive and efficient code searches to find the best secrecy-good TB isodual codes for different memory constraints for even lengths up to 108.
- Numerical results are presented to demonstrate that the best secrecy-good TB isodual codes are comparable (and often coincide) with the best isodual codes obtained from the conventional pure double circulant code (PDCC) construction for all even lengths up to 40. While performing an exhaustive PDCC search is computationally expensive for lengths greater than 40, a complete code search of TB isodual codes with a moderate complexity can be accomplished quickly up to length 108.
- A necessary condition to verify the secrecy-optimality of a Construction A lattice obtained from a formally self-dual $\mathscr{C}$ of a given length n by considering its weight enumerator was provided in [5, Th. 46]. This condition is verified for the best secrecy-good codes compared to all the possible even-length TB and PDCC isodual codes. All the best ones in Table I are checked to satisfy the necessary condition.

The paper is organized as follows: Sec. II recalls general definitions about codes, lattices, and TB convolutional codes, Sec. III presents the main results about the calculation of the secrecy gain for Construction A lattices, Sec. IV describes the search for secrecy-good TB lattices and finally, Sec. V discusses the main results and improvements of our search.

This work was supported in part by the Norwegian Research Council through the qsIoT grant, project number 274889.

979-8-3503-2611-6/23/.00

II. Definitions and Preliminaries

A. Notation

We denote by $\mathbb{N}$, $\mathbb{Z}$, and $\mathbb{R}$ the set of naturals, integers, and reals, respectively. $[i:j] \triangleq \{i, i+1, \ldots, j\}$ for $i, j \in \mathbb{Z}$, $i \leq j$. Vectors are *row* vectors and boldfaced, e.g., $\boldsymbol{x}$. The all-zero vector is denoted by $\mathbf{0}$. Matrices and sets are represented by capital sans serif letters and calligraphic uppercase letters, respectively, e.g., X and $\mathcal{X}$. $\mathsf{X}_{k\times n}$ represents a matrix of size $k \times n$, and a square matrix of size n is denoted by X_n. An identity matrix is denoted by I. We denote by $w_{\mathrm{H}}(\boldsymbol{x})$ the *Hamming* weight of a vector $\boldsymbol{x} \in \{0,1\}^n$. We use the code parameters $[n,k]$ or $[n,k,d_{\mathrm{H}}]$ to denote a linear code $\mathscr{C}$ of length n, dimension k, and minimum Hamming distance. $\phi\colon \{0,1\}^n \to \mathbb{Z}^n$ is defined as the natural embedding, i.e., $\phi(x)$ maps each element $x \in \{0,1\}$ to the corresponding integer.

B. Basics on Codes and Lattices

This section briefly reviews well-known concepts related to codes and lattices.

The *weight enumerator* of a $[n,k]$ binary code $\mathscr{C}$ is

$$W_{\mathscr{C}}(x,y) = \sum_{\boldsymbol{c}\in\mathscr{C}} x^{n-w_{\mathrm{H}}(\boldsymbol{c})} y^{w_{\mathrm{H}}(\boldsymbol{c})}.$$

A $[2k,k]$ binary code $\mathscr{C}$ is a *pure double circulant code (PDCC)* if it is generated by $\mathsf{G} = (\mathsf{I}_k \ \mathsf{B}_k)$, where B_k is a circulant matrix

$$\mathsf{B}_k = \begin{pmatrix} b_1 & b_2 & \ldots & b_k \\ b_k & b_1 & \ldots & b_{k-1} \\ \vdots & \vdots & \ldots & \vdots \\ b_2 & b_3 & \ldots & b_1 \end{pmatrix}.$$

A (full rank) *lattice* $\Lambda \subset \mathbb{R}^n$ is a discrete additive subgroup of $\mathbb{R}^n$, which can be represented as $\Lambda = \{\boldsymbol{\lambda} = \boldsymbol{u}\mathsf{L}_n \colon \boldsymbol{u} \in \mathbb{Z}^n\}$, where the n rows of $\mathsf{L} = \mathsf{L}_n$ form a lattice basis in $\mathbb{R}^n$. The *volume* of Λ is $\mathrm{vol}(\Lambda) = |\det(\mathsf{L})|$. The lattice $\Lambda^\star \subset \mathbb{R}^n$ generated by $\left(\mathsf{L}^{-1}\right)^{\mathsf{T}}$ is called the *dual lattice* of Λ. For lattices, the analog of the weight enumerator of a code is the *theta series*, defined as follows.

