Confusing Eavesdroppers with Algebraic Number Theory

Camilla Hollanti[1]
Department of Mathematics and System Analysis
Aalto University, Finland
camilla.hollanti@aalto.fi

Symbolic Computation and Post-Quantum Cryptography Webinar
22.3.2012

[1] Joint work with Emanuele Viterbo, ECSE, Monash University, Australia

Outline

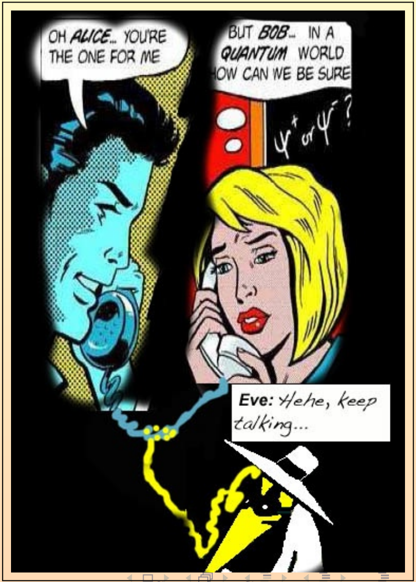
- Wiretap channel
- Problem setting
- Fading channel model
- Lattices and number fields
- Probability bounds from Dedekind zeta functions
- Finer bounds from geometric analysis

Wiretap channel

- In modern wireless communications secrecy plays an ever increasing role.
- Wiretap channels were introduced by Dr. Aaron D. Wyner (1939-1997), an American information theorist, already in 1975 and have recently regained interest, especially in the context of physical layer security.

The basic problem setting

- In a wiretap channel, Alice is transmitting confidential data to the intended receiver Bob over a fading channel, while an eavesdropper Eve tries to intercept the data received over another fading channel.
- How to transmit data reliably to Bob so that Eve cannot intercept it?


OH ALICE.. YOU'RE THE ONE FOR ME
BUT BOB.. IN A QUANTUM WORLD OW CAN WE BE SURE
ψ^+ or ψ^- ?
Eve: Hehe, keep talking...

Transmission setting

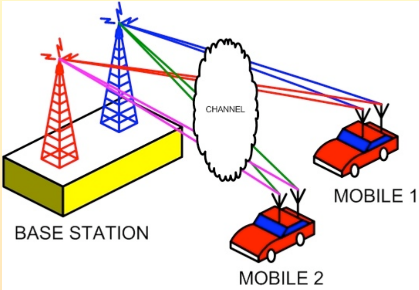
- The secrecy is based on the assumption that Bob's signal-to-noise ratio (SNR) is sufficiently large compared to Eve's SNR, that is, Eve's channel is weaker and noisier. Note that Eve is allowed to have infinite computational power.
- In addition, a coset coding strategy introduced by Wyner is employed in order to confuse Eve. In coset coding, random bits are transmitted in addition to the data bits.
- We assume Alice is using a number field lattice code enabling coset coding, and that both Bob and Eve have high enough SNRs in order to perfectly decode their observed lattices.
- Due to the SNR assumption, Bob can retrieve the data bits with high probability, while Alice is only able to retrieve the random bits.

In a restaurant

- The above could be naively compared to the scenario where Alice and Bob are discussing over a table in a noisy restaurant, and Eve is eavesdropping in a nearby table located far enough (or behind a wall, for instance) not to hear the essential contents of the conversation.
- In coset coding, random bits could be thought of as Alice yelling something irrelevant (Eve hears this), and data bits are whispered just loud enough so that Bob can hear, but Eve can't because of the longer distance and higher noise level.
- Hence, the secrecy is merely based on the channel quality. Obviously, this is not always a valid assumption.
- The finer lattice intended to Bob is denoted by Λ_b (whispering), and the more coarse lattice $\Lambda_e \subset \Lambda_b$ (yelling) embeds random bits in order to confuse Eve.

Fading channel model

- The channel can be described by the equation $y = hx + n$, where x, y are the transmitted and received signal vectors and h, n describe the random channel effect and noise (distribution known, often assumed circular Gaussian with zero mean).



- Here, for simplicity, we assume one transmit and one receive antenna, so $x, y, n \in \mathbb{R}^{n \times 1}, h \in \mathbb{R}^{n \times n}$ (diagonal).

