Towards to Anonymity in Physical-Layer Network Coding

Oksana Trushina

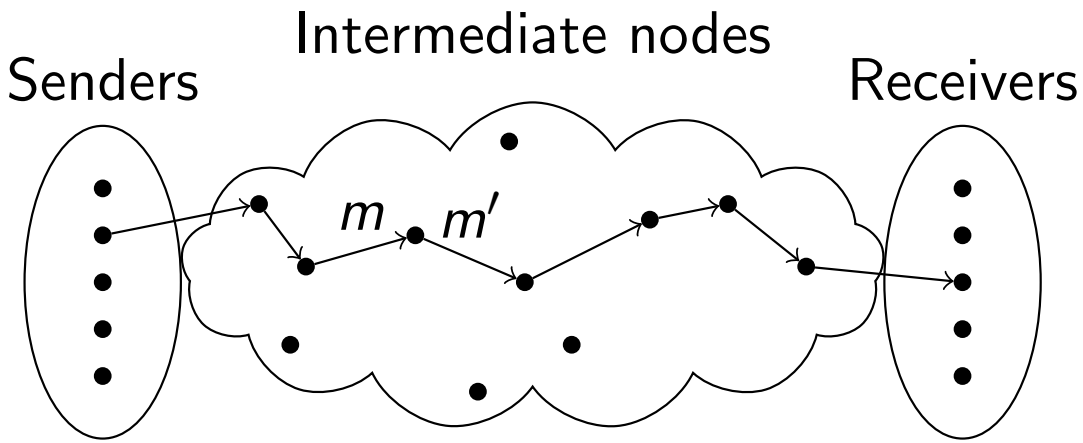
Moscow Institute of Physics and Technology
(State University)

2014

Content

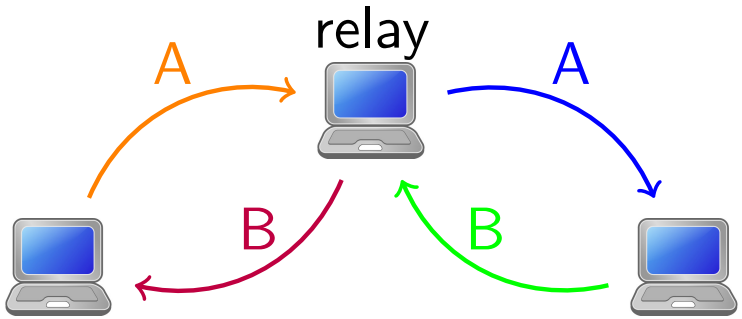
Anonymous Transmission

- is to guarantee a forwarding to be untraceable

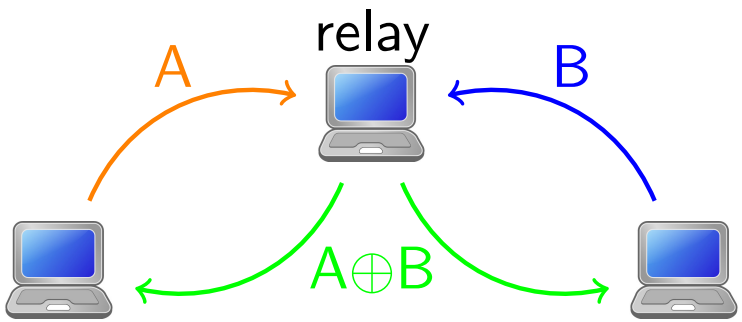


Adversary: Are m and m' the same?
Can I reveal the previous and next path nodes of m'?

