Gaussian Wiretap Lattice Codes from Binary Self-dual Codes

Fuchun Lin and Frédérique Oggier
Division of Mathematical Sciences, School of Physical and Mathematical Sciences,
Nanyang Technological University, 21 Nanyang Link, Singapore 637371
Emails: linf0007@e.ntu.edu.sg and frederique@ntu.edu.sg

***Abstract*—We consider lattice coding over a Gaussian wiretap channel with respect to the secrecy gain, a lattice invariant introduced in [1] to characterize the confusion that a chosen lattice can cause at the eavesdropper. The secrecy gain of the best unimodular lattices constructed from binary self-dual codes in dimension $n,\ 24 \leq n \leq 32$ are calculated. Numerical upper bounds on the secrecy gain of unimodular lattices in general and of unimodular lattices constructed from binary self-dual codes in particular are derived for all even dimensions up to 168.**

I. Introduction

A wiretap channel as first introduced by Wyner [2] is a discrete memoryless broadcast channel where the sender Alice transmits confidential messages to a legitimate receiver Bob, in the presence of an eavesdropper Eve. Both reliable and confidential communication between Alice and Bob should be ensured at the same time, by exploiting the physical difference between the channel to Bob and that to Eve via coding. This paper considers the case of a Gaussian wiretap channel, that is both channels to Bob and Eve are additive white Gaussian noise channels. Its *secrecy capacity*, namely, the highest information rate that can be achieved with perfect secrecy was established in [4]. Gaussian wiretap codes designed for binary input have been proposed in [5]. A different approach was adopted in [1], where lattice codes were proposed, using as design criterion a new lattice invariant called *secrecy gain*, which was shown to characterize the confusion at the eavesdropper. In [6], [7], encoding via a classic lattice construction involving binary error correction codes called *Construction A* was specified. The special class of *unimodular* lattices has been studied with particular emphasis on *even* unimodular lattices: the secrecy gain of *extremal* even unimodular lattices was computed, and the asymptotic behavior of the average secrecy gain as a function of the dimension n was investigated. The results show that maximizing the secrecy gain is meaningful in small dimensions and infinite secrecy gain is possible as n grows to infinity, in fact, all even unimodular lattices behave almost the same when n is large. Unimodular lattices in small dimensions, both odd and even, were considered in [8], [9] resulting in a complete classification in dimension $n,\ n \leq 23$, featuring some odd lattices outperforming their even counter parts. In this paper, we derive an upper bound on the secrecy gain of unimodular lattices, which shows that extremal lattices have the maximum secrecy gain (at least for all even dimensions up to 168 which we verified numerically). We compute as examples the secrecy gains of unimodular lattices from Construction A and classify the best lattices in dimension $n,\ 24 \leq n \leq 32$ (the best unimodular lattices in even dimension $n,\ n \leq 23$ are all lattices from Construction A [9]). An upper bound on the secrecy gain of such lattices is also given to compare with that of unimodular lattices in general, exhibiting a big gap between the two bounds.

II. Preliminaries and previous results

A Gaussian wiretap channel is a broadcast Gaussian channel modeled by

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v_b} \\ \mathbf{z} &= \mathbf{x} + \mathbf{v_e}, \end{aligned} \tag{1}$$

where $\mathbf{x}$ is the codeword sent by the transmitter (Alice), $\mathbf{y}$ and $\mathbf{z}$ are the received signals at the legitimate receiver (Bob), respectively at the eavesdropper (Eve), with corresponding noise vectors $\mathbf{v_b}$ and $\mathbf{v_e}$, whose components are i.i.d. Gaussian distributed with zero mean and respective variance σ_b^2 and σ_e^2. It is assumed that $\sigma_b^2 < \sigma_e^2$ in order to have a positive secrecy capacity [4]. We suppose that $\mathbf{x} \in \mathbb{R}^n$ is a lattice codeword, where by a lattice Λ we mean a discrete set of points in $\mathbb{R}^n$, which can be conveniently described by

$$\Lambda = \{\mathbf{x} = G\mathbf{u} | \mathbf{u} \in \mathbb{Z}^n\},$$

where the *generator matrix* G stores as column vectors a basis for Λ and the determinant of G is the *volume* of Λ. The *dual* of a lattice Λ of dimension n is defined to be

