Lattice Coding for Strongly Secure Compute-and-Forward in a Bidirectional Relay

Shashank Vatedka and Navin Kashyap

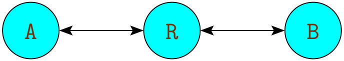
{shashank,nkashyap}@ece.iisc.ernet.in
Department of ECE
Indian Institute of Science
Bangalore, India

International Symposium on Information Theory
Istanbul, Turkey
July 2013

Acknowledgements

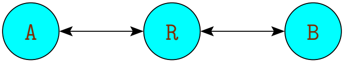
- ISIT Student Travel Grant.
- IISc (GARP) Travel Grant.
- SPCOM 2012 Student Travel Grant.

Bidirectional relay



No direct link between user nodes. All links are wireless with unit gain and AWGN.

Bidirectional relay



No direct link between user nodes. All links are wireless with unit gain and AWGN.

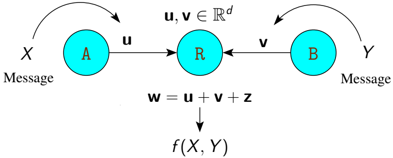


Figure: MAC phase

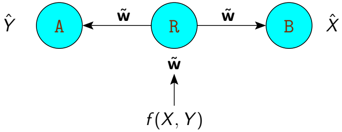
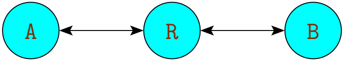


Figure: Broadcast phase

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

where $\mathbf{z}$ is AWGN with mean zero and variance σ^2.

Bidirectional relay



No direct link between user nodes. All links are wireless with unit gain and AWGN.

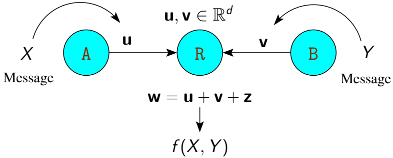


Figure: MAC phase

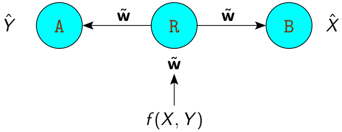


Figure: Broadcast phase

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

where $\mathbf{z}$ is AWGN with mean zero and variance σ^2.

- Relay acts as passive eavesdropper.
- We want strong secrecy: $\mathcal{I}(X; \mathbf{w}), \mathcal{I}(Y; \mathbf{w}) \to 0$ as $d \to \infty$.

Wilson et al. (2010), Nazer and Gastpar (2011).

Messages X and Y are mapped to elements of a suitably chosen finite Abelian group $(\mathbb{G}, \oplus)$.

Here, $\mathbf{u}, \mathbf{v} \in \mathbb{R}^d$, and $f(X, Y) = X \oplus Y$.

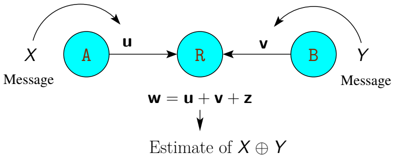


Figure: MAC phase

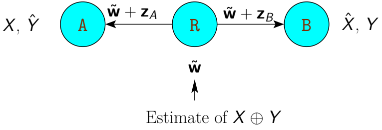


Figure: Broadcast phase

Compute-and-forward

Wilson et al. (2010), Nazer and Gastpar (2011).

Messages X and Y are mapped to elements of a suitably chosen finite Abelian group $(\mathbb{G}, \oplus)$.

Here, $\mathbf{u}, \mathbf{v} \in \mathbb{R}^d$, and $f(X, Y) = X \oplus Y$.

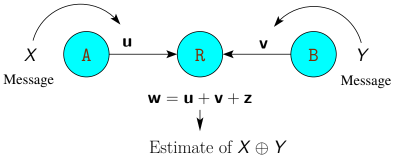


Figure: MAC phase

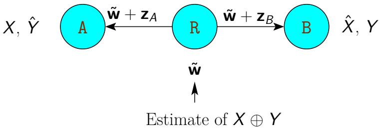


Figure: Broadcast phase

- We assume X and Y are uniformly distributed over the set of messages.
- Then, $(X \oplus Y) \perp\!\!\!\perp X$ and $(X \oplus Y) \perp\!\!\!\perp Y$.