Goals and results

- When employing lattice codes based on algebraic number fields in wiretap channel coding, certain norm sums pop up in the expression of the probability of correct decision for Eve the Eavesdropper.
- These norm sums closely resemble the famous Dedekind zeta function.
- First, numerical analysis reveals a performance-secrecy-complexity tradeoff: higher secrecy can be achieved with suboptimal lattices at the cost of slightly reduced (asymptotic) performance. The security level can be further improved by using skewed lattices, but at the cost of increased complexity.
- The final aim in this talk is to present more universal bounds for Eve's probability of correct decision in Rayleigh fading channels by using zeta functions and geometric analysis.
- Let us start with some useful definitions.

Lattices

Definition

A *lattice* Λ is a discrete abelian subgroup of a real vector space,

$$\Lambda = \mathbb{Z}\beta_1 \oplus \mathbb{Z}\beta_2 \cdots \oplus \mathbb{Z}\beta_s \subset \mathbb{R}^n,$$

where the elements $\beta_1, \ldots, \beta_s \in \mathbb{R}^n$ are linearly independent, *i.e.*, form a lattice basis, and $s \leq n$ is called the *rank* of the lattice. Here we only consider full lattices ($s = n$).

Let M be the generator matrix of the lattice. The *volume* of the fundamental parallelotope (=basic building block) of the lattice is

$$\mathrm{Vol}(\Lambda) = |\det(M)|.$$

- Examples of lattices: lattice of integers $\mathbb{Z}$, lattice of gaussian integers $\mathbb{Z}[j]$, "golden ratio" lattice $\mathbb{Z}[\frac{1+\sqrt{5}}{2}]$, cyclotomic lattices $\mathbb{Z}[e^{2\pi j/k}]$ etc.

Product distance

In terms of error probability, the performance of number field codes can be measured by the product distance.

Definition

The *minimum product distance* of a lattice Λ is

$$d_{p,min}(\Lambda) = \min_{0 \neq \mathbf{x} \in \Lambda} \prod_{i=1}^{n} |x_i|,$$

where $\mathbf{x} = (x_1, \ldots, x_n) \in \Lambda$.

Maximizing $d_{p,min}$ minimizes the error probability (of Bob).

Lattices from number fields

- Let $K/\mathbb{Q}$ be a totally real number field extension of degree n and $\sigma_1, \dots, \sigma_n$ its embeddings to $\mathbb{R}$.
- Let $\mathcal{O}_K$ denote the ring of integers in K, and $N_{K/\mathbb{Q}}(x) = \sigma_1(x) \cdots \sigma_n(x)$ the algebraic norm of x.

Definition

Let $x \in \mathcal{O}_K$. The *canonical embedding* $\psi : K \hookrightarrow \mathbb{R}$ defines a lattice $\Lambda = \psi(\mathcal{O}_K)$ in $\mathbb{R}^n$:

$$\psi(x) = (\sigma_1(x), \dots, \sigma_n(x)) \in \psi(\mathcal{O}_K) \subset \mathbb{R}^n.$$

- We further have that:

Proposition

$$d_{p,min}(\psi(\mathcal{O}_K)) = \min_{0 \neq x \in \mathcal{O}_K} |N_{K/\mathbb{Q}}(x)| = 1.$$

Lattices from number fields

- As an example, let us consider the field extension $\mathbb{Q}(\theta)$ over the rationals $\mathbb{Q}$, and the golden ratio lattice $\mathbb{Z}[\theta] \subset \mathbb{Q}(\theta)$, where $\theta = \frac{1+\sqrt{5}}{2}$.
- The degree of the extension is two with a minimal polynomial $x^2 - x - 1$ and integral basis $\{1, \theta\}$.
- The embeddings to $\mathbb{R}$ are

$$\sigma_1 = id_{\mathbb{Q}(\theta)} : \theta \mapsto \theta, \text{ and } \sigma_2 : \theta \mapsto \overline{\theta} = \frac{1-\sqrt{5}}{2}.$$

- The code lattice is formed as a finite subset of vectors

$$\psi(x) = (a + b\theta, a + b\overline{\theta}) \quad (a, b \in \mathbb{Z}).$$

- The minimum product distance is

$$d_{p,min}(\psi(\mathbb{Z}[\theta])) = \min_{0 \neq x \in \mathbb{Z}[\theta]} |\sigma_1(x)||\sigma_2(x)| = \min_{0 \neq x \in \mathbb{Z}[\theta]} |N_{K/\mathbb{Q}}(x)| = 1.$$

Coset coding

- Let us denote the lattice intended to Bob by $\Lambda_b = \psi(\mathcal{O}_K)$, and by $\Lambda_e \subset \Lambda_b$ a sublattice embedding the random bits intended for Eve.
- Now the transmitted codeword $\mathbf{x}$ is picked from a certain coset $\Lambda_e + \mathbf{c}$ belonging to the disjoint union

  $$\Lambda_b = \cup_{j=1}^{2^k} \Lambda_e + \mathbf{c_j}$$

  embedding k bits:

  $$\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c},$$

  where $\mathbf{r}$ embeds the random bits, and $\mathbf{c}$ contains the data bits.

