Title of Thesis

A Thesis

Submitted for the Degree of

Doctor of Philosophy

in the **Faculty of Engineering**

by

Your Name

under the Guidance of

Advisor

Electrical Communication Engineering

Indian Institute of Science

Bangalore – 560 012, INDIA

Month Year

TO

Write a dedication here.

Some fancy quotes...

If numbers aren't beautiful, I don't know what is.

— Paul Erdős

Acknowledgments

Acknowledgments go here.

Statement of Originality

I hereby declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at any university or other institute of higher education.

I certify that to the best of my knowledge, the intellectual content of this thesis is the product of my own work and that all the assistance received in preparing this thesis and sources have been acknowledged.

Publications based on this Thesis

Journal

J1 Journal 1

Conference

C1 Conference 1

Preface

Describe who did what, collaborations, etc.

Also mention what content was published in the papers mentioned previously.

Abstract

Abstract here. Limit to around 2 pages.

Contents

List of Tables

List of Figures

Keywords

Information theory, nested lattice codes, physical-layer security, etc...

Notation

Sets

$\mathbb{R}$	The set of real numbers
$\mathbb{R}^+$	The set of nonnegative real numbers
$\mathbb{Z}$	The set of integers
$\mathbb{Z}^+$	The set of nonnegative integers
$\mathbb{F}_p$	Finite field with p elements
$\mathbb{Z}_p$	The set of integers modulo p
$\mathrm{vol}(\mathcal{S})$	Volume of the set $\mathcal{S}$
$\bigtimes_{i=1}^{m} A_i$	Cartesian product of the sets $A_1, \ldots, A_m$

Vectors and matrices

$\mathcal{S}^n$	Set of column vectors of length n with entries from $\mathcal{S}$
$\mathbf{x}, \mathbf{y}, \mathbf{u}, \mathbf{v}, \mathbf{w}, \ldots$	Vectors
$\mathsf{A}, \mathsf{B}, \mathsf{G}, \ldots$	Matrices
A^T	Transpose of A
I_n	$n \times n$ identity matrix
$\lVert\mathbf{x}\rVert$	ℓ^2-norm of $\mathbf{x}$
$\mathrm{Supp}(\mathbf{x})$	Support of the vector $\mathbf{x}$, i.e., the set of indices corresponding to nonzero entries of $\mathbf{x}$

Random Variables and Events

pmf	Probability mass function
pdf	Probability density function
iid	Independent and identically distributed
$U, V, X, Y, Z, \ldots$	Random variables
$\mathbf{U}, \mathbf{V}, \mathbf{W}, \mathbf{Z}, \ldots$	Random vectors
$\Pr[A]$	Probability of event A
$\mathbb{E}[Z]$	Expectation of the random variable Z
$H(X)$	Entropy of the random variable X
$H(X\|Y)$	Conditional entropy of X given Y
$I(X;Y)$	Mutual information between X and Y
$X \perp\!\!\!\perp Y$	X and Y are independent random variables
$X \sim \mathcal{N}(a, \sigma^2)$	X is a Gaussian random variable with mean a and variance σ^2

Sequences

$f(n) = O(g(n))$	$\exists c > 0$ such that $f(n) < cg(n)$ for all sufficiently large n
$f(n) = \Omega(g(n))$	$\exists c > 0$ such that $g(n) < cf(n)$ for all sufficiently large n
$f(n) = o(g(n))$	$f(n)/g(n) \to 0$ as $n \to \infty$
$f(n) = o_n(1)$	$f(n) \to 0$ as $n \to \infty$

Graphs

$\mathcal{G} = (\mathcal{V}, \mathcal{E})$	Graph $\mathcal{G}$ with vertex set $\mathcal{V}$ and edge set $\mathcal{E}$
$\mathcal{G} = ((\mathcal{L}, \mathcal{R}), \mathcal{E})$	Bipartite graph $\mathcal{G}$ with vertex set $\mathcal{L} \cup \mathcal{R}$ and edge set $\mathcal{E}$. Here, $\mathcal{L}$ denotes the set of left vertices, and $\mathcal{R}$ denotes the set of right vertices.
$\mathtt{u}, \mathtt{v}, \ldots$	Vertices
$N(\mathtt{u})$	Neighbourhood of $\mathtt{u}$, i.e., the set of all vertices $\mathtt{v}$ such that $(\mathtt{u}, \mathtt{v})$ is an edge
$\mathcal{A}, \mathcal{B}, \ldots$	Subsets of $\mathcal{V}$
$N(\mathcal{A})$	Neighbourhood of $\mathcal{A}$, i.e., $\cup_{\mathtt{u} \in \mathcal{A}} N(\mathtt{u})$