Prior work using nested lattice coding

Secure Compute-and-forward:

- Weak secrecy using random binning: He and Yener, *"Providing secrecy using lattice codes,"* Allerton '08.
- Strong secrecy using universal hash functions: He and Yener, *"Strong secrecy and reliable byzantine detection in the presence of an untrusted relay,"* IEEE Trans. Inf. Theory '12.
- Perfect secrecy using well chosen pmfs satisfying an average power constraint: Kashyap et al., *"Secure Computation in a Bidirectional Relay,"* ISIT '12.

Gaussian wiretap channel:

- Semantic security using nested lattice codes and sampled Gaussian pmfs: Ling et al., *"Semantically Secure Lattice Codes for the Gaussian Wiretap Channel,"* arXiv:1210.6673.

Lattices

Let $\mathbf{v}_1, \mathbf{v}_2, \ldots, \mathbf{v}_d$ be linearly independent vectors in $\mathbb{R}^d$. Then the set $\Lambda = \{\sum_{i=1}^{d} a_i \mathbf{v}_i : a_i \in \mathbb{Z}\}$ is called a lattice.

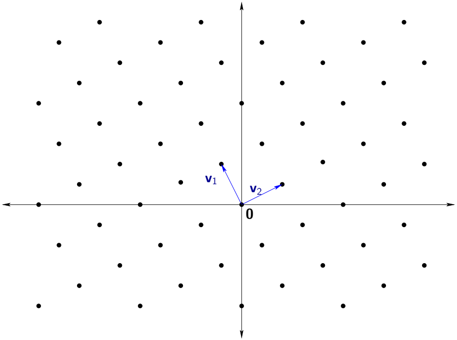


Figure: A lattice in $\mathbb{R}^2$.

Define the nearest neighbour quantizer for Λ as $Q_\Lambda(\mathbf{x}) := \arg\min_{\lambda\in\Lambda}\|\mathbf{x}-\lambda\|$. The fundamental Voronoi region of Λ is defined as $\mathcal{V}(\Lambda) := \{\mathbf{y} : Q_\Lambda(\mathbf{y}) = \mathbf{0}\}$.

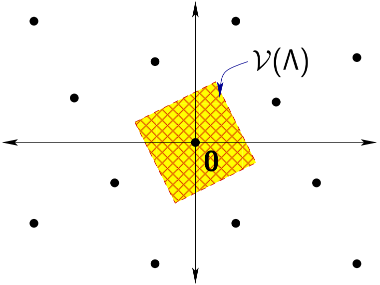


Figure: Fundamental Voronoi region of Λ, $\mathcal{V}(\Lambda)$.

$$\mathrm{vol}(\Lambda) := \mathrm{vol}\big(\mathcal{V}(\Lambda)\big).$$

Illustration: Nested lattices

If Λ and Λ_0 are lattices in $\mathbb{R}^d$ with $\Lambda_0 \subset \Lambda$, then Λ_0 is said to be nested within Λ, or Λ_0 is a sublattice of Λ.

Λ is called the fine lattice and Λ_0 is called the coarse lattice.

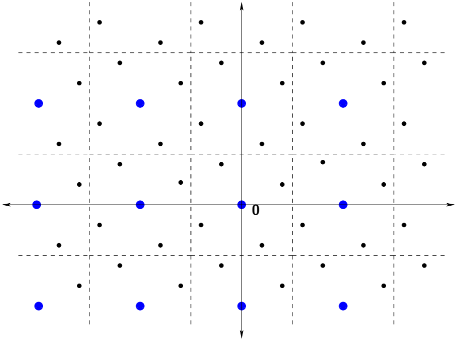


Figure: The blue dots indicate the coarse lattice Λ_0.