Definition 1 (Theta series): Let Λ 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* [8, eq. (19), Ch. 4]

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

A lattice 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 a *unimodular* lattice. A lattice Λ is called *isodual* if it can be obtained from its dual $\Lambda^\star$ by (possibly) a rotation or reflection. In [4], a new and broader family was presented, namely, the *formally unimodular lattices*, that consists of lattices having the same theta series as their duals, i.e., $\Theta_\Lambda(z) = \Theta_{\Lambda^\star}(z)$.

From [5, Prop. 12], a formally unimodular lattice Λ has $\mathrm{vol}(\Lambda) = 1$. Hence, the theta series of a formally unimodular lattice is such that

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

Lattices can be constructed from binary linear codes via the so-called Construction A [8], defined as follows.

Definition 2 (Construction A): Let $\mathscr{C}$ be a binary $[n,k]$ code, then $\Lambda_{\mathrm{A}}(\mathscr{A}) \triangleq \frac{1}{\sqrt{2}}(\phi(\mathscr{C}) + 2\mathbb{Z}^n)$ is a lattice.

C. TB Convolutional Codes

An (n,k) binary convolutional code $\mathcal{C}$ of memory m is a k-dimensional subspace of $\mathbb{F}_2^n(D)$, where D is an indeterminate variable. $\mathbb{F}_2(D)$ consists of all rational functions in D, such that the maximum degree of the generator polynomials of $\mathscr{C}$ is m. Hence, a rate k/n *convolutional code* is a linear mapping

$$\begin{aligned} \gamma : \mathbb{F}_2^k(D) &\to \mathbb{F}_2^n(D) \\ \boldsymbol{u}(D) &\mapsto \boldsymbol{v}(D) = \boldsymbol{u}(D)\mathsf{G}(D), \end{aligned}$$

where $\mathsf{G}(D)$ is a generator matrix with rank k with entries in $\mathbb{F}_2(D)$.

One technique to construct a block code from a convolutional code is *tail-biting* [9], [10], which we define next. Consider a convolutional code of rate $1/2$ and a given memory m. Let $\mathcal{C}_0$ be the $[2\ell, \ell - m]$ block code consisting of all codewords of $\mathcal{C}$ obtained by traversing the trellis [10] of $\mathcal{C}$, collecting code symbols from trellis edge labels along the way, starting at time 0 in state 0 of the trellis and ending in state 0 at time ℓ. Similarly, for each of the $2^m - 1$ nonzero states s, let $\mathcal{C}_s$ be the set of sequences obtained by traversing the trellis from state s at time 0 to state s at time ℓ. The set $\mathscr{C} = \cup_{s=0}^{2^m} \mathcal{C}_s$ is a $[2\ell, \ell]$ linear block code, known as a *tail-biting (TB) code*. By a *tail-biting (TB) lattice*, we mean a lattice obtained by Construction A from a TB code.

III. Secrecy Gain of Construction A Lattices

This section presents a secrecy goodness criterion called *secrecy gain* [3]. It quantifies the success probability of an eavesdropper to guess the correct information sent on a wiretap channel when a lattice Λ is chosen in the coset encoding, which works as follows: a pair of nested lattices $\Lambda_{\mathrm{e}} \subseteq \Lambda_{\mathrm{b}}$ is selected, and the lattice Λ_{b} for Bob is written as the union of 2^k disjoint cosets $\Lambda_{\mathrm{b}} = \cup_{j=1}^{2^k} \left(\Lambda_{\mathrm{e}} + \boldsymbol{c}_j\right)$. The information vector or message $\boldsymbol{s} \in \{0,1\}^k$ is mapped into $\boldsymbol{s} \mapsto \Lambda_{\mathrm{e}} + \boldsymbol{c}_j(\boldsymbol{s})$ and Alice chooses a random point $\boldsymbol{x} \in \Lambda_{\mathrm{e}} + \boldsymbol{c}_j(\boldsymbol{s})$ to send over the wiretap channel. More details on the error probability analysis can be found at [3, App. A] or [5, Sec. IV-B].

