Secure Compute-and-Forward Using Nested Lattice Codes

Navin Kashyap

Department of Electrical Communication Engineering
Indian Institute of Science

February 17, 2014

Joint work with Shashank V. and Andrew Thangaraj

Network Coding:

- Multiple sources and destinations connected via intermediate relay nodes
- Source messages belong to $\mathbb{F}^k$ for some finite field $\mathbb{F}$
- Relay nodes compute and forward some function (e.g., a linear combination over $\mathbb{F}$) of their incoming messages

Wireless Networks:

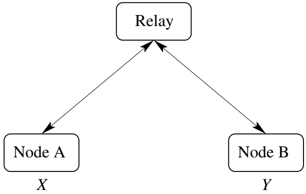
- All links between nodes are wireless with additive white Gaussian noise (AWGN)
- $\mathbb{R}$- or $\mathbb{C}$-valued signals broadcast to all neighbouring nodes
- Superposition of signals received simultaneously at receiver:

$$\mathbf{y} = \sum_{i=1}^{t} h_i \mathbf{x}_i + \text{ noise},$$

h_i being the fading coefficient of the link from ith transmitter to receiver; h_is are known to receiver

Bidirectional Relay

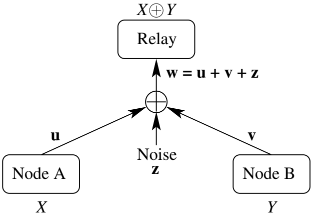
A useful primitive in physical-layer network coding:



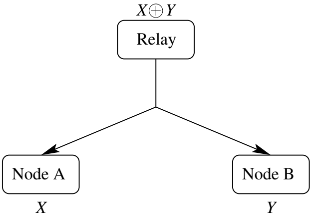
- Nodes A and B have messages X and Y, respectively, which they want to exchange.
- There is no direct link between the two nodes; they can only communicate through an intermediate relay node.
- The messages belong to some finite set $\mathbb{G}$; to facilitate message exchange, $\mathbb{G}$ is equipped with a suitable addition operation $\oplus$ that makes it a finite Abelian group.

Compute-and-Forward

(a) MAC phase:



(b) Broadcast phase:

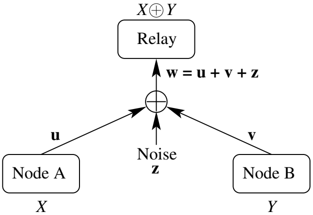


- $\mathbf{u}, \mathbf{v}$ are vectors (codewords) in $\mathbb{R}^d$
- $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \sigma^2 I)$
- Equal channel gains:

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

  ($+$ denotes addition over $\mathbb{R}$)

(a) MAC phase:

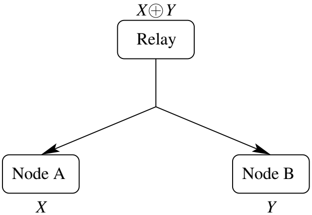


- $\mathbf{u}, \mathbf{v}$ are vectors (codewords) in $\mathbb{R}^d$
- $\mathbf{z} \sim \mathcal{N}(\mathbf{0}, \sigma^2 I)$
- Equal channel gains:

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

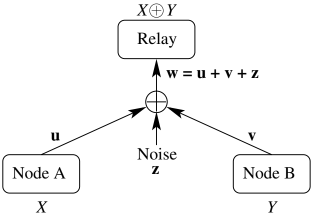
(+ denotes addition over $\mathbb{R}$)

(b) Broadcast phase:



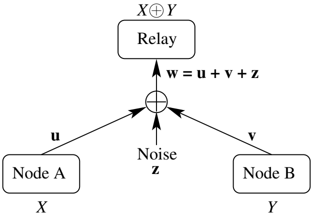
The broadcast phase is not relevant to our work.

Reliable Computation of $X \oplus Y$ at the Relay



- Rate: $R = \frac{1}{d} \log_2 |\mathbb{G}|$
- Power Constraint: $\frac{1}{d}\|\mathbf{u}\|^2 \leq \mathcal{P}$ and $\frac{1}{d}\|\mathbf{v}\|^2 \leq \mathcal{P}$

Reliable Computation of $X \oplus Y$ at the Relay



- Rate: $R = \frac{1}{d} \log_2 |\mathbb{G}|$
- Power Constraint: $\frac{1}{d}\|\mathbf{u}\|^2 \leq \mathcal{P}$ and $\frac{1}{d}\|\mathbf{v}\|^2 \leq \mathcal{P}$

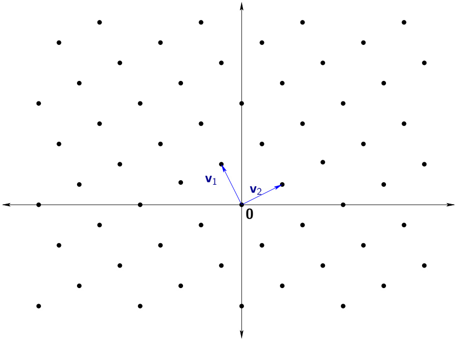
Reliable computation of $X \oplus Y$ at the relay is possible (for suitably defined $\oplus$) at any rate R up to

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

[Narayanan et al. (2007), Nazer & Gastpar (2007)]

Lattices

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



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

Define $Q_\Lambda(\mathbf{x}) := \arg\min_{\lambda \in \Lambda} \|\mathbf{x} - \boldsymbol{\lambda}\|$.

