

LDPC Codes for the Gaussian Wiretap Channel

Demijan Klinc* Jeongseok Ha[†] Steven W. McLaughlin*
Joao Barros[‡] Byung-Jae Kwak[◇]

*Georgia Institute of Technology †KAIST
‡Universidade do Porto ◇ETRI

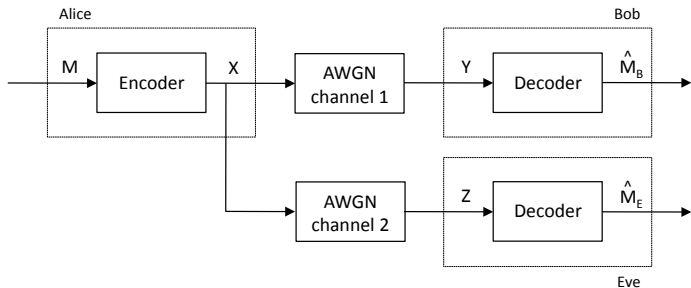
Information Theory Workshop, Taormina
October 12, 2009

- 1 Motivation and Problem Statement
- 2 Code Construction and Results
- 3 Efficient Encoding
- 4 Summary

Motivation

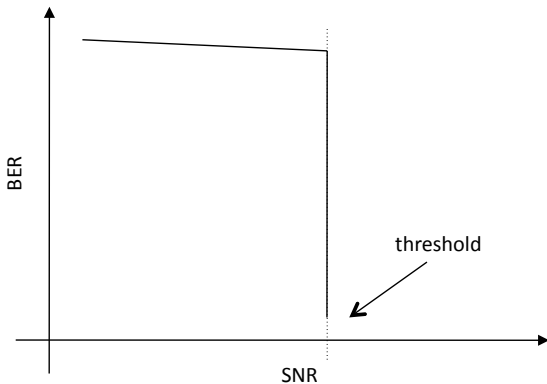
- data security is currently addressed at layers above the physical layer
- wireless systems do not take advantage of the stochastic nature of communication channels for security
- information theory: security can be addressed at the physical layer
- practical code constructions are elusive

Gaussian Wiretap Channel

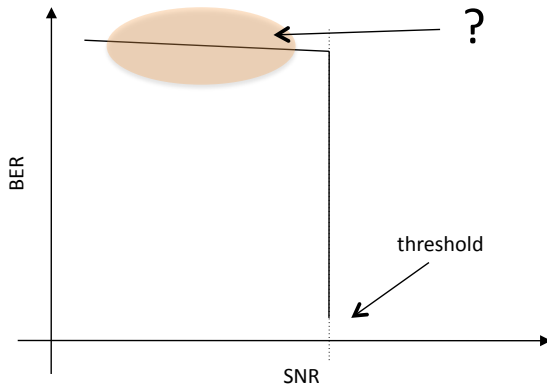


- Captures the relationship between a legitimate receiver and an eavesdropper
- Assumption: Eve is passive and her SNR is lower than Bob's

LDPC codes: Threshold behavior

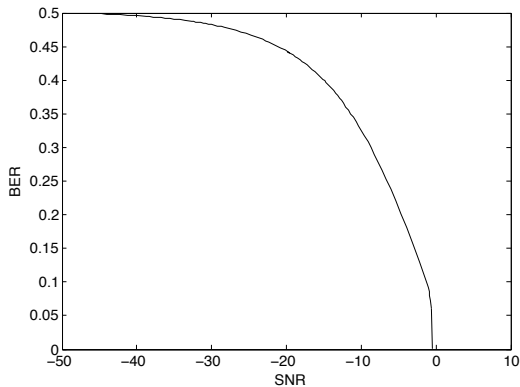


LDPC codes: Threshold behavior



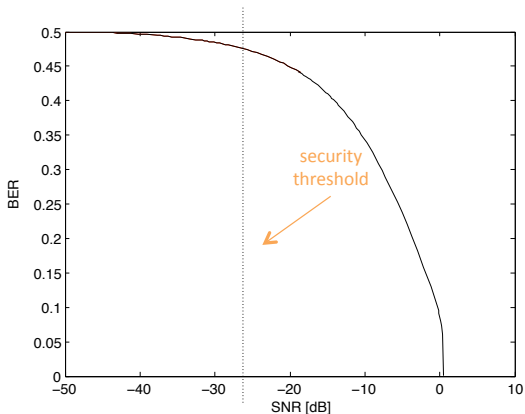
BER in the low SNR region, security threshold

