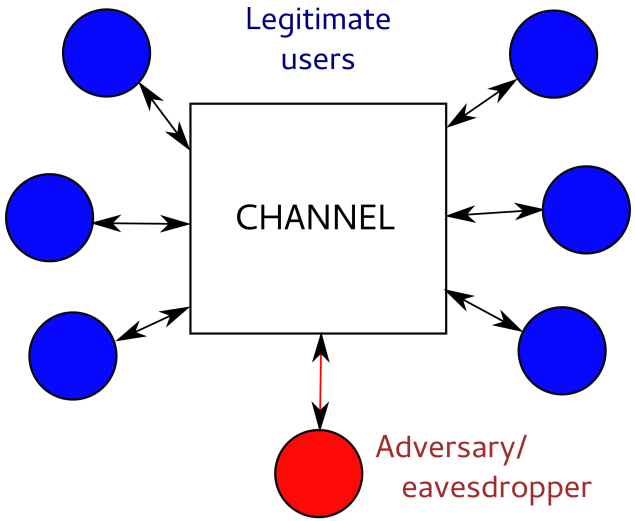
Lattice Codes for Secure Communication and Secret Key Generation

Shashank Vatedka
Advisor: Prof. Navin Kashyap

{shashank,nkashyap}@ece.iisc.ernet.in
Dept. of Electrical Communication Engineering

EECS Research Students Symposium - 2016

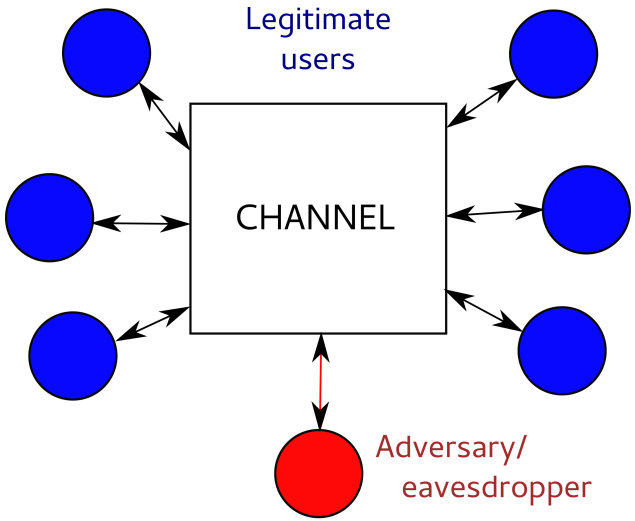
Information-Theoretic Security



Wireless communication channels:

- Noisy
- Insecure

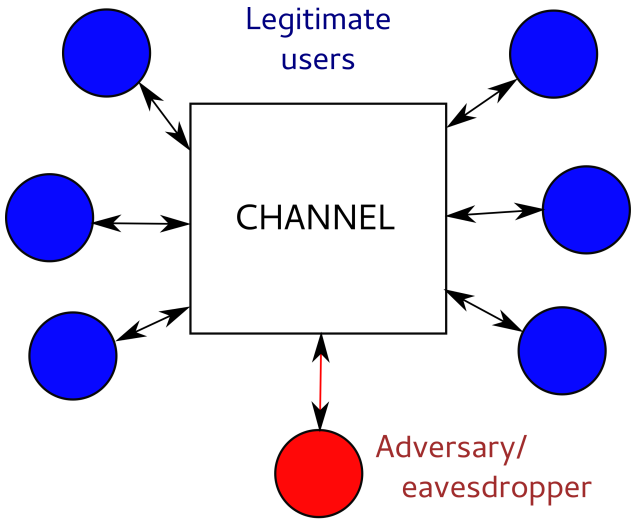
Information-Theoretic Security



Wireless communication channels:

- Noisy $\rightarrow$ Reliability
- Insecure $\rightarrow$ Security

Information-Theoretic Security



Wireless communication channels:

- Noisy $\rightarrow$ Reliability
- Insecure $\rightarrow$ Security

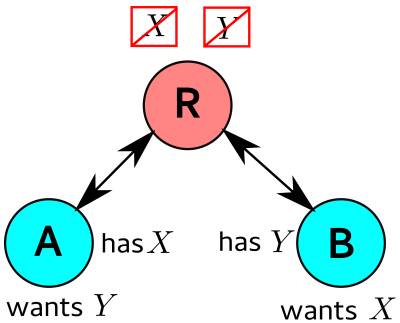
An information-theoretic approach:

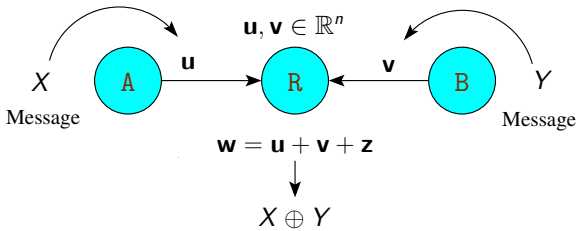
- Messages drawn at random
- No assumptions on computational power of eavesdropper
- *Average-case* security:
  Want Eve's observations W to be independent of messages X_i.
  (perfect secrecy), or

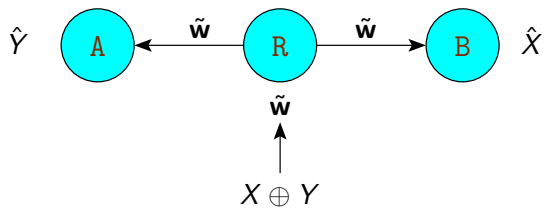
$$I(W; X_i) = \sum_{w, x_i} p(w, x_i) \log_2 \frac{p(w, x_i)}{p(w)p(x_i)}$$

"is small".
(strong secrecy)

Secure Bidirectional Relaying

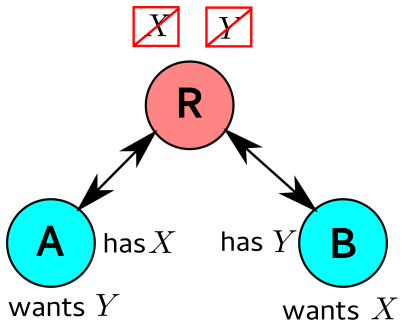


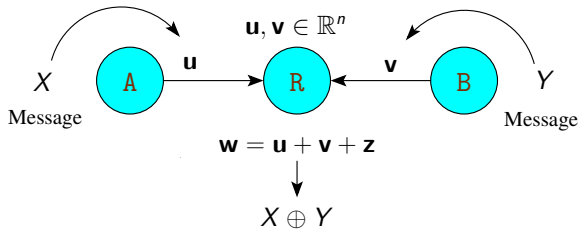


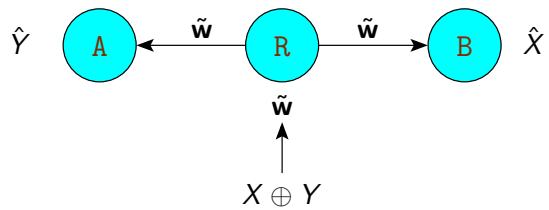


- Messages $X, Y \in \mathbb{G}$
- Power constraint:
  $\frac{1}{n}\mathbb{E}\|\mathbf{u}\|^2 < P$ and $\frac{1}{n}\mathbb{E}\|\mathbf{v}\|^2 < P$
- Reliability:
  Probability of decoding error is small.
- Transmission rate:
  $R = \frac{1}{n}\log_2|\mathbb{G}|$

Secure Bidirectional Relaying







- Messages $X, Y \in \mathbb{G}$
- Power constraint:
  $\frac{1}{n}\mathbb{E}\|\mathbf{u}\|^2 < P$ and $\frac{1}{n}\mathbb{E}\|\mathbf{v}\|^2 < P$
- Reliability:
  Probability of decoding error is small.
- Transmission rate:
  $R = \frac{1}{n}\log_2|\mathbb{G}|$