The probability expression and the inverse norm power sum

- Let us recall the expression $P_{c,e}$ for the probability of a correct decision for Eve, when observing a lattice Λ_e.
- For the fast fading case (Belfiore-Oggier ICC 2011),

$$P_{c,e} \simeq \left(\frac{1}{4\gamma_e^2}\right)^{n/2} \mathrm{Vol}(\Lambda_b) \sum_{0 \neq \mathbf{x} \in \Lambda_e} \prod_{i=1}^{n} \frac{1}{|x_i|^3}, \tag{1}$$

where γ_e is the average SNR for Eve assumed sufficiently large so that Eve can perfectly decode Λ_e.

- Here Λ_b denotes the lattice intended to Bob, and $\Lambda_e \subset \Lambda_b$. It can be concluded that the smaller the sum

$$\sum_{0 \neq \mathbf{x} \in \Lambda_e} \prod_{i=1}^{n} \frac{1}{|x_i|^3},$$

the more confusion Eve is experiencing.

The probability expression and the inverse norm power sum

- Let $x \in \mathcal{O}_K$. The transmitted lattice vector in the fast fading case is

$$\mathbf{x} = \psi(x) = (\sigma_1(x), \sigma_2(x), \ldots, \sigma_n(x)) \in \Lambda_e \subset \mathbb{R}^n, \tag{2}$$

where ψ denotes the canonical embedding and σ_i are the (now all real) embeddings of K into $\mathbb{R}$.

- The corresponding probability of Eve's correct decision yields the following *inverse norm power sum* to be minimized:

$$S_M = \sum_{0 \neq x \in \mathcal{O}_K} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3}, \tag{3}$$

where M denotes the generator matrix of the lattice Λ_e.

The probability expression and the inverse norm power sum

- The above sum S_M may not converge, since infinitely many elements can have the same norm.
- This happens *e.g.* when the unit group is infinite, which is the case for all field extensions other than the trivial one and imaginary quadratic fields.
- In practice, however, we always consider finite signaling alphabets, so the sum becomes truncated and converges.

Example codes

- Let us next describe three alternative constructions for the fast fading channel built from different number fields of degree four.
- Optimal and nearly optimal unitary lattice generator matrices in terms of the minimum product distance are provided at Professor Emanuele Viterbo's home page.
- We will first analyze two orthogonal lattices denoted here by Λ_1 and Λ_2 with the respective unitary (*i.e.*, $MM^T = I_4$) generator matrices M_1 (optimal) and M_2 (suboptimal).

Example codes

- The first construction corresponds to the canonical embedding of $\mathcal{O}_{\mathbb{Q}(\delta)}$, where $\delta^4 - \delta^3 - 3\delta^2 + \delta + 1 = 0$.
- The second construction is based on the Kronecker product of the lattice generator matrices corresponding to the canonical embeddings of the rotated $\mathbb{Z}^2$ lattices $\alpha_1\mathbb{Z}[\sqrt{2}]$ and $\alpha_2\mathbb{Z}[\theta]$, where $\theta = \frac{1+\sqrt{5}}{2}$, $\alpha_1 = \frac{1}{2\sqrt{2}+4}$ and $\alpha_2 = 3 - \theta$.
- Both lattices are rotated versions of $\mathbb{Z}^4$ with full diversity and good minimum product distances,

$$Nd_{p,min}(\Lambda_1) = \frac{1}{\sqrt{5^2 \cdot 29}} \approx 0.037139...$$

and

$$Nd_{p,min}(\Lambda_1) = \frac{1}{40} \approx 0.025.$$

Example codes

- Let us now compare these two (finite) orthogonal constructions by computing truncated sums

$$S_M(P_{lim}) = \sum_{0 \neq \mathbf{x} \in \Lambda_e, ||\mathbf{x}||_E^2 \leq P_{lim}} \frac{1}{|N_{K/\mathbb{Q}}(x)|^3} \qquad (4)$$

  for a given power limit P_{lim}.