The fundamental Voronoi region of Λ is defined as

$$\mathcal{V}(\Lambda) := \{\mathbf{y} \in \mathbb{R}^d : Q_\Lambda(\mathbf{y}) = \mathbf{0}\}$$

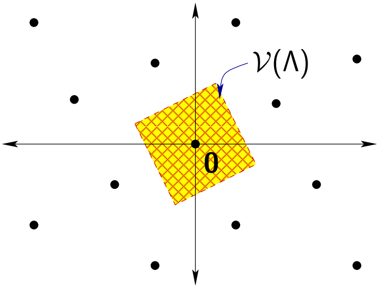


Figure: Fundamental Voronoi region of Λ.

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.

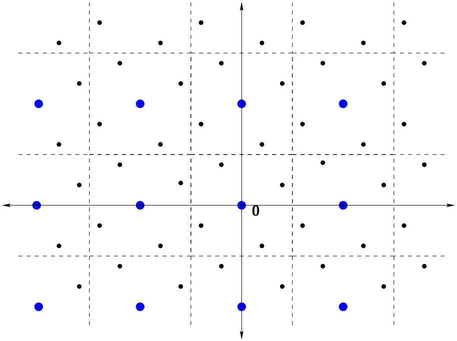
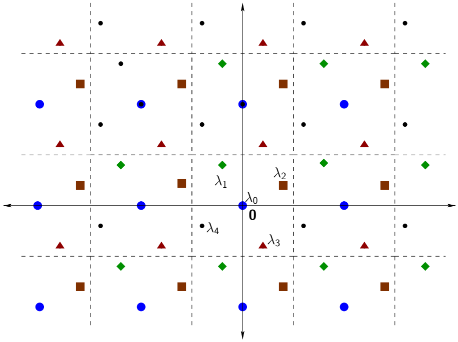


Figure: The blue dots indicate the coarse lattice Λ_0.

Cosets and Coset Representatives

The cosets of Λ_0 in Λ form a finite Abelian group $\mathbb{G} = \Lambda/\Lambda_0$.



● : Λ_0 ◆ : Λ_1 ■ : Λ_2

▲ : Λ_3 • : Λ_4

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

Nested Lattice Codes

Choose a pair of nested lattices $\Lambda_0 \subset \Lambda$ in $\mathbb{R}^d$.

- Messages: The message set $\mathbb{G}$ is identified with Λ/Λ_0. Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$ be the elements of Λ/Λ_0.
- Codebook: $\mathcal{C} = \Lambda \cap \mathcal{V}(\Lambda_0) = \{\boldsymbol{\lambda}_0, \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{N-1}\}$.

Nested Lattice Codes

Choose a pair of nested lattices $\Lambda_0 \subset \Lambda$ in $\mathbb{R}^d$.

- Messages: The message set $\mathbb{G}$ is identified with Λ/Λ_0. Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$ be the elements of Λ/Λ_0.
- Codebook: $\mathcal{C} = \Lambda \cap \mathcal{V}(\Lambda_0) = \{\boldsymbol{\lambda}_0, \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{N-1}\}$.
- Encoding: Given message Λ_j, encoder transmits the coset representative $\boldsymbol{\lambda}_j$.

  Thus, the coset reps must satisfy the power constraint:

$$\frac{1}{d}\|\boldsymbol{\lambda}_j\|^2 \leq \mathcal{P} \quad \text{for all } j$$

Nested Lattice Codes

Choose a pair of nested lattices $\Lambda_0 \subset \Lambda$ in $\mathbb{R}^d$.

- Messages: The message set $\mathbb{G}$ is identified with Λ/Λ_0. Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$ be the elements of Λ/Λ_0.
- Codebook: $\mathcal{C} = \Lambda \cap \mathcal{V}(\Lambda_0) = \{\boldsymbol{\lambda}_0, \boldsymbol{\lambda}_1, \ldots, \boldsymbol{\lambda}_{N-1}\}$.
- Encoding: Given message Λ_j, encoder transmits the coset representative $\boldsymbol{\lambda}_j$.

  Thus, the coset reps must satisfy the power constraint:

$$\frac{1}{d}\|\boldsymbol{\lambda}_j\|^2 \leq \mathcal{P} \quad \text{for all } j$$

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

  This is called nearest lattice point decoding.

Achievable Rates

- The rate of the nested lattice code is $R = \frac{1}{d}\log_2|\Lambda/\Lambda_0|$.
- By choosing a "good" sequence of nested lattice pairs $(\Lambda_0^{(d)}, \Lambda^{(d)})$, with $d \to \infty$, reliable computation of $X \oplus Y$ at the relay is possible at any rate R up to

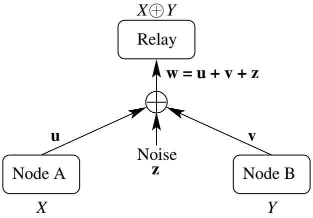
$$\frac{1}{2}\log_2\left(\frac{\mathcal{P}}{\sigma^2}\right).$$

- The techniques of "uniform dithering" and "MMSE equalization" at the decoder are used to achieve rates up to

