Counterexample to the Generalized Belfiore-Solé Secrecy Function Conjecture for l-modular lattices

Anne-Maria Ernvall-Hytönen and B. A. Sethuraman

***Abstract*—In this paper, we show that the secrecy function conjecture that states that the maximum of the secrecy function of an l-modular lattice occurs at $1/\sqrt{l}$ is false, by proving that the 4-modular lattice $C^{(4)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus 2\mathbb{Z}$ fails to satisfy this conjecture. After this, we indicate how the secrecy function must be modified in the l-modular case to provide a more meaningful comparison for l-modular lattices, and show that this new secrecy function indeed has a maximum at $1/\sqrt{l}$ for various 2-modular lattices and for $C^{(4)}$. We conjecture that this must hold true for all l-modular lattices.**

***Index Terms*—Wiretap coding, Secrecy function, Belfiore-Solé Secrecy Function Conjecture, l-modular lattice, l-modular secrecy function conjecture.**

I. Introduction

Wyner [1] introduced the wiretap channel as a discrete memoryless and possibly noisy broadcast channel, where the sender transmits confidential messages to a legitimate receiver in the presence of an eavesdropper. In the current paper, we consider the case where the channel is noisy, and the noise is Gaussian distributed. This noise is then exploited in confusing the eavesdropper. If the eavesdropper has a worse channel (i.e., more noise) than the legitimate receiver, one can use lattices in such a way that the coding encrypts the message.

Essentially, one picks two lattices Λ and Λ' such that $\Lambda' \subset \Lambda$, and the coding is performed by using cosets Λ/Λ' as alphabets. In practice, one picks a representative from a coset, and transmits the representative over the channel. This representative does not always have to be the same. The finer of the lattices, Λ is assumed to be chosen in such a way that the legitimate receiver can distinguish between points in the lattice even after the addition of the noise. The coarser lattice, Λ' is thought to be assigned to the eavesdropper, and in the optimal case, it is chosen in such a way that the eavesdropper can just decode this lattice, but not obtain any information about the actual points being transmitted (points of the finer lattice).

The secrecy function was introduced in [2] by Oggier and Belfiore, who considered the problem of wiretap code design for the Gaussian channel, using lattice-based coset coding. The function was further refined by Belfiore and Solé in [3, Definition 3] to take into account the volume of the lattice Λ. It is defined for an l-modular lattice Λ (actually for any lattice) in dimension n by

$$\Xi(y) = \frac{\Theta_{\lambda\mathbb{Z}^n}(y\imath)}{\Theta_\Lambda(y\imath)}. \tag{1}$$

Here, y is a positive real variable, $\lambda = l^{n/4}$ is the volume of the l-modular lattice Λ, $\lambda\mathbb{Z}^n$ denotes the cubic lattice $\mathbb{Z}^n$ scaled to have the volume λ (thus, each dimension of $\lambda\mathbb{Z}^n$ is scaled by $l^{1/4}$), and for any $\tau \in \mathbb{C}$ with $im(\tau) > 0$ and any lattice L, $\Theta_L(\tau)$ denotes the *theta series* of L, that is, the series $\sum_{j=0}^{\infty} a_j e^{\imath\pi j\tau}$, were a_j is the number of vectors in L of norm (squared length) j.

The secrecy function was studied in detail in [3] by Belfiore and Solé. Assuming that the noise variance σ_e^2 on Eve's channel is much higher than the corresponding variance σ_b^2 on Bob's channel, they analyze both the legitimate receiver's error probability and the probability of Eve making a correct decision and determine conditions under which Eve's probability of correct decoding is minimized. If $\Lambda_e \subset \Lambda_b$ are the lattices used in the coset-coding paradigm, they express these conditions in terms

Anne-Maria Ernvall-Hytönen was with Department of Mathematics and Statistics, 00014 University of Helsinki, Finland; her current affiliiation is Department of Mathematics and Statistics, Åbo Akademi University, Fänriksgatan 3, 20500 Åbo, Finland. Email: anne-maria.ernvall-hytonen@abo.fi

B. A. Sethuraman is with Department of Mathematics, California State University Northridge, Northridge, CA 91330, USA. Email: al.sethuraman@csun.edu

Portions of this paper were presented at ISIT 2015.

of the theta series of Λ_e. For a given choice of lattice Λ_e, it follows from these considerations that the value of y at which the secrecy function $\Xi_{\Lambda_e}(y)$ of Λ_e obtains its maximum yields the value of the signal-to-noise ratio in Eve's channel that causes maximum confusion to Eve, as compared to using the standard lattice $\mathbb{Z}^n$. (The maximal achievable value of the secrecy function is called the *secrecy gain* of the lattice Λ_e.)

Belfiore and Solé studied the secrecy function for various lattices and conjectured in [3] that for a unimodular lattice ($l = 1$), the secrecy function attains its (global) maximum at $y = 1$. This has since been verified for a large number of lattices (see e.g., [4], [5], [6], [7]), and it was proven in [6] that infinitely many unimodular lattices satisfy the conjecture, but the full conjecture is still open. In [8], Oggier, Solé and Belfiore further extended this conjecture to l-modular lattices ($l > 1$) ([8, Proposition 2, and Conjecture 1]:

Conjecture 1 (l-modular Belfiore-Solé conjecture)**.** *The secrecy function*

$$\Xi(y) = \frac{\Theta_{\lambda\mathbb{Z}^n}(y\imath)}{\Theta_\Lambda(y\imath)}$$

of an l-modular lattice Λ attains its maximum at $y = \frac{1}{\sqrt{l}}$.

We show in this note that this extended conjecture does not hold for all lattices. We show that the 4-modular lattice $C^{(4)} = \mathbb{Z}\oplus\sqrt{2}\mathbb{Z}\oplus 2\mathbb{Z}$ fails to satisfy the conjecture. We show that in fact that the secrecy function of $C^{(4)}$ has a global *minimum* at $y = 1/\sqrt{4}$, and thus behaves contrary to what is expected by the conjecture.

We also indicate how the conjecture must be modified to have a reasonable chance of being true: the numerator in the secrecy function should be replaced by a suitable power of the theta series of $D^{(l)}$, where $D^{(l)} = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$. We show that the modified secrecy function conjecture holds for various 2-modular lattices, and in fact, provide a necessary and sufficient criterion for a 2-modular lattice to satisfy the modified conjecture.

II. Preliminaries

A theta function of a lattice Λ is defined as a sum

$$\Theta_\Lambda(\tau) = \sum_{x\in\Lambda} e^{\pi\imath|x|^2\tau}.$$

For example,

$$\Theta_{\mathbb{Z}}(\tau) = \sum_{n\in\mathbb{Z}} e^{\pi\imath n^2\tau} = 1 + 2\sum_{n\geq 1} e^{\pi\imath n^2\tau}.$$

To shorten the notation, we write $q = e^{\imath\pi\tau}$, which is standard in the theory of theta functions. The Jacobi theta functions are defined using the following formulas

$$\begin{aligned}\vartheta_2(\tau) &= \sum_{n=-\infty}^{\infty} q^{(n+1/2)^2} \\ &= 2q^{1/4}\prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n})^2 \\ \vartheta_3(\tau) &= \sum_{n=-\infty}^{\infty} q^{n^2} = \prod_{n=1}^{\infty}(1-q^{2n})(1+q^{2n-1})^2 \\ \vartheta_4(\tau) &= \sum_{n=-\infty}^{\infty} (-1)^n q^{n^2} \\ &= \prod_{n=1}^{\infty}(1-q^{2n})(1-q^{2n-1})^2\end{aligned} \tag{2}$$

These converge if and only if $im(\tau) > 0$. These functions are useful in representing theta functions of various lattices.