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n : \mathbf{x} \cdot \lambda \in \mathbb{Z}, \lambda \in \Lambda\},$$

where $\mathbf{x} \cdot \lambda$ is the inner product of $\mathbf{x}$ and λ. A lattice Λ is called a *unimodular* lattice if $\Lambda = \Lambda^*$. The *norm* (squared length) $||\mathbf{x}||^2 = \mathbf{x} \cdot \mathbf{x}$ of a lattice point $\mathbf{x}$ in a unimodular lattice Λ is an integer. If the norm is an even integer for any lattice point in Λ, then Λ is called an *even unimodular* lattice or a *type II* lattice. Otherwise, it is called an *odd unimodular* lattice or a *type I* lattice.

Lattice encoding for the wiretap channel (1) is done via a generic coset coding strategy [1]: let $\Lambda_e \subset \Lambda_b$ be two nested lattices, specially chosen such that the quotient group Λ_b/Λ_e is of size 2^k. A k-bit message is then mapped to a coset in Λ_b/Λ_e, after which a vector is randomly chosen from the coset as the encoded word. The lattice Λ_e will be interpreted as introducing confusion for Eve, while Λ_b as ensuring reliability

for Bob. A bound [1] on Eve's probability $P_{c,e}$ of correct decoding shows that to minimize $P_{c,e}$ is to minimize

$$\sum_{\lambda\in\Lambda_e} e^{-||\lambda||^2/2\sigma_e^2}. \tag{2}$$

Let $\mathcal{H} = \{a + ib \in \mathbb{C} | b > 0\}$ denote the upper half plane and set

$$q = e^{\pi i \tau},\ \tau \in \mathcal{H}.$$

Definition II.1. *The theta series of a lattice Λ is defined by*

$$\Theta_\Lambda(\tau) = \Sigma_{\lambda\in\Lambda} q^{||\lambda||^2}.$$

By combining the terms with the same exponent, the theta series can be written as

$$\Theta_\Lambda(\tau) = \Sigma_{n=0}^{\infty} A_n q^n \tag{3}$$

and interpreted as a record of the number of vectors $\lambda \in \Lambda$ with norm n in the coefficient A_n.

It is easily recognized that (2) is in fact the theta series of Λ_e at $\tau = \frac{i}{2\pi\sigma_e^2}$. Motivated by the above argument, the confusion brought by the lattice Λ_e with respect to no coding (namely, use the lattice $\mathbb{Z}^n$ scaled to the same volume) is measured as follows [1]:

Definition II.2. *Let Λ be an n-dimensional lattice of volume V. The secrecy function of Λ is given by*

$$\Xi_\Lambda(\tau) = \frac{\Theta_{\sqrt[n]{V}\mathbb{Z}^n}(\tau)}{\Theta_\Lambda(\tau)}, \tau = yi,\ y > 0.$$

The *secrecy gain* is then the maximal value of the secrecy function with respect to τ and is denoted by χ_Λ. χ_Λ will be used as code design criterion: we need to compute the secrecy gain to find the best lattice in a given dimension.

Definition II.3. *The Jacobi's theta series are defined by*

$$\begin{aligned}\vartheta_2(\tau) &= \Sigma_{n\in\mathbb{Z}} q^{(n+\frac{1}{2})^2},\\ \vartheta_3(\tau) &= \Sigma_{n\in\mathbb{Z}} q^{n^2},\\ \vartheta_4(\tau) &= \Sigma_{n\in\mathbb{Z}} (-q)^{n^2}.\end{aligned}$$

From the definition of the theta series of a lattice, we have

$$\Theta_{\mathbb{Z}^k}(\tau) = \vartheta_3(\tau)^k. \tag{4}$$

The theta series of unimodular lattices are actually *modular forms* [10]. The following decomposition [11] will play an important role in analyzing the secrecy gain of unimodular lattices.