- Perfect secrecy:

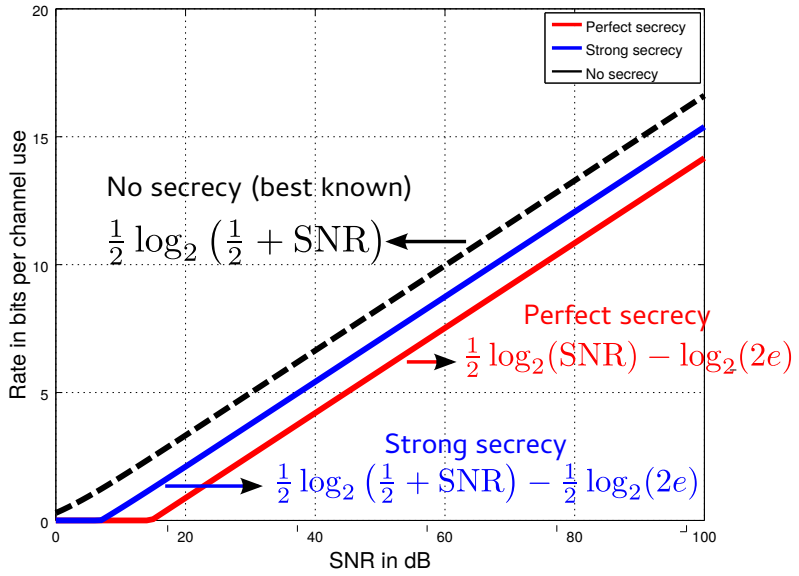
$$\mathbf{w} \perp\!\!\!\perp X \text{ and } \mathbf{w} \perp\!\!\!\perp Y$$

- Strong secrecy:

$$\lim_{n\to\infty} I(X;\mathbf{w}) = \lim_{n\to\infty} I(Y;\mathbf{w}) = 0$$

Highlights

- Explicit coding scheme that achieves perfect secrecy: irrespective of noise distribution.
- Coding scheme for strong secrecy: irrespective of noise distribution.

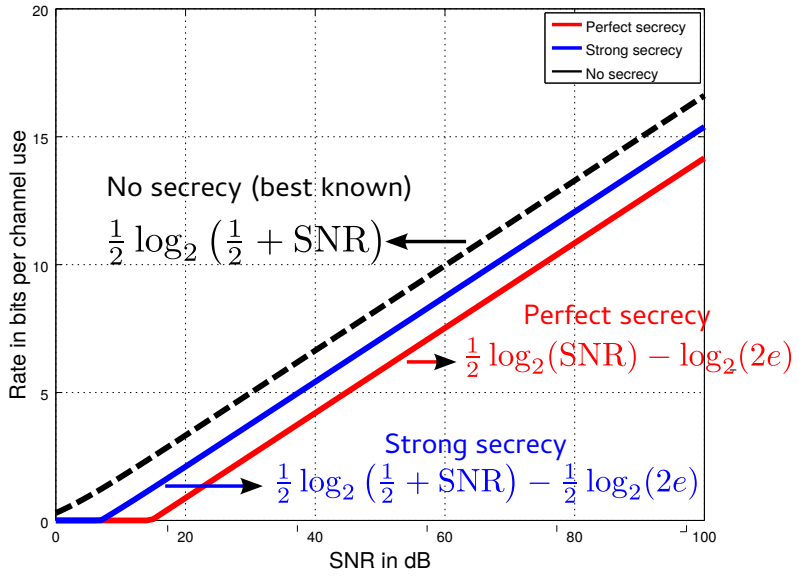


[1] "Secure Compute-and-Forward in a Bidirectional Relay," IEEE Transactions on Information Theory, May 2015.

[2] "Nested Lattice Codes for Secure Bidirectional Relaying with Asymmetric Channel Gains," ITW 2015.

Highlights

- Explicit coding scheme that achieves perfect secrecy: irrespective of noise distribution.
- Coding scheme for strong secrecy: irrespective of noise distribution.



