Applications of Lattices in Telecommunications

Amin Sakzad
Dept of Electrical and Computer Systems Engineering
Monash University
amin.sakzad@monash.edu

Oct. 2013

Channel Model

- We consider n-dimensional signal constellation $\mathcal{A}$ carved from the lattice Λ with generator matrix $\mathbf{G}$, for example 4-QAM.

Channel Model

- We consider n-dimensional signal constellation $\mathcal{A}$ carved from the lattice Λ with generator matrix $\mathbf{G}$, for example 4-QAM.
- Hence, $\mathbf{x} = \mathbf{u}\mathbf{G}$ represent a transmitted signal.

Channel Model

- We consider n-dimensional signal constellation $\mathcal{A}$ carved from the lattice Λ with generator matrix $\mathbf{G}$, for example 4-QAM.
- Hence, $\mathbf{x} = \mathbf{u}\mathbf{G}$ represent a transmitted signal.
- The received vector $\mathbf{y} = \boldsymbol{\alpha} \cdot \mathbf{x} + \mathbf{z}$, where α_i, are independent real Rayleigh random variables with unit second moment and z_i are real Gaussian distributed with zero mean and variance $\sigma/2$.

Channel Model

- We consider n-dimensional signal constellation $\mathcal{A}$ carved from the lattice Λ with generator matrix $\mathbf{G}$, for example 4-QAM.
- Hence, $\mathbf{x} = \mathbf{uG}$ represent a transmitted signal.
- The received vector $\mathbf{y} = \boldsymbol{\alpha} \cdot \mathbf{x} + \mathbf{z}$, where α_i, are independent real Rayleigh random variables with unit second moment and z_i are real Gaussian distributed with zero mean and variance $\sigma/2$.
- With perfect Channel State Information (CSI) at the receiver, the ML decoder requires to solve the following optimization problem

$$\min \sum_{i=1}^{n} |y_i - \alpha_i x_i|^2.$$

Pairwise error probability

Using standard Chernoff bound technique one can estimate pairwise error probability under ML decoder as

$$\Pr(\mathbf{x} \to \mathbf{x}') \leq \frac{1}{2} \prod_{x_i \neq x'_i} \frac{4\sigma}{(x_i - x'_i)^2} = \frac{(4\sigma)^\ell}{2 d_{\min,p}^{(\ell)}(\mathbf{x}, \mathbf{x}')^2},$$

where the ℓ-product distance is

$$d_{\min,p}^{(\ell)}(\mathbf{x}, \mathbf{x}') \triangleq \prod_{x_i \neq x'_i} |x_i - x'_i|.$$

Goal

Definition

The parameter $L = \min(\ell)$ is called modulation diversity.

Goal

Definition

The parameter $L = \min(\ell)$ is called modulation diversity.

Definition

We define the product distance as $d_{\min,p} = \min d_{\min,p}^{(L)}$.

Goal

Definition

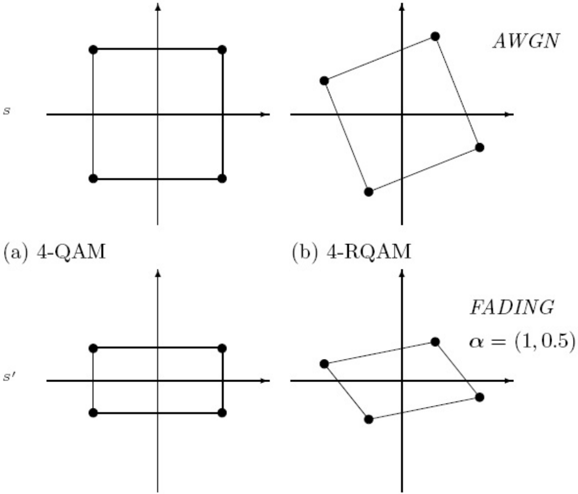
The parameter $L = \min(\ell)$ is called modulation diversity.

Definition

We define the product distance as $d_{\min,p} = \min d_{\min,p}^{(L)}$.

To minimize the error probability, one should increase both L and $d_{\min,p}$

Rotated $\mathbb{Z}^n$-lattice constellations



Rotated $\mathbb{Z}^n$-lattice constellations

- "Algebraic Number Theory" has been used as a strong tool to construct good lattices for signal constellations.