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

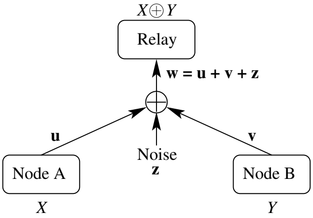
[Narayanan et al. (2007), Nazer & Gastpar (2007)]

Reliable and Secure Computation of $X \oplus Y$



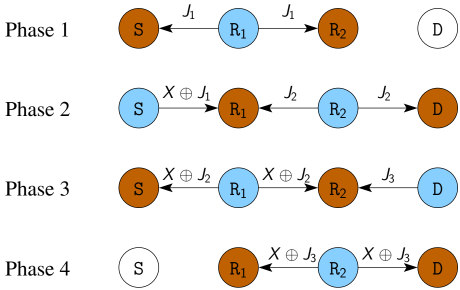
- X, Y uniformly distributed over some finite Abelian group $\mathbb{G}$
- $\mathbf{u}, \mathbf{v}$ are vectors (codewords) in $\mathbb{R}^d$
- $\mathbf{z} \in \mathcal{N}(0, \sigma^2 I)$
- Relay receives $\mathbf{w} = \mathbf{u} + \mathbf{v} + \mathbf{z}$ and must compute $X \oplus Y$.

Reliable and Secure Computation of $X \oplus Y$

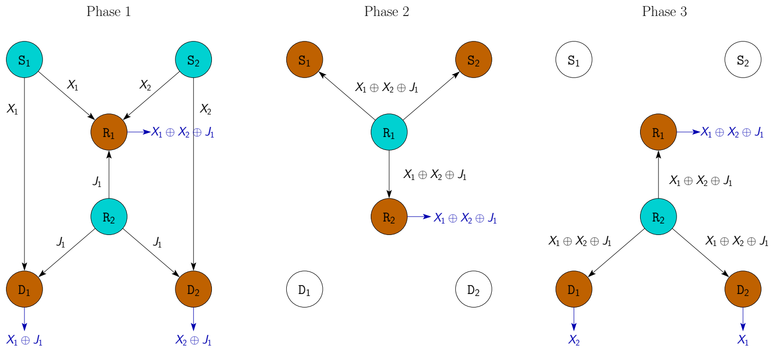


- X, Y uniformly distributed over some finite Abelian group $\mathbb{G}$
- $\mathbf{u}, \mathbf{v}$ are vectors (codewords) in $\mathbb{R}^d$
- $\mathbf{z} \in \mathcal{N}(0, \sigma^2 I)$
- Relay receives $\mathbf{w} = \mathbf{u} + \mathbf{v} + \mathbf{z}$ and must compute $X \oplus Y$.
- Security Constraint:
  - Perfect Secrecy: $\mathbf{w} \perp\!\!\!\perp X$ and $\mathbf{w} \perp\!\!\!\perp Y$
  - Strong Secrecy: $\mathcal{I}(\mathbf{w}; X) \to 0$ and $\mathcal{I}(\mathbf{w}; Y) \to 0$ as $d \to \infty$.
  - Weak Secrecy: $\frac{1}{d}\mathcal{I}(\mathbf{w}; X) \to 0$ and $\frac{1}{d}\mathcal{I}(\mathbf{w}; Y) \to 0$ as $d \to \infty$.

Multi-hop line network using cooperative jamming:
[He and Yener (2008)]



Butterfly network:



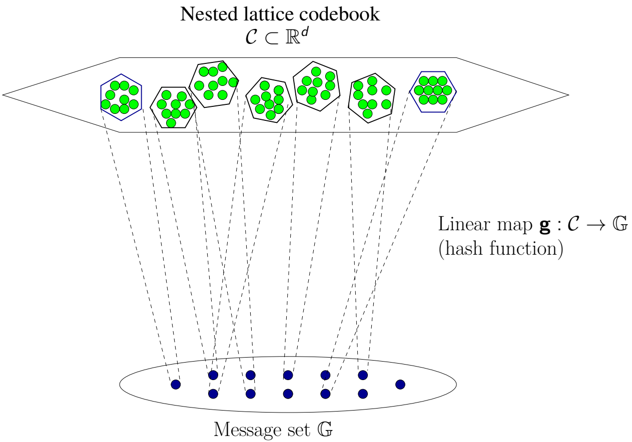
- Weak secrecy using random binning:
  He and Yener, Allerton, 2008.
- Strong secrecy using universal hash functions:
  He and Yener, IEEE Trans. Inf. Theory, Jan 2013.

Reliable and (strongly) secure computation of $X \oplus Y$ at the relay is possible, using nested lattice codes, at any rate R up to

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

[He and Yener (2013)]

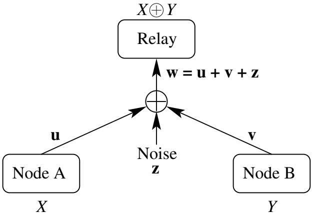
He-Yener Coding Scheme



Randomized Encoding: Given message $a \in \mathbb{G}$, a codeword is picked uniformly at random from $\mathbf{g}^{-1}(a)$ and transmitted.

