An Integrated Signaling-Encryption Mechanism to Reduce Error Propagation in Wireless Communications

Mohammed Olama
Miljko Bobrek

Computational Sciences and Engineering Division

Oak Ridge National Laboratory

Mustafa Matalgah

Electrical Engineering Department

University of Mississippi

IEEE CQR 2015

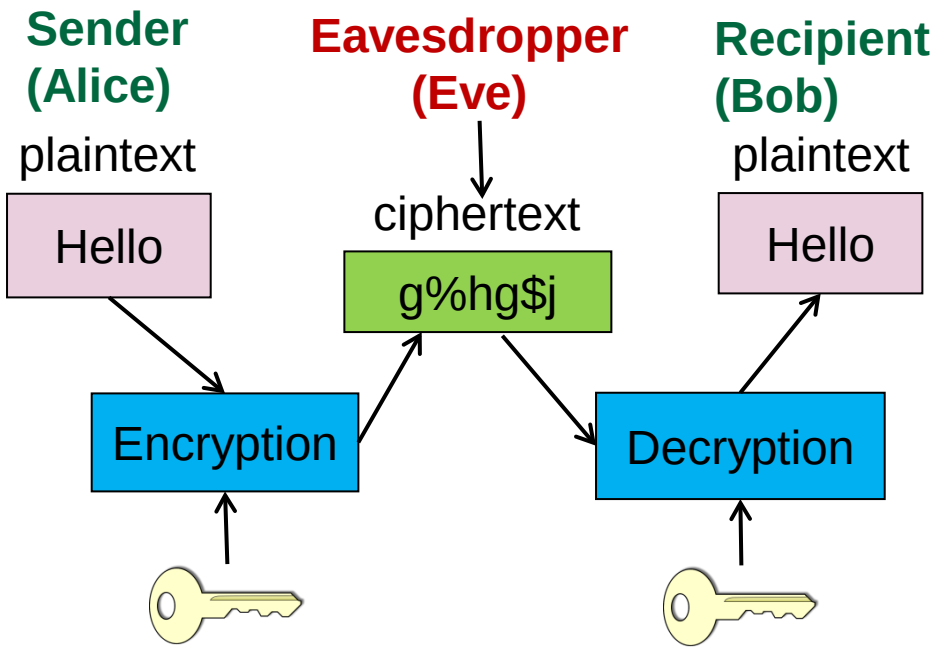
Outline

- Wireless cryptography
- Avalanche criterion
- Problems of encryption standards
- Integrated signaling-encryption mechanism
- BER and throughput analysis
- Numerical results
- Conclusion and future work

Oak Ridge National Laboratory

Wireless Cryptography

- Techniques for secure communication in the presence of third parties (adversaries).
- Encryption
  - Requires packet overhead
  - Causes processing time delays
  - Suffers from QoS deterioration
- Applications:
  - Military
  - Government
  - Smart grid
  - Mobile phones
  - Computer security
  - Network security
  - Others