Cosets and coset representatives

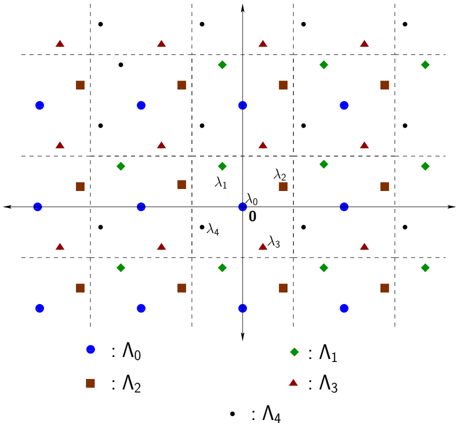


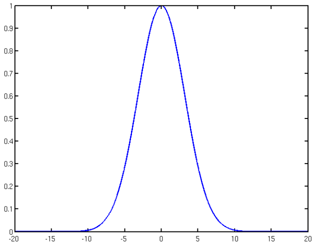
Figure: λ_i is the coset representative of Λ_i within $\mathcal{V}(\Lambda_0)$.

Basic idea to get secrecy

- Fix nested lattice pair (Λ, Λ_0) (e.g. $(\mathbb{Z}, 2\mathbb{Z})$).
- Cosets correspond to different messages. Given message Λ_i, transmit random point from Λ_i.

Basic idea to get secrecy

- Fix nested lattice pair (Λ, Λ_0) (e.g. $(\mathbb{Z}, 2\mathbb{Z})$).
- Cosets correspond to different messages. Given message Λ_i, transmit random point from Λ_i.
- Select a pdf $f(\cdot)$ over $\mathbb{R}^d$.



Basic idea to get secrecy

- Fix nested lattice pair (Λ, Λ_0) (e.g. $(\mathbb{Z}, 2\mathbb{Z})$).
- Cosets correspond to different messages. Given message Λ_i, transmit random point from Λ_i.
- Select a pdf $f(\cdot)$ over $\mathbb{R}^d$.
- Probability of transmitting $\mathbf{u} \in \Lambda_j$ is $f(\mathbf{u})/(\sum_{\mathbf{v}\in\Lambda_j} f(\mathbf{v}))$.

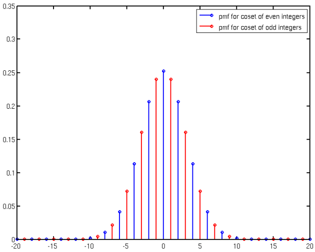


Figure: pmfs for the nested lattice pair $(\mathbb{Z}, 2\mathbb{Z})$.

- Don't use nested lattice shaping.
- Nested lattice shaping: Codewords chosen from $\Lambda \cap \mathcal{V}(\Lambda_0)$.
- Different choices of $f(\cdot)$ gives different secrecy properties![a]

[a] *"Secure compute-and-forward in a bidirectional relay,"* online: http://ece.iisc.ernet.in/~shashank/publications.html

Notation and definitions

For any $\mathbf{x}, \mathbf{z} \in \mathbb{R}^d$, and real $\kappa > 0$, we define

$$g_{\kappa,\mathbf{x}}(\mathbf{z}) := \frac{1}{\left(\sqrt{2\pi}\kappa\right)^n} e^{-\frac{\|\mathbf{z}-\mathbf{x}\|^2}{2\kappa^2}}, \tag{1}$$

Notation and definitions

For any $\mathbf{x}, \mathbf{z} \in \mathbb{R}^d$, and real $\kappa > 0$, we define

$$g_{\kappa,\mathbf{x}}(\mathbf{z}) := \frac{1}{(\sqrt{2\pi}\kappa)^n} e^{-\frac{\|\mathbf{z}-\mathbf{x}\|^2}{2\kappa^2}}, \tag{1}$$

For any lattice Λ in $\mathbb{R}^d$, we define

$$g_{\kappa,\mathbf{x}}(\Lambda) := \sum_{\lambda\in\Lambda} g_{\kappa,\mathbf{x}}(\lambda). \tag{2}$$

We denote, $g_{\kappa,\mathbf{0}}(\mathbf{z})$ by $g_{\kappa}(\mathbf{z})$, and $g_{\kappa,\mathbf{0}}(\Lambda)$ by $g_{\kappa}(\Lambda)$.

