SECURE CHANNEL CODING SCHEME BASED ON LDPC CODES OVER THE BEC

ALEKSANDRA ARSIĆ

MATHEMATICAL INSTITUTE SASA, BELGRADE

INTRODUCTION

Математички институт САНУ

- Combining encription process and coding theory
- Reducing the overall processing cost
- Faster and more efficient implementation
- 1978 - first public key cryptosystem based on algebric coding theory
- Decoding problem for general linear codes is NP-complete

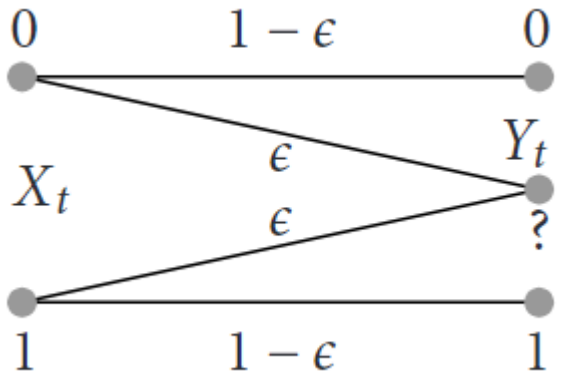
ELEMENTS OF CRYPTOSISTEM

Математички институт САНУ

- BEC – Binary Erasure Channel
- LDPC CODES – Low Density Parity Check Codes
  - QC-LDPC CODES
  - RAPTOR CODES
  - POLAR CODES

BEC – BINARY ERASURE CHANNEL

- Comunication channel
- Information may be lost, but it is never corrupted
- Simplest form:
  - Single bits are transmitted and either received correctly or known to be lost



LDPC CODES

Математички институт САНУ

- Discovered by Gallager
- Parity check and generator matrices for decoding and encoding algorithms
- General cases:
  - Encoding algorithm - $O(n^2)$
  - Decoding algorithm - $O(n^3)$

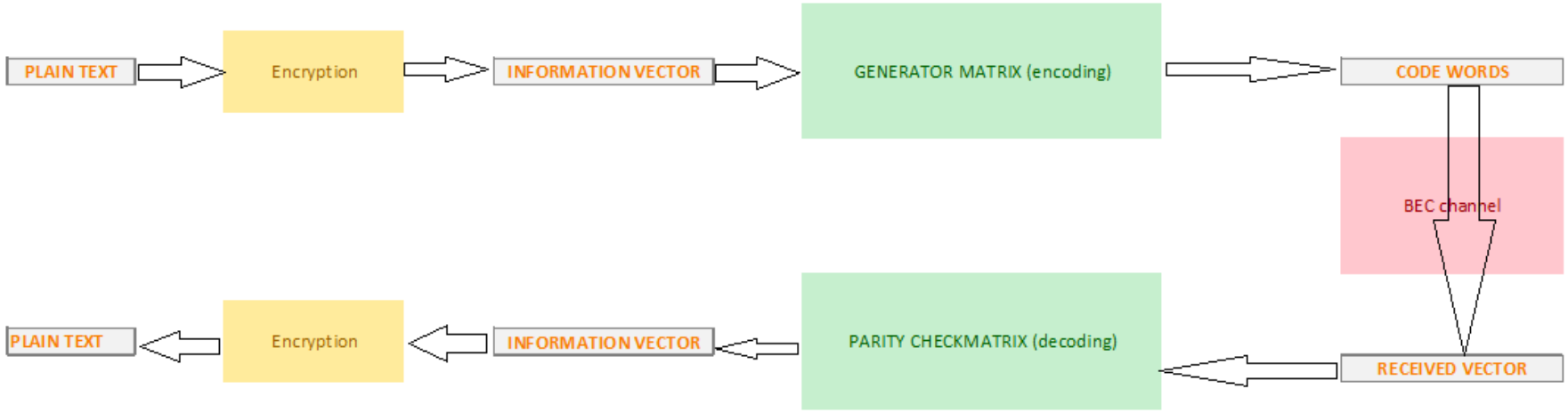
CLASSES OF LDPC CODES

CODE	QC-LDPC	RAPTOR	POLAR
ENCODING COMPLEXITY	$O(N)$	$O(N)$	$O(N \log N)$
DECODING COMPLEXITY	$O(N^3)$	$O(N)$	$O(N^2 \log N)$

SYSTEM DESIGN

Математички институт САНУ

- Improvement of encryption algorithm - security
- Block or stream cipher can be used
- LDPC code
- BEC channel



EFFICIENCY AND SECURITY

Математички институт САНУ

- Key size
- Complexity of encoding algorithm
- Complexity of decoding algorithm
- Security against the best known attacks

CONCLUSIONS AND FUTURE WORKS

Математички институт САНУ

- Goals:
  - Increase information rate
  - Reduce key size
  - Decrease computation complexity
  - Imporove security
- Algorithm for decoding – modification / improvment
- New class of LDPC code
- New concept of cryptosystem

THANK YOU FOR ATTENTION!