Encryption is the first layer of defense against attacks

Avalanche Criterion

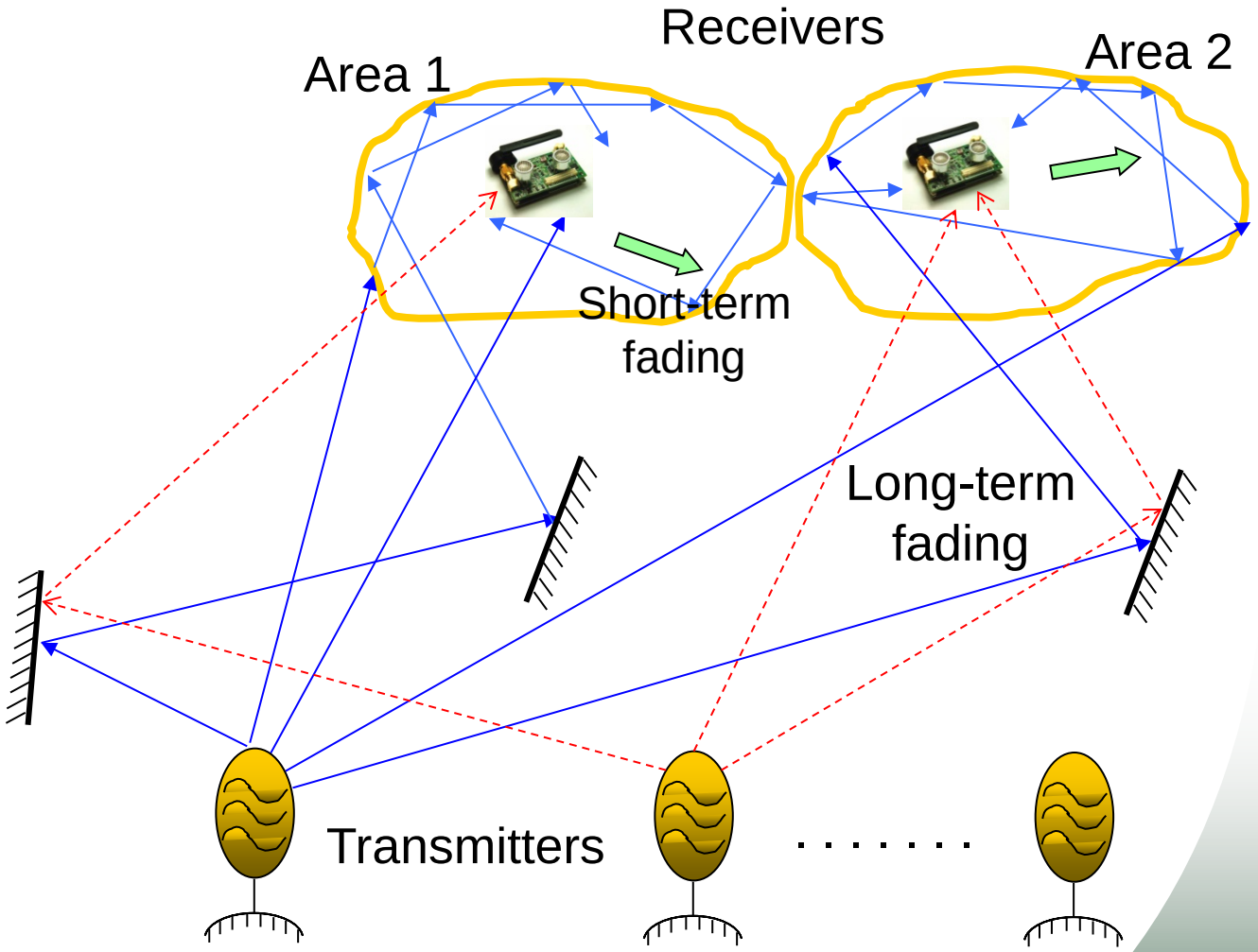
- A desirable property in cryptography.
- A small change in the plaintext, or key, (e.g., flipping a single bit) causes a drastic change in the ciphertext (e.g., half the output bits flip).
- This fact guarantees a highly secured data transmission assuming that the communication channel causes no error of the information packet, and an ideal channel can offer that.

