부호 및 암호 연구실

Coding and Cryptography Laboratory

지도교수 : 노 종 선 교수님

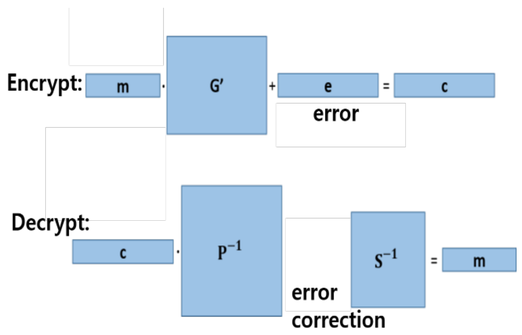
주요 연구 분야

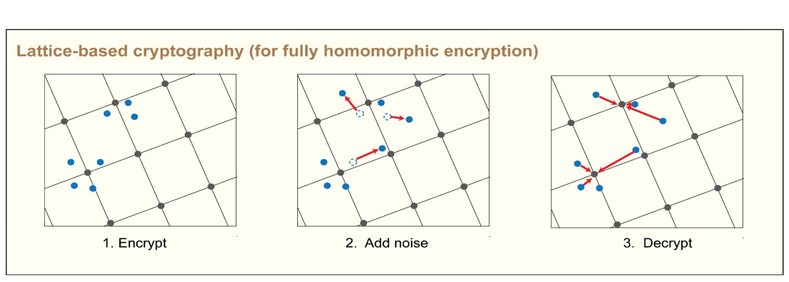
1. Cryptography
2. Coding Theory
3. MIMO Communication Systems
4. OFDM Systems

1. Cryptography

포스트 양자 암호(Post-Quantum Cryptography)

- 양자 컴퓨팅의 등장에 따라 기존 상용 암호(RSA, ECC 등)의 사용이 어려워질 것으로 전망
- 기존의 암호화 기법보다 신뢰성이 높고 연산 속도가 빠른 기술 연구
- 부호 기반(code-based) 암호, 격자 기반(lattice-based) 암호





2. Coding Theory - Error Correcting Codes

Error Correcting Codes (ECC)

데이터에 발생하는 noise, erasure, fading, jamming 등을 극복하여 데이터를 복원 및 보호하는 기법

Classical ECC

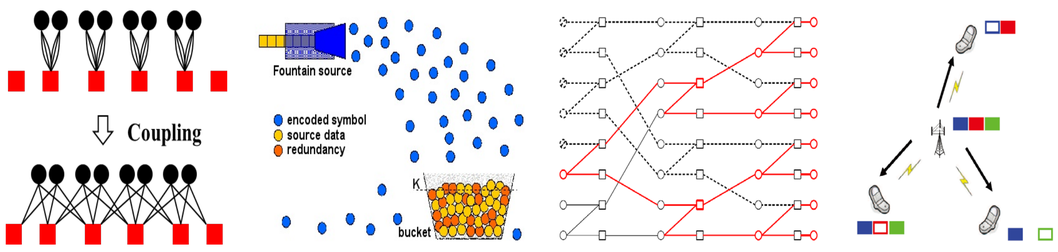
- Hamming codes
- BCH codes
- Reed-Solomon codes
  - ✓ Data storage
- Convolutional codes
  - ✓ 2G mobile communication systems

Modern ECC

- Turbo codes
  - ✓ 3G mobile communications systems
- LDPC codes
  - ✓ 3G mobile communications systems, digital video broadcasting
- Fountain codes

Network Coding

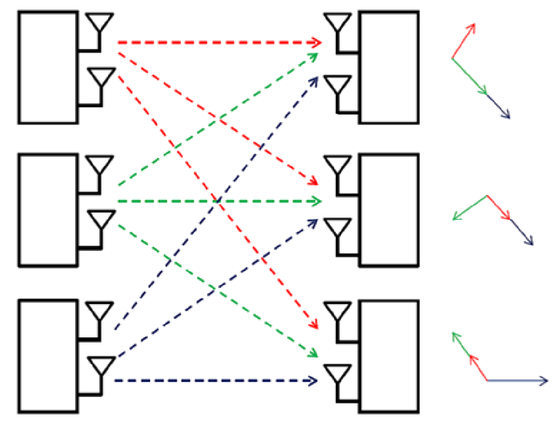
- Index coding
- Codes for distributed storage systems



3. MIMO Communication Systems

Multi-User MIMO Wireless Network

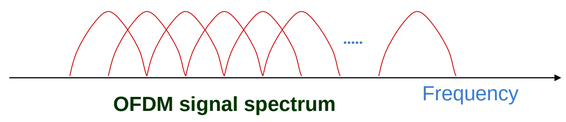
- Enhancement of multiplexing and diversity gain
- Robust beamforming design algorithm for MIMO systems
- MIMO Spatial Interference alignment
- Topological Interference Management
- Full-duplex Cellular Network
- Energy Harvesting via Interference
- Wireless Caching



4. OFDM Systems – PAPR Problem

Orthogonal Frequency Division Multiplexing (OFDM)

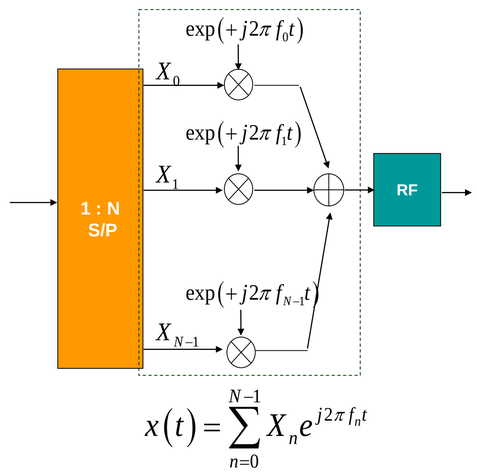
직교성의 성질을 갖는 다수의 부반송파를 사용한 전송 방식



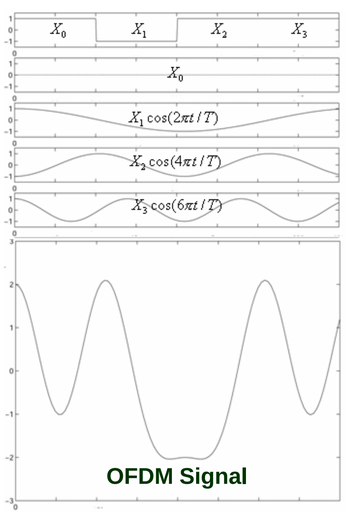
- High rate data by multiple low rate sub-channels
- Each sub-channel becomes flat fading channel
  - ✓ Robust to frequency selective fading
- Efficient bandwidth utilization by allowing overlapped sub-channels

Peak-to-Average Power Ratio (PAPR)

- 신호의 왜곡을 줄이기 위한 PAPR 감소방법 연구
- 차세대 샘플링 기법인 압축 센싱(Compressed Sensing)과의 결합



OFDM Transmitter



OFDM Signal

연구실 정보

지도교수 : 노종선 교수님 (132동 407호) / jsno@snu.ac.kr

- ➢ 전 한국통신학회 회장
- ➢ IEEE Information Theory (IT) society 석학회원 (Fellow)
- ➢ USC 전기공학 공학박사

- ✓ 연구실 설립: 1999년 2학기
- ✓ 졸업생: 박사 25명, 석사 26명
- ✓ 연구실 구성: 박사과정 13명, 석사과정 6명
- ✓ 연락처: 880-1773 (301동 652-1,2호), 880-8437 (132동 417호)