Theorem II.1. *(Hecke) If Λ is a unimodular lattice then*

$$\Theta_\Lambda(\tau) = \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \vartheta_3^{n-8r}(\tau)\Delta_8^r(\tau), a_r \in \mathbb{Z}, \tag{5}$$

where the discriminant function $\Delta_8(\tau)$ can be represented by $\vartheta_2(\tau)$ and $\vartheta_4(\tau)$:

$$\Delta_8(\tau) = \frac{1}{16}\vartheta_2^4(\tau)\vartheta_4^4(\tau). \tag{6}$$

In this paper, we majorly discuss unimodular lattices constructed from binary self-dual codes through the so-called *Construction A*. We will use some terminology from error correction codes. Unfamiliar readers can refer to [12].

Let ρ be the map of component-wise reduction modulo 2 defined on $\mathbb{Z}^n$:

$$\rho : \mathbb{Z}^n \to \mathbb{F}_2^n,$$

where $\mathbb{F}_2$ is the Galois field of 2 elements. Let C be a binary $[n, k, d]$ code. Then the pre-image $\rho^{-1}(C)$ of C in $\mathbb{Z}^n$ is a lattice in $\mathbb{R}^n$. We only need to scale the lattice to the right volume.

Definition II.4. *Let C be a binary $[n, k, d]$ code. Then the lattice Γ_C generated by C is*

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

We list some connections between Γ_C and C [13] before we end this section.

Theorem II.2. *Let C be a binary linear code.*

1) *Γ_C is unimodular if and only if C is self-dual.*
2) *Γ_C is a type II lattice if and only if C is a type II code.*
3) *Γ_C is a type I lattice if and only if C is a type I code.*

Theorem II.3. *Let $W_C(x, y)$ be the weight enumerator of the binary self-dual code C. Then the theta series of Γ_C is*

$$\Theta_{\Gamma_C}(\tau) = W_C(\vartheta_3(2\tau), \vartheta_2(2\tau)). \tag{7}$$

III. Secrecy gains of unimodular lattices from Construction A in dimensions $24 \le n \le 32$

With (4) and (7), the secrecy function of Γ_C is obtained once the weight distribution of C is known. Binary self-dual codes were enumerated in lengths up to 32 with the weight distribution of each code given in [14]. The number of self-dual codes grows rapidly when n grows. For example, there are 85 type II codes and 3210 type I codes when $n = 32$.

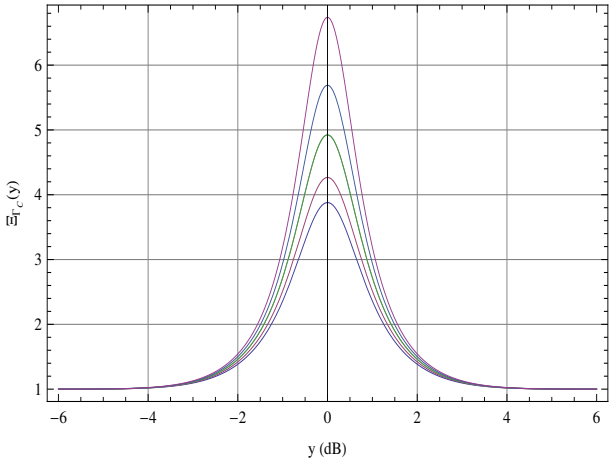

Fig. 1. Secrecy functions of the best unimodular lattices from Construction A in dimension $24 \le n \le 32$.