plaintext		ciphertext
1		0
1		0
1	Encryption →	1
0		1
0		0
1		1
0		1

plaintext		ciphertext
0		1
1		1
1	Encryption →	1
0		0
0		0
1		1
0		0

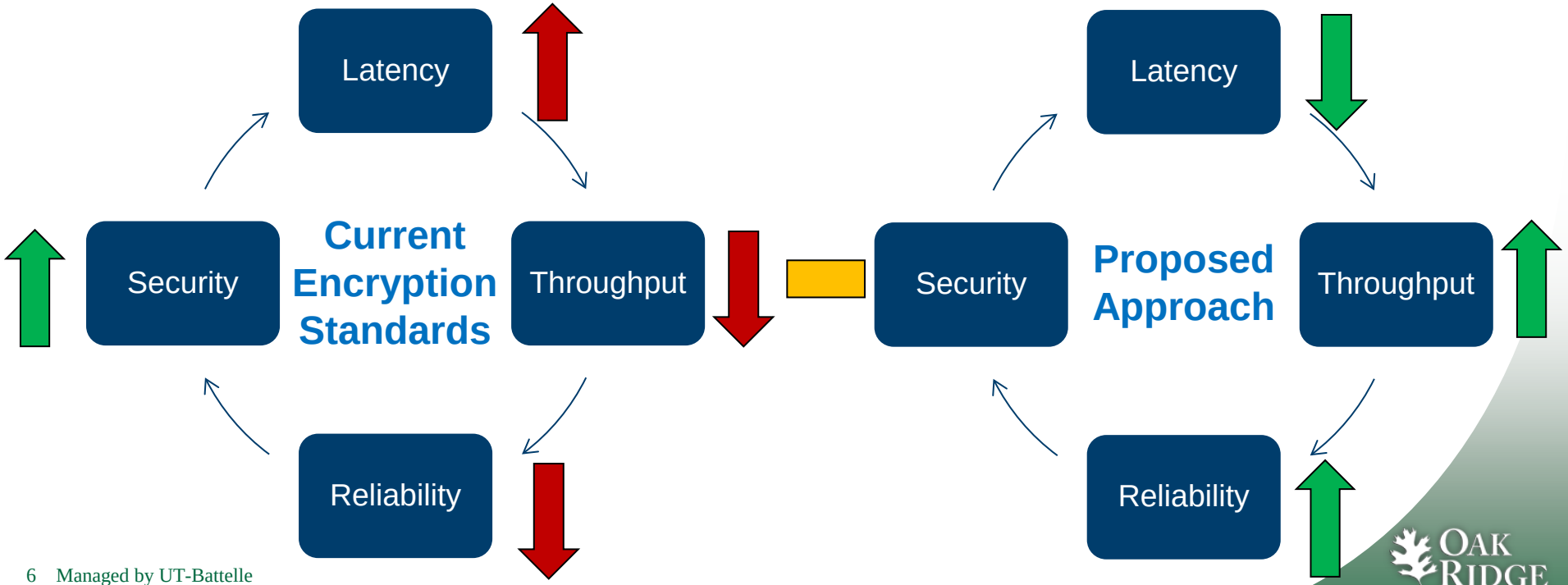
Typical Wireless Communication Channel

- Ideal channel does not exist
- Multipath fading
- Interference
- Cause random errors to the ciphertext
- Random bit-errors increase dramatically due to the avalanche effect

