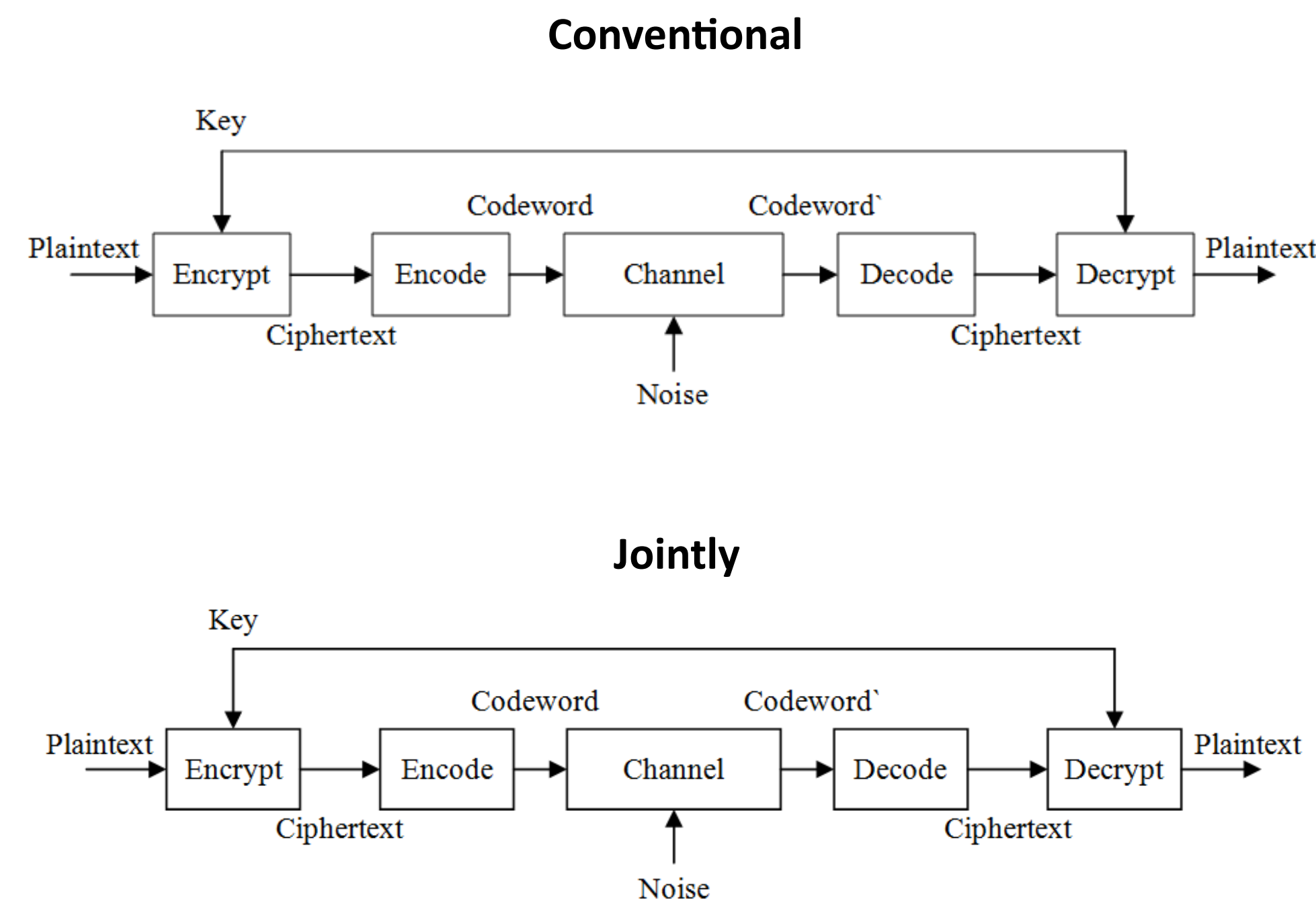