Rotated $\mathbb{Z}^n$-lattice constellations

- "Algebraic Number Theory" has been used as a strong tool to construct good lattices for signal constellations.
- For these lattices, the minimum product distance will be related to the volume of the lattice and the "discriminant" of the underlying number field.

Rotated $\mathbb{Z}^n$-lattice constellations

- "Algebraic Number Theory" has been used as a strong tool to construct good lattices for signal constellations.
- For these lattices, the minimum product distance will be related to the volume of the lattice and the "discriminant" of the underlying number field.
- The "signature" of a number field determines the modulation diversity.

Rotated $\mathbb{Z}^n$-lattice constellations

- "Algebraic Number Theory" has been used as a strong tool to construct good lattices for signal constellations.
- For these lattices, the minimum product distance will be related to the volume of the lattice and the "discriminant" of the underlying number field.
- The "signature" of a number field determines the modulation diversity.
- List of good algebraic rotations are available online. See Emanuele's webpage.

Optimization Problem

The problem is to solve the following:

$$\min_{\mathbf{x}\in\Lambda} \|\mathbf{y}-\mathbf{x}\|^2 = \min_{\mathbf{w}\in\mathbf{y}-\Lambda} \|\mathbf{w}\|^2.$$

Algorithm[Viterbo'99]

- Set $\mathbf{x} = \mathbf{u}\mathbf{G}$, $\mathbf{y} = \boldsymbol{\rho}\mathbf{G}$, and $\mathbf{w} = \boldsymbol{\zeta}\mathbf{G}$ for $\mathbf{u} \in \mathbb{Z}^n$ and $\boldsymbol{\rho}, \boldsymbol{\zeta} \in \mathbb{R}^n$.

Algorithm[Viterbo'99]

- Set $\mathbf{x} = \mathbf{u}\mathbf{G}$, $\mathbf{y} = \boldsymbol{\rho}\mathbf{G}$, and $\mathbf{w} = \boldsymbol{\zeta}\mathbf{G}$ for $\mathbf{u} \in \mathbb{Z}^n$ and $\boldsymbol{\rho}, \boldsymbol{\zeta} \in \mathbb{R}^n$.
- Let the Gram matrix $\mathbf{M} = \mathbf{G}\mathbf{G}^T$ has the following Cholesky decomposition $\mathbf{M} = \mathbf{R}\mathbf{R}^T$, where $\mathbf{R}$ is an upper triangular matrix.

Algorithm[Viterbo'99]

- Set $\mathbf{x} = \mathbf{u}\mathbf{G}$, $\mathbf{y} = \boldsymbol{\rho}\mathbf{G}$, and $\mathbf{w} = \boldsymbol{\zeta}\mathbf{G}$ for $\mathbf{u} \in \mathbb{Z}^n$ and $\boldsymbol{\rho}, \boldsymbol{\zeta} \in \mathbb{R}^n$.
- Let the Gram matrix $\mathbf{M} = \mathbf{G}\mathbf{G}^T$ has the following Cholesky decomposition $\mathbf{M} = \mathbf{R}\mathbf{R}^T$, where $\mathbf{R}$ is an upper triangular matrix.
- We have

$$\|\mathbf{w}\|^2 = \boldsymbol{\zeta}\mathbf{R}\mathbf{R}^T\boldsymbol{\zeta}^T = \sum_{i=1}^{n} q_{ii}U_i^2 \leq C,$$

where U_i, q_{ii} are based on r_{ij} and ζ_i, for $1 \leq i, j \leq n$.

