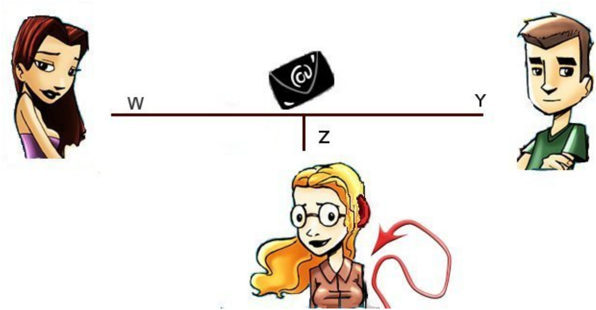
An Error Probability Approach to Wiretap Code Design

Frédérique Oggier
(joint work with Jean-Claude Belfiore)
frederique@ntu.edu.sg

Nanyang Technological University

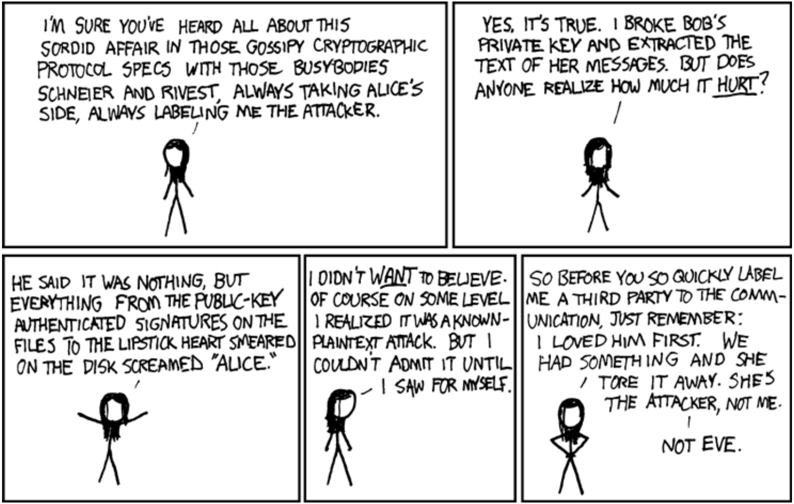
Algebraic Structure in Network Information Theory, Banff, August 2011

The usual Alice and Bob story ...



...from a coding point of view.

The unusal Alice and Bob story (by xkcd)



System Model

- Gaussian wiretap channel:

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e \end{aligned}$$

System Model

- Gaussian wiretap channel:

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e \end{aligned}$$

- Fast fading wiretap channel:

$$\begin{aligned} \mathbf{y} &= \mathrm{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathrm{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e \end{aligned}$$

System Model

- Gaussian wiretap channel:

$$\begin{aligned} \mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e \end{aligned}$$

- Fast fading wiretap channel:

$$\begin{aligned} \mathbf{y} &= \mathrm{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathrm{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e \end{aligned}$$

- MIMO wiretap channel:

$$\begin{aligned} Y &= H_b X + V_b \\ Z &= H_e X + V_e. \end{aligned}$$

System Model

- Gaussian wiretap channel:

$$\begin{aligned}\mathbf{y} &= \mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathbf{x} + \mathbf{v}_e\end{aligned}$$

- Fast fading wiretap channel:

$$\begin{aligned}\mathbf{y} &= \mathrm{diag}(\mathbf{h}_b)\mathbf{x} + \mathbf{v}_b \\ \mathbf{z} &= \mathrm{diag}(\mathbf{h}_e)\mathbf{x} + \mathbf{v}_e\end{aligned}$$

- MIMO wiretap channel:

$$\begin{aligned}Y &= H_b X + V_b \\ Z &= H_e X + V_e.\end{aligned}$$

- Amount of information that Eve gets should be minimized.

Lattice Coding

- Alice uses lattice coding.

Lattice Coding

- Alice uses lattice coding.
- $\mathbf{x} \in \Lambda \subset \mathbb{C}^n$, with

$$\Lambda = \{\mathbf{x} = M\mathbf{u} \mid \mathbf{u} \in \mathbb{Z}[i]^n\}.$$

Lattice Coding

- Alice uses lattice coding.
- $\mathbf{x} \in \Lambda \subset \mathbb{C}^n$, with

$$\Lambda = \{\mathbf{x} = M\mathbf{u} \mid \mathbf{u} \in \mathbb{Z}[i]^n\}.$$

- For MIMO, we mean

$$\mathbf{x} = \mathrm{vec}(X) = M\mathbf{u}$$

(holds for example for linear dispersion codes).