- Results for unequal channel gains, i.e.,

$$\mathbf{w} = h_1\mathbf{u} + h_2\mathbf{v} + \mathbf{z},$$

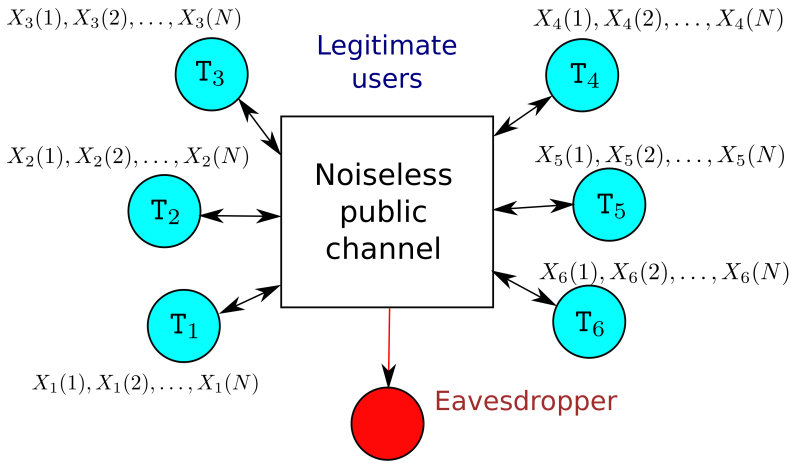
  when h_1, h_2 unknown to users.
- Larger networks.

---

[1] "Secure Compute-and-Forward in a Bidirectional Relay," IEEE Transactions on Information Theory, May 2015.

[2] "Nested Lattice Codes for Secure Bidirectional Relaying with Asymmetric Channel Gains," ITW 2015.

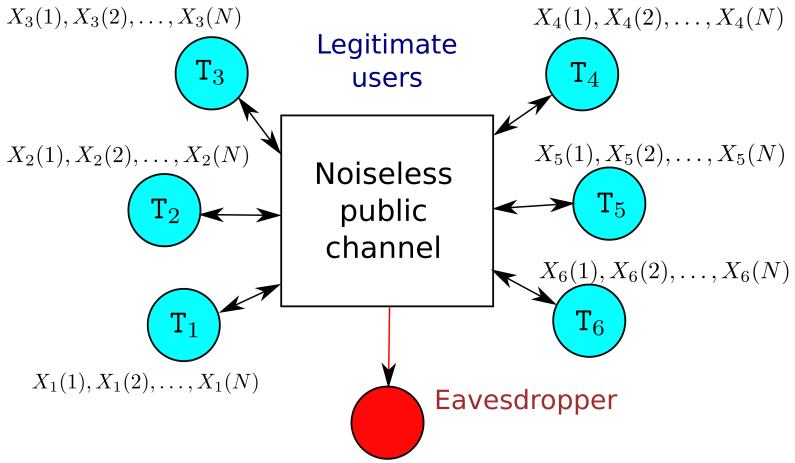
Secret Key Generation from Correlated Gaussian Sources



- T_i has N iid samples of a Gaussian source X_i.
- $(X_1(t), X_2(t), \ldots, X_m(t))$ are correlated Gaussian rvs.
- Agree on secret key using correlated rvs and public communication.

[1] "A Lattice Coding Scheme for Secret Key Generation from Gaussian Markov Tree Sources", accepted, ISIT 2016

Secret Key Generation from Correlated Gaussian Sources



- T_i has N iid samples of a Gaussian source X_i.
- $(X_1(t), X_2(t), \ldots, X_m(t))$ are correlated Gaussian rvs.
- Agree on secret key using correlated rvs and public communication.

