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

Anne-Maria Ernvall-Hytönen
Department of Mathematics and Statistics
00014 University of Helsinki
Finland
Email: anne-maria.ernvall-hytonen@helsinki.fi

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

***Abstract*—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.**

***Index Terms*—l-Modular Lattice, Wiretap Coding, Secrecy Function.**

I. Introduction

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 $l = 1$, of course, an l-modular lattice is known as a *unimodular* lattice.

The secrecy function was introduced in [7] 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 [1, 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

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

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. As indicated in the equation above, when working exclusively with purely imaginary values $\imath y$ of τ, we will simply write $\Theta_L(y)$ for $\Theta_L(\imath y)$.

The secrecy function was studied in detail in [1] by Belfiore and Solé. Assuming that the noise variance σ_e^2 on Eve's channel is much higher than the corresponding variance σ_e^2 on Bob's channel, they analyze the probability of both users 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 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 [1] that for a unimodular lattice ($l = 1$), the secrecy function assumes its (global) maximum at $y = 1$. This has since been verified for a large number of lattices (see e.g., [4], [5], [9], [10]), and it was proven in [9] 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 ($l > 1$): they conjectured that the secrecy function of l-modular lattices attains its (global) maximum at $y = 1/\sqrt{l}$ ([8, Proposition 2, and Conjecture 1].

We show in this paper that this extended conjecture is false in general. 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 suggest how the secrecy function should be modified in the l-modular situation ($l > 1$) so as to compare likes with likes.

II. 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 Equation 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).

Recall the Jacobi theta functions $\vartheta_3(q)$, $\vartheta_2(q)$ and $\vartheta_4(q)$, where $q = e^{\imath\pi\tau}$, $im(\tau) > 0$. We will interchangeably use the notation $\vartheta_3(\tau)$, $\vartheta_2(\tau)$ and $\vartheta_4(\tau)$ when thinking of these as functions of τ instead of q, the usage will be clear from the context. These are given by

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

These functions satisfy, for instance, the following formulas ([3, page 104]):

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

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

In this paper we will be concerned with purely imaginary values of τ: $\tau = \imath y$ where $y > 0$. As with theta series of lattices, we will simply write $\vartheta_3(y)$, $\vartheta_2(y)$ and $\vartheta_4(y)$ for $\vartheta_3(\imath y)$, $\vartheta_2(\imath y)$ and $\vartheta_4(\imath y)$. The Jacobi theta functions ϑ_2, ϑ_3 and ϑ_4 are useful in representing the theta functions of various lattices. A thorough introduction to the theory of these functions can be found in [13, 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 [3, page 102] for instance, but note the slight difference in the definitions of Θ in [13] and [3].)

Note that the theta series of $C^{(4)}$ (for $\tau = \imath y$, $y > 0$) is given by $\vartheta_3(y)\vartheta_3(2y)\vartheta_3(4y)$, and the theta series of $(\sqrt{2}\mathbb{Z})^3$ is given by $\vartheta_3(2y)^3$. We find it convenient to work with the reciprocal of the secrecy function:

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

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

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

(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 [2]; a summary of what we need is in [2, Section 4.6, Page 137]. We build on the notation "k" and "l" of [2] 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 of Equations 3 above.) Finally, we write

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

As described in [2], $M_2(q)$ 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 ([2, Section 4.6, Page 137] (these can also be directly derived from the properties of theta functions in Equations 3)

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

and

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

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

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

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

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

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 [10, Proof of Lemma 1], or [2, Exercise 4, Section 2.3] along with [2, 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 ([2, Equation 2.3.9, Page 42]), 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 $1 < y < \infty$; 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.

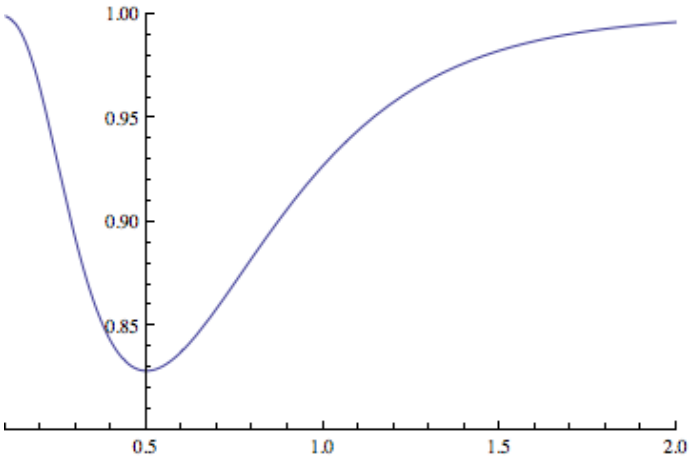

Fig. 1. Graph of secrecy function of lattice $C^{(4)}$. Notice that according to the original conjecture, the function should have its maximum at $x = \frac{1}{2}$, but it has a minimum.

III. 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 $\mathbb{Z}^n$. 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 another reference l-modular lattice, scaled suitably to match volumes.

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 exactly like the lattice $C^{(4)}$ in Section II—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

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

(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.)

When l is not a square, n must necessarily be even, as we have noted in Section I. 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 to modify the original conjecture and make the following *l-modular secrecy function conjecture:* that for all l-modular lattices, the l-modular secrecy function attains its (global) maximum at $1/\sqrt{l}$. In future work we will show 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:

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

But we have already seen above in Section II that $\Xi_l(y)^2 = \frac{\vartheta_3(y)\vartheta_3(4y)}{\vartheta_3^2(2y)}$ 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].

Acknowledgment

A full-length version of this paper, consisting of other results besides the ones above, has been submitted for publication elsewhere and is undergoing review ([14]). The authors wish to thank Daniel Katz for some illuminating discussions at the start of this project, and Jean-Claude Belfiore for some discussions on the results in this paper. 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, 138522 and 283262, and by the Finnish Cultural Foundation, while that of B.A. Sethuraman was supported by U.S. National Science Foundation grant CCF-1318260.

References

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

[2] Jonathan M. Borwein and Peter B. Borwein, PI and the AGM, Canadian Math. Society Series of Monographs and Advanced Texts, John Wiley.
[3] J. H. Conway and N. J. A. Sloane, Sphere packings, lattices and groups, third edition, Springer-Verlag, 1999.
[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] 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
[7] Frédérique Oggier and Jean-Claude Belfiore, "Secrecy Gain: a Wiretap Lattice Code Design," in *ISITA*, 2010, pp. 174–178.
[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] Julia Pinchak, "Wiretap Codes: Families of Lattices Satisfying the Belfiore-Solé Secrecy Function Conjecture," Proceedings of ISIT 2013, pp. 2617–2620.
[10] 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
[11] H.-G. Quebbemann, "Modular Lattices in Euclidean Spaces", Journal of Number Theory, **54**, pp.190–202, 1995.
[12] 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.
[13] E. M. Stein and R. Shakarchi, Princeton Lectures in Analysis II Complex Analysis, Princeton University Press, 2003.
[14] A.-M. Ernvall-Hytönen and B.A. Sethuraman, "Counterexample to the Generalized Belfiore-Solé Secrecy Function Conjecture for l-modular lattices," submitted for publication, available at http://arxiv.org/abs/1409.3188