Coset Encoding

- Partition

$$\Lambda_b = \cup_{j=1}^{2^k} (\Lambda_e + \mathbf{c}_j)$$

with $\Lambda_e \subset \Lambda_b$, $\mathbf{c}$ not in Λ_e and 2^k cosets to be labelled by $\mathbf{s} \in \{0, 1\}^k$.

Coset Encoding

- Partition

$$\Lambda_b = \cup_{j=1}^{2^k} (\Lambda_e + \mathbf{c}_j)$$

  with $\Lambda_e \subset \Lambda_b$, $\mathbf{c}$ not in Λ_e and 2^k cosets to be labelled by $\mathbf{s} \in \{0,1\}^k$.

- Once

$$\mathbf{s} \mapsto \Lambda_e + \mathbf{c}_{j(\mathbf{s})},$$

  Alice randomly chooses $\mathbf{x} \in \Lambda_e + \mathbf{c}_{j(\mathbf{s})}$, or equivalently

$$\mathbf{x} = \mathbf{r} + \mathbf{c} \in \Lambda_e + \mathbf{c}.$$

Coset Decoding

- $\mathbf{x}_k$ in $\mathbb{C}^n$ with Voronoi cell $\mathcal{V}(\mathbf{x}_k)$, over a Gaussian channel with noise variance σ^2, probability of correct decision

$$\frac{1}{(\sigma^2 2\pi)^n} \int_{\mathcal{V}(\mathbf{x}_k)} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u}.$$

Coset Decoding

- $\mathbf{x}_k$ in $\mathbb{C}^n$ with Voronoi cell $\mathcal{V}(\mathbf{x}_k)$, over a Gaussian channel with noise variance σ^2, probability of correct decision

$$\frac{1}{(\sigma^2 2\pi)^n} \int_{\mathcal{V}(\mathbf{x}_k)} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u}.$$

- $\mathbf{x}_k = \mathbf{r}_k + \mathbf{c}_k \in \Lambda_b$ sent, the probability P_c of finding the correct coset is (no boundary effect)

$$P_c = \frac{1}{(\sigma^2 2\pi)^n} \sum_{\mathbf{r} \in \Lambda_e} \int_{\mathcal{V}(\mathbf{x}_k)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u}.$$

Eve's probability of correct decision: the Gaussian case

- Low SNR assumption for Eve, a Taylor expansion at order 0 gives

$$\int_{\mathcal{V}(\Lambda_b)+\mathbf{r}} e^{-||\mathbf{u}||^2/2\sigma^2} d\mathbf{u} = \int_{\mathcal{V}(\Lambda_b)} e^{-||\mathbf{w}+\mathbf{r}||^2/2\sigma^2} d\mathbf{w}$$

$$\simeq \mathrm{vol}(\mathcal{V}(\Lambda_b)) e^{-||\mathbf{r}||^2/2\sigma^2}.$$

- The probability of making a correct decision for Eve is then

$$P_{c,e} \simeq \frac{1}{(2\pi\sigma_e^2)^n} \mathrm{vol}(\mathcal{V}(\Lambda_b)) \sum_{\mathbf{r}\in\Lambda_e} e^{-\|\mathbf{r}\|^2/2\sigma_e^2}.$$

Design Criteria

- Gaussian channel: maximize the secrecy function

$$\boxed{\frac{\Theta_{\nu\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)},}$$

where $\Theta_\Lambda(y) = \sum_{\mathbf{x}\in\Lambda} q^{||\mathbf{x}||^2}$.

Design Criteria

- Gaussian channel: maximize the secrecy function

$$\boxed{\frac{\Theta_{\nu\mathbb{Z}^n}(y)}{\Theta_\Lambda(y)},}$$

  where $\Theta_\Lambda(y) = \sum_{\mathbf{x}\in\Lambda} q^{||\mathbf{x}||^2}$.
- For extremal unimodular lattices, the maximum is reached at $y = 1$ (shown for extremal even unimodular lattices by A.-M. Ernvall-Hytönen) thanks to an explicit formula for the theta series of unimodular lattices.