LDPC code with $R = 2/3$, threshold SNR = -0.48 dB



BER in the low SNR region, security threshold

LDPC code with $R = 2/3$, threshold SNR = -0.48 dB



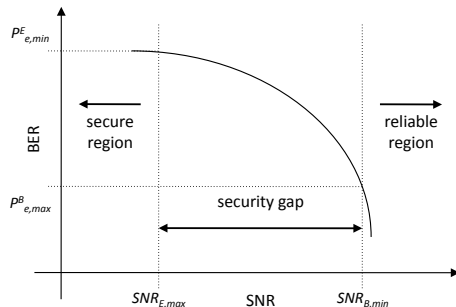
Code Design for Gaussian Wiretap Channel

- Let P_e^B be Bob's BER and let ϵ be a constant arbitrarily close to 0
- Let P_e^E be Eve's BER and let $P_{e,\min}^E$ be a constant close to 0.5

Constraints:

- $P_e^B \leq \epsilon$
- $P_e^E \geq P_{e,\min}^E$

Minimize the Security Gap

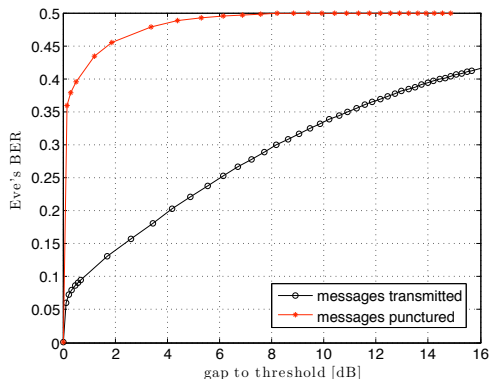


Secure LDPC codes

- main idea: transmit messages over punctured bits to hide data from the eavesdroppers
- the proposed method is evaluated asymptotically using density evolution
- bitwise-MAP decoding
- if p is the fraction of punctured bits, the code rate is:

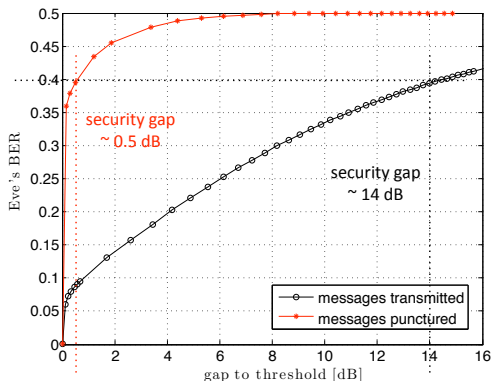
$$R = \frac{p}{1 - p}$$

Secure LDPC Codes



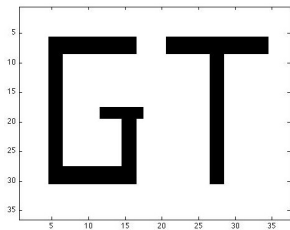
- black: $R = 2/3$
- red: mother code rate: 0.5, $p = 0.40$, $R = 0.4/0.6 = 2/3$
- if messages are punctured, Eve's SNR grows very fast to 0.5 as her SNR deteriorates
- if Eve's signal is only a few dB lower than Bob's she is forced to BERs close to 0.5, even if she has the capability to use a bitwise-MAP decoder

Secure LDPC Codes



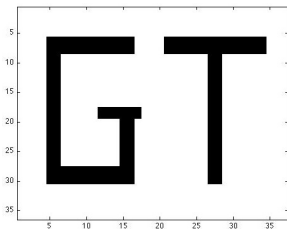
- black: $R = 2/3$
- red: mother code rate: 0.5, $\rho = 0.40$, $R = 0.4/0.6 = 2/3$
- if messages are punctured, Eve's SNR grows very fast to 0.5 as her SNR deteriorates
- if Eve's signal is only a few dB lower than Bob's she is forced to BERs close to 0.5, even if she has the capability to use a bitwise-MAP decoder