Lattices

Λ, Λ_0	Lattices
$\Lambda^{(n)}, \Lambda_0^{(n)}$	Lattices in $\mathbb{R}^n$.
$Q_\Lambda(\mathbf{x})$	Lattice point (in Λ) closest to $\mathbf{x}$
$[\mathbf{x}] \bmod \Lambda$	$\mathbf{x} - Q_\Lambda(\mathbf{x})$
$\mathcal{V}(\Lambda)$	Fundamental Voronoi region of Λ
$r_{\text{cov}}(\Lambda)$	Covering radius of Λ
$r_{\text{pack}}(\Lambda)$	Packing radius of Λ
$r_{\text{eff}}(\Lambda)$	Effective radius of Λ
$\text{vol}\Lambda$ or $\det \Lambda$	Volume of the fundamental Voronoi region of Λ

Chapter 1

Introduction

This is an introductory chapter. Describe what your thesis is all about here.

Use some equations:

$$H(X) = -\sum_{x\in\mathcal{X}} p(x)\log_2 p(x).$$

Add some figures, like Fig. 1.1 or Fig. 1.2.

Cite many papers [1, 2].

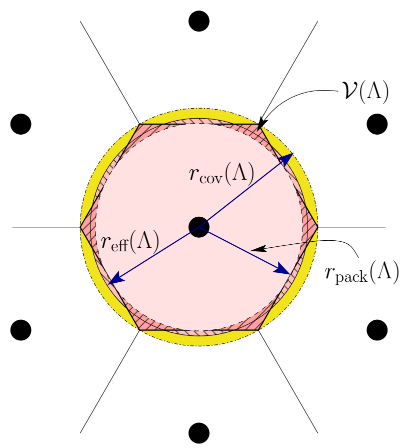

Figure 1.1: Illustrating the covering, packing and effective radii of the hexagonal lattice.

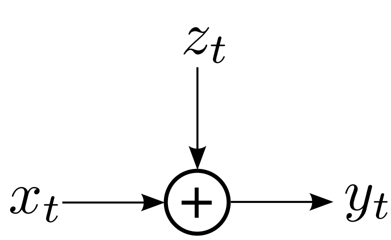

Figure 1.2: The AWGN channel.

Chapter 2

Introduction

References

[1] R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography. Part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 7, pp. 1121–1132, Jul. 1993.

[2] S. Agrawal and S. Vishwanath, “On the secrecy rate of interference networks using structured codes,” *Proc. 2009 IEEE Int. Symp. Information Theory*, Seoul, Korea, pp. 2091–2095.

[3] I.-J. Baik and S.-Y. Chung, “Network coding for two-way relay channels using lattices,” *Proc. IEEE Int. Conf. Communications*, Beijing, China, 2008, pp. 3898–3902.

[4] A. Barg and G. Zémor, “Concatenated codes: Serial and parallel,” *IEEE Trans. Inf. Theory,* vol. 51, no. 5, pp. 1625–1634, May 2005.

[5] A. Barvinok, *Math 669: Combinatorics, Geometry and Complexity of Integer Points*. [Online]. Available: `http://www.math.lsa.umich.edu/~barvinok/latticenotes669.pdf`.

[6] J.-C. Belfiore and F. Oggier, “Secrecy gain: A wiretap lattice code design,” *Proc. 2010 Int. Symp. Information Theory and Its Applications*, Taichung, Taiwan, pp. 174–178.

[7] J.-C. Belfiore, “Lattice codes for the compute-and-forward protocol: The flatness factor,” in *Proc. 2011 Information Theory Workshop*, Paraty, Brazil.

[8] M. Bellare, S. Tessaro, and A. Vardy, “Semantic security for the wiretap channel,”

Adv. Cryptology–CRYPTO 2012, Berlin, Germany: Springer Berlin-Heidelberg, pp. 294–311, 2012.

[9] A. L. Bertozzi, J. B. Garnett, and T. Laurent, "Characterization of radially symmetric finite time blowup in multidimensional aggregation equations," *SIAM J. Math. Anal.*, vol. 44, no. 2, pp. 651–681, 2012.