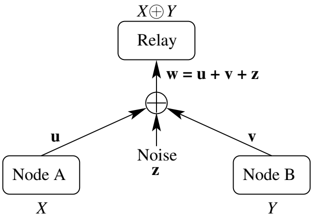
- Each $\mathbf{g}^{-1}(a)$ contains $\sim 2^d$ codewords

Randomized Encoders



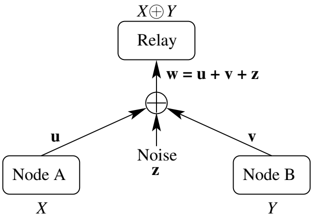
- Messages X, Y i.i.d. $\sim \text{Unif}(\mathbb{G})$
- Codebook $\mathcal{C} \subset \mathbb{R}^d$ is, in general, much larger than $\mathbb{G}$
- At Node A, given $X = a$, the transmitted codeword $\mathbf{u} \in \mathcal{C}$ is picked according to some prob. distribution $\Pr[\,\cdot\,|X = a]$; similarly at Node B

Randomized Encoders



- Messages X, Y i.i.d. $\sim \text{Unif}(\mathbb{G})$
- Codebook $\mathcal{C} \subset \mathbb{R}^d$ is, in general, much larger than $\mathbb{G}$
- At Node A, given $X = a$, the transmitted codeword $\mathbf{u} \in \mathcal{C}$ is picked according to some prob. distribution $\Pr[\,\cdot\,|X = a]$; similarly at Node B
- Rate: $R = \frac{1}{d}\log_2|\mathbb{G}|$
- Power Constraint: $\frac{1}{d}\|\mathbf{u}\|^2 \le \mathcal{P}$ and $\frac{1}{d}\|\mathbf{v}\|^2 \le \mathcal{P}$

Randomized Encoders



- Messages X, Y i.i.d. $\sim$ Unif($\mathbb{G}$)
- Codebook $\mathcal{C} \subset \mathbb{R}^d$ is, in general, much larger than $\mathbb{G}$
- At Node A, given $X = a$, the transmitted codeword $\mathbf{u} \in \mathcal{C}$ is picked according to some prob. distribution $\Pr[\,\cdot\,|X = a]$; similarly at Node B
- Rate: $R = \frac{1}{d}\log_2 |\mathbb{G}|$
- Average Power Constraint: $\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 \leq \mathcal{P}$ and $\frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2 \leq \mathcal{P}$

Our Main Result

Theorem (Shashank, K. and Thangaraj (2013))

(a) *Reliable and perfectly secure computation of $X \oplus Y$ at the relay is possible at any rate R up to*

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

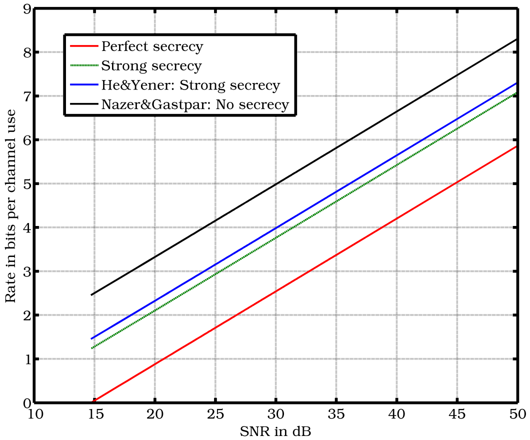
under an average power constraint.

(b) *If perfect secrecy above is relaxed to strong secrecy, then any rate R up to*

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

is achievable under an average power constraint.

A Comparison of Achievable Rates



Nazer and Gastpar: $\frac{1}{2}\log_2\left(\frac{1}{2}+\frac{\mathcal{P}}{\sigma^2}\right)$

He and Yener: $\frac{1}{2}\log_2\left(\frac{1}{2}+\frac{\mathcal{P}}{\sigma^2}\right)-1$

Shashank-K.-Thangaraj:

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

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

Our Coding Scheme

Choose a "good" pair of nested lattices $\Lambda_0 \subset \Lambda$ in $\mathbb{R}^d$.

Choose a "good" probability density $f(\mathbf{x})$ defined on $\mathbb{R}^d$.

- Messages: The message set $\mathbb{G}$ is identified with Λ/Λ_0. Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$ be the elements of Λ/Λ_0.
- Codebook: $\mathcal{C} = \Lambda$
- Randomized Encoding: Given message Λ_j, encoder picks a codeword $\mathbf{u} \in \Lambda_j$ to be transmitted, according to a prob. distrib. p_j defined as follows:

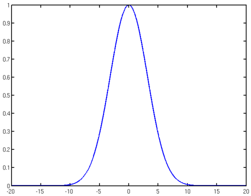
$$p_j(\mathbf{u}) = \begin{cases} \frac{1}{Z(\Lambda_j)} f(\mathbf{u}) & \text{if } \mathbf{u} \in \Lambda_j \\ 0 & \text{otherwise} \end{cases}$$

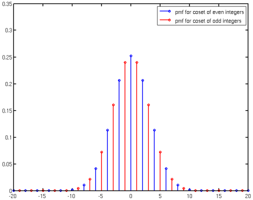
  where $Z(\Lambda_j) = \sum_{\mathbf{u} \in \Lambda_j} f(\mathbf{u})$.
- Decoding: Nearest lattice point decoding

Major Departures from Previous Coding Schemes

- Codebook $\mathcal{C}$ is countably infinite
- Prob. distributions used for randomization are obtained by sampling a pdf f at lattice points:

  e.g., $(\Lambda, \Lambda_0) = (\mathbb{Z}, 2\mathbb{Z})$ and a Gaussian density f





- pdf f chosen so that $\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 \leq \mathcal{P}$ and $\frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2 \leq \mathcal{P}$

Secrecy via Choice of f

The choice of pdf f determines the secrecy properties of our coding scheme!