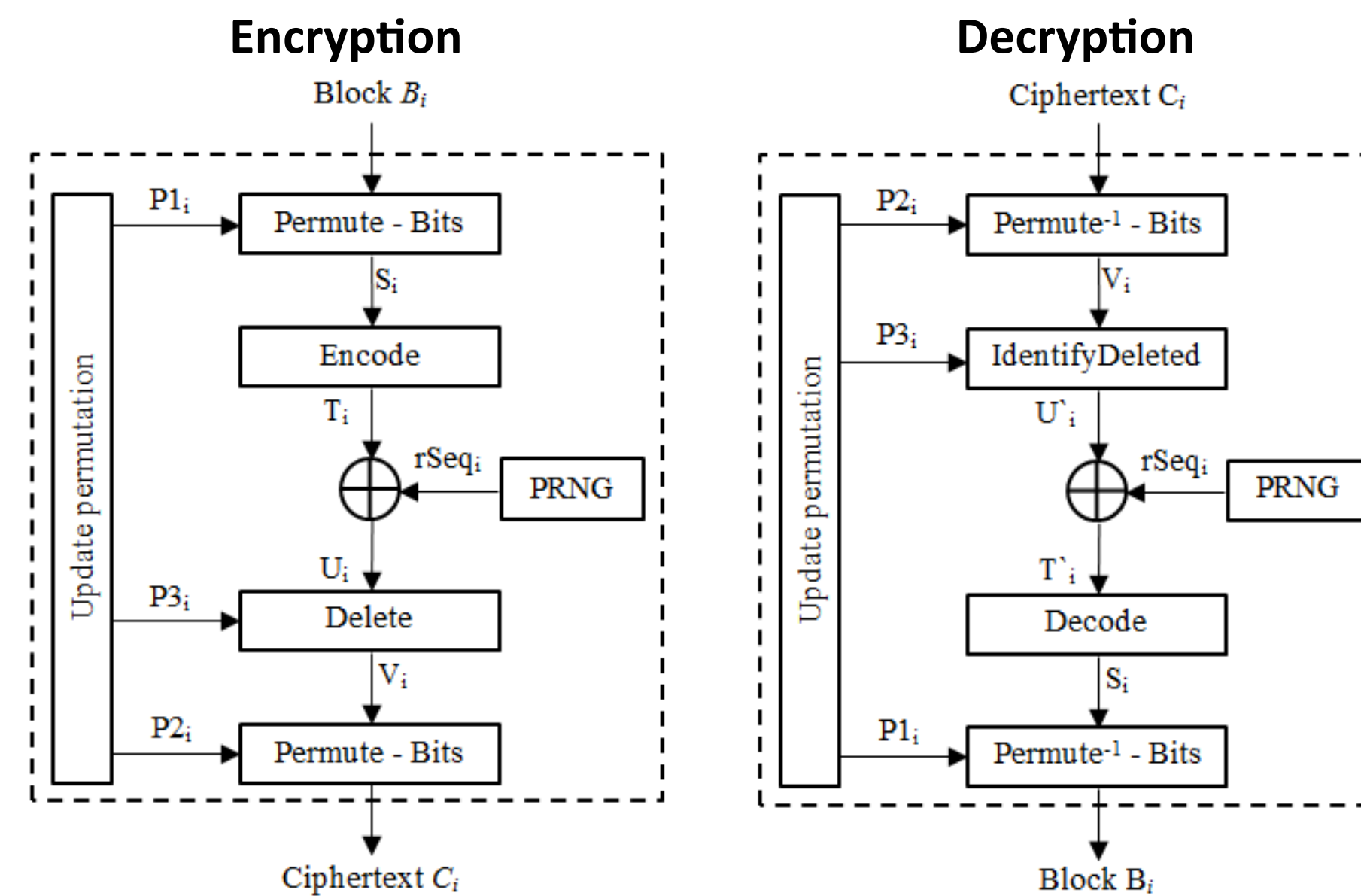