These functions satisfy, for instance, the following formulas ([9, page 104]):

$$\begin{aligned}\vartheta_3^4(\tau) &= \vartheta_2^4(\tau) + \vartheta_4^4(\tau) \\ 2\vartheta_3^2(2\tau) &= \vartheta_3^2(\tau) + \vartheta_4^2(\tau) \\ 2\vartheta_2^2(2\tau) &= \vartheta_3^2(\tau) - \vartheta_4^2(\tau).\end{aligned} \tag{3}$$

(Notice that the last two equations yield $\vartheta_3^2(\tau) = \vartheta_3^2(2\tau) + \vartheta_2^2(2\tau)$.)

A thorough introduction to the theory of these functions can be found in [10, Chap. 10], in terms of the "master" theta function $\Theta(z|\tau) = \sum_{n=-\infty}^{\infty} e^{2\pi\imath nz+\pi\imath n^2\tau}$. (We may write our functions ϑ_2, ϑ_3, ϑ_4 in terms of Θ as $\vartheta_2(\tau) = e^{\imath\pi\tau/4}\Theta(\frac{\tau}{2}|\tau)$, $\vartheta_3(\tau) = \Theta(0|\tau)$, and $\vartheta_4(\tau) = \Theta(\frac{1}{2}|\tau)$–see [9, page 102] for instance, but note the slight difference in the definitions of Θ in [10] and [9].)

Recall [11] that an integral lattice $\Lambda \subset \mathbb{R}^n$ is said to be *l-modular* if there exists a similarity of $\mathbb{R}^n$ of norm l, that is, an orthogonal transformation S followed by a scaling of lengths by $\sqrt{l}$, such that $\sqrt{l}S(\Lambda^*) = \Lambda$. Here, Λ^* is the dual of Λ, and $\Lambda \subset \Lambda^*$ because of integrality. It follows from elementary considerations that l must necessarily be an integer and that Λ must have determinant $l^{n/2}$. Since the determinant of Λ is an integer, we find immediately that n must be even, unless l is itself a square. When $l = 1$, an l-modular lattice is known as a *unimodular* lattice. Theta functions of unimodular lattices can be written as polynomials in Jacobi theta functions. An l-modular lattice is said to be even if all squared norms of its vectors are even, and otherwise it is odd.

III. The Lattice $C^{(4)}$.

In this section we show that for the 4-modular lattice $C^{(4)} = \mathbb{Z} \oplus \sqrt{2}\mathbb{Z} \oplus 2\mathbb{Z}$, the secrecy function of $C^{(4)}$ defined in (1) attains a minimum at $y = 1/2$, showing that the secrecy function conjecture is false in general. First note that $C^{(4)}$ is indeed 4-modular: it is easy to see that its dual is the lattice $\mathbb{Z} \oplus (1/\sqrt{2})\mathbb{Z} \oplus (1/2)\mathbb{Z}$, and the map $\mathbb{R}^3 \to \mathbb{R}^3$ that sends (x, y, z) to $(2z, 2y, 2x)$ indeed provides an isomorphism between $\mathbb{Z} \oplus (1/\sqrt{2})\mathbb{Z} \oplus (1/2)\mathbb{Z}$ and $C^{(4)}$, and this map is indeed a similarity that multiplies lengths by 2 (and norms by 4).

Let us first show that the theta series of $C^{(4)}$ is given by $\vartheta_3(\tau)\vartheta_3(2\tau)\vartheta_3(4\tau)$: The lattice $C^{(4)}$ consists of points of the form $(r, \sqrt{2}s, 2t)$, where $r, s, t \in \mathbb{Z}$. The definition of the theta series is

$$\sum_{n=0}^{\infty} r(n) e^{\imath\pi\tau n},$$

where $r(n)$ is the number of vectors of length n. Since every point in the lattice is of the form $(r, \sqrt{2}s, 2t)$, and its distance from the origin is $\sqrt{r^2 + 2s^2 + 4t^2}$, we conclude that $r(n)$ is the number of integer solutions of the equation $n^2 = r^2 + 2s^2 + 4t^2$. On the other hand

$$\begin{aligned}
&\vartheta_3(\tau)\vartheta_3(2\tau)\vartheta_3(4\tau) = \\
&\quad \sum_{k=-\infty}^{\infty} e^{\imath\pi\tau k^2} \sum_{m=-\infty}^{\infty} e^{\imath\pi 2\tau m^2} \sum_{n=-\infty}^{\infty} e^{\imath\pi 4\tau n^2} \\
&\quad = \sum_{k=-\infty}^{\infty} \sum_{m=-\infty}^{\infty} \sum_{n=-\infty}^{\infty} e^{\imath\pi\tau(k^2 + 2m^2 + 4n^2)}.
\end{aligned}$$

Writing $\ell = k^2 + 2m^2 + 4n^2$, we conclude that the expression above can be written in the form

$$\sum_{\substack{\ell = k^2 + 2m^2 + 4n^2 \\ k,m,n \in \mathbb{Z}}} e^{\imath\pi\tau\ell} = \sum_{\ell=0}^{\infty} r(\ell) e^{\imath\pi\tau\ell},$$

so the product gives the same expression as direct use of theta functions definitions. Similarly we can conclude that the theta series of $(\sqrt{2}\mathbb{Z})^3$ is given by $\vartheta_3(2y)^3$.

We may now limit to the purely imaginary values. Write $\tau = y\imath$. We find it convenient to work with the reciprocal of the secrecy function:

$$\begin{aligned}
1/\Xi_{C^{(4)}}(y) &= \frac{\vartheta_3(y\imath)\vartheta_3(2y\imath)\vartheta_3(4y\imath)}{\vartheta_3^3(2y\imath)} \qquad (4) \\
&= \frac{\vartheta_3(y\imath)\vartheta_3(4y\imath)}{\vartheta_3^2(2y\imath)}.
\end{aligned}$$

We find it convenient as well to put $z = 2y$. Thus, to show that the secrecy function of $C^{(4)}$ defined in (1) attains a minimum at $y = 1/2$, we need to show that the modified function

$$f(y) = \frac{\vartheta_3(y\imath/2)\vartheta_3(2y\imath)}{\vartheta_3^2(y\imath)} \qquad (5)$$

(where by abuse of notation we have retained the symbol y for the new variable z) has a maximum at $y = 1$.

We now invoke results connecting theta functions at the purely imaginary values $\tau = \imath y$ $(y > 0)$ and $\tau/2$ (i.e., at $q = e^{-\pi y}$ and $\sqrt{q}$) from [12]; a summary of what we need is in [12, Section 4.6, Page 137]. We build on the notation "k" and "l" of [12] and write more specifically $k(q)$, $k'(q)$, $l(q)$, and $l'(q)$ for the objects:

$$\begin{aligned}
k(q) &= \frac{\vartheta_2^2(q)}{\vartheta_3^2(q)} \qquad (6) \\
k'(q) &= \sqrt{1 - k^2(q)} = \frac{\vartheta_4^2(q)}{\vartheta_3^2(q)} \\
l(q) &= k(\sqrt{q}) = \frac{\vartheta_2^2(\sqrt{q})}{\vartheta_3^2(\sqrt{q})} \\
l'(q) &= k'(\sqrt{q}) = \frac{\vartheta_4^2(\sqrt{q})}{\vartheta_3^2(\sqrt{q})}
\end{aligned}$$

(The expression for $k'(q)$ arises from the first equation of (3) above.) Finally, we write

$$M_2(q) = \frac{\vartheta_3^2(q)}{\vartheta_3^2(\sqrt{q})}. \qquad (7)$$

As described in [12], $M_2(q)$ can be written in terms of $k(q)$, $k'(q)$, $l(q)$, and $l'(q)$, and further, $k(q)$ and $l(q)$ are connected by a "modular equation." We have the relations ([12, Section 4.6, Page

137] (these can also be directly derived from the properties of theta functions in (3))

$$M_2(q) = \frac{1}{1+k(q)} = \frac{1+l'(q)}{2}, \tag{8}$$

and

$$\begin{aligned} l(q) &= \frac{2\sqrt{k(q)}}{1+k(q)} \\ k(q) &= \frac{1-l'(q)}{1+l'(q)} \end{aligned} \tag{9}$$