Notation and definitions

For any $\mathbf{x}, \mathbf{z} \in \mathbb{R}^d$, and real $\kappa > 0$, we define

$$g_{\kappa,\mathbf{x}}(\mathbf{z}) := \frac{1}{(\sqrt{2\pi}\kappa)^n} e^{-\frac{\|\mathbf{z}-\mathbf{x}\|^2}{2\kappa^2}}, \tag{1}$$

For any lattice Λ in $\mathbb{R}^d$, we define

$$g_{\kappa,\mathbf{x}}(\Lambda) := \sum_{\lambda \in \Lambda} g_{\kappa,\mathbf{x}}(\lambda). \tag{2}$$

We denote, $g_{\kappa,\mathbf{0}}(\mathbf{z})$ by $g_\kappa(\mathbf{z})$, and $g_{\kappa,\mathbf{0}}(\Lambda)$ by $g_\kappa(\Lambda)$.

Observation: The function

$$p(\mathbf{u}) = \begin{cases} \frac{g_\kappa(\mathbf{u})}{g_\kappa(\Lambda)}, & \mathbf{u} \in \Lambda \\ 0 & \text{otherwise.} \end{cases}$$

is a probability mass function supported over Λ.

Coding scheme

Our objective

We want a randomized coding scheme $X \to \mathbf{u}$, $Y \to \mathbf{v}$ such that

(S1) $\mathbf{u}, \mathbf{v} \in \mathbb{R}^d$, and $(X, \mathbf{u}) \perp\!\!\!\perp (Y, \mathbf{v})$.

(S2) $\mathbf{u} + \mathbf{v}$ must determine $X \oplus Y$ (for a suitably defined $\oplus$).

(S3) $\mathcal{I}(X; \mathbf{u} + \mathbf{v})$ and $\mathcal{I}(Y; \mathbf{u} + \mathbf{v})$ must go to 0 as $d \to \infty$.

Coding scheme

Our objective

We want a randomized coding scheme $X \to \mathbf{u}$, $Y \to \mathbf{v}$ such that

(S1) $\mathbf{u}, \mathbf{v} \in \mathbb{R}^d$, and $(X, \mathbf{u}) \perp\!\!\!\perp (Y, \mathbf{v})$.

(S2) $\mathbf{u} + \mathbf{v}$ must determine $X \oplus Y$ (for a suitably defined $\oplus$).

(S3) $\mathcal{I}(X; \mathbf{u} + \mathbf{v})$ and $\mathcal{I}(Y; \mathbf{u} + \mathbf{v})$ must go to 0 as $d \to \infty$.

- Observe that $X \to (\mathbf{u} + \mathbf{v}) \to (\mathbf{u} + \mathbf{v} + \mathbf{z})$ forms a Markov chain.
- Therefore, $\mathcal{I}(X; \mathbf{u} + \mathbf{v} + \mathbf{z}) \leq \mathcal{I}(X; \mathbf{u} + \mathbf{v})$.
- Hence, (S3) guarantees secrecy even in presence of noise.

A strongly secure coding scheme

- Code: $(\Lambda^{(d)}, \Lambda_0^{(d)})$ nested lattice code with $\Lambda_0^{(d)} \subset \Lambda^{(d)}$.

A strongly secure coding scheme

- Code: $(\Lambda^{(d)}, \Lambda_0^{(d)})$ nested lattice code with $\Lambda_0^{(d)} \subset \Lambda^{(d)}$.
- Messages: Chosen uniformly at random from the quotient group $\mathbb{G}^{(d)} := \Lambda^{(d)}/\Lambda_0^{(d)}$. Denote the elements of $\Lambda^{(d)}/\Lambda_0^{(d)}$ by $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$, where $N = |\Lambda^{(d)}/\Lambda_0^{(d)}|$.