[10] M. Bloch, J. Barros, M.R. Rodrigues, and S.W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.

[11] M. Bloch and J. Barros, *Physical-Layer Security: From Information Theory to Security Engineering,* Cambridge, U.K.: Cambridge University Press, 2011.

[12] F. Boccardi, R.W. Heath, A. Lozano, T.L. Marzetta, and P. Popovski, "Five disruptive technology directions for 5G," *IEEE Comm. Mag.*, vol. 52, no. 2, pp. 74–80, Feb. 2014.

[13] G. Bresler, A. Parekh, and D.N.C. Tse, "The approximate capacity of the many-to-one and one-to-many Gaussian interference channels," *IEEE Trans. Inf. Theory*, vol. 56, no. 9, pp. 4566–4592, Sep. 2010.

[14] J.H. Conway and N.J. Sloane, *Sphere Packings, Lattices and Groups*, New York: Springer-Verlag, 1988.

[15] T. Cover and J. Thomas, *Elements of Information Theory*, 2nd ed. New York: Wiley-Interscience, 1996.

[16] R. Cramer, Y. Dodis, S. Fehr, C. Padro, and D. Wichs, "Detection of algebraic manipulation with applications to robust secret sharing and fuzzy extractors," *Adv. Cryptology–EUROCRYPT 2008*, Berlin, Germany: Springer Berlin-Heidelberg, pp. 471–488, 2008.

[17] I. Csiszár and J. Körner. "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory,* vol. 24, no. 3, pp. 339–348, May 1978.

[18] I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” *IEEE Trans. Inf. Theory,* vol. 46, no. 3, pp. 344–366, Mar. 2000.

[19] I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec. 2004.

[20] R. de Buda, “Some optimal codes have structure,” *IEEE J. Sel. Areas in Communications*, vol. 7, no. 6, pp. 893–899, 1989.

[21] N. di Pietro, “On infinite and finite lattice constellations for the additive white Gaussian noise channel,” Ph.D. dissertation, Math. Dept., Univ. Bordeaux, Bordeaux, France, 2014.

[22] N. di Pietro, J.J. Boutros, G. Zémor, and L. Brunel, “Integer low-density lattices based on Construction A,” *Proc. 2012 Information Theory Workshop*, Lausanne, Switzerland, 2012, pp. 422–426.

[23] N. di Pietro, J.J. Boutros, G. Zémor, and L. Brunel, “New results on low-density integer lattices,” *Proc. 2013 Information Theory and Applications Workshop*, San Diego, 2013, pp. 10–15.

[24] N. di Pietro, G. Zémor, and J. J. Boutros, “New results on Construction A lattices based on very sparse parity-check matrices,” in *Proc. 2013 IEEE Int. Symp. Information Theory*, Istanbul, Turkey, pp. 1675–1679.

[25] N. di Pietro, G. Zémor, and J. J. Boutros, “LDA Lattices Without Dithering Achieve Capacity on the Gaussian Channel,” arXiv preprint, 2016. [Online] Available: `http://arxiv.org/abs/1603.02863`.

[26] A. Dasgupta, *Probability for Statistics and Machine Learning*, New York: Springer Texts in Statistics, 2011.

[27] W. Ehm, T. Gneiting, and D. Richards, “Convolution roots of radial positive definite functions with compact support,” *Trans. AMS*, vol. 356, no. 11, pp. 4655–4685, May 2004.

[28] U. Erez and R. Zamir, “Achieving 1/2log(1+SNR) on the AWGN channel with lattice encoding and decoding,” *IEEE Trans. Inf. Theory*, vol. 50, no. 10, pp. 2293–2314, Oct. 2004.

[29] U. Erez, S. Litsyn, and R. Zamir, “Lattices which are good for (almost) everything,” *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3401–3416, Oct. 2005.

[30] U. Erez, S. Shamai, and R. Zamir, “Capacity and lattice strategies for canceling known interference,” *IEEE Trans. Inf. Theory*, vol. 51, no. 11, pp. 3820–3833, Nov. 2005.

[31] U. Erez and S. ten Brink, “A close-to-capacity dirty paper coding scheme,” *IEEE Trans. Inf. Theory*, vol. 51, no. 10, pp. 3417–3432, Oct. 2005.

[32] A. Elbert and A. Laforgia, “An asymptotic relation for the zeros of Bessel functions,” *J. Math. Analysis and Applications*, vol. 98, no. 2, pp. 502–510, 1984.