Since $f(y) = \dfrac{M_2(q^2)}{M_2(q)}$, Equations (8) show that

$$\begin{aligned} f(y) = \frac{1+k(q)}{1+k(q^2)} &= \frac{(1+k(q))(1+l'(q^2))}{2} \\ &= \frac{(1+k(q))(1+k'(q))}{2}. \end{aligned} \tag{10}$$

Thus, we need to maximize $(1+k(q))(1+k'(q))$ where $k(q)^2 + k'(q)^2 = 1$. Putting $k(q) = \cos(\alpha) = \dfrac{1-t^2}{1+t^2}$ and $k'(q) = \sin(\alpha) = \dfrac{2t}{1+t^2}$, where $t = \tan(\alpha/2)$, we find need to determine the extrema of

$$f(t) = \frac{(1+t)^2}{(1+t^2)^2}. \tag{11}$$

Now $0 < k(q) < 1$ and $0 < k'(q) < 1$ by definition of $k(q)$, $k'(q)$ and the relation $k(q)^2 + k'(q)^2 = 1$. Thus, $0 < \alpha < \pi/2$, so $0 < \alpha/2 < \pi/4$. It follows that $0 < t < 1$. Calculus now shows that that $t = \sqrt{2} - 1$ is the unique (and hence global) maximum of $f(t)$ in the region $0 < t < 1$.

Corresponding to $t = \sqrt{2} - 1$, we find $\alpha/2 = \pi/8$, i.e., $\alpha = \pi/4$. Thus, q is such that $k(q) = k'(q)$, i.e., $\vartheta_2(y) = \vartheta_4(y)$. This occurs precisely at $y = 1$ (see for instance [7, Proof of Lemma 1], or [12, Exercise 4, Section 2.3] along with [12, Exercise 8b, Section 3.1]). Further, we see that $f(y)$ considered as a function of y has the same increase/decrease behavior on either side of $y = 1$ as $f(t)$ does on either side of $t = \sqrt{2} - 1$ when considered as a function of t: The map $y \mapsto k(e^{-\pi y})$ is a monotonically decreasing map ([12, Equation 2.3.9, Page 42], this also follows from Lemma 3 ahead, and the fact that $k^2 + k'^2 = 1$), while the map $k(e^{-\pi y}) = \cos(\alpha) \mapsto t = \tan(\alpha/2)$ is also monotonically decreasing. The chain rule now shows that df/dy and df/dt have the same sign. It follows that $f(y)$ increases for $0 < y < 1$ and decreases for $1 < y < \imath!nfty$; correspondingly, since $1/\Xi_{C^{(4)}}(y) = f(2y)$, we find $\Xi_{C^{(4)}}$ *decreases* for $0 < y < 1/2$ and *increases* for $1/2 < y < \infty$.

Thus, $C^{(4)}$ violates the conjecture.

Remark 1. The graph of the secrecy function of $C^{(4)}$ may be computed (approximately), using Mathematica®. The graph is shown in Figure 1, and verifies our analysis above.

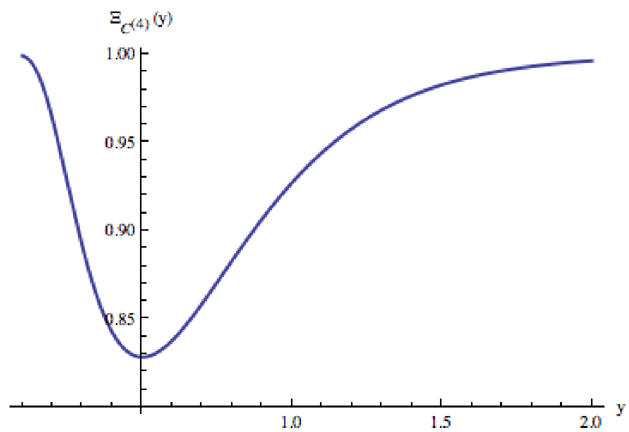

Fig. 1. Secrecy function of lattice $C^{(4)}$. Notice that according to the original conjecture, the function should have its maximum at $y = \frac{1}{2}$, but it has a minimum.

IV. Modified Secrecy Function

The current definition of the secrecy function compares the theta series of an l-modular lattice in $\mathbb{R}^n$ to the theta series of the (scaled) unimodular lattice $\lambda\mathbb{Z}^n$, which is not l-modular unless $l = 1$. A more natural definition would be one that compared likes with likes: that compared the theta series of an l-modular lattice to that of the simplest possible l-modular lattice, replicated suitably to match volumes.

Belfiore, Solé and Oggier [8] normalised the theta function of a given lattice using a scaled cubic lattice in the same dimension. (This could be interpreted as comparing the confusion proved at Eve's end using the given lattice for coding with the confusion provided when there is no coding.) However, since the scaled cubic lattice lattice is not modular (unless $l = 1$), this function is very difficult to work with. For instance, consider the case of $C^{(4)}$ (see Figure 1): since higher values of the secrecy function correspond to higher confusion at Eve's end, we find that the behavior of the current secrecy function does not yield insights into where the lattice provides maximum confusion compared to $\mathbb{Z}^n$, instead it only shows where the confusion is *least.* Thus, a different normalization is needed.

The simplest l-modular lattice is $D^{(l)} = \mathbb{Z} \oplus \sqrt{l}\mathbb{Z}$ (when $l = 1$, we take $D^{(l)} = \mathbb{Z}$). Note that $D^{(l)}$ can be proved to be l-modular for $l > 1$ exactly like the lattice $C^{(4)}$ in Section III—the dual is the lattice $\mathbb{Z} \oplus (1/\sqrt{l})\mathbb{Z}$, and the required map on $\mathbb{R}^2$ is the one that takes (x, y) to $(\sqrt{l}y, \sqrt{l}x)$. Accordingly, we write $n = k \dim(D^{(l)})$ $(= 2k$ for $l > 1)$, and for an l-modular lattice Λ in $\mathbb{R}^n$, we define the *l-modular secrecy function* $\Xi_l(y)$ (or $\Xi_{l,\Lambda}(y)$ if the lattice Λ needs to be emphasized), by

$$\Xi_l(y) = \Xi_{l,\Lambda}(y) := \frac{\Theta_{D^{(l)}}(y\imath)^k}{\Theta_\Lambda(y\imath)}, \quad y > 0. \tag{12}$$

(Note that when $l = 1$, $k = n$, $D^{(l)} = \mathbb{Z}$, and this definition reduces to the earlier definition of the secrecy function of a unimodular lattice. Note too that this modified function is only to be used for comparing two different l-modular lattices, not two arbitrary lattices. It can be interpreted as comparing the confusion caused at Eve's end using this lattice for coding with the confusion provided when the simplest l-modular lattice is used for coding: the higher the value of the l-modular secrecy function, the greater the confusion caused compared to $D^{(l)}$.)

When l is not a square, n must necessarily be even, as we have noted in Section II. When l is a square, n need not be even, as the example of $C^{(4)}$ attests. In such cases, the definition above of the secrecy function involves a square root of the theta series of $D^{(l)}$. (Of course, we are scaling up the theta series, not the lattice!)

It is reasonable now, particularly in the light of results we present in the next section, to modify the original conjecture and make the following *l-modular secrecy function conjecture:*

Conjecture 2 (l-modular secrecy function conjecture)**.** *Let Λ be an l-modular lattice in dimension n. Write $n = k \dim(D^{(l)})$. Then*

$$\Xi_{l,\Lambda}(y) := \frac{\Theta_{D^{(l)}}(y\imath)^k}{\Theta_\Lambda(y\imath)},$$

defined for $y > 0$, attains its (global) maximum at $1/\sqrt{l}$.