Strong secrecy obtained by choosing f to be an $\mathcal{N}(\mathbf{0}, \mathcal{P}\, I_d)$ density:

$$f(\mathbf{x}) = \frac{1}{(2\pi\mathcal{P})^{d/2}} e^{-\frac{\|\mathbf{x}\|^2}{2\mathcal{P}}}$$

Secrecy via Choice of f

The choice of pdf f determines the secrecy properties of our coding scheme!

Strong secrecy obtained by choosing f to be an $\mathcal{N}(\mathbf{0}, \mathcal{P}\, I_d)$ density:

$$f(\mathbf{x}) = \frac{1}{(2\pi\mathcal{P})^{d/2}} e^{-\frac{\|\mathbf{x}\|^2}{2\mathcal{P}}}$$

Nested lattice codes with discrete Gaussian distributions were previously proposed for the Gaussian wiretap channel by Ling, Luzzi, Belfiore and Stehlé [ArXiv:1210.6673]

Secrecy via Choice of f

The choice of pdf f determines the secrecy properties of our coding scheme!

Strong secrecy obtained by choosing f to be an $\mathcal{N}(\mathbf{0}, \mathcal{P}\, I_d)$ density:

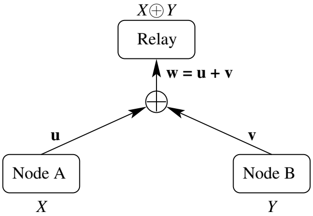
$$f(\mathbf{x}) = \frac{1}{(2\pi\mathcal{P})^{d/2}} e^{-\frac{\|\mathbf{x}\|^2}{2\mathcal{P}}}$$

Nested lattice codes with discrete Gaussian distributions were previously proposed for the Gaussian wiretap channel by Ling, Luzzi, Belfiore and Stehlé [ArXiv:1210.6673]

Finding an f that yields perfect secrecy is a more interesting story

...

Noiseless Setting



X, Y i.i.d. Bernoulli(1/2) rvs, $X \oplus Y$ is their modulo-2 sum

Want real-valued rvs U and V such that

(1) $(X, U) \perp\!\!\!\perp (Y, V)$

(2) $U + V$ determines $X \oplus Y$

(3) $U + V \perp\!\!\!\perp X$ and $U + V \perp\!\!\!\perp Y$

Use the nested lattice pair $(\Lambda, \Lambda_0) = (\mathbb{Z}, 2\mathbb{Z})$: $\mathbb{Z}/2\mathbb{Z} \cong \mathbb{Z}_2$.

Randomized Encoding

At Node A:

- If $X = 0$, transmit an even integer U picked according to

$$\Pr[U = k \mid X = 0] = p_0(k)$$

for a pmf p_0 supported within the even integers.

- If $X = 1$, transmit an odd integer U picked according to

$$\Pr[U = k \mid X = 1] = p_1(k)$$

for a pmf p_1 supported within the odd integers.

At Node B:

- If $Y = b$, for $b \in \{0, 1\}$, transmit V picked according to p_b.

Randomized Encoding

At Node A:

- If $X = 0$, transmit an even integer U picked according to

$$\Pr[U = k \mid X = 0] = p_0(k)$$

for a pmf p_0 supported within the even integers.

- If $X = 1$, transmit an odd integer U picked according to

$$\Pr[U = k \mid X = 1] = p_1(k)$$

for a pmf p_1 supported within the odd integers.

At Node B:

- If $Y = b$, for $b \in \{0, 1\}$, transmit V picked according to p_b.

$$\left.\begin{array}{l} p_{U|X=0} = p_{V|Y=0} = p_0 \\ p_{U|X=1} = p_{V|Y=1} = p_1 \end{array}\right\} \implies p_U = p_V = p \triangleq \frac{1}{2}(p_0 + p_1)$$

How to Ensure (3) $U + V \perp\!\!\!\perp X$ and $U + V \perp\!\!\!\perp Y$?

To satisfy

(3) $U + V \perp\!\!\!\perp X$ and $U + V \perp\!\!\!\perp Y$

we need

$$\Pr[U + V = k \mid X = a] = \Pr[U + V = k]$$

for all $k \in \mathbb{Z}$ and $a \in \{0, 1\}$.

In other words, $p_{U|X=a} * p_V = p_U * p_V$ for $a \in \{0, 1\}$, i.e.,

$$p_0 * p = p_1 * p = p * p.$$

(Recall: $p_U = p_V = p \triangleq \frac{1}{2}(p_0 + p_1)$)

Properties Required of p_0 and p_1

To summarize, we need pmfs p_0 and p_1 such that

p_0 is supported within the even integers,
p_1 is supported within the odd integers

and

$$p_0 * p = p_1 * p = p * p,$$

where $p = \frac{1}{2}(p_0 + p_1)$.

Properties Required of p_0 and p_1

To summarize, we need pmfs p_0 and p_1 such that

p_0 is supported within the even integers,
p_1 is supported within the odd integers

and

$$p_0 * p = p_1 * p = p * p,$$

where $p = \frac{1}{2}(p_0 + p_1)$.

Let $\varphi_*(t) = \sum_{k\in\mathbb{Z}} p_*(k)e^{ikt}$ be the characteristic function of p_*.