[33] W. Feller, *An Introduction to Probability Theory and Its Applications, Vol. 2*, 2nd ed. New York: Wiley, 1971.

[34] G.D. Forney, *Concatenated Codes,* Cambridge, U.K.: MIT press, 1966.

[35] G.D. Forney and M.D. Trott, “The dynamics of group codes: Dual abelian group codes and systems,” *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 2935–2965, Dec. 2004.

[36] A. Gersho, “Asymptotically optimal block quantization,” *IEEE Trans. Inf. Theory,* vol. 25, no. 4, pp. 373–380, 1979.

[37] R.M. Gray and D.L. Neuhoff, “Quantization,” *IEEE Trans. Inf. Theory,* vol. 44, no. 6, pp. 2325–2383, Oct. 1998.

[38] T.C. Gulcu and A. Barg, “Achieving secrecy capacity of the wiretap channel and broadcast channel with a confidential component,” in *Proc. 2015 Inf. Theory Workshop,* Jerusalem, Israel.

[39] D. Hankerson, A.J. Menezes, and S. Vanstone, *Guide to Elliptic Curve Cryptography,* Springer Science & Business Media, 2006.

[40] X. He and A. Yener, "Providing secrecy with lattice codes," *Proc. 46th Annual Allerton Conf. on Communication, Control, and Computing*, Monticello, IL, 2008, pp. 1199–1206.

[41] X. He and A. Yener, "Strong secrecy and reliable Byzantine detection in the presence of an untrusted relay," *IEEE Trans. Inf. Theory*, vol. 59, no. 1, pp. 177–192, Jan. 2013.

[42] X. He and A. Yener, "End-to-end secure multi-hop communication with untrusted relays," *IEEE Trans. Wireless Comm.*, vol. 12, no. 1, pp. 1–11, Jan. 2013.

[43] X. He and A. Yener, "Providing secrecy with structured codes: Two-user Gaussian channels," *IEEE Trans. Inf. Theory*, vol. 60, no. 4, pp. 2121–2138, Apr. 2014.

[44] I.N. Herstein, *Topics in Algebra*, 2nd ed. New York: Wiley, 1975.

[45] A. Joseph and A.R. Barron, "Least squares superposition codes of moderate dictionary size are reliable at rates up to capacity," *IEEE Trans. Inf. Theory*, vol. 58, no. 5, pp. 2541–2557, May. 2012.

[46] A. Joseph and A.R. Barron, "Fast sparse superposition codes have near exponential error probability for $R < C$," *IEEE Trans. Inf. Theory*, vol. 60, no. 2, pp. 919–942, Feb. 2014.

[47] D.A. Karpuk and A. Chorti, "Perfect secrecy in physical layer network coding systems from structured interference," *arXiv preprint,* arXiv:1507.01098, 2015.

[48] N. Kashyap, V. Shashank, and A. Thangaraj, "Secure computation in a bidirectional relay," *Proc. 2012 IEEE Int. Symp. Information Theory*, Cambridge, MA, pp. 1162–1166.

[49] D. Krithivasan and S. Pradhan, "A proof of the existence of good nested lattices," Univ. Michigan, Jul. 2007 [Online]. Available: `http://www.eecs.umich.edu/techreports/systems/cspl/cspl-384.pdf`.

[50] S. Kudekar, T.J. Richardson, and R.L. Urbanke, "Threshold saturation via spatial coupling: why convolutional LDPC ensembles perform so well over the BEC," *IEEE Trans. Inf. Theory*, vol. 57, no. 2, pp. 803–834, Feb. 2011.

[51] S. Kudekar, T. Richardson, and R.L. Urbanke, "Spatially coupled ensembles universally achieve capacity under belief propagation," *IEEE Trans. Inf. Theory*, vol. 59, no. 12, pp. 7761–7813, Dec. 2013.

[52] S. Leung-Yan-Cheong and M.E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 451–456, Jul. 1978.

[53] Y. Liang and H.V. Poor, "Information theoretic security," *Found. Trends in Comm. Inf. Theory,* vol. 5, no. 4-5, pp. 355–580, 2009.

[54] E. Lieb, "Sharp constant in the Hardy-Littlewood-Sobolev and related inequalities," *Annals of Mathematics*, vol. 118, no. 2, pp. 349–374, Sep. 1983.