We show in the next section that this new conjecture holds for various 2-modular lattices in small dimension. But we can see immediately that it holds for $C^{(4)}$ as follows:

$$\begin{aligned} \Xi_l(y) &= \Xi_{l,C^{(4)}}(y) \\ &= \frac{(\vartheta_3(y\imath)\vartheta_3(4y\imath))^{3/2}}{\vartheta_3(y\imath)\vartheta_3(2y\imath)\vartheta_3(4y\imath)} \\ &= \frac{(\vartheta_3(y\imath)\vartheta_3(4y\imath))^{1/2}}{\vartheta_3(2y\imath)}. \end{aligned} \tag{13}$$

But we have already seen above in Section III that $\Xi_l(y)^2 = \dfrac{\vartheta_3(y\imath)\vartheta_3(4y\imath)}{\vartheta_3^2(2y\imath)}$ has a global maximum at $y = 1/2$, so $\Xi_l(y)$ also has a global maximum at $y = 1/2$. Thus, our modified conjecture is true for $C^{(4)}$.

Remark 2. The l-modular secrecy function exhibits "multiplicative symmetry" about the point $1/\sqrt{l}$, that is, $\Xi_l(a) = \Xi_l(b)$ when $ab = 1/l$. The proof is the same as that for the originally defined secrecy function, [8, Prop. 2].

V. 2-MODULAR LATTICES

In the following, we will show that the l-modular secrecy function conjecture stated above holds for all the 2-modular lattices considered in [13]. The starting point is the following description of the theta series of such a lattice:

Theorem 1. *The theta series of a 2-modular lattice Λ in dimension $n = 2k$ is a polynomial*

$$\begin{aligned} \Theta_\Lambda(y\imath) &= f_1(y)^k \left(\sum_{i=0}^{\lfloor k/2 \rfloor} a_i f_2(y)^i \right) \\ &= \sum_{i=0}^{\lfloor k/2 \rfloor} a_i f_1^{k-2i} \Delta_4(y)^i, \end{aligned} \tag{14}$$

where $f_1(y) = \Theta_{C^{(2)}}(y\imath)$, $f_2(y) = \dfrac{\vartheta_2^2(2y\imath)\vartheta_4^2(y\imath)}{4\vartheta_3^2(y\imath)\vartheta_3^2(2y\imath)}$, and $\Delta_4 = f_1^2 f_2$.

This theorem follows from a more general theorem of Rains and Sloane ([14, Theorem 9, Corollary 3]. Although it is only applied to odd 2-modular lattices in [13, Eqns 29, 30], the theorem above actually holds for any 2-modular lattice. We can see this as follows: the theorem and corollary referred to in [14] apply to strongly l-modular lattices that are rationally equivalent to $(C^{(l)})^k$ (where $n = 2k$).

The definition of strongly modularity in [14] (see the discussion in that paper, following Theorem 6) shows that when l is prime, any l-modular lattice is automatically strongly l-modular. We thus need the following theorem to enable us to apply the results of [14, Theorem 9, Corollary 3] to any 2-modular lattice:

Theorem 2. *All 2-modular lattices in $\mathbb{R}^n$ ($n = 2k$) are rationally equivalent to $(C^{(2)})^k$.*

Proof. This is well known, and falls out easily from the classification theorem for quadratic forms over $\mathbb{Q}$. For lack of a specific reference, we sketch the proof in Appendix A. $\square$

For us, since 2 is prime, $C^{(2)}$ is the same as $D^{(2)}$, we find

$$\Xi_{2,\Lambda}(y) = \Xi_2(y) = \left(\sum_{i=0}^{\lfloor k/2 \rfloor} a_i f_2(y)^i\right)^{-1}. \tag{15}$$

We will study the general behavior of such a polynomial function of f_2 and then apply our results to the specific theta series computed in [13].

We have, using (3):

$$\begin{aligned} f_2(y) &= \frac{\vartheta_2^2(2y\imath)\vartheta_4^2(y\imath)}{4\vartheta_3^2(y\imath)\vartheta_3^2(2y\imath)} \qquad (16)\\ &= \frac{(\vartheta_3^2(y\imath) - \vartheta_4^2(y\imath))\vartheta_4^2(y\imath)}{4(\vartheta_3^2(y\imath) + \vartheta_4^2(y\imath))\vartheta_3^2(y\imath)} \\ &= \frac{(1-\alpha)\alpha}{4(1+\alpha)}, \end{aligned}$$

where $\alpha = \alpha(y) = \dfrac{\vartheta_4^2}{\vartheta_3^2}(y\imath)$.

Lemma 3. *The function $\dfrac{\vartheta_4}{\vartheta_3}(y\imath)$ is strictly increasing for (positive) real y, and as $y \to 0$, the function approaches 0, and as $y \to \infty$, the function approaches 1.*

Proof. A formal proof that takes care of intricacies of infinite products and interchanges of limits is in Appendix A. The intuition is as follows: Using the product representations of ϑ_4 and ϑ_3 in (2), we have

$$\frac{\vartheta_4}{\vartheta_3}(y\imath) = \frac{\prod_{m=1}^{\infty}(1-q^{2m})(1-q^{2m-1})^2}{\prod_{m=1}^{\infty}(1-q^{2m})(1+q^{2m-1})^2}$$
$$= \prod_{m=1}^{\infty}\left(\frac{1-q^{2m-1}}{1+q^{2m-1}}\right)^2 = \prod_{m=1}^{\infty}\left(\frac{2}{1+q^{2m-1}} - 1\right)^2$$

Now, as y increases, q decreases, and hence, $\left(\frac{2}{1+q^{2m-1}} - 1\right)$ increases. This shows that the function is increasing. Furthermore, as $y \to 0$, $q^{2m-1} \to 1$, and $\left(\frac{2}{1+q^{2m-1}} - 1\right) \to 0$. As $y \to \infty$, $q^{2m-1} \to 0$, and $\left(\frac{2}{1+q^{2m-1}} - 1\right) \to 1$.

$\square$

Lemma 4. *The function*

$$f(x) = \frac{(1-x)x}{(1+x)}$$

has a unique maximum in the open interval $(0, 1)$, and this maximum is met at the point $x = \sqrt{2} - 1$.

Proof. This is straightforward. $\square$

Remark 3. The value of f_2 when $\alpha = \sqrt{2} - 1$ is $\dfrac{(1-(\sqrt{2}-1))(\sqrt{2}-1)}{4(1+\sqrt{2}-1)} \approx 0.0429$. We will denote this value by β in what follows.

Lemma 5. *The quantity $\dfrac{\vartheta_4^2}{\vartheta_3^2}(y\imath)$ takes on the value $\sqrt{2} - 1$ precisely when $y = 1/\sqrt{2}$.*

Proof. This is in Appendix A $\square$

We now use the previous results to prove the following:

Proposition 6. *A necessary and sufficient condition for $\Xi_2(y)$ to have a global maximum at $y = 1/\sqrt{2}$ is that the polynomial $(\Xi_2(f_2))^{-1} = \left(\sum_{i=0}^{\lfloor k/2 \rfloor} a_i f_2(y)^i\right)$ in the variable f_2, restricted to the domain $0 < f_2 \leq \beta$ where β as in Remark 3 above, have a global minimum at $f_2 = \beta$.*

Proof. By (16), $f_2(y) = \dfrac{(1-\alpha)\alpha}{4(1+\alpha)}$, where $\alpha = \alpha(y) = \dfrac{\vartheta_4^2}{\vartheta_3^2}(y\imath)$, so by Lemma 4, $f_2(\alpha)$ has a unique maximum when $\alpha = \sqrt{2} - 1$. By Remark 3 this maximum is β. Moreover, by Lemma 5, $\alpha = \sqrt{2}-1$ precisely when $y = 1/\sqrt{2}$. Thus, for other values of y, $f_2(y) < \beta$, and of course, $f_2(y) > 0$ by the definition of f_2 and by the fact that $\alpha \in (0, 1)$. We thus find that as y ranges in $(0, \infty)$, $f_2(y)$ ranges in $(0, \beta]$, and $f_2(y) = \beta$ precisely when $y = 1/\sqrt{2}$. It is now clear that $\Xi_2(y)$, with $0 < y < \infty$, attains its global maximum when $y = 1/\sqrt{2}$ if and only if $(\Xi_2(y))^{-1}$, with $0 < y < \infty$, attains its global minimum when $y = 1/\sqrt{2}$ if and only if $(\Xi_2(f_2))^{-1}$, with $f_2 \in (0, \beta]$, attains its global minimum at $f_2 = \beta$.