Algorithm[Viterbo'99]

- Set $\mathbf{x} = \mathbf{u}\mathbf{G}$, $\mathbf{y} = \boldsymbol{\rho}\mathbf{G}$, and $\mathbf{w} = \boldsymbol{\zeta}\mathbf{G}$ for $\mathbf{u} \in \mathbb{Z}^n$ and $\boldsymbol{\rho}, \boldsymbol{\zeta} \in \mathbb{R}^n$.
- Let the Gram matrix $\mathbf{M} = \mathbf{G}\mathbf{G}^T$ has the following Cholesky decomposition $\mathbf{M} = \mathbf{R}\mathbf{R}^T$, where $\mathbf{R}$ is an upper triangular matrix.
- We have

$$\|\mathbf{w}\|^2 = \boldsymbol{\zeta}\mathbf{R}\mathbf{R}^T\boldsymbol{\zeta}^T = \sum_{i=1}^{n} q_{ii}U_i^2 \leq C,$$

  where U_i, q_{ii} are based on r_{ij} and ζ_i, for $1 \leq i, j \leq n$.
- Starting from U_n and working backward, one can find bounds on U_i, these will be transformed to bounds on u_i.

Comments

- The sphere decoding algorithm can be adapted to work on fading channels as well.

Comments

- The sphere decoding algorithm can be adapted to work on fading channels as well.
- Choosing the radius C is a crucial part of the algorithm. Covering radius is an excellent choice.

Comments

- The sphere decoding algorithm can be adapted to work on fading channels as well.
- Choosing the radius C is a crucial part of the algorithm. Covering radius is an excellent choice.
- The complexity is reasonable for low dimensions, $n = 64$.

Lattice Reduction Algorithms; Key to Application

Given a basis set, a lattice reduction technique is a process to obtain a new basis set of the lattice with shorter vectors.

Given a basis set, a lattice reduction technique is a process to obtain a new basis set of the lattice with shorter vectors.

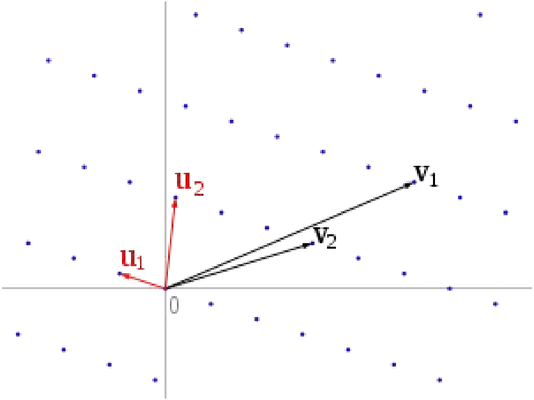


Figure: Geometrical view of Lattice Reduction.

Gram-Schmidt Orthogonalization

The orthogonal vectors generated by the Gram-Schmidt orthogonalization procedure are denoted by $\{\mathsf{GS}(\mathbf{g}_1), \ldots, \mathsf{GS}(\mathbf{g}_n)\}$ which spans the same space of $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$.

Gram-Schmidt Orthogonalization

The orthogonal vectors generated by the Gram-Schmidt orthogonalization procedure are denoted by $\{\mathrm{GS}(\mathbf{g}_1), \ldots, \mathrm{GS}(\mathbf{g}_n)\}$ which spans the same space of $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$.

Definition

We define

$$\mu_{m,j} \triangleq \frac{\langle GS(\mathbf{g}_m), GS(\mathbf{g}_j)\rangle}{\|GS(\mathbf{g}_j)\|^2},$$

where $1 \leq m, j \leq n$.

Gram-Schmidt Orthogonalization

The orthogonal vectors generated by the Gram-Schmidt orthogonalization procedure are denoted by $\{\mathrm{GS}(\mathbf{g}_1), \ldots, \mathrm{GS}(\mathbf{g}_n)\}$ which spans the same space of $\{\mathbf{g}_1, \ldots, \mathbf{g}_n\}$.

Definition

We define

$$\mu_{m,j} \triangleq \frac{\langle GS(\mathbf{g}_m), GS(\mathbf{g}_j)\rangle}{\|GS(\mathbf{g}_j)\|^2},$$

where $1 \leq m, j \leq n$.

Definition

The m–th successive minima of a lattice, denoted by λ_m, is the radius of the smallest possible closed ball around origin containing m or more linearly independent lattice points forming a basis.