[55] S.C. Liew, S. Zhang, and L. Lu, "Physical-layer network coding: Tutorial, survey, and beyond", *Phys. Comm.*, vol. 6, pp. 4–42, Mar. 2013.

[56] T. Linder, C. Schlegel, and K. Zeger, "Corrected proof of de Buda's theorem [lattice channel codes]," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 1735–1737, Sep. 1993.

[57] C. Ling, L. Luzzi, and M.R. Bloch, "Secret key generation from Gaussian sources using lattice hashing," *Proc. 2013 IEEE International Symposium on Information Theory (ISIT)*, Istanbul, Turkey, pp. 2621–2625.

[58] C. Ling, L. Luzzi, J.-C. Belfiore, and D. Stehlé, "Semantically secure lattice codes for the Gaussian wiretap channel," *IEEE Trans. Inf. Theory*, vol. 60, no. 10, pp. 6399–6416, Oct. 2014.

[59] H.A. Loeliger, "Averaging bounds for lattices and linear codes," *IEEE Trans. Inf. Theory,* vol. 43, no. 6, pp. 1767–1773, Nov. 1997.

[60] A. Lubotzky, R. Phillips, and P. Sarnak, "Ramanujan graphs," *Combinatorica,* vol. 8, no. 3, pp. 261–277, 1988.

[61] E. Lukacs, *Characteristic Functions*, 2nd ed. London, U.K.: Griffin, 1970.

[62] H. Mahdavifar and A. Vardy, "Achieving the secrecy capacity of wiretap channels using polar codes," *IEEE Trans. Inf. Theory,* vol. 57, no. 10, Oct. 2011.

[63] A.W. Marcus, D.A. Spielman, and N. Srivastava, "Interlacing families I: bipartite Ramanujan graphs of all degrees," *Annals of Mathematics,* vol. 182, no. 1, pp. 307–325, Jul. 2015.

[64] U.M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Trans. Inf. Theory*, vol. 39, no. 5, pp. 733–742, May 1993.

[65] U. Maurer and S. Wolf. "Information-theoretic key agreement: From weak to strong secrecy for free," in *Adv. Cryptology–EUROCRYPT 2000*, Berlin, Germany: Springer Berlin-Heidelberg, pp. 351–368, 2000.

[66] D. Micciancio and O. Regev, "Lattice-based cryptography," in *Post-Quantum Cryptography,* D.J. Bernstein, Eds. Berlin, Germany: Springer Berlin-Heidelberg, 2009.

[67] H. Minkowski, *Geometrie der Zahlen*, Teubner, Leipzig, 1896.

[68] M. Mondelli, S.H. Hassani, and R. Urbanke, "Unified scaling of polar codes: Error exponent, scaling exponent, moderate deviations, and error floors," arXiv preprint, 2015. [Online] Available: `http://arxiv.org/abs/1501.02444`.

[69] B. Nazer and M. Gastpar, "Compute-and-forward: harnessing interference through structured codes," *IEEE Trans. Inf. Theory*, vol. 57, no. 10, pp. 6463–6486, Oct. 2011.

[70] B. Nazer and M. Gastpar, "Reliable physical layer network coding," *Proc. of the IEEE*, vol. 99, no. 3, pp. 438–460, Mar. 2011.

[71] S. Nitinawarat and P. Narayan, "Secret key generation for correlated Gaussian sources," *IEEE Trans. Inf. Theory*, vol. 58, no. 6, pp. 3373–3391, Jun. 2012.

[72] F. Oggier, P. Solé, and J.-C. Belfiore, "Lattice codes for the wiretap Gaussian channel: construction and analysis," arXiv preprint, 2011. [Online] Available:: `http://arxiv.org/abs/1103.4086`.

[73] O. Ordentlich and U. Erez, "A simple proof for the existence of "good" pairs of nested lattices," in *Proc. 2012 IEEE 27th Conv. Electrical and Electronics Engineers in Israel,* Eilat, Israel, pp. 1–12.

[74] G. Poltyrev, "On coding without restrictions for the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 40, no. 2, pp. 409–417, Mar. 1994.

[75] P. Popovski and H. Yomo, "Physical network coding in two-way wireless relay channels," in *Proc. IEEE Int. Conf. Communications*, Glasgow, Scotland, 2007, pp. 707–712.