Definition 3 (Secrecy function and secrecy gain [3, Defs. 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 $\tau \triangleq -iz > 0$. The *(strong) secrecy gain* of a lattice is given by $\xi_\Lambda \triangleq \sup_{\tau>0} \Xi_\Lambda(\tau)$.

The higher the secrecy gain of a lattice, the more secure the lattice wiretap code is [3]. Hence, the objective is to design good lattices to achieve a high secrecy gain. The first family of lattices studied in the literature was unimodular lattices [11], [12] due to the tractability of their theta functions. Also, for unimodular lattices, Belfiore and Solé conjectured that the following holds.

Conjecture 1 ([4], [13]): The secrecy function of a unimodular lattice attains its maximum at $\tau = 1$.

This result was demonstrated to hold for infinitely many unimodular lattices [14]. Recently, techniques to extend this result to formally unimodular lattices constructed from binary and quaternary codes were discussed in [4], [6], [7], together with indications of superior results for the secrecy gain, when compared to unimodular lattices.

The following result facilitates the maximization of the secrecy function for lattices Λ obtained via Construction A from formally self-dual codes.

Theorem 1 ([4, Th. 2]): Let $\mathscr{C}$ be a formally self-dual code (including the isodual code). Then

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

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 $0 < t < 1$.

Theorem 1 implies that maximizing the secrecy function $\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$ is equivalent to determining the minimum of $f_{\mathscr{C}}(t)$ on $t \in (0,1)$. This optimization process can also be interpreted as a function of the weight enumerator of the code $\mathscr{C}$.

We have observed that in practice, all Construction A formally unimodular lattices we studied achieve its strong secrecy gain at $t = {1}/{\sqrt{2}}$. Furthermore, to investigate the best secrecy-good formally self-dual codes that maximize the secrecy gain of a given dimension, we use the secrecy function $\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$ to give a slightly weaker definition of a secrecy-optimal formally self-dual code.

Definition 4 ([5, Def. 45]): A formally self-dual code $\mathscr{C}^\diamond$ of length n is said to be (weakly) secrecy-optimal if for all $\tau > 0$,

$$\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C}^\diamond)}(\tau) \geq \Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$$

for any formally self-dual code $\mathscr{C}$ of length n.

A necessary condition for a formally self-dual code/isodual code $\mathscr{C}$ to be secrecy-optimal by considering its weight distribution $\{A_w(\mathscr{C})\}_{w=0}^n$ was given in [5, Thm. 46].

Theorem 2 ([5, Th. 46]): Given a dimension $n \geq 2$, if $\mathscr{C}^\diamond$ is secrecy-optimal, then

$$\mathscr{C}^\diamond = \underset{\mathscr{C}\,:\text{ formally self-dual}}{\operatorname{argmin}} \left\{ \sum_{w=0}^{n} \frac{A_w(\mathscr{C})}{w+1} \right\}. \tag{1}$$

Theorem 2 suggests that in order to exactly determine the secrecy-optimal code $\mathscr{C}^\diamond$ of a given length, one can check if $\mathscr{C}^\diamond$ satisfies (1) compared to all the possible weight enumerators of formally self-dual codes.

Algorithm 1: Computing the weight enumerators and secrecy gains of TB codes. $W_{\ell,w}^{\text{total}}$ is the number of codewords of length 2ℓ and weight w in the TB code. $W_{\ell,s,w}$ is the number of paths of length ℓ and weight w, starting and ending in state s.

for *each* $(2,1)$ *convolutional code* $\mathcal{C}$ **do**
  Find weight enumerator:
  Initialize $W_{\ell,w}^{\text{total}} = 0$, $\forall\, \ell = 1, 2, \ldots, \texttt{MaxDim}$, $\forall\, w$
  for *each state* s *(among* 2^m *states)* **do**
    Use the Viterbi algorithm to compute $W_{\ell,s,w}$ for $\ell = 1, 2, \ldots, \texttt{MaxDim}$, $w \leq 2\ell$
    $W_{\ell,w}^{\text{total}} = W_{\ell,w}^{\text{total}} + W_{\ell,s,w}, \forall\, \ell, 0 \leq w \leq 2\ell$
  end
  For each dimension ℓ, the TB code $\mathscr{C}_\ell$ has:
  $W_{\mathscr{C}_\ell}(x,y) = \sum_{w=0}^{2\ell} W_{\ell,w}^{\text{total}} x^{2\ell-w} y^w$.
  Compute secrecy gain (Theorem 1)
  Select best code for each ℓ
end