Some more results

- Asymptotic formula for the secrecy gain for even unimodular lattices.

Some more results

- Asymptotic formula for the secrecy gain for even unimodular lattices.
- Examples of code constructions using Construction A, so far only in small dimensions.

Some more results

- Asymptotic formula for the secrecy gain for even unimodular lattices.
- Examples of code constructions using Construction A, so far only in small dimensions.
- Fairly open for non-unimodular lattices.

Eve's probability of correct decision: the fast fading case

- We can rewrite the fast fading channel, given $\mathbf{h}_b$, $\mathbf{h}_e$:

$$\begin{aligned} \mathbf{y} &= [\mathrm{diag}(\mathbf{h}_b) M_b]\mathbf{u} + \mathbf{v}_b \\ \mathbf{z} &= [\mathrm{diag}(\mathbf{h}_e) M_b]\mathbf{u} + \mathbf{v}_e. \end{aligned}$$

Eve's probability of correct decision: the fast fading case

- We can rewrite the fast fading channel, given $\mathbf{h}_b$, $\mathbf{h}_e$:

$$\begin{aligned} \mathbf{y} &= [\mathrm{diag}(\mathbf{h}_b) M_b]\mathbf{u} + \mathbf{v}_b \\ \mathbf{z} &= [\mathrm{diag}(\mathbf{h}_e) M_b]\mathbf{u} + \mathbf{v}_e. \end{aligned}$$

- Thus

$$P_{c,e,\mathbf{h}_e} = \left(\frac{1}{2\pi\sigma_e^2}\right)^n \mathrm{Vol}(\Lambda_b) \sum_{\mathbf{x}\in\Lambda_e} \prod_{i=1}^{n} \left(|h_{e,i}| \, e^{-\frac{\left|h_{e,i} x_i\right|^2}{2\sigma_e^2}} \right).$$

Eve's probability of correct decision: the fast fading case

- We can rewrite the fast fading channel, given $\mathbf{h}_b$, $\mathbf{h}_e$:

$$\begin{aligned}\mathbf{y} &= [\mathrm{diag}(\mathbf{h}_b)M_b]\mathbf{u} + \mathbf{v}_b \\ \mathbf{z} &= [\mathrm{diag}(\mathbf{h}_e)M_b]\mathbf{u} + \mathbf{v}_e.\end{aligned}$$

- Thus

$$P_{c,e,\mathbf{h}_e} = \left(\frac{1}{2\pi\sigma_e^2}\right)^n \mathrm{Vol}(\Lambda_b) \sum_{\mathbf{x}\in\Lambda_e} \prod_{i=1}^{n} \left(|h_{e,i}|\, e^{-\frac{\left|h_{e,i}x_i\right|^2}{2\sigma_e^2}} \right).$$

- On average

$$\bar{P}_{c,e} \simeq \left(\frac{\sigma_{h,e}^2}{\pi\sigma_e^2}\right)^n \mathrm{Vol}(\Lambda_b) \sum_{\mathbf{x}\in\Lambda_e} \prod_{i=1}^{n} \frac{1}{\left(1 + |x_i|^2 \frac{\sigma_{h,e}^2}{\sigma_e^2}\right)^2}.$$

Design Criteria

Design Criteria

- Fast fading channel:

$$\boxed{\min_{\Lambda_e} \sum_{\mathbf{x}\in\Lambda_e\backslash 0} \frac{1}{\left(\prod_{i=1}^{n} |x_i|^2\right)^2}}.$$

Design Criteria

- Fast fading channel:

$$\boxed{\min_{\Lambda_e} \sum_{\mathbf{x}\in\Lambda_e\setminus 0} \frac{1}{\left(\prod_{i=1}^{n} |x_i|^2\right)^2}}.$$

- In the case of an algebraic lattice, this is not without recalling Dedekind zeta functions.