CLLL Reduction

A generator matrix $\mathbf{G}'$ for a lattice Λ is called *LLL-reduced* if it satisfies

1. $|\mu_{m,j}| \leq 1/2$ for all $1 \leq j < m \leq n$, and
2. $\delta \|\mathsf{GS}\left(\mathbf{g}'_{m-1}\right)\|^2 \leq \|\mathsf{GS}\left(\mathbf{g}'_m\right) + \mu^2_{m,m-1}\mathsf{GS}\left(\mathbf{g}'_{m-1}\right)\|^2$ for all $1 < m \leq n$,

where $\delta \in (1/4, 1]$ is a factor selected to achieve a good quality-complexity tradeoff.

Mikowski Lattice Reduction

A lattice generator matrix $\mathbf{G}'$ is called Minkowski-reduced if for $1 \leq m \leq n$, the vectors $\mathbf{g}'_m$ are as short as possible.

Mikowski Lattice Reduction

A lattice generator matrix $\mathbf{G}'$ is called Minkowski-reduced if for $1 \leq m \leq n$, the vectors $\mathbf{g}'_m$ are as short as possible.

In particular, $\mathbf{G}'$ is Minkowski-reduced if for $1 \leq m \leq n$, the row vector $\mathbf{g}'_m$ has minimum possible energy amongst all the other lattice points such that $\{\mathbf{g}'_1, \ldots, \mathbf{g}'_m\}$ can be extended to another basis of Λ.

HKZ Lattice Reduction

A generator matrix $\mathbf{G}'$ for a lattice Λ is called HKZ-reduced if it satisfies

1. $|\mathbf{R}_{m,j}| \leq \frac{1}{2}|\mathbf{R}_{m,m}|$ for all $1 \leq m \leq j \leq n$, and
2. $\mathbf{R}_{j,j}$ be the length of the shortest vector of a lattice generated by the columns of the sub matrix $\mathbf{R}\left([j, j+1, \ldots, n], [j, j+1, \ldots, n]\right)$.

Note that $\mathbf{G}' = \mathbf{QR}$ is the QR decomposition of $\mathbf{G}'$.

Properties

The m-th row vector in $\mathbf{G}'$ is upper bounded by a scaled version of the m-th successive minima of Λ.

- For CLLL reduction, we have

$$\beta^{1-m}\lambda_m^2 \leq \|\mathbf{g}'_m\|^2 \leq \beta^{n-1}\lambda_m^2, \text{ for } 1 \leq m \leq n,$$

where $\beta = (\delta - 1/4)^{-1}$.

Properties

The m-th row vector in $\mathbf{G}'$ is upper bounded by a scaled version of the m-th successive minima of Λ.

- For CLLL reduction, we have

$$\beta^{1-m}\lambda_m^2 \leq \|\mathbf{g}'_m\|^2 \leq \beta^{n-1}\lambda_m^2, \text{ for } 1 \leq m \leq n,$$

  where $\beta = (\delta - 1/4)^{-1}$.

- For the Minkowski reduction, we have

$$\lambda_m^2 \leq \|\mathbf{g}'_m\|^2 \leq \max\left\{1, \left(\frac{5}{4}\right)^{n-4}\right\}\lambda_m^2, \text{ for } 1 \leq m \leq n.$$

Properties

The m-th row vector in $\mathbf{G}'$ is upper bounded by a scaled version of the m-th successive minima of Λ.

- For CLLL reduction, we have

$$\beta^{1-m}\lambda_m^2 \leq \|\mathbf{g}'_m\|^2 \leq \beta^{n-1}\lambda_m^2, \text{ for } 1 \leq m \leq n,$$

  where $\beta = (\delta - 1/4)^{-1}$.
- For the Minkowski reduction, we have

$$\lambda_m^2 \leq \|\mathbf{g}'_m\|^2 \leq \max\left\{1, \left(\frac{5}{4}\right)^{n-4}\right\}\lambda_m^2, \text{ for } 1 \leq m \leq n.$$

- For the HKZ reduction, we have

$$\frac{4\lambda_m^2}{m+3} \leq \|\mathbf{g}'_m\|^2 \leq \frac{(m+3)\lambda_m^2}{4}, \text{ for } 1 \leq m \leq n.$$

One Example of Using Lattice Reduction Algorithms

MIMO Channel Model

- We consider a flat-fading MIMO channel with n transmit antennas and n receive antennas.