IV. Secrecy-good Construction A lattices obtained from TB codes

This work extends and improves on what was initially proposed in [5]. We present here an efficient and complete search for secrecy-good Construction A lattices obtained from TB codes, the TB lattices, which allows the extension to higher dimensions. The techniques implemented here allow us, by taking into account the structure of TB convolutional codes, to exhaustively search for the best codes (resp. lattices) of each length (resp. dimension) and therefore, present the best achievable secrecy gain. The current results outperform the secrecy gains obtained previously in some dimensions. Observe that here, we only consider formally unimodular lattices in even dimensions.

One important property we highlight is that $(2,1)$ TB codes are isodual, allowing us to apply Theorem 1 for the search of secrecy-good TB lattices. Proposition 1 states this property.

Proposition 1 ([5, Prop. 50]): Consider a $(2,1)$ binary convolutional code with memory m. Then, any $[2\ell, \ell]$ binary linear (block) code $\mathscr{C}$ obtained from it is isodual, for $\ell \geq m+1$.

Therefore, the remaining task of the search for secrecy-good TB lattices is to characterize the weight enumerator of TB convolutional codes. Algorithm 1 summarizes this procedure, which uses the Viterbi algorithm (for more details, see [10, Sec. 12.3]) for computing the weight enumerator $W_{\mathscr{C}_\ell}(x,y)$ for each even TB code length 2ℓ. Based on $W_{\mathscr{C}_\ell}(x,y)$, we calculate $\Xi_{\Lambda_{\mathrm{A}}(\mathscr{C})}(\tau)$ at $t = {1}/{\sqrt{2}}$ according to Theorem 1 and verify the minimization of $f_{\mathscr{C}}(t)$ on $t \in (0,1)$. Finally, the best secrecy-good TB code is determined over all possible TB generator matrices. Codes yielding the best secrecy gains for even lengths $12 \leq n \leq 40$ are tabulated in Table I.

V. Results and analysis

One approach to finding TB codes with good secrecy gain is to start with codes with good distance properties, that

TABLE I
COMPARISON OF (STRONG) SECRECY GAINS FOR SEVERAL VALUES OF EVEN DIMENSIONS n.

n	Upper bound for unimodular lattices [11]	$\xi_{\Lambda_A(\mathscr{C})}$[5]	PDCC	$m=3$	$m=4$	$m=5$	$m=6$
12	1.60	**1.657**	**1.657**	**1.657**	**1.657**	**1.657**	**1.657**
14	1.78	**1.875**	1.828	1.828	1.828	1.828	1.828
16	2.21	**2.141**	**2.141**	**2.141**	**2.141**	**2.141**	**2.141**
18	2.49	**2.485**	**2.485**	**2.485**	**2.485**	**2.485**	**2.485**
20	2.81	**2.868**	**2.868**	2.813	2.813	**2.868**	2.813
22	3.20	**3.335**	**3.335**	3.243	3.243	**3.335**	**3.335**
24	3.88	**3.879**	**3.879**	3.674	3.716	3.750	**3.879**
26	4.43	–	**4.356**	4.306	4.306	**4.356**	**4.356**
28	5.08	–	**5.082**	4.909	5.019	5.044	**5.082**
30	5.84	**5.843**	**5.843**	5.685	5.759	**5.843**	**5.843**
32	7.00	6.748	**6.776**	6.490	6.641	6.757	6.726
34	8.06	–	**7.851**	7.460	7.744	7.845	7.771
36	9.31	–	**9.150**	8.511	8.863	9.083	9.022
38	10.77	–	**10.653**	9.736	10.281	10.553	10.440
40	12.81	12.364	**12.419**	11.094	11.903	12.248	12.403

is, codes that have a significant minimum distance and few codewords of this minimum distance. Such codes can be found by starting from good convolutional codes [10], but for given block lengths we can also study codes from searches specifically performed for TB codes [15]. However, since these searches focus on minimum distance, they do not capture the precise optimization of the secrecy gain, which depends on the entire weight enumerator. Therefore, for short block lengths, we have exhaustively searched for the best TB codes based on convolutional codes of memory m up to 6. Table I shows the results of this search. Note that depending on the block length, different underlying convolutional codes may optimize the secrecy gains. Figure 1 visualizes the best TB codes of lengths up to 40.

