Lattice Codes for Secure Communication and Secret Key Generation

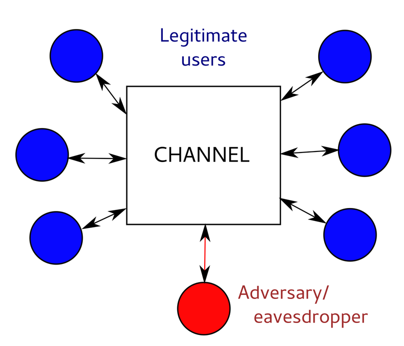
Shashank Vatedka & Navin Kashyap

Dept. of Electrical Communication Engineering, Indian Institute of Science

Overview

- 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.

Information-Theoretic Security



Wireless communication channels:

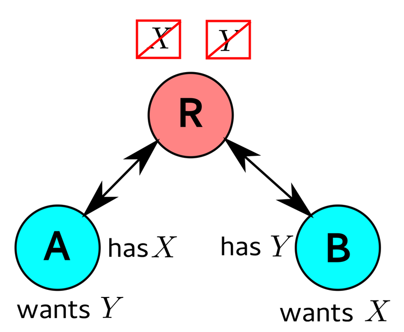
- Noisy $\rightarrow$ Reliability and Insecure $\rightarrow$ Security.

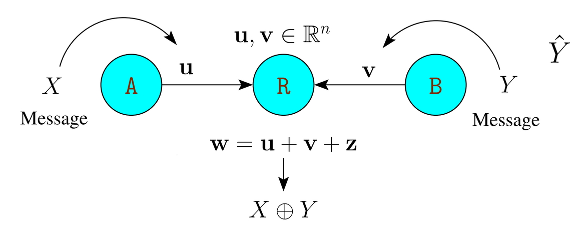
An information-theoretic approach to security:

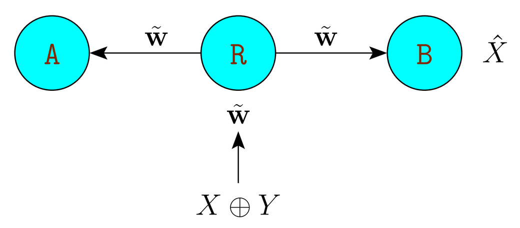
- Messages drawn at random; No assumptions on computational power of eavesdropper.
- Want eve's observations W to be independent of messages X_i. (perfect secrecy), or

$$I(W;X_i) = \sum_{w,x_i} p(w,x_i) \log_2 \frac{p(w,x_i)}{p(w)p(x_i)} \text{ to be "small". (strong secrecy)}$$

Secure Bidirectional Relaying



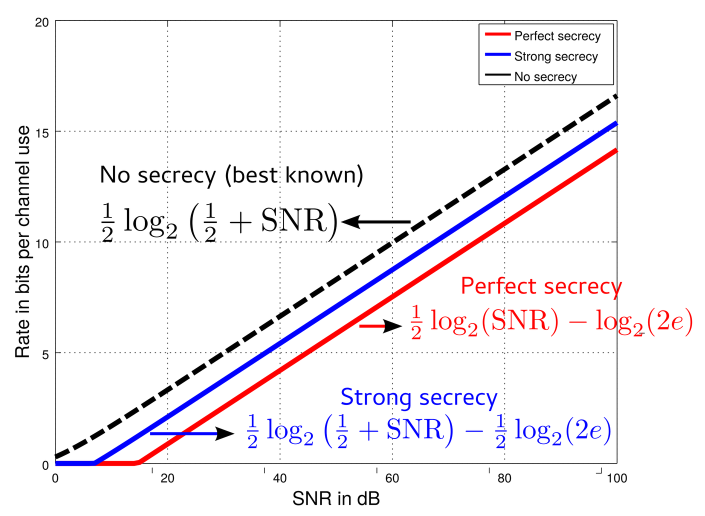




- Messages $X, Y \in \mathbb{G}$.
- Power constraint: $\frac{1}{n}\mathbb{E}\|\mathbf{u}\|^2 < P$ and $\frac{1}{n}\mathbb{E}\|\mathbf{v}\|^2 < P$.
- Reliability: Probability of decoding error is small.
- Transmission rate: $R = \frac{1}{n}\log_2|\mathbb{G}|$.
- Perfect secrecy: $\mathbf{w} \perp\!\!\!\perp X$ and $\mathbf{w} \perp\!\!\!\perp Y$.
- Strong secrecy: $\lim_{n\to\infty} I(X;\mathbf{w}) = \lim_{n\to\infty} I(Y;\mathbf{w}) = 0$.