- For a fair comparison, the lattices are normalized to unit energy, *i.e.*, to have $\mathrm{Vol}(\Lambda_e) = 1$. The volumes of the corresponding superlattices Λ_b of Bob will then scale accordingly.

Comparison of orthogonal codes

Table: Values of $S_M(P_{lim})$ for orthogonal lattices $(n = 4)$ with $P_{lim} = P_{max}$ and with a codebook size $|\mathcal{C}_{ort}| = (2m+1)^4$.

m	P_{max}	P_{ave}	$S_{M_1}(P_{lim})$	$S_{M_2}(P_{lim})$
1	4	2.67	$9.12264 \cdot 10^7$	$2.83706 \cdot 10^6$
2	16	8.00	$2.24565 \cdot 10^{10}$	$6.46037 \cdot 10^6$
3	**36**	**16.00**	$\mathbf{2.49382 \cdot 10^{11}}$	$\mathbf{1.16395 \cdot 10^7}$
4	64	26.67	$2.49829 \cdot 10^{11}$	$1.52838 \cdot 10^7$
5	100	40.00	$2.49851 \cdot 10^{11}$	$1.99487 \cdot 10^7$
6	144	56.00	$2.50437 \cdot 10^{11}$	$2.38188 \cdot 10^7$
7	196	74.67	$2.61395 \cdot 10^{11}$	$2.69652 \cdot 10^7$
8	256	96.00	$2.61736 \cdot 10^{11}$	$3.00791 \cdot 10^7$
9	324	120.00	$2.61739 \cdot 10^{11}$	$3.42272 \cdot 10^7$
10	400	146.67	$2.71764 \cdot 10^{11}$	$3.68287 \cdot 10^7$

Skewed lattice

- Next, we extend our analysis by computing the inverse norm power sums for a skewed lattice, denoted by Λ_3, corresponding to the maximal real subfield
$$\mathbb{Q}(\tau = \zeta_{15} + \zeta_{15}^{-1})$$
of the 15th cyclotomic field.
- Here τ satisfies
$$\tau^4 - \tau^3 - 4\tau^2 + 4\tau + 1 = 0.$$
- The generator matrix is denoted by M_3.
- The minimum product distance of this lattice is
$$Nd_{p,min}(\Lambda_3) = \frac{1}{\sqrt{1125}} \approx 0.02981...$$
putting it in between the lattices Λ_1 and Λ_2 in terms of $Nd_{p,min}(\Lambda)$.

Skewed lattice

Table: Values of $S_M(P_{lim}, m)$ for a skewed lattice ($n = 4$) with bounded energy.

m	P_{lim}	P_{max}	P_{ave}	$\lvert\mathcal{C}_{sph}\rvert$	$\lvert\mathcal{C}_{ort}\rvert$	$S_{M_3}(P_{lim}, m)$
8	4	3.63	2.66	79	81	$1.89195 \cdot 10^6$
5	16	15.71	9.18	555	625	$4.24298 \cdot 10^6$
6	16	15.71	9.56	715	625	$4.77423 \cdot 10^6$
7	**36**	**35.57**	**20.33**	**2405**	**2401**	$\mathbf{7.13024 \cdot 10^6}$
12	**36**	**24.00**	**15.24**	**2401**	**2401**	$\mathbf{2.29374 \cdot 10^6}$
9	64	63.89	35.67	6929	6561	$9.93903 \cdot 10^6$
10	100	99.97	55.72	13663	14641	$1.20680 \cdot 10^7$
11	100	99.97	55.57	16053	14641	$1.29038 \cdot 10^7$
14	196	195.98	106.63	50975	50625	$1.29038 \cdot 10^7$
18	324	323.93	175.95	137273	130321	$2.18703 \cdot 10^7$
20	400	399.90	217.31	208411	194481	$2.40716 \cdot 10^7$

Skewed lattice

- We can conclude that skewed lattices may significantly increase the secrecy at practical SNR levels compared to orthogonal lattices.
- One has to notice, however, that this bares the price of increased complexity as we need to carve spherical codebooks by using a bigger alphabet in order to get the possible benefits.
- Block fading channels can be treated analogously.

Something more universal than numerical analysis?

- The above numerical analysis gives us some insight to the behavior of the norm sums and hence to the probability of Eve's correct decision.
- However, it would be nice to gain deeper understanding of the nature of the problem. To this end, we derive algebraic probability bounds arising from Dedekind zeta functions.
- Let us start with definitions.