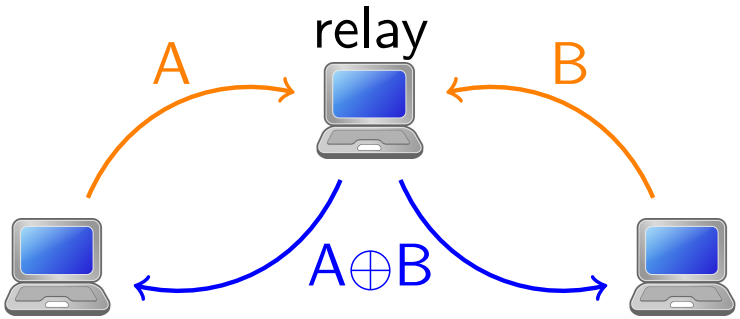
Traditional transmission



Network Coding



Physical-Layer Network Coding



Physical-Layer Network Coding

- is not only time slots saving

  but

- is a new approach to interference: using instead avoiding
- is easily scalable: each relay deals with some linear combination

  however

- has a problem: phase misalignment $\Rightarrow$ performance issue

  solution: compute-and-forward

Compute-and-forward

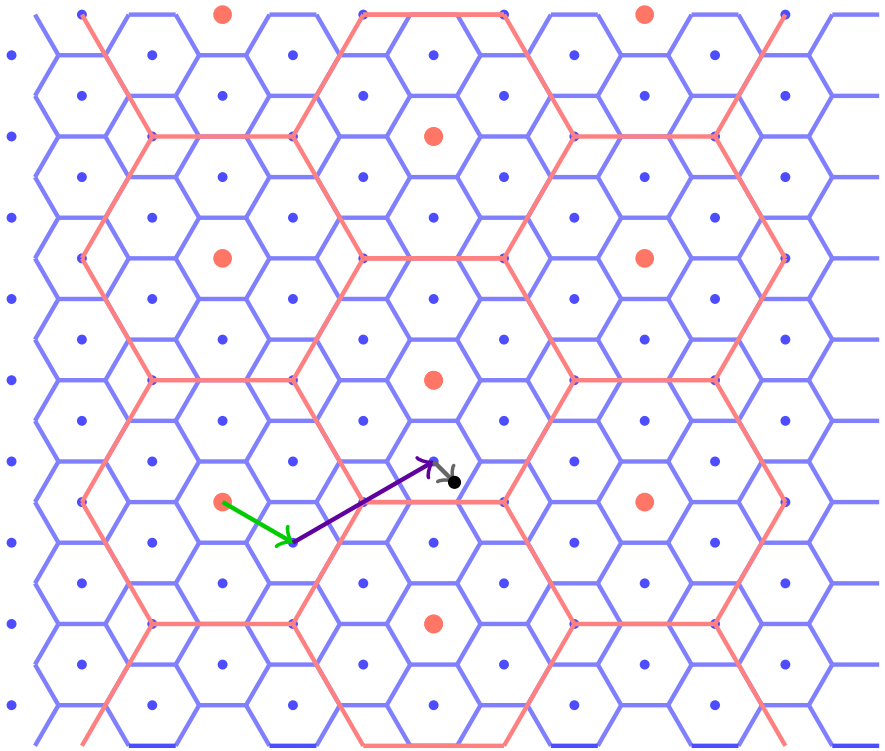
Key point:
Voronoi constellation

Underlying structure:
nested lattices $\Lambda_a \subset \Lambda_r$
messages are mapped to lattice points $m \in \mathbb{F}_q^n \to x \in \Lambda_r/\Lambda_a$

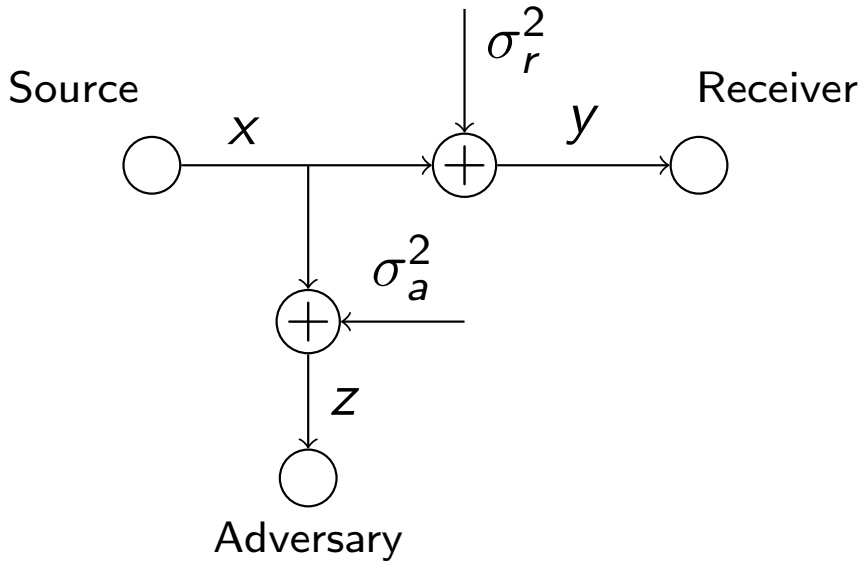
Key properties:

- integer linear combinations of lattice points are again lattice points
- linear combination of lattice points = linear combination of messages

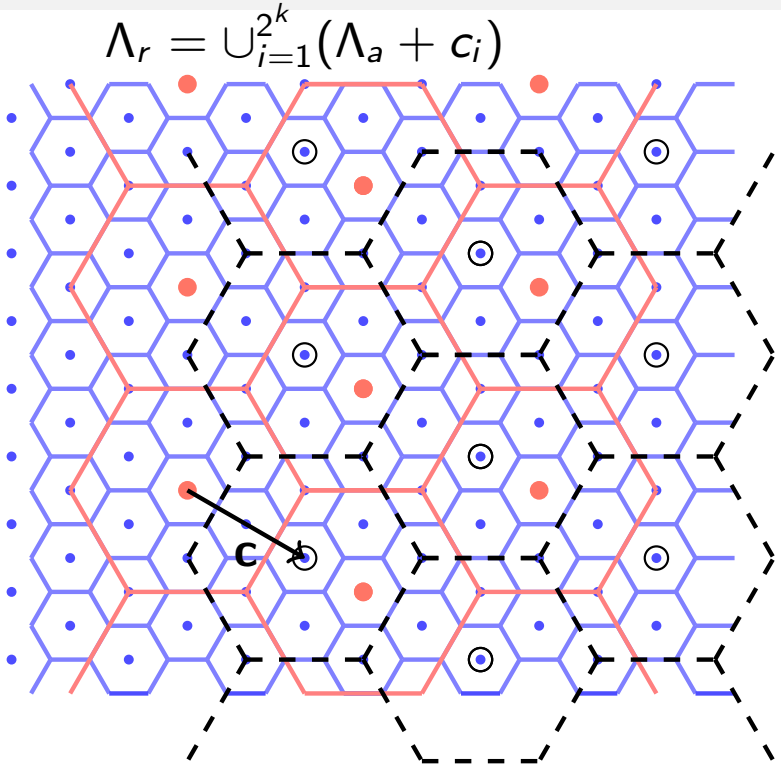
channel: $y = x_1 + 2x_2 + v$



Coset Coding



$y = x + v_r,\ v_r \sim N(0, \sigma_r^2)$
$z = x + v_a,\ v_a \sim N(0, \sigma_a^2)$