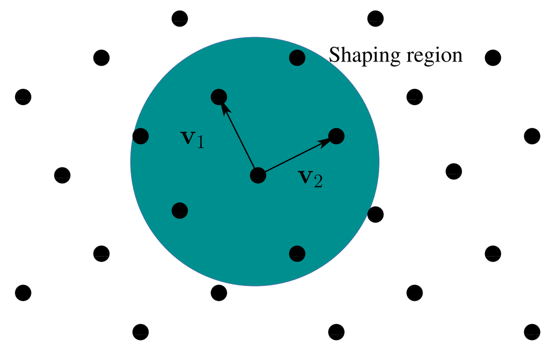
Main results:

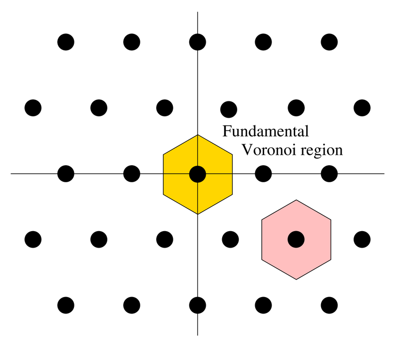
- Explicit coding scheme that achieves perfect secrecy: irrespective of noise distribution [1].
- Coding scheme for strong secrecy: irrespective of noise distribution [1].
- Results for unequal channel gains, i.e., $\mathbf{w} = h_1\mathbf{u} + h_2\mathbf{v} + \mathbf{z}$, when h_1, h_2 unknown to users [2].
- Larger networks [1].

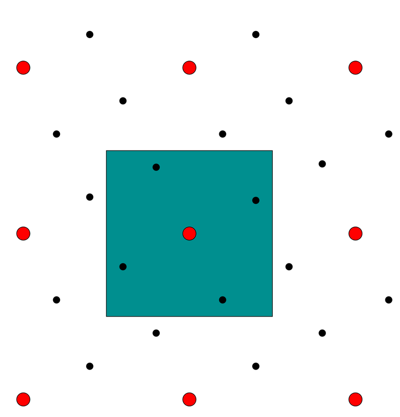


Lattices and Lattice Codes

- $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_n$ a basis for $\mathbb{R}^n$. Then, $\Lambda = \{\sum_{i=1}^n a_i\mathbf{v}_i : a_i \in \mathbb{Z}\}$ 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.







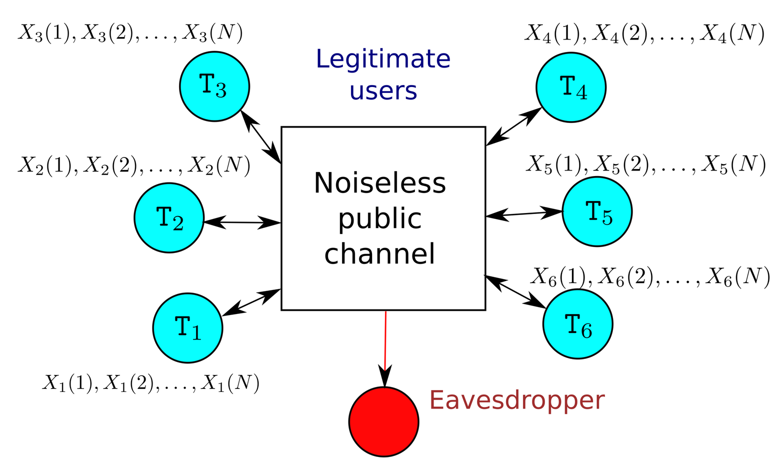
Nested Lattice Codes for Gaussian Channels

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

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.
- Each terminal operates under a quantization rate constraint, and only the quantized random variables can be used to generate secret keys.
- Objective: Generate secret key using correlated rvs and public communication.
- Reliability: All terminals must agree on same secret key K with high probability.
- Security: The key K must be "almost independent" of public communication.
- Key rate: $\frac{1}{N}\log_2|\text{key space}|$.

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.

Low-Density Construction-A (LDA) Lattices

- Lattices constructed from low-density parity-check (LDPC) codes.
- Proposed by di Pietro et al. (2012) [6].
- Admit low-complexity message-passing decoders.
- We studied some structural properties of these lattices.
- Specifically, we showed that they are good for packing and MSE quantization, and their duals are good for packing [4].
- Under closest lattice point decoding, nested LDA lattice codes achieve capacity of AWGN channel (di Pietro et al. 2014) [7].
- They are also useful for communication over other Gaussian networks, vector quantization, and physical-layer security [4].

Concatenated Lattice Codes with Polynomial Encoding and Decoding Complexity

Concatenated lattice codes achieve the capacity of the AWGN channel. [5]

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

First constructions to have poly-time complexity and exponentially decaying probability of error.
Extensions to Gaussian wiretap channel, Physical-layer network coding and Secret key generation.

References

[1] S. Vatedka, N. Kashyap, and A. Thangaraj, "Secure Compute-and-Forward in a Bidirectional Relay," IEEE Trans. Inf. Theory, May 2015.

[2] S. Vatedka and N. Kashyap, "Nested Lattice Codes for Secure Bidirectional Relaying with Asymmetric Channel Gains," ITW 2015.

[3] S. Vatedka and N. Kashyap, "A Lattice Coding Scheme for Secret Key Generation from Gaussian Markov Tree Sources", accepted, ISIT 2016.

[4] S. Vatedka and N. Kashyap, "Some Goodness Properties of LDA Lattices", submitted, Problems of Information Transmission, Dec. 2015.

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

[6] N. di Pietro, J.J. Boutros, G. Zémor, and L. Brunel, "Integer low-density lattices based on Construction A," ITW 2012.

[7] N. di Pietro, "On infinite and finite lattice constellations for the additive white Gaussian noise channel," Ph.D. dissertation, 2014.