TABLE I
BEST UNIMODULAR LATTICES FROM CONSTRUCTION A IN DIMENSIONS $24 \leq n \leq 32$

n	weight distribution of C	χ_{Γ_C}
24	$(1,0,0,0,759,0,2576\|\cdots)$	3.88
26	$(1,0,1,21,546,1021,2506\|\cdots)$	4.27
28	$(1,0,0,26,442,1560,3653,5020\|\cdots)$ $(1,0,1,12,503,1488,3591,5192\|\cdots)$	4.92
30	$(1,0,0,19,393,1848,5192,8931\|\cdots)$	5.69
32	$(1,0,0,0,364,2048,6720,14336,18598\|\cdots)$	6.74

The weight distribution is given in half to avoid redundancy and only the even weights are given because self-dual codes are even codes.

Fig. 1 gives a plot of the secrecy functions of 6 unimodular lattices from Construction A in dimension $24 \leq n \leq 32$, whose corresponding self-dual codes are listed in Table I. We set $\tau = yi$ and y is plotted in decibels. We can see clearly that the secrecy functions of unimodular lattices have a symmetry point at $y = 0$ dB corresponding to $\tau = i$, which was shown in [6], [7]. It was conjectured in [6] that the secrecy gain of a unimodular lattice is achieved at $\tau = i$, the symmetry point of the secrecy function. This conjecture was recently proved for a special class of lattices called *extremal* even unimodular lattices [15] and for unimodular lattices in dimension n, $8 < n \leq 23$ [9]. The idea of the proof [15] is to substitute (5) into the secrecy function of a lattice Λ and rewrite it as

$$\Xi_\Lambda(\tau) = \frac{1}{\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{z}{16}\right)^r}, \text{where } z = \frac{\vartheta_2^4(\tau)\vartheta_4^4(\tau)}{\vartheta_3^8(\tau)} = \frac{16\Delta_8(\tau)}{\vartheta_3^8(\tau)}.$$

It was shown in the paper that

$$z \in [0, \frac{1}{4}]$$

and the maximum of z is achieved at $\tau = i$. The rest of the proof consists of showing that the polynomial function $\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r \left(\frac{z}{16}\right)^r$ is decreasing in $[0, \frac{1}{4}]$. We have proved the conjecture for all the unimodular lattices that appear in this paper and the detail is omitted due to the space constraint. Now we can use the following formula [8], [9] to calculate the secrecy gain of unimodular lattices:

$$\chi_\Lambda = \frac{1}{\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} a_r (\frac{1}{2^6})^r}, \tag{8}$$

where the a_r's are the coefficients in (5). The lattices shown in Table I turn out to be the best in their respective dimensions in terms of the secrecy gain.

In [9], the best unimodular lattices in dimensions $n \leq 24$ were classified and in dimension 16, the first incident of an odd unimodular lattice outperforming even unimodular lattices has been found. Here we find that as n grows, examples of odd lattices outperforming even lattices exist in great number. The best unimodular lattice from Construction A in dimension 32 is the type I lattice (represented by the weight distribution of C and χ_{Γ_C})

$$(1,0,0,0,364,2048,6720,14336,18598|\cdots)$$
6.74.

It outperforms all the type II lattices generated from the 85 type II codes of length 32 [14]. Here we only give the best among the 85 lattices:

$$(1,0,0,0,620,0,13888,0,36518|\cdots)$$
6.56.

On the other hand, we compared the lattice code design criterion with the classic error correction code design criterion, namely, the minimum distance. We found that the best lattice is always given by codes with large minimum distance, but not necessarily the code with the largest minimum distance. For example, in dimension 28,

$$(1,0,0,26,442,1560,3653,5020|\cdots)$$
4.92

and

$$(1,0,1,12,503,1488,3591,5192|\cdots)$$
4.92

have the same secrecy gain, which is the best in that dimension. In dimension 26, the best lattice is

$$(1,0,1,21,546,1021,2506|\cdots)$$
4.27,

while the code with the largest minimum distance generates

$$(1,0,0,52,390,1313,2340|\cdots)$$
4.20.

A more comprehensive analysis will follow in next section where we investigate the contributions of the first few terms of the theta series of a unimodular lattice to its secrecy gain to derive upper bounds.