We need characteristic functions that satisfy

$$\varphi_0 \cdot \varphi = \varphi_1 \cdot \varphi = \varphi^2,$$

with $\varphi = \frac{1}{2}(\varphi_0 + \varphi_1)$.

Support of p_0 and p_1

It can be shown that

- finitely-supported p_0 and p_1 cannot have the required properties;
- in fact, light-tailed pmfs p_0 and p_1 cannot have the required properties. [M. Krishnapur]

The Main Tool

Proposition

Let f be a pdf on $\mathbb{R}$ whose char. function ψ is supported within $(-\pi/2, \pi/2)$, i.e., $\psi(t) = 0$ for $|t| \geq \pi/2$. For any $s \in \mathbb{R}$, define

$$\Psi(t) = \sum_{n=-\infty}^{\infty} (-1)^{sn} \psi(t + n\pi).$$

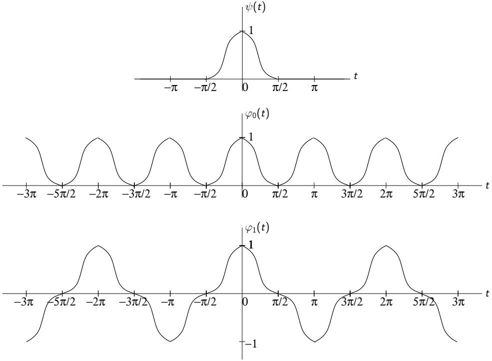
Then,

(a) *$\Psi(t)$ is the char. function of a pmf p_s supported within the set $2\mathbb{Z} + s = \{2k + s : k \in \mathbb{Z}\}$, and*

(b) *for all $u \in 2\mathbb{Z} + s$, we have $p_s(u) = 2f(u)$.*

The proof is based upon the Poisson summation formula of Fourier analysis.

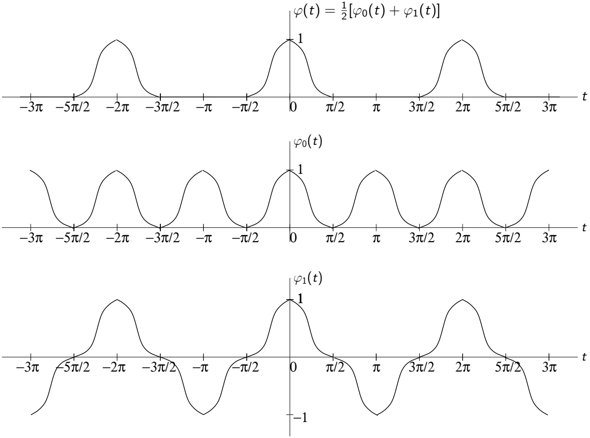
The Basic Construction



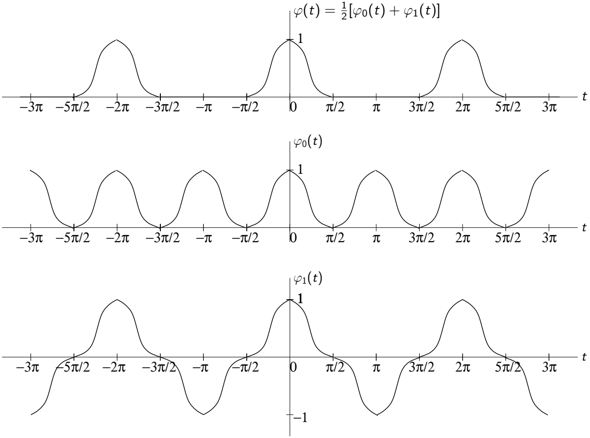
$$\psi \quad \xrightarrow{\mathcal{F}^{-1}} \quad f(x) = \frac{1}{2\pi} \int \psi(t) e^{-ixt}\, dt$$

$$\varphi_0 \quad \xrightarrow{\mathcal{F}^{-1}} \quad p_0(k) = 2f(k) \text{ for all even } k \in \mathbb{Z} \text{ (and 0 otherwise)}$$

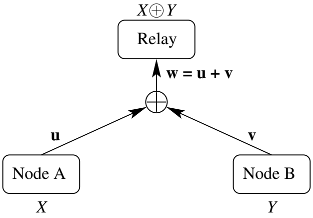
$$\varphi_1 \quad \xrightarrow{\mathcal{F}^{-1}} \quad p_1(k) = 2f(k) \text{ for all odd } k \in \mathbb{Z} \text{ (and 0 otherwise)}$$


φ(t) = ½[φ0(t) + φ1(t)]
1
t
−3π −5π/2 −2π −3π/2 −π −π/2 0 π/2 π 3π/2 2π 5π/2 3π
φ0(t)
1
t
−3π −5π/2 −2π −3π/2 −π −π/2 0 π/2 π 3π/2 2π 5π/2 3π
φ1(t)
1
t
−3π −5π/2 −2π −3π/2 −π −π/2 0 π/2 π 3π/2 2π 5π/2 3π
−1

The Basic Construction



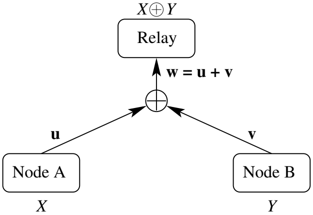
$$\varphi^2 = \varphi\varphi_0 = \varphi\varphi_1$$



X, Y i.i.d. Bernoulli(1/2) rvs

1. Start with a pdf f having char. func. ψ supported within $(-\pi/2, \pi/2)$.
2. Let $p_0(k) = 2\,f(k)$ for even $k \in \mathbb{Z}$, and 0 otherwise.
   Let $p_1(k) = 2\,f(k)$ for odd $k \in \mathbb{Z}$, and 0 otherwise.
3. If $X = 0$ (resp. $Y = 0$),
   choose U (resp. V) according to the pmf p_0.
   If $X = 1$ (resp. $Y = 1$),
   choose U (resp. V) according to the pmf p_1.