For all small even lengths (up to lengths 40), the number of potential PDCCs to search is small, and the weight enumerator of each code is easy to compute. Hence, PDCCs can be optimized for secrecy gain. However, brute force optimization becomes infeasible as the length enters the practical range, e.g., when the code length is over 40. In contrast, TB codes have limited trellis complexity, and as long as the trellis can be represented, the weight enumerator can easily be computed for any block length. In this paper, we perform the exhaustive code search for even lengths up to 108, which is not straightforward to do via PDCC construction. Figure 1 show that the best TB codes perform equally to or very close to the best PDCCs.[1]

Short block length may be of limited practical value for high secrecy purposes. In Figure 2, we show how the secrecy gain of TB codes from *fixed* convolutional codes develop as the block length increases. In general, low-complexity codes perform equal to or better than high-complexity ones for short block lengths. All TB codes in Figure 2 demonstrate that the secrecy gain grows exponentially as the block length increases. Still, the increase is faster for the higher complexity codes, as expected.

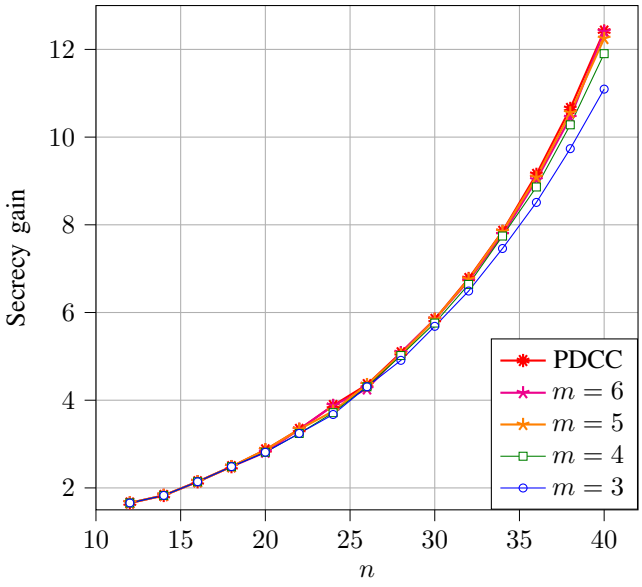

Fig. 1. Comparison of the best-found secrecy gains of Construction A lattices obtained from TB isodual codes with memory $m = 3, 4, 5, 6$, and *the best* PDCCs, for even lengths $12 \leq n \leq 40$.

[1] In fact, another observation behind the searches of Figure 1 is that PDCCs of these lengths are better than the best TB codes, and this fact was not known.

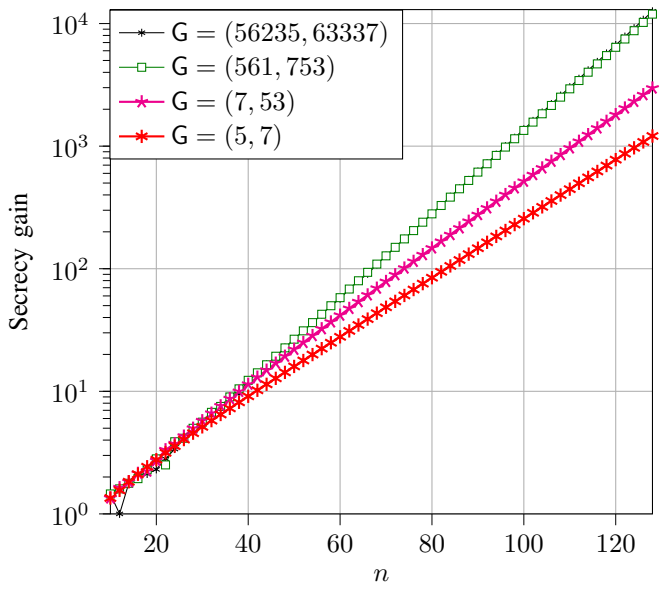

Fig. 2. Secrecy gain evolution for fixed codes. Convolutional codes, with generator matrices in octal notion, are selected from [10], [15].

In Table I, the upper bound from [11] refers to the secrecy gain achieved by unimodular lattices. Therefore, one can expect this bound to be exceeded by formally unimodular lattices, fact that happened for $n = 40$. We have checked that the conditions for applying Theorem 2 are satisfied in all cases. Boldfaced values indicate the best-known values for secrecy gain.