IV. UPPER BOUNDS

Since $\vartheta_3(\tau)$ and $\Delta_8(\tau)$ are known series, we can substitute them into (5) to obtain a q-expansion with coefficients represented by a_r's. Then a linear system in a_r's can be obtained by comparing this q-expansion with (3) and equaling the first $\lfloor \frac{n}{8} \rfloor + 1$ coefficients. In other words, we have the following linear system:

$$MX = A, \tag{9}$$

where $A = (A_0,\ A_1, \cdots,\ A_{\lfloor \frac{n}{8} \rfloor})^T$ contains the first $\lfloor \frac{n}{8} \rfloor + 1$ coefficients of (3), $X = (a_0,\ a_1, \cdots,\ a_{\lfloor \frac{n}{8} \rfloor})^T$ contains the a_r's in (5) and the matrix

$$M = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ M_{21} & 1 & \cdots & 0 \\ & \cdots & & \\ M_{\lfloor \frac{n}{8} \rfloor+1,1} & M_{\lfloor \frac{n}{8} \rfloor+1,2} & \cdots & 1 \end{pmatrix}$$

contains as columns the first $\lfloor \frac{n}{8} \rfloor + 1$ coefficients of the power series $\vartheta_3^{n-8r}(\tau)\Delta_8^r(\tau),\ r = 0, 1, \cdots,\ \lfloor \frac{n}{8} \rfloor$.

The matrix M is obviously invertible and $X = M^{-1}A$. Let $\{\mathbf{e}_1,\ \mathbf{e}_2,\ \cdots,\ \mathbf{e}_{\lfloor \frac{n}{8} \rfloor+1}\}$ denote the standard basis. The solution can be written as

$$X = \sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} A_r M^{-1} \mathbf{e}_{r+1}. \tag{10}$$

Finally, let $\mathbf{w} = (1,\ 2^{-6},\ \cdots,\ 2^{-6\lfloor \frac{n}{8} \rfloor})$ and substitute (10) into (8). We have

$$\chi_\Lambda = \frac{1}{\mathbf{w}X} = \frac{1}{\sum_{r=0}^{\lfloor \frac{n}{8} \rfloor} A_r \mathbf{w} M^{-1} \mathbf{e}_{r+1}}. \tag{11}$$

Now we can see clearly that χ_Λ is determined by the A_r's and the contribution of each A_r is weighted by the constant $\mathbf{w}M^{-1}\mathbf{e}_{i+1}$.

We have calculated the $\mathbf{w}M^{-1}\mathbf{e}_{i+1}$'s for all the even dimensions n from 2 to 168 and they are all positive, which implies that the only way to maximize the secrecy gain is to minimize each A_r's. Therefore we arrive at our two upper bounds on the secrecy gains of unimodular lattices in general and of unimodular lattices from Construction A in particular.

Definition IV.1. *Let Λ be a lattice of dimension n. Λ is said to be an extremal lattice if its minimal norm is $\lfloor \frac{n}{8} \rfloor + 1$.*

This definition of extremal is following [11], in which it was shown that extremal lattices only exist in dimensions $n = 1 \sim 8,\ 12,\ 14,\ 15,\ 23$ and 24. Since $A = (1,\ 0, \cdots,\ 0)^T$ for any extremal lattice, the secrecy gain is then

$$\chi_\Lambda = \frac{1}{\mathbf{w}M^{-1}\mathbf{e}_1}. \tag{12}$$

Theorem IV.1. *The secrecy gain of unimodular lattices in even dimensions $n,\ 2 \le n \le 168$ is upper-bounded by $\frac{1}{\mathbf{w}M^{-1}\mathbf{e}_1}$.*

The value of $\frac{1}{\mathbf{w}M^{-1}\mathbf{e}_1}$ for each n is shown in Table II. This bound is tight only in dimensions $n = 2,\ 4,\ 6,\ 8,\ 12,\ 14$ and 24, when extremal unimodular lattices exist.

Let us come back to unimodular lattices from Construction A. Since we only need the first $\lfloor \frac{n}{8} \rfloor + 1$ coefficients of Θ_{Γ_C}, we no longer need the complete weight distribution of C. Let us first see an example.