Main contributions:

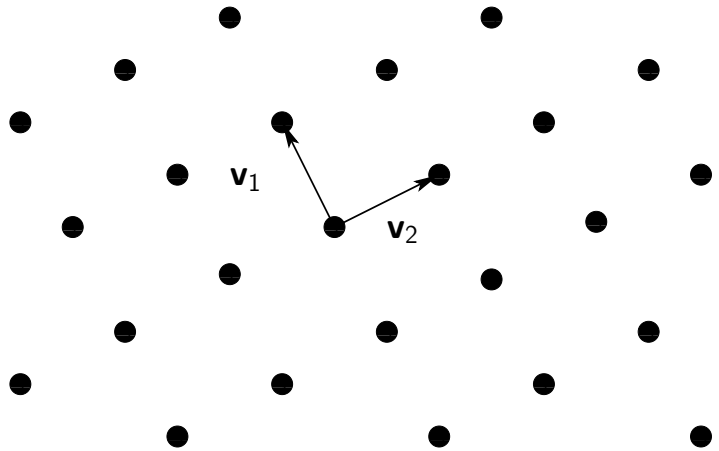
- We give a coding scheme that generates strongly secure secret keys.
- Encoding and decoding complexities are polynomial in N.
- Characterize achievable secret key rates when joint distribution of sources is a Markov tree.

[1] "A Lattice Coding Scheme for Secret Key Generation from Gaussian Markov Tree Sources", accepted, ISIT 2016

Lattices and Lattice Codes

$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ a basis for $\mathbb{R}^n$.

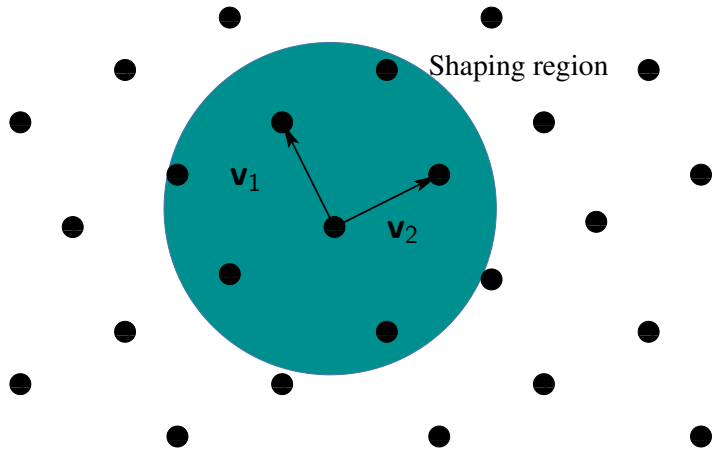
- $\Lambda = \{\sum_{i=1}^{n} a_i \mathbf{v}_i : a_i \in \mathbb{Z}\}$ is a lattice.



Lattices and Lattice Codes

$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ a basis for $\mathbb{R}^n$.

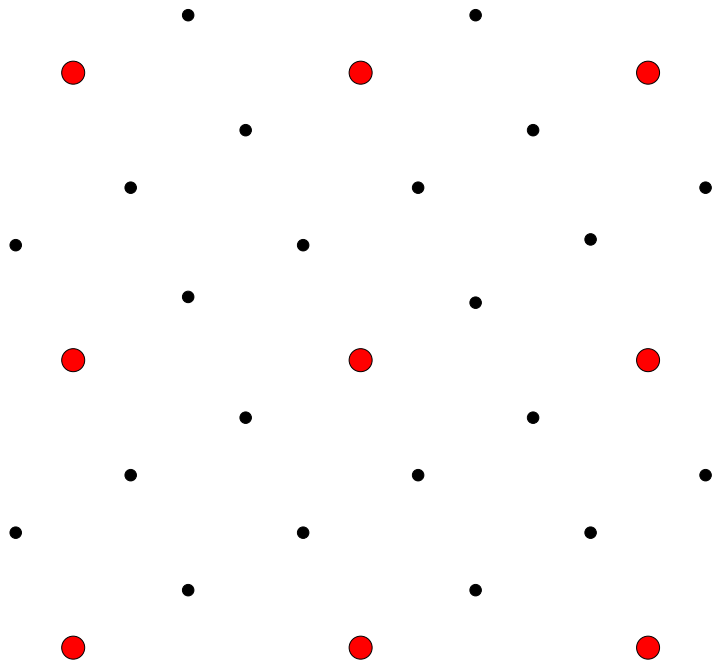
- $\Lambda = \{\sum_{i=1}^{n} a_i \mathbf{v}_i : a_i \in \mathbb{Z}\}$ is a lattice.
- Lattice code: All lattice points within a shaping region $\mathcal{S}$.