Coding Scheme for Noiseless Setting



Fact

The resulting $\mathbb{Z}$-valued rvs U and V have finite second moment iff ψ is twice-differentiable. In this case,

$$\mathbb{E}[U^2] = \mathbb{E}[V^2] = -\psi''(0)$$

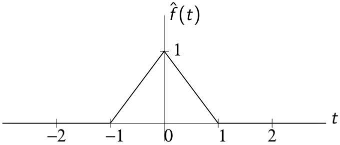
Thus, U and V can satisfy an average power constraint.

Compactly Supported Characteristic Functions

Example: The probability density function

$$f(x) = \begin{cases} \frac{1}{2\pi} & \text{if } x = 0 \\ \frac{1-\cos x}{\pi x^2} & \text{if } x \neq 0 \end{cases}$$

has char. function $\hat{f}(t) = \max\{0, 1 - |t|\}$, shown below:

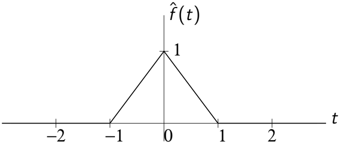


Compactly Supported Characteristic Functions

Example: The probability density function

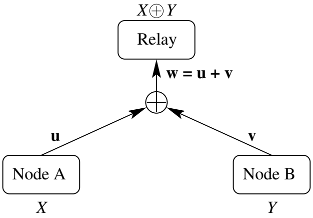
$$f(x) = \begin{cases} \frac{1}{2\pi} & \text{if } x = 0 \\ \frac{1-\cos x}{\pi x^2} & \text{if } x \neq 0 \end{cases}$$

has char. function $\hat{f}(t) = \max\{0, 1 - |t|\}$, shown below:



The function $\hat{f}$ above is not twice-differentiable. Instead, consider $\psi(t) = \frac{3}{2}(\hat{f} * \hat{f})(t)$, which is supported within $(-2, 2)$.

- ψ is the char. function of a pdf
- ψ is twice-differentiable, with $\psi''(0) = -3$.

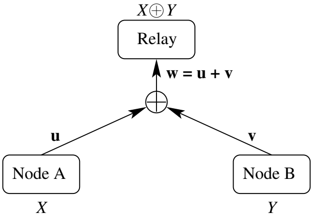


X, Y i.i.d. rvs unif. distrib. over an Abelian group $(\mathbb{G}, \oplus)$ of size N.

1. Select a nested lattice pair $\Lambda_0 \subseteq \Lambda$ in $\mathbb{R}^d$ such that $\mathbb{G} \cong \Lambda/\Lambda_0$. Let $\Lambda_0, \Lambda_1, \ldots, \Lambda_{N-1}$ be the cosets of Λ_0 in Λ.
2. Select a pdf $f : \mathbb{R}^d \to \mathbb{R}_+$ with char. func. ψ supported within a ball of radius $2\pi\rho(\Lambda_0^*)$ around the origin, where $\rho(\Lambda_0^*)$ is the packing radius of the dual of Λ_0.
3. For $j = 0, 1, \ldots, N-1$, define

$$p_j(\mathbf{k}) = \text{vol}(\mathcal{V}(\Lambda_0))\, f(\mathbf{k}) \text{ for } \mathbf{k} \in \Lambda_j; \text{ and 0 otherwise}$$

Secure Computation over $\mathbb{G}$



4. If $X = \Lambda_j$ (resp. $Y = \Lambda_j$),
choose $\mathbf{u} \in \Lambda_j$ (resp. $\mathbf{v} \in \Lambda_j$) according to the pmf p_j.

Fact

The resulting Λ-valued rvs $\mathbf{u}$ and $\mathbf{v}$ have finite second moment iff ψ is twice-differentiable. In this case,

$$\mathbb{E}\|\mathbf{u}\|^2 = \mathbb{E}\|\mathbf{v}\|^2 = -\Delta\psi(\mathbf{0}),$$

where $\Delta = \sum_{j=1}^{d} \partial_j^2$ denotes the Laplacian operator.

The EGR Theorem

Let j_k denote the first positive zero of the Bessel function J_k.

Theorem (Ehm, Gneiting and Richards (2004))

If $\psi : \mathbb{R}^d \to \mathbb{C}$ is a characteristic function supported within a ball of radius ρ around the origin, then

$$-\Delta\psi(\mathbf{0}) \geq \frac{4}{\rho^2} j^2_{\frac{d-2}{2}} \tag{1}$$

with equality iff $\psi(\mathbf{t})$ equals a certain $\psi^*(\mathbf{t})$.

The EGR Theorem

Let j_k denote the first positive zero of the Bessel function J_k.