CSEEC: CRYPTO-SYSTEM WITH EMBEDDED ERROR CONTROL

Encryption & Encoding



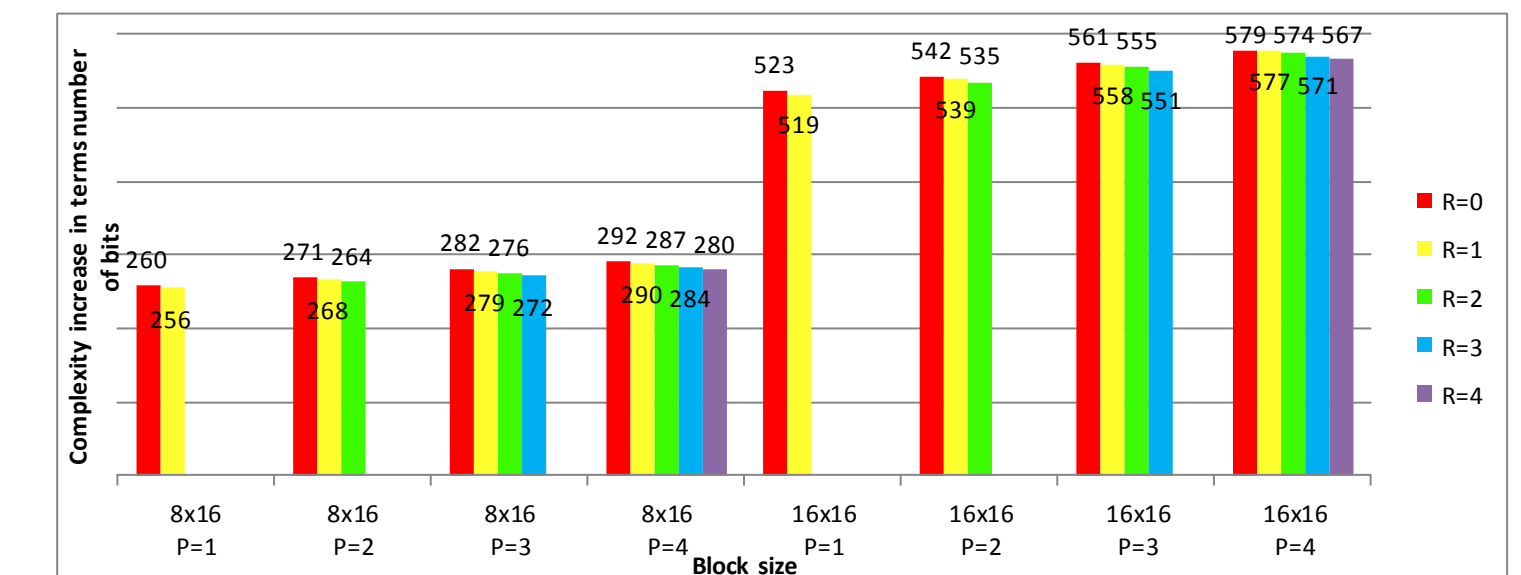
Algorithm



Security:

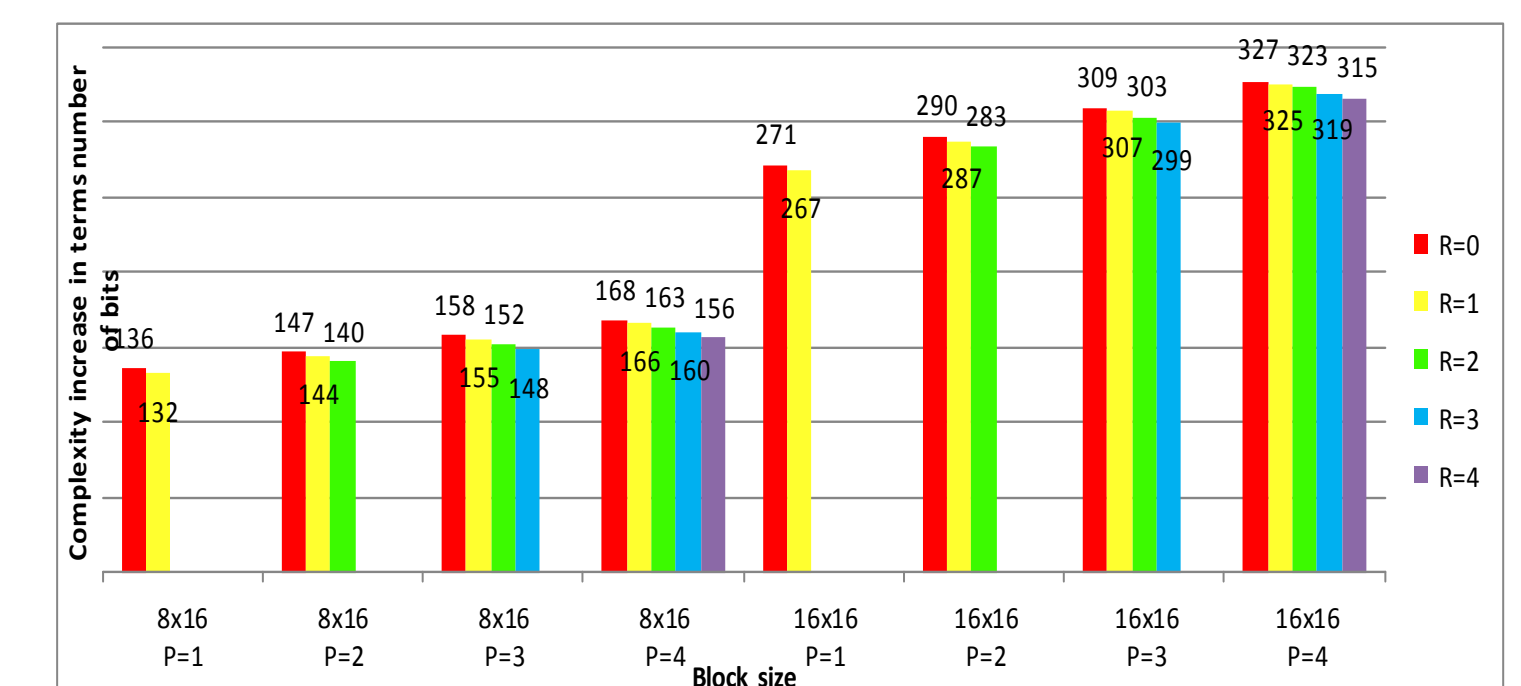
- Present unreliable PRNG output to an attacker
 - Increase the complexity of PRNG attacks
 - Known plaintext attacks

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



- Chosen plaintext attacks

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



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

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)

Randomness Tests:

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