Lattices and Lattice Codes

$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ a basis for $\mathbb{R}^n$.

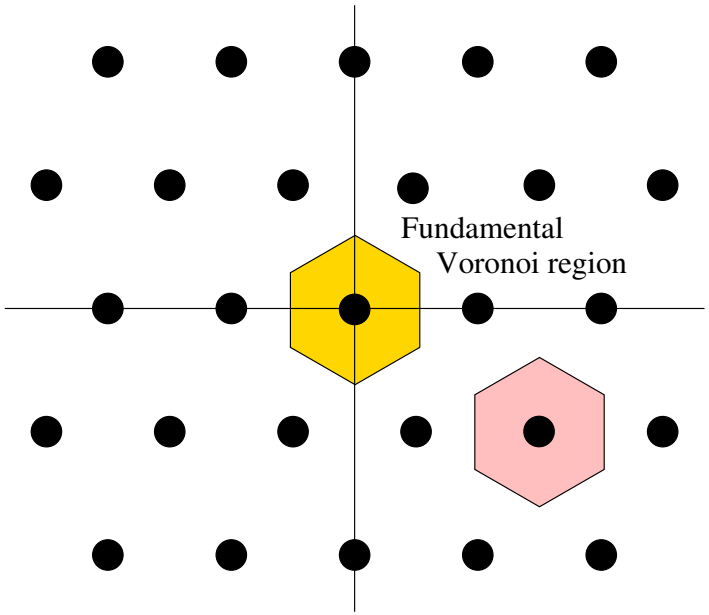
- $\Lambda = \{\sum_{i=1}^{n} a_i \mathbf{v}_i : a_i \in \mathbb{Z}\}$ is a lattice.
- Lattice code: All lattice points within a shaping region $\mathcal{S}$.
- Nested lattices: (Λ, Λ_0), where $\Lambda_0 \subset \Lambda$ are lattices in $\mathbb{R}^n$.



Lattices and Lattice Codes

$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ a basis for $\mathbb{R}^n$.

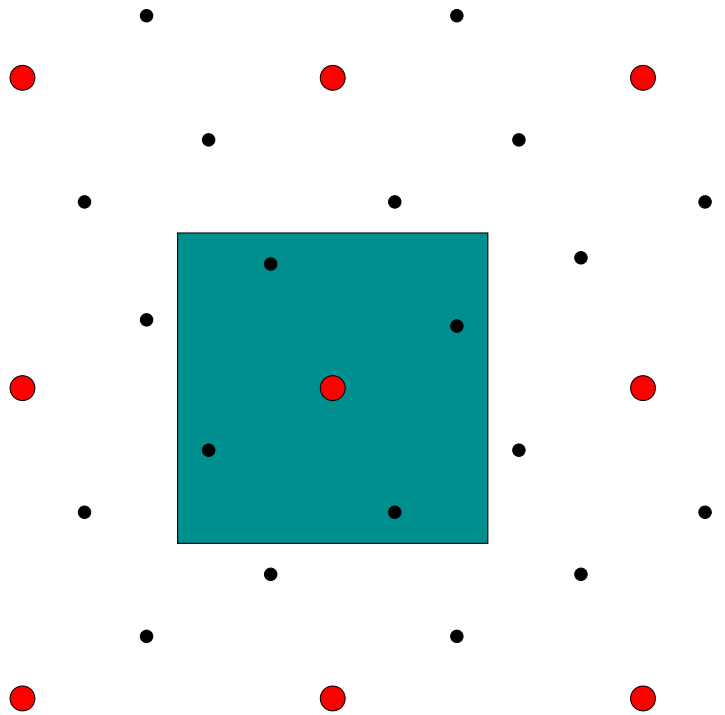
- $\Lambda = \{\sum_{i=1}^{n} a_i \mathbf{v}_i : a_i \in \mathbb{Z}\}$ is a lattice.
- Lattice code: All lattice points within a shaping region $\mathcal{S}$.
- Nested lattices: (Λ, Λ_0), where $\Lambda_0 \subset \Lambda$ are lattices in $\mathbb{R}^n$.
- Fundamental Voronoi region: set of points of $\mathbb{R}^n$ closest to the zero lattice point.