Eve's probability of correct decision: the MIMO case

- We can rewrite the MIMO fading channel, given H_b, H_e:

$$\begin{aligned}\mathrm{vec}(Y) &= [\mathrm{diag}(H_b,\ldots,H_b)M_b]\mathbf{u} + \mathrm{vec}(V_b)\\ \mathrm{vec}(Z) &= [\mathrm{diag}(H_e,\ldots,H_e)M_b]\mathbf{u} + \mathrm{vec}(V_e)\end{aligned}$$

- Thus

$$P_{c,e,H_e} \simeq \frac{\mathrm{vol}(\Lambda_b)}{(2\pi\sigma_e^2)^{n_t T}} \det(H_e H_e^*)^T \sum_{\mathbf{x}\in\Lambda_e} e^{-\|H_e X\|_F^2/2\sigma_e^2}$$

- On average

$$\bar{P}_{c,e} \simeq \frac{\mathrm{vol}(\Lambda_b)\pi^{n_e n_t}\Gamma_{n_t}(n_e+T)}{\Gamma_{n_t}(n_e)(2\pi\sigma_e^2)^{n_t T}(2\pi\sigma_{H_e}^2)^{n_e n_t}} \sum_{\mathbf{x}\in\Lambda_e} \det\left(\frac{1}{2\sigma_{H_e}^2}\mathbf{I}_{n_t} + \frac{1}{2\sigma_e^2}XX^*\right)$$

Design Criteria

Design Criteria

- MIMO channel:

$$\boxed{\min_{\Lambda_e} \sum_{\mathbf{x}\in\Lambda_e\setminus 0} \frac{1}{\det(XX^*)^{n_e+T}}}.$$

The Alamouti Code

- Alamouti codewords:

$$X = \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix}, \ x_1, x_2 \in \mathbb{Z}[i],$$

The Alamouti Code

- Alamouti codewords:

$$X = \begin{bmatrix} x_1 & x_2 \\ -x_2^* & x_1^* \end{bmatrix}, \; x_1, x_2 \in \mathbb{Z}[i],$$

- We need to study

$$\sum_{\mathbf{x} \in \Lambda_e \setminus \{\mathbf{0}\}} \det \left(XX^* \right)^{-n_e - T} = \sum_{\mathbf{x} \in \Lambda_e \setminus \{\mathbf{0}\}} \frac{1}{\|\mathbf{x}\|^{2(2(n_e+T))}} = \zeta_{\Lambda_e} \left(2 \left(n_e + 2 \right) \right)$$

where we recognize the Epstein zeta function of a scaled lattice $\mu\Lambda$ ($\mu > 0$), defined by

$$\zeta_{\mu\Lambda}(s) = \sum_{\mathbf{x} \in \Lambda \setminus \{\mathbf{0}\}} \frac{1}{\mu^{2s}} \frac{1}{\|\mathbf{x}\|^{2s}} = \frac{1}{\mu^{2s}} \zeta_{\Lambda}(s).$$

The Alamouti Code

Since $\mathbf{x} \in \mathbb{Z}[i]^2 \simeq \mathbb{Z}^4$, we have

- $\Lambda_e = \mathbb{Z}^4$ itself, with Epstein zeta function

$$\zeta_{\mathbb{Z}^4}(s) = 8\left(1 - 4^{1-s}\right)\zeta(s)\zeta(s-1),$$

The Alamouti Code

Since $\mathbf{x} \in \mathbb{Z}[i]^2 \simeq \mathbb{Z}^4$, we have

- $\Lambda_e = \mathbb{Z}^4$ itself, with Epstein zeta function

$$\zeta_{\mathbb{Z}^4}(s) = 8\left(1 - 4^{1-s}\right)\zeta(s)\zeta(s-1),$$

- $\Lambda_e = D_4$, with Epstein zeta function

$$\zeta_{D_4}(s) = 3 \cdot 4^{2-s}\left(2^{s-1} - 1\right)\zeta(s)\zeta(s-1),$$

where $\zeta(s) = \sum_{n>0} \frac{1}{n^s}$ is the Riemann zeta function.

Conclusion

- Approach wiretap channels from a coding point of view.

Conclusion

- Approach wiretap channels from a coding point of view.
- Analysis of lattice codes in terms of probability of error.

Conclusion

- Approach wiretap channels from a coding point of view.
- Analysis of lattice codes in terms of probability of error.
- Works for Gaussian channels, fast and block fading channels, as well as MIMO channels.

Conclusion

- Approach wiretap channels from a coding point of view.
- Analysis of lattice codes in terms of probability of error.
- Works for Gaussian channels, fast and block fading channels, as well as MIMO channels.
- Lots of unexpected exciting connections with theta series, modular forms, and different types of zeta functions!

Thanks