□

Corollary 7. *If the polynomial $(\Xi_2(f_2))^{-1}$ is decreasing in $(0, \beta]$, then Ξ_2 has a global maximum at $y = 1/\sqrt{2}$.*

We now consider the odd 2-modular lattices in [13, Table 2]. The authors have computed their theta series in terms of f_2 and $\Delta_4 = f_1^2 f_2$. Factoring $f_1^{n/2}$ from these series (where n is the ambient dimension), we have the following table, where the third column contains the derivative of the polynomial $(\Xi_2(f_2))^{-1}$, and the fourth column checks that this derivative is negative in $(0, \beta]$, i.e, (Corollary 7) that $(\Xi_2(f_2))^{-1}$ is decreasing in $(0, \beta]$:

Dim	$(\Xi_2(f_2))^{-1}$	$d/df_2\,(\Xi_2(f_2))^{-1}$	Neg in $(0,\beta]$?
8	$1-8f_2$	-8	Yes
12	$1-12f_2$	-12	Yes
16	$1-16f_2$	-16	Yes
18	$1-18f_2+18f_2^2$	$-18+36f_2$	Yes
20	$1-20f_2+40f_2^2$	$-20+80f_2$	Yes
22	$1-22f_2+66f_2^2$ $-4f_2^3$	$-22+132f_2-12f_2^2$	Yes
24	$1-24f_2+96f_2^2$ $-28f_2^3$	$-24+192f_2-84f_2^2$	Yes
26	$1-26f_2+130f_2^2$ $-80f_2^3$	$-26+260f_2-240f_2^2$	Yes
28	$1-28f_2+168f_2^2$ $-176f_2^3+32f_2^4$	$-28+336f_2-528f_2^2$ $+128f_2^3$	Yes
30	$1-30f_2+210f_2^2$ $-282f_2^3+112f_2^4$	$-30+420f_2-846f_2^2$ $+448f_2^3$	Yes

TABLE I
VERIFYING CONJECTURE 2 FOR THE ODD 2-MODULAR LATTICES IN [13, TABLE 2]

Clearly, the modified conjecture holds for these lattices.

For illustration, we graph the l-modular secrecy function for the odd 2-modular lattice in dimension 22 considered above in Figure 2.

We turn our attention now to the even 2-modular lattices considered in [13, Table 1]. There are three of them: D_4, BW_{16}, HS_{20}. There, their theta series have been developed in terms of two functions: the theta series of D_4 itself, and Δ_{16}:

$$\begin{aligned}\Theta_{BW_{16}} &= \Theta_{D_4}^4 - 96\Delta_{16}, \quad \text{and}\\ \Theta_{HS_{20}} &= \Theta_{D_4}^5 - 120\Theta_{D_4}\Delta_{16}.\end{aligned}$$

By Theorem 1, these theta series can be also expressed as polynomials in $\Theta_{C^{(2)}}$ and Δ_4. By

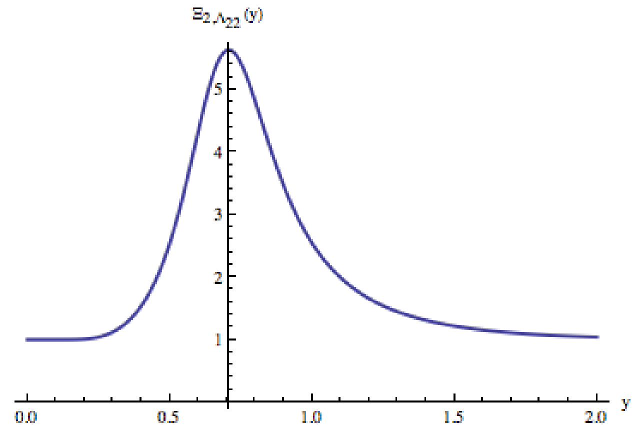

Fig. 2. The l-modular secrecy function of the odd 2-modular 22-dimensional lattice considered in [13, Table 2]. It has its maximum at $y = \frac{1}{\sqrt{2}}$.

comparing coefficients, we have

$$\begin{aligned}\Theta_{D_4} &= \Theta_{C^{(2)}}^2 - 4\Delta_4\\ \Theta_{BW_{16}} &= \Theta_{C^{(2)}}^8 - 16\Delta_4\Theta_{C^{(2)}}^6 -\\ &\quad 256\Delta_4^3\Theta_{C^{(2)}}^2 + 256\Delta_4^4\\ \Theta_{HS_{20}} &= \Theta_{C^{(2)}}^{10} - 20\Theta_{C^{(2)}}^8\Delta_4 +\\ &\quad 40\Theta_{C^{(2)}}^6\Delta_4^2 - 160\Theta_{C^{(2)}}^4\Delta_4^3 +\\ &\quad 1280\Theta_{C^{(2)}}^2\Delta_4^4 - 1024\Delta_4^5.\end{aligned}$$

Since $\Theta_{C^{(2)}} = f_1$ and $\Delta_4 = f_1^2 f_2$, the 2-modular secrecy functions Ξ_2 are

$$\begin{aligned}\Xi_{2,D_4} &= (1-4f_2)^{-1}\\ \Xi_{2,BW_{16}} &= (1-16f_2-256f_2^3+256f_2^4)^{-1}\\ \Xi_{2,HS_{20}} &= (1-20f_2+40f_2^2 -\\ &\quad 160f_2^3+1280f_2^4-1024f_2^5)^{-1}.\end{aligned}$$

The function $(1-4f_2)^{-1}$ is clearly increasing in the range of f_2. As for $\Xi_{2,BW_{16}}$, the derivative of the denominator is

$$-16 - 768f_2^2 + 1024f_2^3,$$

which has its only real zero at $f_2 \approx 0.78$, and therefore, the denominator is decreasing and the function increasing in $[0, \beta]$. Finally, the derivative of the denominator of the 2-modular secrecy function of HS_{20} is

$$-20 + 80f_2 - 480f_2^2 + 5120f_2^3 - 5120f_2^4.$$

The first positive real zero is at $f_2 \approx 0.17$, and therefore the denominator is decreasing and the function increasing in $[0, \beta]$.

VI. Discussion

Based on our numerical and preliminary work, it seems that a similar l-modular counterexample to Conjecture 1 can be found for all $l > 1$. Here is the graph for for $l = 3$ produced by Mathematica®, which suggests that $l = 3$ is also a counterexample.

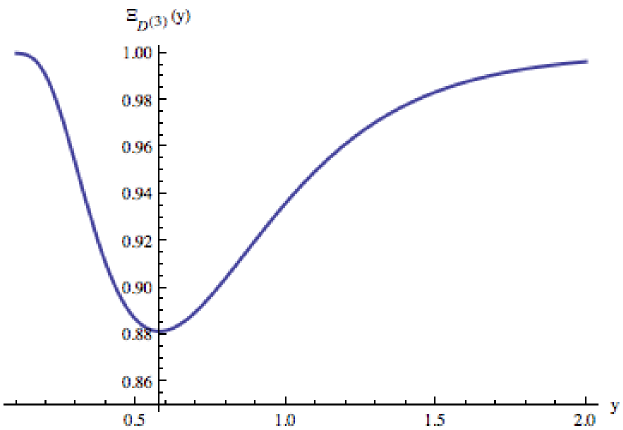

Fig. 3. The secrecy function of $D^{(3)} = \mathbb{Z} \oplus \sqrt{3}\mathbb{Z}$. According to the original conjecture, it should have its maximum at $y = \frac{1}{\sqrt{3}}$ but it has its minimum.

The original and modified secrecy functions differ only by the scaling factor which is the same for all n-dimensional l-modular lattices when n and l do not vary. They both accomplish the task of minimizing Eve's probability, namely, ranking lattices based on the behavior of the theta function of Eve's lattice. The new function is easier to analyze since its both denominator and numerator are theta functions of l-modular lattices. Since the old and new functions are closely connected, analyzing the new function can also be used to analyze the older function.