RFID experimental data

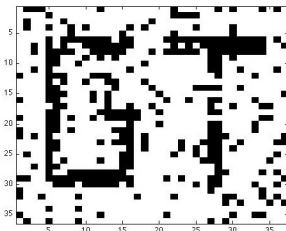


Original image

RFID experimental data



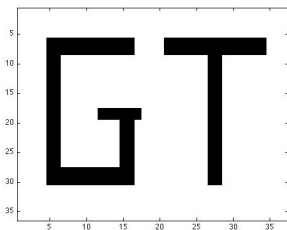
Original image



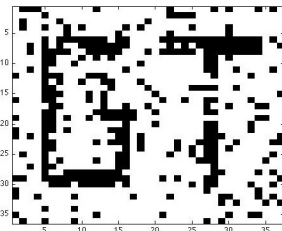
Messages transmitted

BER = 0.150

RFID experimental data

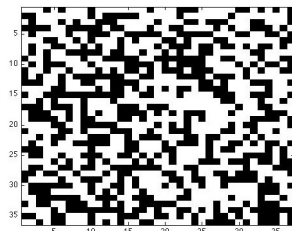


Original image



Messages transmitted

BER = 0.150



Messages punctured

BER = 0.460

Optimize Puncturing Distributions

- a puncturing distribution is captured by a polynomial

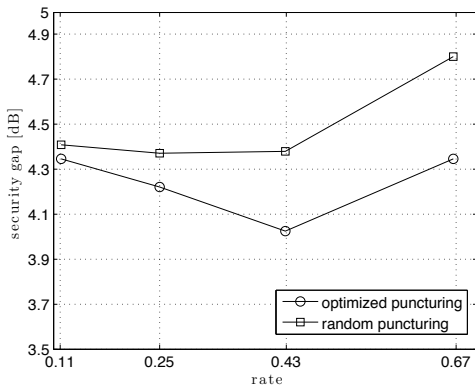
$$\pi(x) = \sum_{i=2}^{d_v} \pi_i x^{i-1}$$

- the security gap of an LDPC code can be optimized by choosing an appropriate puncturing distribution
- the optimization is generally non-linear and we used differential evolution to obtain optimized puncturing distributions with small security gaps, by solving

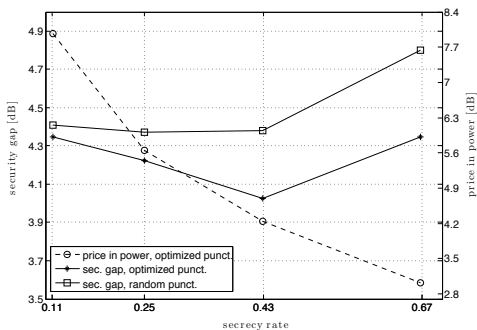
$$\arg \min_{\pi_i \text{'s}} (\text{security gap})$$

Performance of Optimized Secure LDPC Codes

$$P_{e,\min}^E = 0.49$$



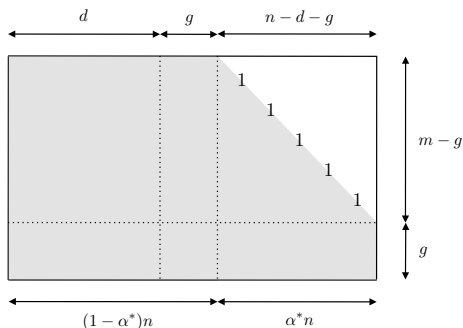
Power Loss



- rate loss: number of messages not equal to the dimension of the code
- power loss can be decreased by using low-rate mother codes

Encoding

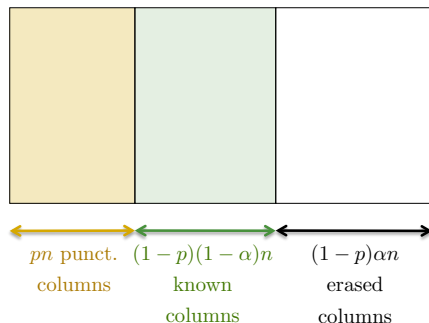
- Richardson, Urbanke 2001:



- Encoding Complexity: $O(n + g^2)$

Encoding

- punctured bits are not transmitted over the channel; need the residual matrix (degree distribution)



Achievable gaps

- Achievable gaps for optimized secure LDPC codes:

p	g	$g^{(T)}$
0	$0.0298n$	0
0.1	$0.0405n$	0
0.2	$0.0303n$	0
0.3	$0.0290n$	$0.0024n$
0.4	$0.0499n$	$0.0160n$

Summary

- alternative approach to physical layer security
- practical code construction based on LDPC codes is proposed
- puncturing messages creates a non-systematic LDPC code that is amenable to analysis
- BER grows very fast to 0.5 even if an eavesdropper has the ability to use a bitwise-MAP decoder
- codes are efficiently encodable and the construction can be extended to finite-block lengths for practical applications