Dedekind zeta function

Definition

The *Dedekind zeta function* of a field K is defined as

$$\zeta_K(s) = \sum_{\mathcal{I} \subseteq \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathcal{I})^s}, \tag{5}$$

where $\mathcal{I}$ runs through the nonzero integral ideals of $\mathcal{O}_K$. The sum converges for $\Re(s) > 1$. Since $N_{K/\mathbb{Q}}(\mathcal{O}_K) = 1$, we always have

$$\zeta_K(s) > 1.$$

- From now on, we assume $2 \leq s \in \mathbb{Z}$ since these are the interesting values for the applications under study.
- Remark: The extended Riemann hypothesis states that if $\zeta_K(s) = 0$ and $0 < \Re(s) < 1$, then $\Re(s) = 1/2$.

Dedekind zeta function

- Analogously to the Riemann zeta function, the values of the Dedekind zeta function at integers encode (at least conjecturally) important arithmetic data of the field K. For instance, the analytic class number formula relates the residue at $s = 1$ to the class number of K, the regulator of K, the number of roots of unity in K, the absolute discriminant of K, and the number of real and complex places of K.
- The Dedekind zeta function can be written as a *Dirichlet series*

  $$\zeta_K(s) = \sum_{n \geq 1} \frac{a_n}{n^s},$$

  where $a_n = 0$ for those n that don't appear as a norm.
- When we derive probability bounds for lattice codes with the aid of zeta functions, we need to use the same normalization for the zeta function as used for the lattice code. Otherwise the comparison of the two norm sums under observation will be meaningless.

Normalization of zeta functions

Definition

The *normalized Dedekind zeta function* is denoted and defined as

$$N\zeta_K(s) = \frac{1}{\rho^{ns} N_{K/\mathbb{Q}}(\alpha)^{s/2}} \sum_{\mathcal{I} \subseteq \mathcal{O}_K} \frac{1}{N_{K/\mathbb{Q}}(\mathcal{I})^s},$$

where $\rho \in \mathbb{R}$ is a real scaling factor such that $\mathrm{Vol}(\rho\Lambda_\alpha) = 1$. This normalized zeta function will then be comparable to the norm sum related to the lattice $\rho\Lambda_\alpha$ of volume 1. Also the normalized zeta functions corresponding to different lattices can be meaningfully compared to each other.

Bounds for the eavesdropper's probability of correct decision

- Let us now derive lower and upper bounds for the inverse norm power sum in the probability expression for the fast fading wiretap channel by using the Dedekind zeta functions.
- Similar bounds can be achieved for the pair-wise error probabilities in the fading channels, see more details in the reference papers (Vehkalahti-Lu, H.-Viterbo 2011).
- For $x \in \mathcal{O}_K$, we trivially have that $S_M > 1$ as $1 \in \mathcal{O}_K$. Albeit straightforward, the following result gives us a nontrivial lower bound $\neq 1$ for the sum S_M.
- Note that in the proposition below, we do not require K to be totally real.

Bounds for the eavesdropper's probability of correct decision

Proposition

(Lower Bound) Assume that $\mathcal{O}_K$ is a principal ideal domain (PID) and Λ_e is as above with $x \in \mathcal{O}_K$. Prior to normalization of the lattice, the Dedekind zeta function $\zeta_K(s)$ evaluated at $s = 3$ provides us with a lower bound for S_M, i.e.,

$$S_M > \zeta_K(3) > 1.$$

More interestingly, if P_{lim} is sufficiently large, the same holds for the truncated sums,

$$S_M(P_{lim}, N) > \zeta_K(3, N) > 1,$$

where N denotes the maximum norm included in the sum; $|N_{K/\mathbb{Q}}(x)| \leq N$ and $N_{K/\mathbb{Q}}(\mathcal{I}) \leq N$.

Bounds for the eavesdropper's probability of correct decision

- Next, let us denote by

$$S_M(P_{lim}, N) = \sum_{n \leq N} \frac{b'_n}{n^3},$$

the truncated sum, where $b'_n \neq 0$ for those n that appear as a norm for $x \in \mathcal{O}_K$, $||x||_E^2 \leq P_{lim}$.

- An upper bound for the truncated sum is achieved from the truncated Dedekind zeta function $\zeta_K(s, N)$ evaluated at $s = 3$.