The old function does not always satisfy the conjecture of Belfiore and Solé. The new function is built using those lattices as scaling lattices which do not satisfy the conjecture using the old function. It seems plausible that these lattices are the least optimal ones, and that thereby, the new function satisfies the conjecture.

Acknowledgement

The authors wish to thank Daniel Katz for some illuminating discussions at the start of this project and for reading portions of the paper, Jean-Claude Belfiore for some discussions on the results in this paper and on further directions, and Eric Rains for some discussions on the proof of Theorem 2. Ernvall-Hytönen wishes to thank the mathematics department of California State University Northridge for her visit there during which this research was initiated. The research of Ernvall-Hytönen was funded by the Academy of Finland grants 138337 and 138522, while that of B.A. Sethuraman was supported by U.S. National Science Foundation grant CCF-1318260.

Appendix

We sketch here the proof of Theorem 2. We assume basic familiarity with quadratic forms. The proof invokes the local-global theory of quadratic forms over number fields; we only sketch the outlines of the theory and only provide as much detail as would enable one to construct the full proof for oneself. An excellent reference is [15]. A very readable account is also in [16].

We recall first the setup behind rational equivalence: Any symmetric $n \times n$ matrix A with entries in $\mathbb{Q}$ (such as the Gram matrix G_L of an integral lattice L in $\mathbb{R}^n$, whose entries are even in $\mathbb{Z}$) determines a quadratic form q on $\mathbb{Q}^n$ in the standard way: if e_i are the standard basis vectors, then $q(x_1e_1 + \cdots + x_ne_n) = v^tAv$, where $v = (x_1, \ldots, x_n)^t$; here the superscript t stands for transpose. Conversely, given a quadratic form q on $\mathbb{Q}^n$, we obtain a symmetric $n \times n$ matrix A with rational entries, with (i, j) entry given by $(q(e_i + e_j) - q(e_i) - q(e_j))/2$, . We say two quadratic forms q_1 and q_2 on $\mathbb{Q}^n$ are equivalent over $\mathbb{Q}$, or *rationally equivalent*, if there exists an invertible $n \times n$ matrix with rational entries S such that $S^tA_1S = A_2$, where A_i is the symmetric matrix associated with q_i as above. Alternatively, two such quadratic forms are rationally equivalent if one can be obtained from the other by a linear change of variables defined over $\mathbb{Q}$. (These definitions extend in the obvious way to quadratic forms over any field of characteristic different from 2.) We apply these considerations to lattices: two integral lattices L_1 and L_2 are said to be rationally equivalent if their associated quadratic forms are rationally equivalent, or equivalently, if the Gram matrices G_1 and G_2 of the two lattices are related by $S^tG_1S = G_2$ for some invertible $n \times n$ matrix S with rational entries.

There is a well-established theory that determines when two quadratic forms defined over $\mathbb{Q}$ are equivalent. By this theory, the rational equivalence class of a quadratic form on $\mathbb{Q}^n$ which is non degenerate, that is, the determinant of the associated symmetric matrix is nonzero, is determined by the following objects: the *discriminant*, the *signature*, and the *Hasse-Witt invariant* at each (integer) prime p. The first two are easy to describe. The *discriminant* of a non degenerate quadratic form defined over $\mathbb{Q}$ is just the class of the determinant of the associated symmetric matrix in $\mathbb{Q}^*/\mathbb{Q}^{*2}$. As for the signature recall first that given any symmetric $n \times n$ matrix A with entries in a field k of characteristic different from 2, there exists a nonsingular $n \times n$ matrix S such that $S^t AS$ is diagonal. The *signature* of a non degenerate quadratic form on $\mathbb{Q}^n$ is just the number of positive entries minus the number of negative entries in any diagonal representation of the quadratic form, thought of as a quadratic form on $\mathbb{R}^n$. (The definition is independent of which diagonal representation is used.) In our situation, note that the quadratic forms arising from the 2-modular lattice L and from $(C^{(2)})^k$ are both positive definite, since they yield lengths of vectors in Euclidean space. It follows that all diagonalizations of either quadratic form must consist only of positive elements along the diagonal. Thus, the signature is the same for both lattices. Further, both lattices clearly have the same determinant for their associated quadratic form, namely 2^k. Thus, to prove the rational equivalence of L and $(C^{(2)})^k$, we only need to consider their Hasse-Witt invariants, and to show that their Hasse-Witt invariants are the same at each prime p.

In fact, the Hasse-Witt invariant is defined not only for each integer prime p, but also, for $\mathbb{R}$. (It is traditional to think of $\mathbb{R}$ as the completion of $\mathbb{Q}$ at the "infinite prime.") In what follows, v will denote either an integer prime p or ∞, and $\mathbb{Q}_v$ will accordingly denoted either the field $\mathbb{Q}_p$ of p-adic rationals (when $v = p$) or $\mathbb{R}$ (when $v = \infty$). Given a non degenerate quadratic form q over the field $\mathbb{Q}_v$, one first takes a diagonal representation $\mathrm{diag}(a_1, \ldots, a_n)$ of the associated symmetric matrix. The *Hasse-Witt invariant* $\epsilon_v(q)$ is defined to be the product of the *Hilbert symbols* $(a_i, a_j)_v$ over all $1 \le i < j \le n$). (The definition is independent of which diagonal representation is used.) In turn, given a and b in $\mathbb{Q}_v^*$, the *Hilbert symbol* $(a, b)_v$ is defined to be 1 if the equation $z^2 - ax^2 - by^2$ has a solution $(x, y, z) \neq (0, 0, 0)$ in $\mathbb{Q}_v$, and -1 otherwise. A few relevant facts about the Hasse-Witt invariant and the Hilbert symbol are the following:

1) The Hasse-Witt invariant of a quadratic form q defined over $\mathbb{Q}^n$ is 1 at all but at most a finite number of primes v. (Here, for each prime v, we first view q as a quadratic form over $\mathbb{Q}_v^n$ and then calculate $\epsilon_v(q)$.)
2) For a quadratic form q defined over $\mathbb{Q}^n$, the product over all primes v of $\epsilon_v(q)$ is 1.
3) For an odd (integer) prime p, given a and b in $\mathbb{Q}_p^*$, the Hilbert symbol $(a, b)_p$ is defined as follows: we first write $a = p^\alpha u$ and $b = p^\beta v$, where u and v are units of $\mathbb{Z}_p$. Then
$$(a, b) = (-1)^{\alpha\beta(p-1)/2} \left(\frac{u}{p}\right)^\beta \left(\frac{v}{p}\right)^\alpha, \quad (17)$$
where $\left(\frac{u}{p}\right)$ is the *Legendre symbol* defined to be 1 if the class of u in $\mathbb{F}_p$ is a square and -1 otherwise.

It follows from the characterization above that if p is odd and a and b are themselves *units* in $\mathbb{Q}_p$ (by units in $\mathbb{Q}_p$ we mean that α and β above are both zero, so these are the units of $\mathbb{Z}_p$), then the Hilbert symbol $(a, b)_p$ is 1. Also, the Hilbert Symbol $(a, b)_\infty$ is 1 whenever both a and b are positive, since $z^2 = ax^2 + by^2$ will clearly have a nontrivial solution, e.g., $(1, 0, \sqrt{a})$, or $(0, 1, \sqrt{b})$. (In fact, it is enough that just one of a or b is positive.) Now apply these considerations to the lattice $(C^{(2)})^k$: the associated quadratic form $q_{(C^{(2)})^k}$ is already diagonal, with k 1s and k 2s along the diagonal. For any odd prime p, 1 and 2 are both units, and therefore, $\epsilon_p(q_{(C^{(2)})^k}) = 1$. It is clear too that $\epsilon_\infty(q_{(C^{(2)})^k}) = 1$ since 1 and 2 are positive. It follows from (2) above that $\epsilon_2(q_{(C^{(2)})^k}) = 1$ as well.