A strongly secure coding scheme

- Code: $(\Lambda^{(d)}, \Lambda_0^{(d)})$ nested lattice code with $\Lambda_0^{(d)} \subset \Lambda^{(d)}$.
- Messages: Chosen uniformly at random from the quotient group $\mathbb{G}^{(d)} := \Lambda^{(d)}/\Lambda_0^{(d)}$. Denote the elements of $\Lambda^{(d)}/\Lambda_0^{(d)}$ by $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$, where $N = |\Lambda^{(d)}/\Lambda_0^{(d)}|$.
- Encoding: Given message Λ_j, encoder outputs a random point $\mathbf{u}$ from Λ_j according to

$$p_j(\mathbf{u}) = \begin{cases} \frac{g_{\sqrt{P}}(\mathbf{u})}{g_{\sqrt{P}}(\Lambda_j)}, & \text{if } \mathbf{u} \in \Lambda_j \\ \mathbf{0}, & \text{otherwise.} \end{cases}$$

A strongly secure coding scheme

- Decoding: The relay has $\mathbf{w} = \mathbf{u} + \mathbf{v} + \mathbf{z}$.
  1. Let $\tilde{\mathbf{w}}$ be the closest point in $\Lambda^{(d)}$ to $\mathbf{w}$.
  2. The estimate of $X \oplus Y$ is the coset to which $\tilde{\mathbf{w}}$ belongs.

A strongly secure coding scheme

- Decoding: The relay has $\mathbf{w} = \mathbf{u} + \mathbf{v} + \mathbf{z}$.
  1. Let $\tilde{\mathbf{w}}$ be the closest point in $\Lambda^{(d)}$ to $\mathbf{w}$.
  2. The estimate of $X \oplus Y$ is the coset to which $\tilde{\mathbf{w}}$ belongs.

- Achievable power-rate pairs: $(\mathcal{P}, \mathcal{R})$ is achievable with strong secrecy if for every $\delta > 0$, there exists a sequence of $(\Lambda^{(d)}, \Lambda_0^{(d)})$ nested lattice codes such that for all sufficiently large d,
  - Avg. transmit power, $\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 = \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2$, is less than $\mathcal{P} + \delta$.
  - Transmission rate, $\frac{1}{d}\log_2|\mathbb{G}^{(d)}|$, is greater than $\mathcal{R} - \delta$.
  - The average probability of decoding $X \oplus Y$ incorrectly from $\mathbf{u} + \mathbf{v} + \mathbf{z}$ is less than δ.
  - The mutual information, $\mathcal{I}(X; \mathbf{u} + \mathbf{v}) = \mathcal{I}(Y; \mathbf{u} + \mathbf{v})$ is less than δ.

Strong secrecy

Define the average variational distance between $U+V$ and X,

$$d_V := \sum_{\mathbf{x}} \sum_{\mathbf{w}\in\Lambda^{(d)}} |p_{U+V,X}(\mathbf{w},\mathbf{x}) - p_{U+V}(\mathbf{w})p_X(\mathbf{x})|$$

Lemma (Csiszár, Narayan (2004))

For $|\mathbb{G}^{(d)}| \geq 4$, we have

$$\mathcal{I}(X;\mathbf{u}+\mathbf{v}) \leq d_V \left(\log_2 |\mathbb{G}^{(d)}| - \log_2 d_V\right).$$

Strong secrecy

For any $\theta > 0$, the flatness factor, $\epsilon_\Lambda(\theta)$, is defined as

$$\epsilon_\Lambda(\theta) = \frac{\max_{\mathbf{x}\in\mathcal{V}(\Lambda)} \left| \left(\sum_{\lambda\in\Lambda} g_{\theta,\lambda}(\mathbf{x})\right) - 1/\mathrm{vol}(\Lambda)\right|}{1/\mathrm{vol}(\Lambda)}. \tag{3}$$

If $\mathbf{z}$ is a $\mathcal{N}(\mathbf{0}, \theta^2\mathbf{I}_d)$ random vector, then $\epsilon_\Lambda(\theta)$ is a measure of how far the distribution of $[\mathbf{z}] \bmod \Lambda$ is from the uniform distribution over $\mathcal{V}(\Lambda)$.

Strong secrecy

For any $\theta > 0$, the flatness factor, $\epsilon_\Lambda(\theta)$, is defined as

$$\epsilon_\Lambda(\theta) = \frac{\max_{\mathbf{x}\in\mathcal{V}(\Lambda)} \left| \left(\sum_{\lambda\in\Lambda} g_{\theta,\lambda}(\mathbf{x})\right) - 1/\mathrm{vol}(\Lambda) \right|}{1/\mathrm{vol}(\Lambda)}. \tag{3}$$

If $\mathbf{z}$ is a $\mathcal{N}(\mathbf{0}, \theta^2 \mathbf{I}_d)$ random vector, then $\epsilon_\Lambda(\theta)$ is a measure of how far the distribution of $[\mathbf{z}] \bmod \Lambda$ is from the uniform distribution over $\mathcal{V}(\Lambda)$.