Lattices and Lattice Codes

$\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ a basis for $\mathbb{R}^n$.

- $\Lambda = \{\sum_{i=1}^{n} a_i \mathbf{v}_i : a_i \in \mathbb{Z}\}$ is a lattice.
- Lattice code: All lattice points within a shaping region $\mathcal{S}$.
- Nested lattices: (Λ, Λ_0), where $\Lambda_0 \subset \Lambda$ are lattices in $\mathbb{R}^n$.
- Fundamental Voronoi region: set of points of $\mathbb{R}^n$ closest to the zero lattice point.
- Nested lattice code: Fundamental Voronoi region of Λ_0 is the shaping region.



Nested Lattice Codes for Gaussian Channels

- Codes for communication over Gaussian channels
- Vector quantization
- Codes for secure communication and secret key generation
- Lattice-based cryptography
- Sphere packing and covering
- Many more

Drawback of general nested lattice codes: Closest lattice point decoding takes exponential time.

Nested Lattice Codes for Gaussian Channels

- Codes for communication over Gaussian channels
- Vector quantization
- Codes for secure communication and secret key generation
- Lattice-based cryptography
- Sphere packing and covering
- Many more

Drawback of general nested lattice codes: Closest lattice point decoding takes exponential time.

Goal: Design nested lattice codes with polynomial encoding-decoding complexity.

Low-Density Construction-A (LDA) Lattices

- Lattices constructed from low-density parity-check (LDPC) codes.
- Proposed by di Pietro et al. (2013).
- Admit low-complexity message-passing decoders.
- We studied some structural properties of these lattices.
- Under closest lattice point decoding, nested LDA lattice codes achieve capacity of AWGN channel (di Pietro et al. 2014).
- We also showed that they yield optimal high-dimensional vector quantizers and sphere packings.

[1] "Some Goodness Properties of LDA Lattices", submitted, Problems of Information Transmission, Dec. 2015

Concatenated Lattice Codes with Polynomial Encoding and Decoding Complexity

Concatenated lattice codes achieve the capacity of the AWGN channel.[1]

- Concatenating with outer Reed-Solomon code:
  Encoding and decoding complexity: $O(N^2)$
  Error probability: $e^{-\Omega(N)}$
- Concatenating with outer expander code:
  Encoding complexity: $O(N^2)$
  Decoding complexity: $O(N \log^2 N)$
  Error probability: $e^{-\Omega(N)}$

First constructions to have poly-time complexity and exponentially decaying probability of error.

Extensions:

- Gaussian wiretap channel
- Physical-layer network coding
- Secret key generation

[1] "A Capacity-Achieving Coding Scheme for the AWGN Channel with Polynomial Encoding and Decoding Complexity," NCC 2016, arXiv:1603.08236.

Summary

- Secure bidirectional relaying: coding schemes and achievable transmission rates.
- Secret key generation: poly-time coding scheme and achievable key rates.
- Lattices from LDPC codes: properties.
- Concatenated lattice codes: capacity-achieving with poly-time encoding and decoding complexity.

Summary

- Secure bidirectional relaying: coding schemes and achievable transmission rates.
- Secret key generation: poly-time coding scheme and achievable key rates.
- Lattices from LDPC codes: properties.
- Concatenated lattice codes: capacity-achieving with poly-time encoding and decoding complexity.

More details

Attend poster session!

`ece.iisc.ernet.in/~shashank/publications.html`