We now consider $\epsilon_v(q_L)$ at each integer prime and at infinity, where q_L is the quadratic form associated to the 2-regular lattice L. As already noted, since q_L is positive definite, any diagonalization over $\mathbb{R}$ must consist of all positive numbers along the diagonal. Thus, $\epsilon_\infty(q_L) = 1$. It is enough now to show that for any odd prime p, $\epsilon_p(q_L) = 1$, for then, by (2) above, $\epsilon_2(q_L)$ will be 1 as well. The key is the following proposition that describes a diagonalization. Recall that $\mathbb{Z}_{(p)}$ denotes the localization of $\mathbb{Z}$ at p, that is, the ring of all reduced fractions a/b such that p does not divide b; $\mathbb{Z}_{(p)}$ is a unique factorization domain with a single prime, namely p, and the reduced fraction a/b above of $\mathbb{Z}_{(p)}$ is divisible by p precisely when a is divisible by p. Under the embedding

$\mathbb{Q} \mapsto \mathbb{Q}_p$, $\mathbb{Z}_{(p)}$ goes to the p-adic integers $\mathbb{Z}_p$, and the elements of $\mathbb{Z}_{(p)}$ not divisible by p live naturally as units in the p-adic integers $\mathbb{Z}_p$.

Proposition 8. *Suppose that A is a symmetric matrix in $M_n(\mathbb{Q})$ and suppose that p does not divide the determinant of A, where p is an odd prime. Then, there exists an $n \times n$ matrix S with entries in $\mathbb{Z}_{(p)}$ of determinant ± 1 such that $S^t AS = diag(a_1, \ldots, a_n)$, where the numerators and denominators of each a_i, when written as a reduced fraction, is not divisible by p.*

(For the full statement of the proposition, see [16, Lemma 5.1].)

Proof. We sketch the proof here. Since p does not divide the determinant, some entry $a_{i,j}$ of A must be prime to p. First suppose that some $a_{i,i}$ is prime to p. Then, we swap the basis vectors e_1 and e_i, a transformation of determinant -1, to ensure that $a_{1,1}$ is prime to p. If all $a_{i,i}$ are divisible by p, some $a_{i,j}$ with $i \neq j$ must be prime to p. We consider $(e_i + e_j)^t A(e_i + e_j)$: this is $a_{i,i} + a_{j,j} + 2a_{i,j}$. Since each $a_{i,i}$ and $a_{j,j}$ are divisible by p and since p is odd and $a_{i,j}$ is prime to p, we find $(e_i+e_j)^t A(e_i+e_j)$ is prime to p. Thus, the transformation $e_1 \mapsto (e_i + e_j)$, $e_i \mapsto e_1$ is of determinant -1, and ensures that $a_{1,1}$ is prime to p. Thus by a change of basis with determinant -1, we can ensure that $a_{1,1}$ is prime to p. We now write A in the block form

$$A = \begin{pmatrix} a_{1,1} & B \\ B^t & C \end{pmatrix},$$

and take S to be the matrix

$$\begin{pmatrix} 1 & -a_{1,1}^{-1}B \\ 0 & I_{n-1} \end{pmatrix}$$

to find

$$S^t AS = \begin{pmatrix} a_{1,1} & 0 \\ 0 & C - a_{1,1}^{-1}B^t B \end{pmatrix}.$$

(Notice that S has determinant 1.) We now proceed by induction, working in $\mathbb{Z}_{(p)}$, noting that the product of the various basis-change matrices at each stage has determinant ± 1.

□

Since the determinant of the matrix associated to q_L is 2^k, we may apply this result to q_L. For a given odd prime p, take a diagonal representation $\mathrm{diag}(a_1, \ldots, a_n)$ of q_L over $\mathbb{Q}_p$ as furnished by the proposition. Each a_i is nonzero element of $\mathbb{Z}_{(p)}$ not divisible by p, and is therefore a unit in $\mathbb{Q}_p$. Thus, by (17) above, the Hasse-Witt invariant $\epsilon_p(q_L)$ is 1. By (2) above, $\epsilon_2(q_L)$ is also 1.

Since L and $(C^{(2)})^k$ have the same Hasse-Witt invariant at every prime in addition to having the same signature and discriminant, they are indeed rationally equivalent as claimed.

Proof of Lemma 3. We use the product representations of the theta functions. Writing $q = e^{-\pi y}$ as usual, so $0 < q < 1$, we have

$$\begin{aligned} \vartheta_4(y\imath) &= \prod_{m=1}^{\infty}(1-q^{2m})(1-q^{2m-1})^2 \\ \vartheta_3(y\imath) &= \prod_{m=1}^{\infty}(1-q^{2m})(1+q^{2m-1})^2 \end{aligned}$$

Since the partial products $P_N = \prod_{m=1}^{N}(1-q^{2m})(1-q^{2m-1})^2$ and $Q_N = \prod_{m=1}^{N}(1-q^{2m})(1+q^{2m-1})^2$ converge to $\vartheta_4(y\imath)$ and $\vartheta_3(y\imath)$ respectively, and since Q_N is clearly not zero for $0 < q < 1$, the quotient P_N/Q_N converges to $\frac{\vartheta_4}{\vartheta_3}(y\imath)$, and we have

$$\begin{aligned} \frac{\vartheta_4}{\vartheta_3}(y\imath) &= \lim_{N\to\infty} \frac{\prod_{m=1}^{N}(1-q^{2m})(1-q^{2m-1})^2}{\prod_{m=1}^{N}(1-q^{2m})(1+q^{2m-1})^2} \\ &= \lim_{N\to\infty} \prod_{m=1}^{N} \left(\frac{1-q^{2m-1}}{1+q^{2m-1}}\right)^2 \\ &= \lim_{N\to\infty} \prod_{m=1}^{N} \left(\frac{2}{1+q^{2m-1}} - 1\right)^2 \\ &= \prod_{m=1}^{\infty} \left(\frac{2}{1+q^{2m-1}} - 1\right)^2. \end{aligned}$$

Note that since $0 < q < 1$,

$$0 < \left(\frac{2}{1+q^{2m-1}} - 1\right)^2 < 1.$$

As y increases, q strictly decreases, and $\left(\frac{2}{1+q^{2m-1}} - 1\right)$ strictly increases. Hence, if $y > y'$, then the partial products (note that these start from 2)

$$R_N(y) = \prod_{m=2}^{N} \left(\frac{2}{1+q^{2m-1}} - 1\right)^2$$

satisfy $P_N(y) > P_N(y')$. It follows that $\lim_{N\to\infty} R_N(y) \geq \lim_{N\to\infty} R_N(y')$. Note that $\lim_{N\to\infty} R_N(y) \neq 0$ for any y with $0 < y < 1$ since $\vartheta_4(y\imath)$ and $\vartheta_3(y\imath)$ and hence $\frac{\vartheta_4}{\vartheta_3}(y\imath)$ are nonzero for any y with $0 < y < 1$. Writing q' for $e^{-\pi y'}$, we have for $m = 1$ that

$$\left(\frac{2}{1+q} - 1\right)^2 > \left(\frac{2}{1+q'} - 1\right)^2.$$

Hence we find

$$\begin{aligned}\frac{\vartheta_4}{\vartheta_3}(y\imath) &= \left(\frac{2}{1+q} - 1\right)^2 \prod_{m=2}^{\infty}\left(\frac{2}{1+q^{2m-1}} - 1\right)^2 \\ &> \left(\frac{2}{1+q'} - 1\right)^2 \prod_{m=2}^{\infty}\left(\frac{2}{1+q'^{2m-1}} - 1\right)^2 \\ &= \frac{\vartheta_4}{\vartheta_3}(y').\end{aligned}$$

Hence, $\frac{\vartheta_4}{\vartheta_3}(y\imath)$ is a strictly increasing function of y.