Theorem

If the sequence of nested lattice pairs, $(\Lambda^{(d)}, \Lambda_0^{(d)})$ is such that the flatness factor, $\epsilon_{\Lambda_0^{(d)}}\left(\sqrt{\mathcal{P}/2}\right)$ is less than $1/2$, then the average variational distance,

$$d_V \;\leq\; 216\, \epsilon_{\Lambda_0^{(d)}}\left(\sqrt{\mathcal{P}/2}\right). \tag{4}$$

Achievable rate

Secrecy good lattices: $\Lambda^{(d)}$ is secrecy good if the flatness factor, $\epsilon_{\Lambda^{(d)}}(\theta)$ decays exponentially in d for all θ that satisfies

$$\frac{(\mathrm{vol}(\Lambda^{(d)}))^{2/d}}{2\pi\theta^2} < 1. \tag{5}$$

[1] Erez et al. (2004, 2005), Ling et al. (2012)

Achievable rate

Secrecy good lattices: $\Lambda^{(d)}$ is secrecy good if the flatness factor, $\epsilon_{\Lambda^{(d)}}(\theta)$ decays exponentially in d for all θ that satisfies

$$\frac{(\mathrm{vol}(\Lambda^{(d)}))^{2/d}}{2\pi\theta^2} < 1. \tag{5}$$

We choose a sequence of nested lattices that satisfy the following "goodness" properties:

- The sequence of coarse lattices, $\Lambda_0^{(d)}$ is good for covering, MSE quantization, AWGN channel coding, and secrecy good.
- The sequence of fine lattices, $\Lambda^{(d)}$ is good for AWGN channel coding and secrecy good.

Nested lattice pairs that satisfy the above properties indeed exist.[1]

[1] Erez et al. (2004, 2005), Ling et al. (2012)

Achievable rate

- To have $\epsilon_{\Lambda_0^{(d)}}(\sqrt{\mathcal{P}/2}) \to 0$ exponentially, we need (5).

$$\frac{\left(\mathrm{vol}(\Lambda_0^{(d)})\right)^{2/d}}{2\pi(\mathcal{P}/2)} < 1.$$

  Scale the nested lattice pair so that $\left(\mathrm{vol}(\Lambda_0^{(d)})\right)^{2/d} = \pi\mathcal{P} - \delta$.
- For the average transmit power to converge to $\mathcal{P}$, we require $\epsilon_{\Lambda^{(d)}}(\sqrt{\mathcal{P}}/2) \to 0$ as $d \to \infty$, which imposes the following constraint:

$$\frac{1}{d}\log_2 |\mathbb{G}^{(d)}| > \frac{1}{2} - \frac{1}{2}\log_2\left(1 - \frac{\delta}{\pi\mathcal{P}}\right).$$

- To have the average probability of error decay to zero as $d \to \infty$, we need[2]

$$\frac{\left(\mathrm{vol}(\Lambda^{(d)})\right)^{2/d}}{2\pi e\sigma^2} > 1.$$

[2] Erez, Zamir (2004)

Achievable rate

Theorem

For any $\mathcal{P} \geq 4e\sigma^2$, a power-rate pair of

$$\left(\mathcal{P}, \frac{1}{2}\log_2\frac{\mathcal{P}}{\sigma^2} - \frac{1}{2}\log_2 2e\right)$$

can be achieved with strong secrecy.