In dimension 24, we will need the first $\lfloor \frac{n}{8} \rfloor + 1 = 4$ terms of Θ_{Γ_C}. In other words, we only need the coefficients of $q^0,\ q^1,\ q^2$ and q^3. The weight distribution of the self-dual code that gives the best unimodular lattice in dimension 24 is $(1, 0, 0, 0, 759, 0, 2576|\cdots)$. By (7),

$$\begin{aligned}\Theta_{\Gamma_C}(\tau) &= W_C(\vartheta_3(2\tau), \vartheta_2(2\tau)) \\ &= \vartheta_3(2\tau)^{24} + 2576\vartheta_3(2\tau)^{12}\vartheta_2(2\tau)^{12} + \vartheta_2(2\tau)^{24} \\ &\quad + 759\left(\vartheta_3(2\tau)^{16}\vartheta_2(2\tau)^8 + \vartheta_3(2\tau)^8\vartheta_2(2\tau)^{16}\right).\end{aligned}$$

The coefficients of $q^0,\ q^1,\ q^2$ and q^3 are determined by $\vartheta_3(2\tau)^{24}$ since the other terms do not contain these powers of q. The first 4 terms of $\vartheta_3(2\tau)^{24}$ are calculated as $1,\ 0q,\ 48q^2,\ 0q^3$ hence

$$A = (1,\ 0,\ 48,\ 0)$$

and

$$\chi_{\Gamma_C} = \frac{1}{\mathbf{w}M^{-1}\mathbf{e}_1 + 48\mathbf{w}M^{-1}\mathbf{e}_3} \approx 3.88.$$

In the above example, we only need the number of code words of weights less than 8 to compute the secrecy gain. In general, we will need to know the coefficients of $q^0,\ q^1, \cdots,\ q^{\lfloor \frac{n}{8} \rfloor}$ in Θ_{Γ_C} and hence, the weight distribution of weights no more than $2\lfloor \frac{n}{8} \rfloor$ of C. This suggests that we can upper-bound the secrecy gain of unimodular lattices from Construction A by assuming that only the term $\vartheta_3(2\tau)^n$ in (7) contains $1,\ q,\ q^2, \cdots,\ q^{\lfloor \frac{n}{8} \rfloor}$, which in coding language translates into "C has a minimum distance $d \ge 2\lfloor \frac{n}{8} \rfloor + 2$".

TABLE II
AN UPPER BOUND ON THE SECRECY GAIN OF UNIMODULAR LATTICES

n	bound	n	bound	n	bound
2	**1**	58	62.16	114	6365.16
4	**1**	60	73.12	116	7511.49
6	**1**	62	86.08	118	8864.62
8	**1.33**	64	102.00	120	10465.92
10	1.45	66	120.07	122	12351.16
12	**1.60**	68	141.41	124	14576.48
14	**1.78**	70	166.62	126	17203.22
16	2.25	72	197.18	128	20309.18
18	2.54	74	232.32	130	23968.83
20	2.89	76	273.82	132	28288.60
22	3.31	78	322.81	134	33387.53
24	**4.06**	80	381.70	136	39413.36
26	4.68	82	449.99	138	46517.29
28	5.41	84	530.62	140	54902.53
30	6.28	86	625.81	142	64800.15
32	7.58	88	739.54	144	76492.53
34	8.82	90	872.19	146	90282.02
36	10.28	92	1028.80	148	106558.56
38	12.01	94	1213.69	150	125770.67
40	14.38	96	1433.71	152	148460.64
42	16.81	98	1691.32	154	175227.13
44	19.68	100	1995.44	156	206821.15
46	23.09	102	2354.44	158	244112.95
48	27.50	104	2780.54	160	288147.70
50	32.26	106	3280.75	162	340103.05
52	37.88	108	3871.21	164	401428.49
54	44.53	110	4568.22	166	473813.88
56	52.87	112	5394.05	168	559276.90