Besides the results presented in Table I, other remarkable ones concerning the secrecy gain of TB lattices in dimensions not previously studied and outperforming the best-known unimodular lattices were also found in the following dimensions

- $n = 60$, $\xi_{\Lambda_A(\mathscr{C})} \approx 54.721$,
- $n = 80$, $\xi_{\Lambda_A(\mathscr{C})} \approx 236.191$,
- $n = 100$, $\xi_{\Lambda_A(\mathscr{C})} \approx 991.887$.

VI. Conclusion and Future Work

We further investigated the secrecy-good isodual lattices obtained from rate 1/2 binary TB convolutional codes with memory up to 6. We showed cases where the secrecy-good TB isodual codes are compatible with the best-found isodual codes obtained from the PDCC construction for dimensions up to 40. While it is computationally expensive to get the best-found isodual codes via PDCC construction for further dimensions over 60, the exhaustive code searches to find the best secrecy-good TB isodual codes of practical complexity are shown to be manageable up to all even lengths less than 108.

In order to limit the scope of this paper, we have omitted the discussion of several relevant topics.

- One major advantage of using trellis-based codes is that efficient decoding is available. TB codes can be decoded with an iterative decoder, with a complexity of a few times the use of a Viterbi decoder, and with a performance close to maximum likelihood. To study this issue in the context of lattice constructions, we need to enter into details of signal modulation. We will postpone this for future work.
- It is known that the trellis structure is also convenient for the computation of estimates of equivocation [16] (that is, the remaining entropy about the sent message conditioned on the eavesdropper's received signal) in coset coding for wiretap channels. Moreover; in the context of lattices-based coset coding, Ling *et al.* [17] have proposed another design criterion for wiretap lattice codes, called the *flatness factor*, to quantify how much confidential information can leak to Eve in terms of mutual information, or equivalently, the concept of equivocation for lattice coset coding. It is interesting to see how trellis structure can be beneficial for lattice coset coding.

References

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[2] 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.
[3] 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.
[4] M. F. Bollauf, H.-Y. Lin, and Ø. Ytrehus, "The secrecy gain of formally unimodular lattices on the Gaussian wiretap channel," in *Proc. Int. Zurich Sem. Inf. Commun. (IZS)*, Zurich, Switzerland, Mar. 2–4, 2022, pp. 69–73.
[5] ——, "Formally unimodular packings for the Gaussian wiretap channel," Jun. 2022, arXiv:2206.14171v1 [cs.IT].
[6] ——, "On the secrecy gain of formally unimodular Construction A_4 lattices," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, Jun. 26–Jul. 1, 2022, pp. 3226–3231.
[7] ——, "Construction and secrecy gain of formally unimodular lattices in odd dimensions," in *Proc. IEEE Inf. Theory Workshop (ITW)*, Saint-Malo, France, Apr. 23–28, 2023.
[8] J. H. Conway and N. J. A. Sloane, *Sphere Packings, Lattices and Groups*, 3rd ed. New York, NY, USA: Springer, 1999.
[9] G. Solomon and H. C. A. van Tilborg, "A connection between block and convolutional codes," *SIAM J. Appl. Math.*, vol. 37, no. 2, pp. 358–369, Oct. 1979.
[10] S. Lin and D. J. Costello, Jr., *Error Control Coding*, 2nd ed. Upper Saddle River, NJ, USA: Pearson Prentice Hall, 2004.
[11] 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.
[12] ——, "A classification of unimodular lattice wiretap codes in small dimensions," *IEEE Trans. Inf. Theory*, vol. 59, no. 6, pp. 3295–3303, Jun. 2013.
[13] 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.
[14] 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.
[15] I. E. Bocharova, R. Johannesson, B. D. Kudryashov, and P. Stahl, "Tailbiting codes: Bounds and search results," *IEEE Trans. Inf. Theory*, vol. 48, no. 1, pp. 137–148, Jan. 2002.
[16] J. Algrøy, A. Barbero, and Ø. Ytrehus, "Determining the equivocation in coded transmission over a noisy channel," in *Proc. IEEE Int. Symp. Inf. Theory (ISIT)*, Espoo, Finland, Jun. 26–Jul. 1, 2022, pp. 1253–1258.
[17] 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.