[76] S. Ramanujan, "A proof of Bertrand's postulate," *J. Indian Math. Soc.*, vol. 11, pp. 181–182, 1919.

[77] T. Richardson and R. Urbanke, *Modern Coding Theory,* Cambridge, U.K.: Cambridge University Press, 2008.

[78] C.A. Rogers, *Packing and Covering,* Cambridge, U.K.: Cambridge University Press, 1964.

[79] R.M. Roth, *Introduction to Coding Theory*, Cambridge, U.K.: Cambridge University Press, 2006.

[80] H. Rubin and T.M. Sellke, "Zeroes of infinitely differentiable characteristic functions," in *A Festschrift for Herman Rubin*, Anirban DasGupta, ed., Institute of

Mathematical Statistics Lecture Notes – Monograph Series, vol. 45, pp. 164–170, 2004.

[81] M.R. Sadeghi, A.H. Banihashemi, and D. Panario, “Low-density parity-check lattices: construction and decoding analysis,” *IEEE Trans. Inf. Theory*, vol. 52, no. 10, pp. 4481–4495, Oct. 2006.

[82] A. Sakzad, M.R. Sadeghi, and D. Panario, “Construction of turbo lattices,” *Proc 2010 48th Ann. Allerton Conference Comm. Contr. Computing*, Allerton, IL, 2010, pp. 14-21.

[83] A. Sakzad, M.R. Sadeghi, and D. Panario, “Turbo lattices: Construction and error decoding performance,” arXiv preprint, 2015. [Online] Available: `http://arxiv.org/abs/1108.1873`.

[84] C.E. Shannon, “A mathematical theory of communication,” *Bell Syst. Tech. J.,* vol. 27, no. 3, pp. 379–423, Jul. 1948.

[85] C.E. Shannon, “Communication theory of secrecy systems,” *Bell Syst. Tech. J.,* vol. 28, no. 4, pp. 656–715, Oct. 1949.

[86] N. Sommer, M. Feder, and O. Shalvi, “Low density lattice codes,” *IEEE Trans. Inf. Theory*, vol. 54, no. 4, pp. 1561–1585, Apr. 2008.

[87] E.M. Stein and G.L. Weiss, *Introduction to Fourier Analysis on Euclidean Spaces*, Princeton, NJ: Princeton Univ. Press, 1971.

[88] A. Subramanian, A. Thangaraj, M. Bloch and S.W. McLaughlin, “Strong secrecy on the binary erasure wiretap channel using large-girth LDPC codes,” *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 585–594, Sept. 2011.

[89] A. Thangaraj, S. Dihidar, A.R. Calderbank, S.W. McLaughlin, and J.M. Merolla, “Applications of LDPC codes to the wiretap channel,” *IEEE Trans. Inf. Theory,* vol. 53, no. 8, pp. 2933–2945, Aug. 2007.

[90] F.G. Tricomi, "Sulle funzioni di Bessel di ordine e argomento pressoché uguali," *Atti Accad. Sci. Torino Cl. Sci. Fis. Mat. Natur.*, vol. 83, pp. 3–20, 1949.

[91] N.E. Tunali, K.R. Narayanan, and H.D. Pfister, "Spatially-coupled low density lattices based on Construction A with applications to compute-and-forward" *Proc. 2013 Information Theory Workshop*, Sevilla, Spain, 2013, pp. 1–5.

[92] H. Tyagi and A. Vardy, "Explicit capacity-achieving coding scheme for the Gaussian wiretap channel," *Proc. 2014 IEEE Int. Symp. Information Theory (ISIT),* Honolulu, HI, 2014, pp.956-960.

[93] R. Urbanke and B. Rimoldi, "Lattice codes can achieve capacity on the AWGN channel," *IEEE Trans. Inf. Theory*, vol. 44, no. 1, pp. 273–278, Jan. 1998.

[94] S. Vatedka and N. Kashyap, "Lattice coding for strongly secure compute-and-forward in a bidirectional relay," *Proc. 2013 Int. Symp. Inf. Theory*, Istanbul, Turkey, 2013, pp. 2775–2779.

[95] S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure compute-and-forward in a bidirectional relay," *IEEE Trans. Inf. Theory,* vol. 51, no. 5, pp. 2531–2556, May 2015.

[96] S. Vatedka and N. Kashyap, "Nested lattice codes for secure bidirectional relaying with asymmetric channel gains," in *Proc. 2015 IEEE Inf. Theory Workshop*, Jerusalem, Israel, 2015.