Theorem IV.2. *The secrecy gain of unimodular lattices from Construction A in even dimensions $n,\ 2 \le n \le 168$ are upper-bounded as shown in Table III.*

This bound is tight in dimensions $n = 2, 4, 6, 8, 12, 14, 22$ according to [9] and $n = 24$ according to Table I. According to [16], a binary self-dual code of length n has a minimum distance $d \le 4\lfloor \frac{n}{24} \rfloor + 4$ except when $n \equiv 22 \pmod{24}$, in which case $d \le 4\lfloor \frac{n}{24} \rfloor + 6$. The existence of self-dual codes meeting this bound in every dimension is not yet completely known. But it is known that such codes do not exist when $n = 10, 26, 28, 30$ and at a few larger lengths. These altogether imply that our upper bound is not tight elsewhere, for the type of C with minimum distance $d \ge 2\lfloor \frac{n}{8} \rfloor + 2$ does not exist at other lengths.

We ran a test to see how good is this upper bound. An *extended quadratic residue* code of length 168 is known with its weight enumerator [17]. The secrecy gain of the type II lattice generated from this code is calculated as 298853.84 while the upper bound for $n = 168$ is 299262.33. The difference is within 0.0014 of the bound.

Before we end this section, let us compare these two upper bounds with an achievable lower bound on the secrecy gain of

TABLE III
AN UPPER BOUND ON THE SECRECY GAIN OF UNIMODULAR LATTICES FROM CONSTRUCTION A

n	bound	n	bound	n	bound
2	**1**	58	51.12	114	4180.14
4	**1**	60	59.61	116	4893.70
6	**1**	62	69.52	118	5729.58
8	**1.33**	64	81.91	120	6718.00
10	1.45	66	95.53	122	7865.54
12	**1.60**	68	111.48	124	9209.80
14	**1.78**	70	130.15	126	10784.54
16	2.21	72	153.13	128	12642.65
18	2.49	74	178.80	130	14804.42
20	2.81	76	208.86	132	17336.85
22	**3.20**	78	244.07	134	20303.55
24	**3.88**	80	286.84	136	23798.36
26	4.43	82	335.22	138	27870.82
28	5.08	84	391.86	140	32884.22
30	5.84	86	458.20	142	38230.71
32	7.00	88	538.09	144	44806.43
34	8.06	90	629.21	146	52478.44
36	9.31	92	735.94	148	61466.27
38	10.77	94	860.93	150	72531.90
40	12.81	96	1010.46	152	84372.01
42	14.83	98	1182.12	154	98825.30
44	17.20	100	1383.18	156	115775.60
46	19.98	102	1618.69	158	135594.45
48	23.66	104	1899.01	160	158893.49
50	27.48	106	2222.38	162	186122.24
52	31.96	108	2601.15	164	218021.65
54	37.21	110	3044.84	166	255393.12
56	43.93	112	3570.98	168	299262.33

even unimodular lattices given in [7]. We plot the three bounds in the same graph as shown in Figure 2. It can be seen that the achievable lower bound and the upper bound for unimodular lattices merge together as n grows, while the upper bound for unimodular lattices from Construction A is obviously lower than the other two bounds. It seems that the achievable lower bound is also the upper bound and the prediction that all even unimodular lattices behave the same way does not take effect at least when $n \leq 168$. The second observation can be further verified by the following naive construction. Take the E_8 lattice in dimension 8 and keep "multiplying" until we get the type II lattice E_8^{21} in dimension 168. The secrecy gain of this lattice is $(\frac{4}{3})^{21} \approx 420.45$, which is much smaller than 298853.84, the secrecy gain of the extended quadratic residue code.

V. CONCLUSION AND FUTURE WORK

In this paper, the secrecy gains of the best unimodular lattices constructed from binary self-dual codes in dimension n, $24 \leq n \leq 32$ are calculated. Numerical upper bounds on the secrecy gain of unimodular lattices in general and of unimodular lattices constructed from binary self-dual codes in particular are derived for all even dimensions up to 168. It is a natural future work to extend these bounds to higher dimensions. Also, decoding complexity of such wiretap codes is under investigation to understand, for example, for what choice of Λ_b and for what range of n they are practical.