Proposition

(Upper Bound) Let $\mathcal{O}_K$ be a PID. Then we have that

$$S_M(P_{lim}, N) \leq \max\{b'_n \mid n \leq N\} \cdot \zeta_K(3, N).$$

An upper bound from geometric analysis

Let w_k be the number of roots of unity in a degree n number field K, and denote the regulator of K by ρ_K. Assume that we are using a hypercube constellation within a lattice, i.e., the vector components have absolute values $\leq R$ for some R. Then we have that

Proposition

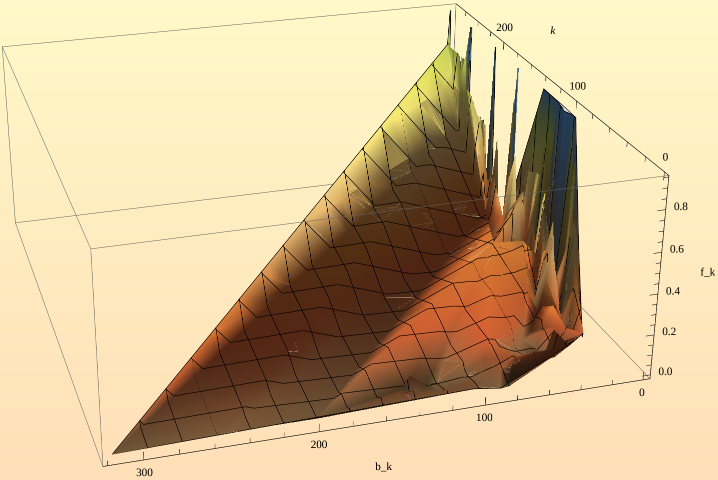
$$P_e \leq K \sum_{m=0}^{n-1} \binom{n-1}{m} (\log(R^n))^{n-1-m} |D_s^{(m)} \zeta_K(3)|,$$

where

$$K = \frac{Cw_k}{(n-1)!\rho_K},$$

and C is a constant related to the SNR and R.

Error Mountain (n=4)



b_k = true number of constellation points with norm k,

f_k = (relative) error $|b_k - n_k|$, where n_k is our estimate.

References

A. Wyner, “The wire-tap channel,” *Bell. Syst. Tech. Journal*, vol. 54, 1975.

S. Leung-Yan-Cheong and M. Hellman, “The gaussian wire-tap channel,” *Information Theory, IEEE Transactions on*, vol. 24, no. 4, pp. 451 – 456, jul 1978.

F. Oggier, P. Solé, and J.-C. Belfiore, “Lattice codes for the wiretap gaussian channel: Construction and analysis,” submitted to *IEEE Trans. Inf. Theory*, 2011, arxiv.org/abs/1103.4086.

J.-C. Belfiore and P. Solé, “Unimodular lattices for the gaussian wiretap channel,” CoRR, abs/1007.0449, 2010.

J.-C. Belfiore and F. E. Oggier, “Secrecy gain: A wiretap lattice code design,” in *ISITA*, 2010, pp. 174–178.

J.-C. Belfiore and F. Oggier, “Lattice code design for the rayleigh fading wiretap channel,” in *ICC 2011*, 2011, arxiv.org/pdf/1012.4161.

A.-M. Ernvall-Hytönen and C. Hollanti, "On the eavesdropper's correct decision in gaussian and fading wiretap channels using lattice codes," submitted to IEEE ITW 2011, arxiv.org/abs/1106.2756.

C. Hollanti and E. Viterbo, "Analysis on wiretap lattice codes and probability bounds from dedekind zeta functions," in *ICUMT'11*, 2011.

C. Hollanti and E. Viterbo, "Probability bounds for wiretap lattice codes based on Dedekind zeta functions and geometric analysis", under preparation.

R. Vehkalahti and H.-F. F. Lu, "An algebraic look into MAC-DMT of lattice space-time codes," in *Proc. IEEE ISIT 2011*.

——, "Diversity-multiplexing gain tradeoff: a tool in algebra?," in Proc. IEEE ITW 2011.

——, "Inverse determinant sums and connections between fading channel information theory and algebra," *IEEE Trans. Inf. Theory*, 2011, submitted.

- F. Oggier and E. Viterbo, "Algebraic number theory and code design for rayleigh fading channels," *Commun. Inf. Theory*, vol. 1, no. 3, pp. 333–416, 2004.
- N. Childress, *Class Field Theory*. Springer Universitext, New York, 2009.
- "Sage open source mathematics software system." [Online]. Available: http://www.sagemath.org/

Acknowledgments

Dr. Roope Vehkalahti (University of Turku/EPFL) is gratefully acknowledged for useful discussions.

Thank you!