MIMO Channel Model

- We consider a flat-fading MIMO channel with n transmit antennas and n receive antennas.
- The channel matrix is denoted by $\mathbf{G} \in \mathbb{C}^{n \times n}$, where the entries of $\mathbf{G}$ are i.i.d. as $\mathcal{CN}(0, 1)$.

MIMO Channel Model

- We consider a flat-fading MIMO channel with n transmit antennas and n receive antennas.
- The channel matrix is denoted by $\mathbf{G} \in \mathbb{C}^{n \times n}$, where the entries of $\mathbf{G}$ are i.i.d. as $\mathcal{CN}(0, 1)$.
- For $1 \leq m \leq n$, the m-th layer is equipped with an encoder $E : \mathcal{R}^k \to \mathbb{C}^N$ which maps a message $\mathbf{m} \in \mathcal{R}^k$ over the ring $\mathcal{R}$ into a lattice codeword $\mathbf{x}_m \in \Lambda \subset \mathbb{C}^N$ in the complex space.

- If $\mathbf{X}$ denotes the matrix of transmitted vectors, the received signal $\mathbf{Y}$ is given by

$$\mathbf{Y}_{n\times N} = \sqrt{P}\mathbf{G}_{n\times n}\mathbf{X}_{n\times N} + \mathbf{Z}_{n\times N},$$

  where $P = \frac{\mathsf{SNR}}{n}$ and SNR denotes the average signal-to-noise ratio at each receive antenna.

- If $\mathbf{X}$ denotes the matrix of transmitted vectors, the received signal $\mathbf{Y}$ is given by

$$\mathbf{Y}_{n\times N} = \sqrt{P}\mathbf{G}_{n\times n}\mathbf{X}_{n\times N} + \mathbf{Z}_{n\times N},$$

  where $P = \frac{\mathsf{SNR}}{n}$ and SNR denotes the average signal-to-noise ratio at each receive antenna.
- We assume that the entries of $\mathbf{Z}$ are i.i.d. as $\mathcal{CN}(0,1)$.

- This model will be used in this section.

- This model will be used in this section.
- Lattice reductions can improve the performance of MIMO channels if employed at either transmitters or receivers.

- This model will be used in this section.
- Lattice reductions can improve the performance of MIMO channels if employed at either transmitters or receivers.
- Lattice-reduction-aided MIMO detectors, Lattice reduction precoders, etc.

- In order to uniquely recover the information symbols, the matrix $\mathbf{A}$ must be invertible over the ring $\mathcal{R}$. Thus, we have

$$\mathbf{Y}' = \mathbf{B}\mathbf{Y} = \sqrt{P}\mathbf{B}\mathbf{G}\mathbf{X} + \mathbf{B}\mathbf{Z}.$$

- In order to uniquely recover the information symbols, the matrix $\mathbf{A}$ must be invertible over the ring $\mathcal{R}$. Thus, we have

$$\mathbf{Y}' = \mathbf{B}\mathbf{Y} = \sqrt{P}\mathbf{B}\mathbf{G}\mathbf{X} + \mathbf{B}\mathbf{Z}.$$

- The goal is to project $\mathbf{G}$ (by left multiplying it with a receiver filtering matrix $\mathbf{B}$) onto a non-singular integer matrix $\mathbf{A}$.

- In order to uniquely recover the information symbols, the matrix $\mathbf{A}$ must be invertible over the ring $\mathcal{R}$. Thus, we have

$$\mathbf{Y}' = \mathbf{B}\mathbf{Y} = \sqrt{P}\mathbf{B}\mathbf{G}\mathbf{X} + \mathbf{B}\mathbf{Z}.$$

- The goal is to project $\mathbf{G}$ (by left multiplying it with a receiver filtering matrix $\mathbf{B}$) onto a non-singular integer matrix $\mathbf{A}$.
- For the IF receiver formulation, a suitable signal model is

$$\mathbf{Y}' = \sqrt{P}\mathbf{A}\mathbf{X} + \sqrt{P}(\mathbf{B}\mathbf{G} - \mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z},$$

where $\sqrt{P}\mathbf{A}\mathbf{X}$ is the desired signal component, and the effective noise is $\sqrt{P}(\mathbf{B}\mathbf{G} - \mathbf{A})\mathbf{X} + \mathbf{B}\mathbf{Z}$.