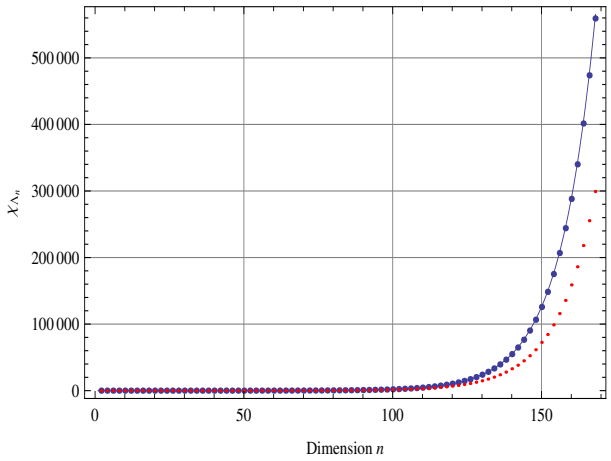

Fig. 2. An achievable lower bound v.s. two upper bounds

ACKNOWLEDGMENT

The research of F. Lin and F. Oggier for this work is supported by the Singapore National Research Foundation under the Research Grant NRF-RF2009-07.

REFERENCES

[1] J.-C. Belfiore and F. Oggier, "Secrecy gain: a wiretap lattice code design," ISITA 2010. http://arXiv:1004.4075v2 [cs.IT].

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

[3] Y. Liang, H.V. Poor and S. Shamai, "Information theoretic security," Foundations and Trends in Communications and Information Theory, Vol. 5, Issue 4-5, 2009, Now Publishers.

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

[5] D. Klinc, J. Ha, S. McLaughlin, J. Barros, and B. Kwak, "LDPC codes for the Gaussian wiretap channel," *IEEE* Trans. Inform. Forensics Security, vol. 6, no. 3, pp. 532-540, Sep 2011.

[6] J.-C. Belfiore and P. Solé, "Unimodular lattices for the Gaussian Wiretap Channel," ITW 2010, Dublin. http://arXiv:1007.0449v1 [cs.IT].

[7] F. Oggier, J.-C. Belfiore, and P. Solé, "Lattice Coding for the Wiretap Gaussian Channel", http://arXiv:1103.4086v1 [cs.IT], 21 Mar 2011.

[8] F. Lin and F. Oggier, "Secrecy Gain of Gaussian Wiretap Codes from Unimodular Lattices," ITW 2011, Paraty. pp. 718-722.

[9] F. Lin and F. Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions", http://arXiv:1201.3688v1 [cs.IT], 18 Jan 2012.

[10] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms", Graduate Texts in Math. No. 97, Springer-Verlag, New York, Second edition, 1993.

[11] J.H. Conway, N.J.A. Sloane, "Sphere Packings, Lattices and Groups", Third edition, Springer-Verlag, New York, 1998.

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

[13] W. Ebeling, "Lattices and Codes", Advanced Lectures in Mathematics, Vieweg & Sohn, Verlagsgesellschaft mbH, Braunschweig/Wiesbaden, 1994.

[14] Online available, http://www.cs.umanitoba.ca/~umbilou1/SelfDualCodes/toc.html.

[15] A.-M. Ernvall-Hytönen, "On a Conjecture by Belfiore and Solé on some Lattices", to appear at *IEEE Transactions on Information Theory*.

[16] E. M. Rains and N. J. A. Sloane, "Self-dual codes", in Handbook of Coding Theory. Amsterdam, The Netherlands: Elsevier, 1998.

[17] W. K. Su, P.Y. Shih, T.C. Lin and T.K. Truong, "On the Minimum Weights of Binary Extended Quadratic Residue Codes", ICACT 2009. pp. 1912 - 1913.