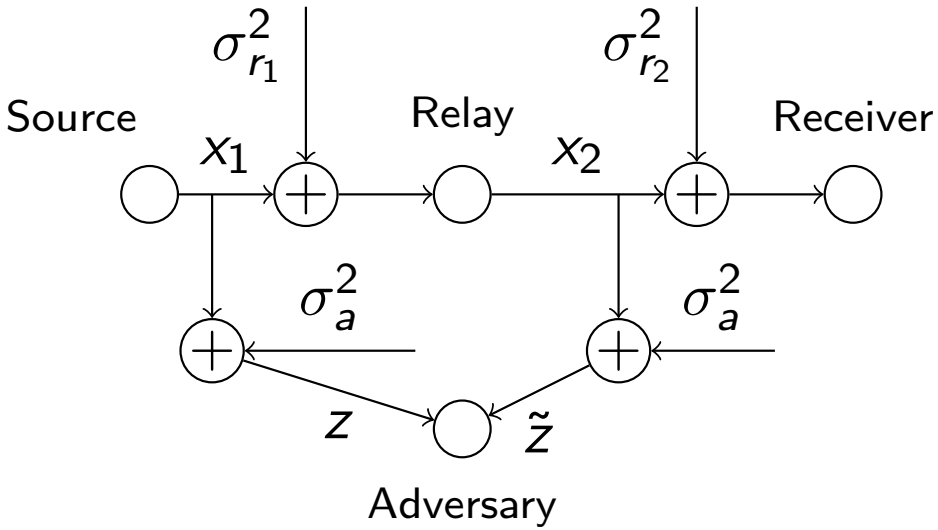


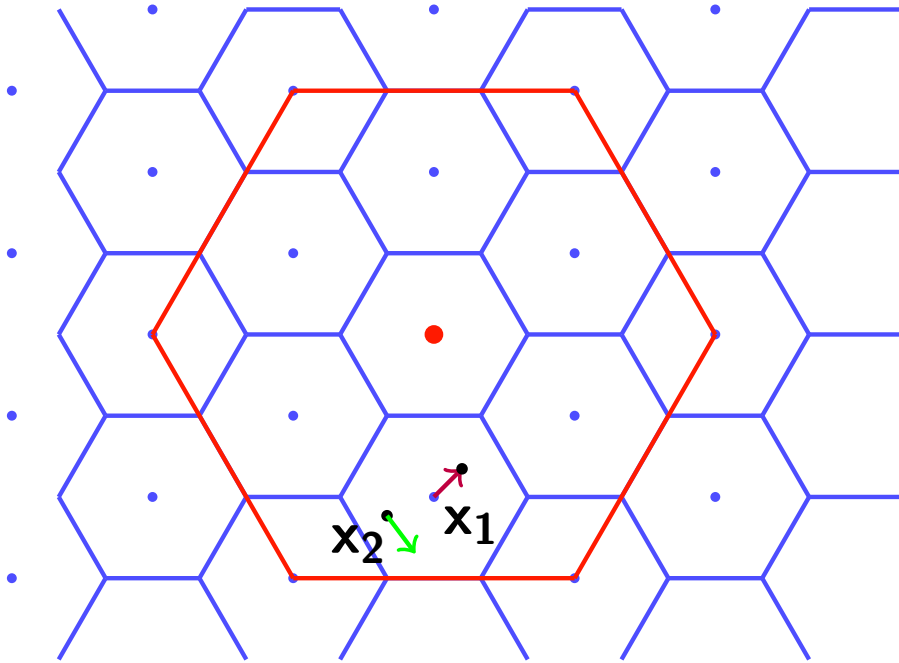
data $s \in \{0,1\}^k \rightarrow$ random $x \in (\Lambda_a + c)$

$\Updownarrow$

data $s \in \{0,1\}^k \rightarrow$ random $r \in \Lambda_a +$ "index" of defined coset c

Providing Anonymity. Basic Idea





Relay:

1. obtains $x_1 \in \Lambda_a + c$ on decoding received $y_r = x_1 + v_{r_1}$
2. is not allowed to change the coset $\rightarrow$ chooses uniformally at random $x_2 \in V_{\Lambda_r}(x_1)-$ Voronoi cell of x_1
3. sends x_2 forward

Provading Anonymity

Λ_r guarantees reliability: $P_{cor,r}$ is high
Λ_a guarantees security: $P_{cor,a}$ is low

Adversary:

$$\begin{cases} z = x_1 + v_{a_1}, \\ \tilde{z} = x_2 + v_{a_2}. \end{cases}$$

v_{a_1} and v_{a_2} are independent

To obtain x_1 and x_2 is unlikely

How to determine relation between z and $\tilde{z}$?

Conclusion

Physical-Layer Network Coding (PNC) reques nested structures

Coset coding (CC) reques nested structures

$\rightarrow$ natural joining of PNC and CC

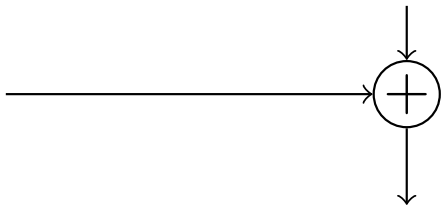
$\updownarrow$

almost free security agains eavesdropper

Lattices features

$\oplus$

Additional operation at relay



Anonymity

Q&A