Problem Formulation

In particular, the effective noise power along the m-th row of $\mathbf{Y}'$ is defined as

$$g(\mathbf{a}_m, \mathbf{b}_m) \triangleq \|\mathbf{b}_m\|^2 + P\|\mathbf{b}_m\mathbf{G} - \mathbf{a}_m\|^2,$$

where $\mathbf{a}_m$ and $\mathbf{b}_m$ denotes the m-th row of $\mathbf{A}$ and $\mathbf{B}$, respectively.

Problem Formulation

In particular, the effective noise power along the m-th row of $\mathbf{Y}'$ is defined as

$$g(\mathbf{a}_m, \mathbf{b}_m) \triangleq \|\mathbf{b}_m\|^2 + P\|\mathbf{b}_m\mathbf{G} - \mathbf{a}_m\|^2,$$

where $\mathbf{a}_m$ and $\mathbf{b}_m$ denotes the m-th row of $\mathbf{A}$ and $\mathbf{B}$, respectively.

Problem Given $\mathbf{G}$ and P, the problem is to find the matrices $\mathbf{B} \in \mathbb{C}^{n\times n}$ and $\mathbf{A} \in \mathbb{Z}[i]^{n\times n}$ such that:

- The $\max_{1\le m\le n} g(\mathbf{a}_m, \mathbf{b}_m)$ is minimized, and
- The corresponding matrix $\mathbf{A}$ is invertible over the ring $\mathcal{R}$.

IF Receiver

- Given $\mathbf{a}$, the optimum value of $\mathbf{b}_m$ can be obtained as

$$\mathbf{b}_m = \mathbf{a}\mathbf{G}^h\mathbf{S}^{-1}.$$

IF Receiver

- Given $\mathbf{a}$, the optimum value of $\mathbf{b}_m$ can be obtained as

$$\mathbf{b}_m = \mathbf{a}\mathbf{G}^h\mathbf{S}^{-1}.$$

- Then, after replacing $\mathbf{b}_m$ in $g(\mathbf{a}, \mathbf{b}_m)$, we get

$$\mathbf{a}_m = \arg \min_{\mathbf{a}\in\mathbb{Z}[i]^n} \mathbf{a}\mathbf{V}\mathbf{D}\mathbf{V}^h\mathbf{a}^h,$$

  where $\mathbf{V}$ is the matrix composed of the eigenvectors of $\mathbf{G}\mathbf{G}^h$, and $\mathbf{D}$ is a diagonal matrix with m-th entry $\mathbf{D}_{m,m} = \left(P\rho_m^2 + 1\right)^{-1}$, where ρ_m is the m-th singular value of $\mathbf{G}$.

IF Receiver; Continued

- With this, we have to obtain n vectors $\mathbf{a}_m$, $1 \leq m \leq n$, which result in the first n smaller values of $\mathbf{aVDV}^h\mathbf{a}^h$ along with the non-singular property on $\mathbf{A}$.

IF Receiver; Continued

- With this, we have to obtain n vectors $\mathbf{a}_m$, $1 \leq m \leq n$, which result in the first n smaller values of $\mathbf{a}\mathbf{V}\mathbf{D}\mathbf{V}^h\mathbf{a}^h$ along with the non-singular property on $\mathbf{A}$.
- The minimization problem is the shortest vector problem for a lattice with Gram matrix $\mathbf{M} = \mathbf{V}\mathbf{D}\mathbf{V}^h$.

IF Receiver; Continued

- With this, we have to obtain n vectors $\mathbf{a}_m$, $1 \leq m \leq n$, which result in the first n smaller values of $\mathbf{a}\mathbf{V}\mathbf{D}\mathbf{V}^h\mathbf{a}^h$ along with the non-singular property on $\mathbf{A}$.
- The minimization problem is the shortest vector problem for a lattice with Gram matrix $\mathbf{M} = \mathbf{V}\mathbf{D}\mathbf{V}^h$.
- Since $\mathbf{M}$ is a positive definite matrix, we can write $\mathbf{M} = \mathbf{L}\mathbf{L}^h$ for some $\mathbf{L} \in \mathbb{C}^{n \times n}$ by using Choelsky decomposition.