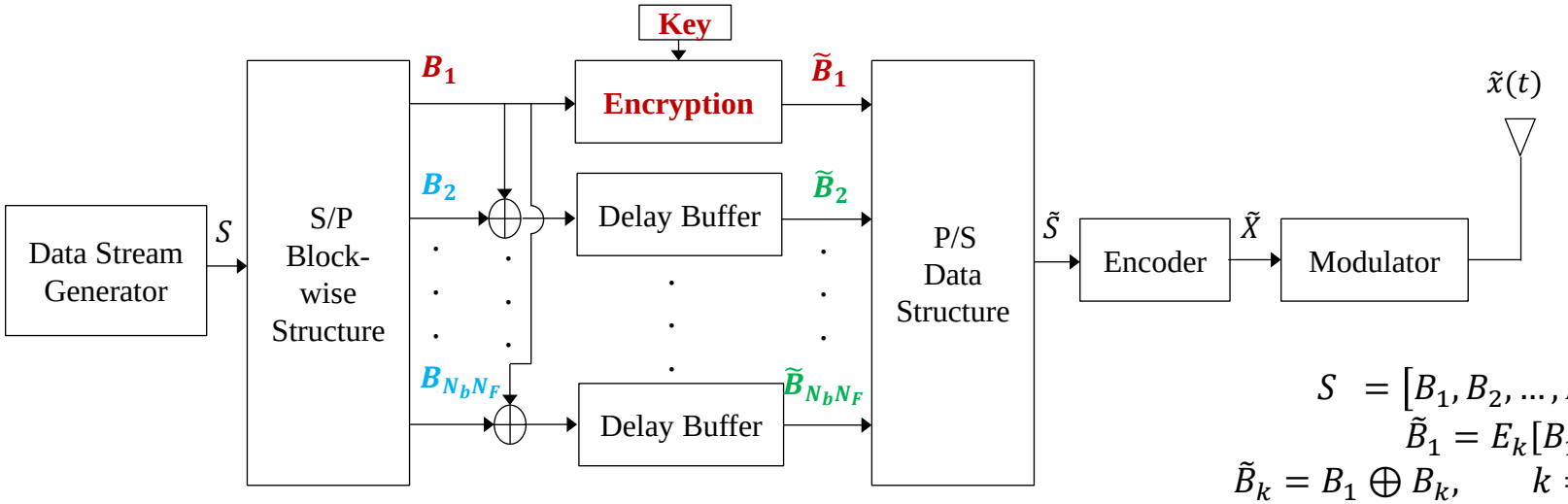


Outstanding Problems of Encryption Standards

- **Regulation**
  - NIST FIPS 1977
  - NSA Suit B (AES)
  - Suite A for higher classification
  - NRC RG 5.71 (NIST 800-53)
- **Problems**
  - Increase information error (BER)
  - Reduce throughput (overhead)
  - Increase computational complexity (latency)



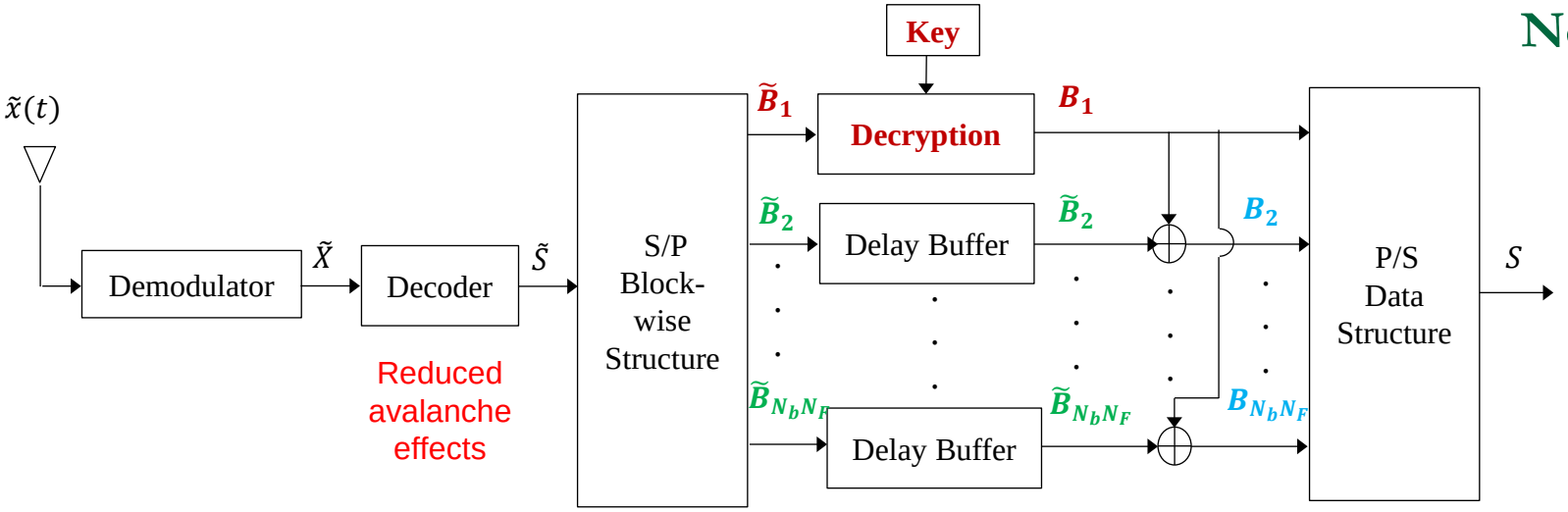
Proposed Approach: A New Integrated Signaling-Encryption Technique (Conceptual Block Diagram)