[97] S. Vatedka and N. Kashyap, "Nested lattice codes for secure bidirectional relaying with asymmetric channel gains," arXiv preprint, 2015. [Online] Available: `http://arxiv.org/abs/1506.02152`.

[98] S. Vatedka and N. Kashyap, "Some goodness properties of LDA lattices," in *Proc. 2015 IEEE Inf. Theory Workshop*, Jerusalem, Israel, 2015.

[99] S. Vatedka and N. Kashyap, "Some goodness properties of LDA lattices," submitted, *Prob. Inf. Transm.*, Dec. 2015.

[100] S. Vatedka and N. Kashyap, "A capacity-achieving coding scheme for the AWGN channel with polynomial encoding and decoding complexity," in *Proc. 2016 Nat. Conf. Comm.*, Guwahati, India, pp. 36–41.

[101] S. Vatedka and N. Kashyap, "A capacity-achieving coding scheme for the AWGN channel with polynomial encoding and decoding complexity," arXiv preprint, 2016. [Online] Available: `http://arxiv.org/abs/1603.08236`

[102] S. Vatedka and N. Kashyap, "A lattice coding scheme for secret key generation from Gaussian Markov tree sources," accepted, *2016 IEEE Int. Symp. Inf. Theory*, Barcelona, Spain, 2016. [Online]. Available: `http://arxiv.org/abs/1603.08236`

[103] S. Vishwanath and S.A. Jafar, "Generalized degrees of freedom of the symmetric Gaussian K-User interference channel," *IEEE Trans. Inf. Theory*, vol. 56, no. 7, pp. 3297–3303, Jul. 2010.

[104] Z. Wang and C. Ling, "On the geometric ergodicity of Metropolis-Hastings algorithms for lattice Gaussian sampling," submitted, *IEEE Trans. Inf. Theory,* 2015. [Online]. Available: `http://arxiv.org/abs/1501.05757`.

[105] C.X. Wang et al., "Cellular architecture and key technologies for 5G wireless communication networks," *IEEE Comm. Mag.*, vol. 52, no. 2, pp. 122–130, Feb. 2014.

[106] S. Watanabe and Y. Oohama, "Secret key agreement from vector Gaussian sources by rate limited communication," *IEEE Trans. Inf. Forensics Security,* vol. 6, no. 3, pp. 541–550, Sep. 2011.

[107] M. Wilson, K. Narayanan, H. Pfister, and A. Sprintson, "Joint physical layer coding and network coding for bidirectional relaying," *IEEE Trans. Inf. Theory*, vol. 56, no. 11, pp. 5641–5654, Nov. 2010.

[108] S.J. Wolfe, "On the finite series expansion of multivariate characteristic functions," *J. Multivariate Anal.*, vol. 3, pp. 328–335, 1973.

[109] A. D. Wyner, “The wire-tap channel,” *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975

[110] Y. Yan, C. Ling, and X. Wu, “Polar lattices: Where Arikan meets Forney,” *Proc. 2013 IEEE Int. Symp. Information Theory*, Istanbul, Turkey, pp. 1292–1296.

[111] Y. Yan, L. Liu, C. Ling, and X. Wu, “Construction of capacity-achieving lattice codes: Polar lattices,” arXiv preprint, 2015. [Online] Available: `http://arxiv.org/abs/1411.0187`.

[112] R. Zamir, *Lattice Coding for Signals and Networks*, Cambridge, U.K.: Cambridge University Press, 2014.

[113] G. Zémor, “On expander codes,” *IEEE Trans. Inf. Theory,* vol. 47, no. 2, pp. 835–837, Feb. 2001.

[114] J. Zhan, B. Nazer, U. Erez, and M. Gastpar, “Integer-forcing linear receivers,” *IEEE Trans. Inf. Theory*, vol. 60, no. 12, pp. 7661–7685, Dec. 2014.

[115] S. Zhang, L. Fan, M. Peng, H.V. Poor, “Near-optimal modulo-and-forward scheme for the untrusted relay channel,” arXiv preprint, 2015. [Online] Available: `http://arxiv.org/abs/1503.08928`.

[116] S. Zhang and S.-C. Liew, “Channel coding and decoding in a relay system operated with physical-layer network coding,” *IEEE J. Sel. Areas Comm.*, vol. 27, no. 5, pp. 788–796, Jun. 2009.