IF Receiver; Continued

- With this, we have to obtain n vectors $\mathbf{a}_m$, $1 \leq m \leq n$, which result in the first n smaller values of $\mathbf{a}\mathbf{V}\mathbf{D}\mathbf{V}^h\mathbf{a}^h$ along with the non-singular property on $\mathbf{A}$.
- The minimization problem is the shortest vector problem for a lattice with Gram matrix $\mathbf{M} = \mathbf{V}\mathbf{D}\mathbf{V}^h$.
- Since $\mathbf{M}$ is a positive definite matrix, we can write $\mathbf{M} = \mathbf{L}\mathbf{L}^h$ for some $\mathbf{L} \in \mathbb{C}^{n \times n}$ by using Choelsky decomposition.
- With this, the rows of $\mathbf{L} = \mathbf{V}\mathbf{D}^{\frac{1}{2}}$ generate a lattice, say Λ.

IF Receiver; Continued

- With this, we have to obtain n vectors $\mathbf{a}_m$, $1 \leq m \leq n$, which result in the first n smaller values of $\mathbf{a}\mathbf{V}\mathbf{D}\mathbf{V}^h\mathbf{a}^h$ along with the non-singular property on $\mathbf{A}$.
- The minimization problem is the shortest vector problem for a lattice with Gram matrix $\mathbf{M} = \mathbf{V}\mathbf{D}\mathbf{V}^h$.
- Since $\mathbf{M}$ is a positive definite matrix, we can write $\mathbf{M} = \mathbf{L}\mathbf{L}^h$ for some $\mathbf{L} \in \mathbb{C}^{n \times n}$ by using Choelsky decomposition.
- With this, the rows of $\mathbf{L} = \mathbf{V}\mathbf{D}^{\frac{1}{2}}$ generate a lattice, say Λ.
- A set of possible choices for $\{\mathbf{a}_1, \ldots, \mathbf{a}_n\}$ is the set of complex integer vectors, whose corresponding lattice points in Λ have lengths at most equal to the n-th successive minima of Λ.

The Proposed Algorithm

The two well-known lattice reduction algorithms satisfying the above property up to constants are HKZ and Minkowski lattice reduction algorithms.

The Proposed Algorithm

The two well-known lattice reduction algorithms satisfying the above property up to constants are HKZ and Minkowski lattice reduction algorithms.

Input: $\mathbf{G} \in \mathbb{C}^{n \times n}$, and P.

Output: A unimodular matrix $\mathbf{A}$.

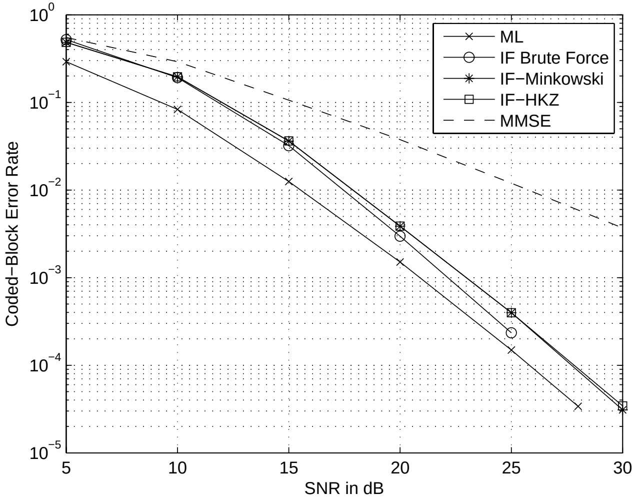
1. Form the generator matrix $\mathbf{L} = \mathbf{V}\mathbf{D}^{\frac{1}{2}}$ of a lattice Λ.
2. Reduce $\mathbf{L}$ to $\mathbf{L}'$ using either HKZ or Minkowski lattice reduction algorithm.
3. The n rows of $\mathbf{L}'\mathbf{L}^{-1}$ provide n rows $\mathbf{a}_m$ of $\mathbf{A}$ for $1 \leq m \leq n$.

