Ernvall-Hytönen, Anne-Maria; Vesalainen, Esa V.

On the secrecy gain of ℓ-modular lattices. (English) Zbl 1447.11077

SIAM J. Discrete Math. 32, No. 2, 1441-1457 (2018).

In a lattice code the codewords are elements of cosets in a quotient Λ/M where Λ is a lattice (namely a discrete additive subgroup of the additive structure of a real vector space) and M a sublattice. The decoding procedure consists of the calculation of the closest coset to the received codeword. This problem is related naturally to the sphere packing problem, in which the centers of the spheres are precisely the lattice points. On the other hand, the kissing number of a lattice packing is the number of balls touching the sphere centered at the origin. When considering the generating function of the number of lattice points for each integer, which is indeed the theta series of the lattice, the kissing number is given by its first non-zero coefficient.

The cubic lattice is the lattice consisting of points in the real space having just integer coordinates, it is $\mathbb{Z}^n$. Belfiore and Oggier defined (see [*F. Oggier* et al., IEEE Trans. Inf. Theory 62, No. 10, 5690–5708 (2016; Zbl 1359.94149)]) the secrecy function of a lattice by comparing its theta series with the theta series of the cubic lattice, $\forall y \in \mathbb{R}^+$, $\Xi_\Lambda(y) = \Theta_{\mathbb{Z}^n}(y)/\Theta_\Lambda(y)$ and it was observed that for unimodular lattices, namely lattices whose primitive cells have volume 1, this function attains its maximum at $y = 1$. An ℓ-modular lattice is an integral lattice such that for an orthogonal map U, $\sqrt{\ell}U(\Lambda^*) \subset \Lambda$. In an ℓ-modular lattice the primitive cell has volume $\ell^{\frac{n}{4}}$ and the secrecy function is defined by comparison with the rescaled cubic lattice $(\ell^{\frac{n}{4}}\mathbb{Z})^n$. Hence, it was conjectured that its maximum is attained at $y = \ell^{-\frac{1}{2}}$. The authors of the reviewed paper refuted this conjecture by a counterexample and they suggested an alternative secrecy function, considering the lattice D^ℓ instead of the cubic lattice, and they re-asserted the above conjecture with respect to their proposed secrecy function. In this paper the authors propose a sufficient condition for the conjecture to hold. The techniques are rather technical but very illustrative of the involved geometrical notions, all of them relevant to these numerical lattices.

Reviewer: Guillermo Morales Luna (Ciudad de México)

MSC:

11H71	Relations with coding theory	Cited in **2** Documents
94A62	Authentication, digital signatures and secret sharing	
11F20	Dedekind eta function, Dedekind sums	
11F27	Theta series; Weil representation; theta correspondences	

Keywords:

lattices; theta-functions; ϑ-functions; secrecy gain; ℓ-modular lattices; secrecy function conjecture

Full Text: DOI

References:

[1] J.-C. Belfiore and F. E. Oggier, \textit{Secrecy gain: A wiretap lattice code design}, in ISITA, 2010, pp. 174–178.

[2] J.-C. Belfiore and P. Solé, \textit{Unimodular lattices for the Gaussian wiretap channel}, in ITW, 2010.

[3] A.-M. Ernvall-Hytönen, \textit{On a conjecture by Belfiore and Solé on some lattices}, IEEE Trans. Inform. Theory, 58 (2012), pp. 5950–5955. · Zbl 1364.11132

[4] A.-M. Ernvall-Hytönen and C. Hollanti, \textit{On the eavesdropper's correct decision in Gaussian and fading wiretap channels using lattice codes}, in ITW, 2011, pp. 210–214.

[5] A.-M. Ernvall-Hytönen and B. A. Sethuraman, \textit{Counterexample to the generalized Belfiore-Solé secrecy function conjecture for l-modular lattices}, IEEE Trans. Inform. Theory, 62 (2016), pp. 4514–4522. · Zbl 1359.94591

[6] M. Faulhuber, \textit{Extremal Bounds of Gaussian Gabor Frames and Properties of Jacobi's Theta Functions}, doctoral dissertation, University of Vienna, Vienna, Austria, 2016.

[7] M. Faulhuber and S. Steinerberger, \textit{Optimal Gabor frame bounds for separable lattices and estimates for Jacobi theta functions}, J. Math. Anal. Appl., 445 (2017), pp. 407–422. · Zbl 1351.42039

[8] B. Hernandez, \textit{Results on the Secrecy Function Conjecture on the Theta Function of Lattices}, master's thesis, California State University, Northridge, CA, 2016.

[9] X. Hou, F. Lin, and F. Oggier, \textit{Construction and secrecy gain of a family of 5-modular lattices}, in ITW, 2014, pp. 117–121.

[10] F. Lin, \textit{Lattice Coding for the Gaussian Wiretap Channel — A Study of the Secrecy Gain}, doctoral dissertation, Nanyang Technical University, Singapore, 2013.

[11] F. Lin and F. Oggier, \textit{Secrecy gain of Gaussian wiretap codes from unimodular lattices}, in ITW, 2011, pp. 718–722.

[12] F. Lin and F. Oggier, \textit{A classification of unimodular lattice wiretap codes in small dimensions}, IEEE Trans. Inform. Theory, 59 (2013), pp. 3295–3303. · Zbl 1364.94761

[13] F. Lin, F. Oggier, and P. Solé, \textit{2- and 3-modular lattice wiretap codes in small dimensions}, Appl. Algebr. Eng. Comm., 26 (2015), pp. 571–590. · Zbl 1343.94098

[14] F. Oggier, P. Solé, and J.-C. Belfiore, \textit{Lattice codes for the wiretap Gaussian channel: Construction and analysis}, IEEE Trans. Inform. Theory, 62 (2016), pp. 5690–5708. · Zbl 1359.94149

[15] J. Pinchak, \textit{Wiretap codes: Families of lattices satisfying the Belfiore-Solé secrecy function conjecture}, in ISIT, 2013, pp. 2617–2620.

[16] J. Pinchak and B. A. Sethuraman, \textit{The Belfiore-Solé conjecture and a certain technique for verifying it for a given lattice}, in ITA, 2014, pp. 486–488.

[17] E. M. Rains and N. J. A. Sloane, \textit{The shadow theory of modular and unimodular lattices}, J. Number Theory, 73 (1998), pp. 359–389. · Zbl 0917.11026

[18] J.-P. Serre, \textit{Cours d'arithmétique}, Le Mathématicien, Presses Universitaires de France, Paris, France, 2007.

[19] B. A. Sethuraman, \textit{private communication}.

[20] G. R. D. A. S. Strey, \textit{A série teta e a funça☒o de sigilo de um reticulado}, master's thesis, University of Campinas, Campinas, Brazil, 2016.

[21] A. D. Wyner, \textit{The wire-tap channel}, Bell. Syst. Tech. J., 54 (1975), pp. 1355–1387. · Zbl 0316.94017

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.