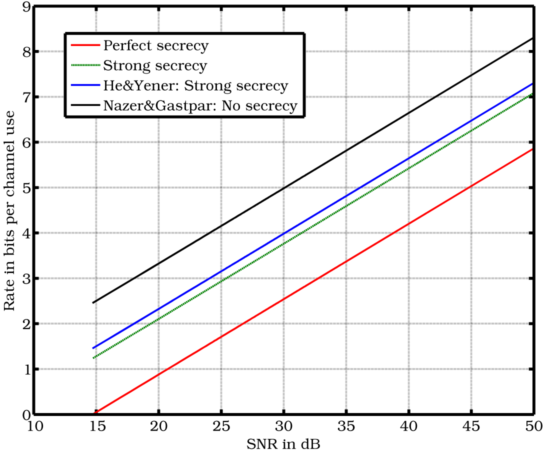
Using dithering techniques and MMSE equalization[3] at the relay, a power-rate pair of

$$\left(\mathcal{P}, \frac{1}{2}\log_2\left(\frac{1}{2} + \frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{2}\log_2 2e\right)$$

can be achieved with strong secrecy.

[3] Erez & Zamir (2004), Nazer & Gastpar(2011)

A comparison of achievable rates



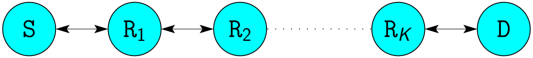
He and Yener (strong secrecy)

$$\mathcal{R} = \frac{1}{2}\log_2\left(\frac{1}{2} + \frac{\mathcal{P}}{\sigma^2}\right) - 1.$$

Kashyap et al. (perfect secrecy)

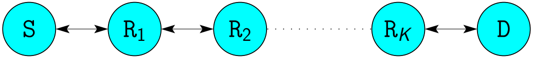
$$\mathcal{R} = \frac{1}{2}\log_2\frac{\mathcal{P}}{\sigma^2} - \log_2 2e.$$

Multi-hop line network with $K + 1$ hops



- All links are identical wireless AWGN links with unit gain.
- Source node $\mathtt{S}$ wants to send M independent messages (chosen uniformly at random) to destination.

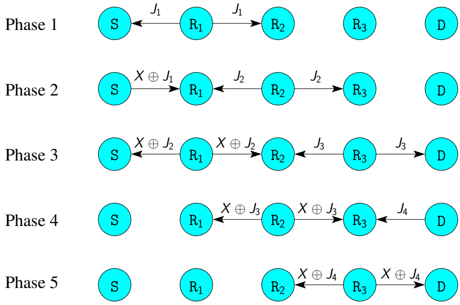
Multi-hop line network with $K + 1$ hops



- All links are identical wireless AWGN links with unit gain.
- Source node $\mathtt{S}$ wants to send M independent messages (chosen uniformly at random) to destination.
- Relay nodes are independent passive eavesdroppers.
- Want strong secrecy at relay nodes.

Multi-hop line network with $K+1$ hops

- He and Yener (Allerton '08) proposed a weakly secure scheme using cooperative jamming.
- Each relay node independently generates a jamming signal J_i $(i = 0, 1, \ldots, K)$. Destination generates M jamming signals.



Multi-hop network

Any strongly secure scheme for the bidirectional relay can be used with the cooperative jamming protocol of He and Yener to achieve strong secrecy.[4]

[4] *"Secure compute-and-forward in a bidirectional relay,"* submitted to IEEE Trans. Inf. Theory, online: http://ece.iisc.ernet.in/∼shashank/publications.html

Multi-hop network

Any strongly secure scheme for the bidirectional relay can be used with the cooperative jamming protocol of He and Yener to achieve strong secrecy.[4]

Theorem

For $\mathcal{P} \geq 4e\sigma^2$, a power-rate pair of

$$\left(\mathcal{P}, \frac{1}{4}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right) - \frac{1}{4}\log_2 2e\right)$$

is achievable with strong secrecy in a multi-hop network.

[4] *"Secure compute-and-forward in a bidirectional relay,"* submitted to IEEE Trans. Inf. Theory, online: http://ece.iisc.ernet.in/~shashank/publications.html

Conclusions

- Nested lattice based coding scheme satisfying an average power constraint that achieves strong secrecy over the bidirectional relay.
- Basic idea: Given the ith message (coset), transmit random point from Λ_i according to a pmf obtained by sampling Gaussian distributions.
- Possible that pmfs obtained by sampling different distributions may give interesting secrecy properties.
- Extension to the multi-hop line network.