Receive Diversity

Theorem (Sakzad'13)

For a MIMO channel with n transmit and n receive antennas over a Rayleigh fading channel, the integer-forcing linear receiver based on lattice reduction achieves full receive diversity.

Performance against exhaustive search



A toy example from Cryptography

Public and private keys

1. GGH involves a private key and a public key.

Public and private keys

1. GGH involves a private key and a public key.
2. The private key of user j is a generator matrix $\mathbf{G}_j$ of a lattice Λ with "nearly orthogonal" basis vectors and a unimodular matrix $\mathbf{U}_j$, for $j \in \{a, b\}$.

Public and private keys

1. GGH involves a private key and a public key.
2. The private key of user j is a generator matrix $\mathbf{G}_j$ of a lattice Λ with "nearly orthogonal" basis vectors and a unimodular matrix $\mathbf{U}_j$, for $j \in \{a, b\}$.
3. The public key of user j is $\mathbf{G}'_j = \mathbf{U}_j \mathbf{G}_j$, which is another generator matrix of the lattice Λ.

Public and private keys

1. GGH involves a private key and a public key.
2. The private key of user j is a generator matrix $\mathbf{G}_j$ of a lattice Λ with "nearly orthogonal" basis vectors and a unimodular matrix $\mathbf{U}_j$, for $j \in \{a, b\}$.
3. The public key of user j is $\mathbf{G}'_j = \mathbf{U}_j\mathbf{G}_j$, which is another generator matrix of the lattice Λ.
4. Security parameters are n and σ.

Public and private keys

1. GGH involves a private key and a public key.
2. The private key of user j is a generator matrix $\mathbf{G}_j$ of a lattice Λ with "nearly orthogonal" basis vectors and a unimodular matrix $\mathbf{U}_j$, for $j \in \{a, b\}$.
3. The public key of user j is $\mathbf{G}'_j = \mathbf{U}_j \mathbf{G}_j$, which is another generator matrix of the lattice Λ.
4. Security parameters are n and σ.
5. Works based on the hardness of closest vector problem (CVP).

Description

1. Alice wants to send a message $\mathbf{m}$ to Bob.

Description

1. Alice wants to send a message $\mathbf{m}$ to Bob.
2. She uses Bob's public key $\mathbf{G}'_b$ and encrypts $\mathbf{m}$ to

$$\mathbf{c} = \mathbf{m}\mathbf{G}'_b + \mathbf{e},$$

where $\mathbf{e} \in \{\pm\sigma\}^n$.

Description

1. Alice wants to send a message $\mathbf{m}$ to Bob.
2. She uses Bob's public key $\mathbf{G}_b'$ and encrypts $\mathbf{m}$ to

$$\mathbf{c} = \mathbf{m}\mathbf{G}_b' + \mathbf{e},$$

where $\mathbf{e} \in \{\pm\sigma\}^n$.

3. Bob employs $\mathbf{U}$ and $\mathbf{G}$ to decrypt $\mathbf{c}$ as follows. Bob first computes

$$\mathbf{c}\mathbf{G}_b^{-1} = \mathbf{m}\mathbf{G}_b'\mathbf{G}_b^{-1} + \mathbf{e}\mathbf{G}_b^{-1} = \mathbf{m}\mathbf{U}_b + \mathbf{e}\mathbf{G}_b^{-1},$$

then

$$\lfloor \mathbf{c}\mathbf{G}_b^{-1} \rceil \mathbf{U}_b^{-1} = \mathbf{m}\mathbf{U}_b\mathbf{U}_b^{-1} = \mathbf{m}.$$

1. Various attacks have been proposed. Almost dead!

1. Various attacks have been proposed. Almost dead!
2. NTRU is a special instance of GGH using a circulant matrix for the public key.

1. Various attacks have been proposed. Almost dead!
2. NTRU is a special instance of GGH using a circulant matrix for the public key.
3. Increase the dimension of the lattice up to 1000.

1. Various attacks have been proposed. Almost dead!
2. NTRU is a special instance of GGH using a circulant matrix for the public key.
3. Increase the dimension of the lattice up to 1000.
4. One very famous attack on these cryptosystems is lattice reduction algorithms.

Thanks for your attention!