As for the limits as y tends to 0 or ∞, note that $y \to 0$ precisely when $q \to 1$, and $y \to \infty$ precisely when $q \to 0$. Now

$$\begin{aligned}\frac{\vartheta_4}{\vartheta_3}(y\imath) &= \left(\frac{2}{1+q} - 1\right)^2 \prod_{m=2}^{\infty}\left(\frac{2}{1+q^{2m-1}} - 1\right)^2 \\ &\leq \left(\frac{2}{1+q} - 1\right)^2,\end{aligned}$$

and of course $\left(\frac{2}{1+q} - 1\right)^2 \to 0$ as $q \to 1$, i.e., when $y \to 0$.

Let us now consider the case $y \to \infty$, i.e. $q \to 0$. Since $\vartheta_4(y\imath)$ is absolutely convergent for $0 < q < 1$, we can group the terms in the following way:

$$\begin{aligned}\vartheta_4(y\imath) &= 1 - 2q + 2(q^4 - q^9) + 2(q^{16} - q^{25}) + \cdots \\ &> 1 - 2q,\end{aligned}$$

since $q^n > q^m$ when $n < m$.

On the other hand $q^4 - q^9 < q^4 < q$; $q^{16} - q^{25} < q^{16} < q^2$, etc., so

$$\begin{aligned}\vartheta_4(y\imath) &< 1 - 2q + 2(q + q^2 + \cdots) \\ &= 1 - 2q + \frac{2q}{1-q}.\end{aligned}$$

Hence, $1 - 2q < \vartheta_4(y\imath) < 1 - 2q + \frac{2q}{1-q}$. Now, as $q \to 0$, the two terms on either side of $\vartheta_4(y\imath)$ tend to 1, so $\vartheta_4(y\imath)$ also tends to 1.

We argue similarly for $\vartheta_3(y\imath)$: $1 < \vartheta_3(y\imath) < 1 + 2(q + q^2 + q^3 + \cdots)$, where we have used $q^4 < q^2$, $q^9 < q^3$, $q^{16} < q^4$, etc. Thus, we find $1 < \vartheta_3(y\imath) < 1 + \frac{2q}{1-q}$. Taking limits as $q \to 0$, we find $\vartheta_3(y\imath)$ tends to 1.

Thus, as $q \to 0$, $\vartheta_4(y\imath)$ and $\vartheta_3(y\imath)$ each tend to 1, so their quotient tends to 1. □

Proof of Lemma 5. By [12, Theorem 2.3], for $k = \frac{\vartheta_2^2(y\imath)}{\vartheta_3^2(y\imath)}$,

$$\pi\frac{K'(k)}{K(k)} = -\log q. \qquad (18)$$

Here,

$$K(k) = \int_0^1 \frac{dt}{(1-t^2)(1-k^2t^2)}$$

and $K'(k) = K(k')$, where $k' = \sqrt{1-k^2}$. By [12, Exercise 4, §1.6],

$$\frac{K'}{K}(\sqrt{2}-1) = \sqrt{2}. \qquad (19)$$

In fact, we can see this as follows: Denoting $\sqrt{2}-1$ temporarily by α, we have $\alpha' = \sqrt{1-\alpha^2} = \sqrt{2\alpha}$. By [12, Theorem 1.2 (a), §1.4],

$$K(\alpha) = \frac{1}{1+\alpha}K\left(\frac{2\sqrt{\alpha}}{1+\alpha}\right).$$

For our choice of α, $\frac{2\sqrt{\alpha}}{1+\alpha}$ is just α', so the relation above becomes $K(\alpha) = \frac{1}{1+\alpha}K'(\alpha)$, which yields (19) above.

Now, since $k' = \frac{\vartheta_4^2(y\imath)}{\vartheta_3^2(y\imath)}$, we have in our situation $k' = \sqrt{2} - 1$, hence, for $k = \sqrt{1-k'^2}$, the expression $\frac{K'(k)}{K(k)}$ on the left side of (18) equals $\frac{K(k')}{K'(k')} = \frac{K}{K'}(\sqrt{2}-1) = 1/\sqrt{2}$. Hence, from (18) and the fact that $q = e^{-\pi y}$, we find $\pi(1/\sqrt{2}) = \pi y$, so $y = 1/\sqrt{2}$. Moreover, by Lemma 3 above, this is the unique value of y for which $\frac{\vartheta_4^2}{\vartheta_3^2}(y\imath)$ attains this value. □

We note that theta functions have been computed for special values of y, some of which can be found in [17] for instance.

References

[1] A. D. Wyner. The wire-tap channel. *Bell. Syst. Tech. Journal*, 54(October), 1975.

[2] Frédérique Oggier and Jean-Claude Belfiore, "Secrecy Gain: a Wiretap Lattice Code Design," in *ISITA*, 2010, pp. 174–178.

[3] Jean-Claude Belfiore and Patrick Solé, "Unimodular Lattices for the Gaussian Wiretap Channel," available online at http://arxiv.org/abs/1007.0449v1

[4] A.-M. Ernvall-Hytönen, "On a conjecture by Belfiore and Solé on some lattices,"IEEE Transactions on Information Theory, 58 (9), 5950–5955. Available online at http://arxiv.org/abs/1104.3739

[5] Fuchun Lin and Frédérique Oggier, "A Classification of Unimodular Lattice Wiretap Codes in Small Dimensions," IEEE Transactions on Information Theory, 59 (6), 3295–3303. Available online at http://arxiv.org/pdf/1201.3688.pdf.

[6] Julia Pinchak, "Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture," Proceedings of ISIT 2013, pp. 2617–2620.

[7] Julia Pinchak and B.A. Sethuraman, "The Belfiore-Solé Conjecture and a Certain Technique for Verifying it for a Given Lattice", Proceedings of ITA 2014, available online at http://www.csun.edu/˜asethura/papers/ITA_2014Mod.pdf

[8] Frédérique Oggier, Patrick Solé, and Jean-Claude Belfiore, "Lattice Codes for the Wiretap Gaussian Channel: Construction and Analysis," available online at http://arxiv.org/abs/1103.4086v1.

[9] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, third edition, Springer-Verlag, 1999.

[10] E. M. Stein and R. Shakarchi, Princeton Lectures in Analysis II Complex Analysis, Princeton University Press, 2003.

[11] H.-G. Quebbemann, "Modular Lattices in Euclidean Spaces", Journal of Number Theory, **54**, pp.190–202, 1995.

[12] Jonathan M. Borwein and Peter B. Borwein, PI and the AGM, Canadian Math. Society Series of Monographs and Advanced Texts, John Wiley.

[13] Fuchun Lin, Frédérique Oggier, and Patrick Solé, "2- and 3-modular Lattice Wiretap Codes in Small Dimensions," available online at http://arxiv.org/abs/1304.4440

[14] E. M. Rains and N. J. A. Sloane, "The Shadow Theory of Modular and Unimodular Lattices," Journal of Number Theory, **73**, pp. 359–389, 1998.

[15] Jean-Pierre Serre, A Course in Arithmetic, GTM 7, Springer-Verlag, 1973.

[16] Gordon Pall, "The Arithmetical Invariants of Quadratic Forms," Bull. Amer. Math. Soc. Volume 51, Number 3 (1945), 185-197. Available online at http://projecteuclid.org/euclid.bams/1183506825

[17] Andreas Dieckmann, http://pi.physik.uni-bonn.de/~dieckman/InfProd/InfProd.html

Author Biography

1) Anne-Maria Ernvall-Hytönen received her PhD at the University of Turku in 2008. Currently, she works at Åbo Akademi University. She is interested in questions in analytic and transcendental number theory, and applications in coding theory.
2) B.A. Sethuraman received his Ph.D degree in Mathematics from the University of California at San Diego in 1991. He is currently a full professor of mathematics at California State University Northridge. His research interests lie in algebraic number theory (particularly division algebras) and algebraic geometry, and in applications of mathematics to wireless communication. He has also authored undergraduate texts in algebra, including one available for free under the GNU license on his website (http://www.csun.edu/~asethura/), as well as other expository articles. He considers it a privilege to have contributed to wireless communication.