CSEEC: CRYPTO-SYSTEM WITH EMBEDDED ERROR CONTROL

SMU | Bobby B. Lyle School of Engineering

R. Alawadhi, S. Nair,

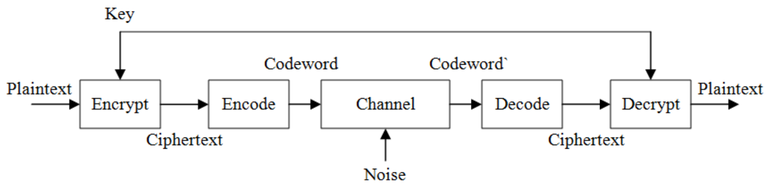
Bobby B. Lyle School of Engineering

Southern Methodist University, Dallas, Texas, USA

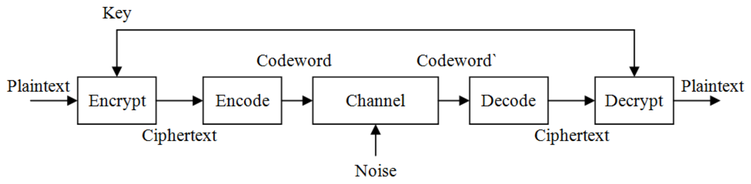
SMU | HACNet High Assurance Computing And Networking Labs

Encryption & Encoding

Conventional



Jointly



Basics:

- Encryption: data secrecy
- Encoding: data reliability

Challenges:

- Secrecy and reliability are competing concerns

Advantages:

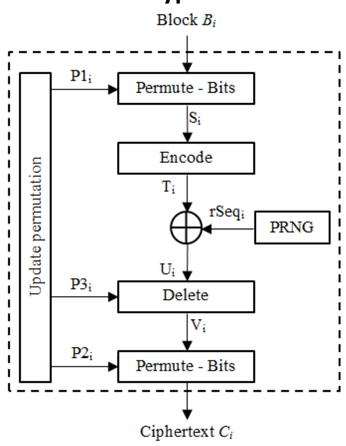
- Achieve data secrecy and reliability, either individually or jointly
- Easy to switch between the two services
- Scale the level of each service

Applications:

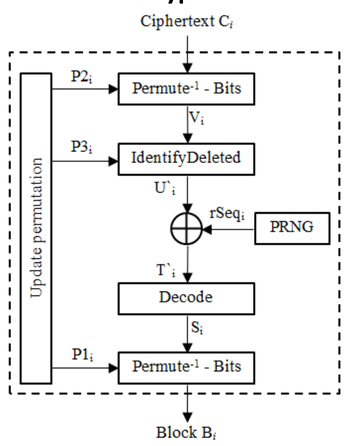
- Multi-path routing in WSN
- Multi-cast video streaming

Algorithm

Encryption



Decryption



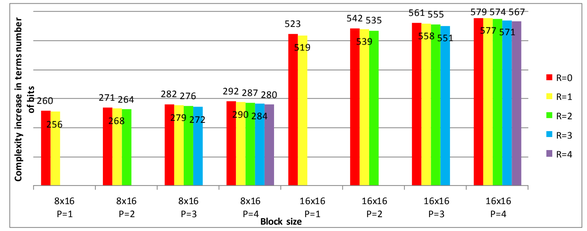
Parameters:

- Error correction code ($\mathcal{C}$)
- Pseudo Random Number Generator (PRNG)
- Number of rows (r)
- Number of columns (c)
- Number of parity or check columns (P)
- Number of parity used toward reliability (R)

Security:

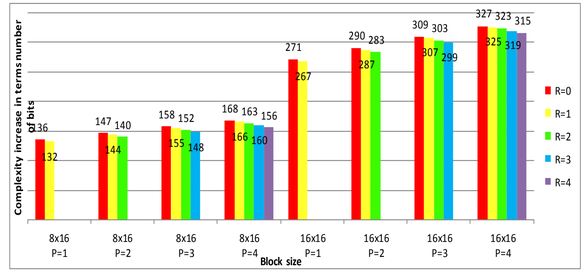
- Present unreliable PRNG output to an attacker
  - Increase the complexity of PRNG attacks
    - Known plaintext attacks

$$\left(\binom{r\times c}{(r\times c)/2} * \binom{c+P}{P-R} * 2^{r\times(P-R)} * \binom{r\times(c+R)}{(r\times(c+R))/2}\right)^{\frac{Q}{r\times c}}$$



    - Chosen plaintext attacks

$$\left(\binom{c+P}{P-R} * 2^{r\times(P-R)} * \binom{r\times(c+R)}{(r\times(c+R))/2}\right)^{\frac{Q}{r\times c}}$$



Randomness Tests:

- NIST statistical test suite for random number generator
  - 15 core tests
  - 7 data sets
- All tests were passed