Theorem (Ehm, Gneiting and Richards (2004))

If $\psi : \mathbb{R}^d \to \mathbb{C}$ is a characteristic function supported within a ball of radius ρ around the origin, then

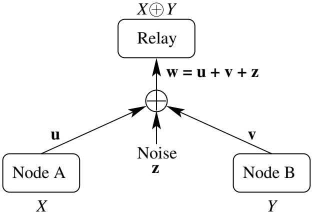
$$-\Delta\psi(\mathbf{0}) \geq \frac{4}{\rho^2}\, j^2_{\frac{d-2}{2}} \tag{1}$$

with equality iff $\psi(\mathbf{t})$ equals a certain $\psi^*(\mathbf{t})$.

Therefore, the *tightest* average power constraint that the Λ-valued rvs $\mathbf{u}$ and $\mathbf{v}$ can satisfy is

$$\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 = \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2 \leq \mathcal{P}(\Lambda_0) := \frac{1}{d\,\pi^2\,\rho(\Lambda_0^*)^2}\, j^2_{\frac{d-2}{2}}$$

Coding Scheme for Noisy Setting



X, Y i.i.d. rvs unif. distrib. over an Abelian group $(\mathbb{G}, \oplus)$ of size N.

Encoding:

As described for secure computation in the noiseless setting

Decoding:

1. Find the closest lattice point $\boldsymbol{\lambda} \in \Lambda$ to the received vector $\mathbf{w}$.
2. Decode to the coset Λ_j to which $\boldsymbol{\lambda}$ belongs.

Performance of Coding Scheme

Perfect Secrecy: As noise $\mathbf{z}$ is independent of everything else, we still have

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

Performance of Coding Scheme

Perfect Secrecy: As noise $\mathbf{z}$ is independent of everything else, we still have

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

Reliability: There exist "good" nested lattice pairs $\Lambda_0 \subseteq \Lambda$ in $\mathbb{R}^d$ for which the resulting coding schemes

- have rate

$$R \approx \frac{1}{2} \log_2 \left(\frac{\overline{\rho}(\Lambda_0)^2}{d\sigma^2} \right),$$

  where $\overline{\rho}(\Lambda_0)$ is the covering radius of Λ_0; and
- compute $X \oplus Y$ within $\mathbb{G} = \Lambda/\Lambda_0$ arbitrarily reliably

Performance of Coding Scheme

Perfect Secrecy: As noise $\mathbf{z}$ is independent of everything else, we still have

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

Reliability: There exist "good" nested lattice pairs $\Lambda_0 \subseteq \Lambda$ in $\mathbb{R}^d$ for which the resulting coding schemes

- have rate

$$R \approx \frac{1}{2} \log_2 \left(\frac{\overline{\rho}(\Lambda_0)^2}{d\sigma^2} \right),$$

  where $\overline{\rho}(\Lambda_0)$ is the covering radius of Λ_0; and
- compute $X \oplus Y$ within $\mathbb{G} = \Lambda/\Lambda_0$ arbitrarily reliably

Average Power Constraint:

$$\frac{1}{d}\mathbb{E}\|\mathbf{u}\|^2 = \frac{1}{d}\mathbb{E}\|\mathbf{v}\|^2 \leq \mathcal{P}(\Lambda_0) := \frac{1}{d\,\pi^2\,\rho(\Lambda_0^*)^2}\, j^2_{\frac{d-2}{2}}$$

Achievable Rate for Coding Scheme

For sufficiently large d, the coarse lattice Λ_0 in $\mathbb{R}^d$ can be chosen so that

- $\overline{\rho}(\Lambda_0) \approx \frac{1}{2e}\sqrt{d\mathcal{P}}$ and $\rho(\Lambda_0^*) \approx \frac{d}{4\pi e}\frac{1}{\overline{\rho}(\Lambda_0)}$

Also,

- $j_{\frac{d-2}{2}} = \frac{d}{2}\left[1 + o(1)\right]$

Theorem (Shashank-K.-Thangaraj (2013))

Reliable and perfectly secure computation of $X \oplus Y$ at the relay is possible (for suitably defined $\oplus$) at any rate R up to

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

under an average power constraint $\mathcal{P}$.

Achievable Rate for Coding Scheme

For sufficiently large d, the coarse lattice Λ_0 in $\mathbb{R}^d$ can be chosen so that

- $\overline{\rho}(\Lambda_0) \approx \frac{1}{2e}\sqrt{d\mathcal{P}}$ and $\rho(\Lambda_0^*) \approx \frac{d}{4\pi e}\frac{1}{\overline{\rho}(\Lambda_0)}$

Also,

- $j_{\frac{d-2}{2}} = \frac{d}{2}\,[1 + o(1)]$

Theorem (Shashank-K.-Thangaraj (2013))

Reliable and perfectly secure computation of $X \oplus Y$ at the relay is possible (for suitably defined $\oplus$) at any rate R up to

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

under an average power constraint $\mathcal{P}$.

Open question: Is this the best one can do?

What Next?

- Higher achievable rates? This question is restricted to coding schemes in which randomization is via pmfs obtained by sampling pdfs at lattice points.
- Converse bounds. No upper bound better than $\frac{1}{2}\log_2\left(1+\frac{\mathcal{P}}{\sigma^2}\right)$ is known for achievable rates for reliable computation at the relay *even without secrecy*.
- Low-complexity decoding. Nearest lattice point decoding is computationally hard.