Transmitter

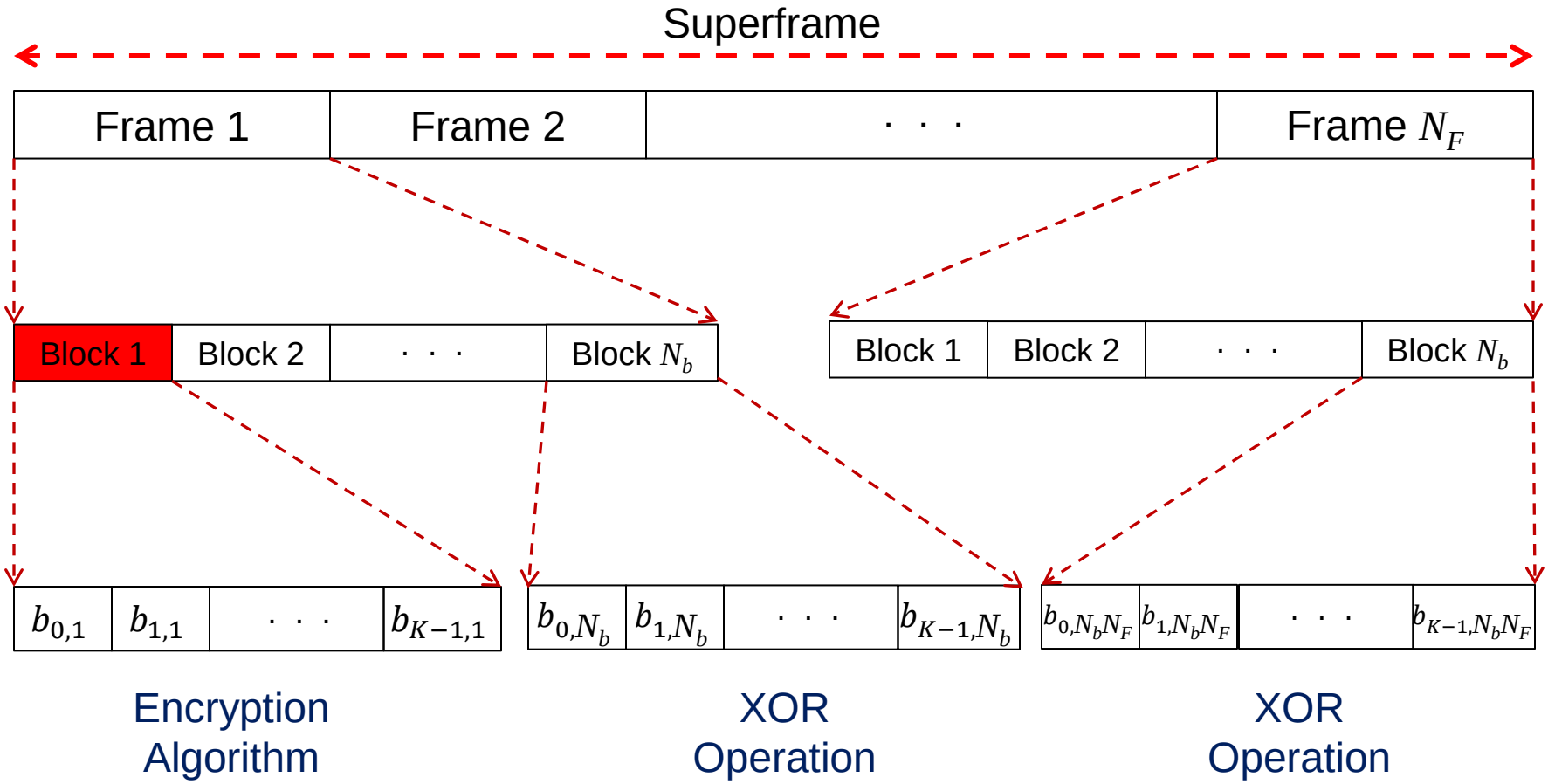
$$S = [B_1, B_2, \dots, B_{N_bN_F}]$$
$$\tilde{B}_1 = E_k[B_1]$$
$$\tilde{B}_k = B_1 \oplus B_k, \qquad k = 2, \dots, N_bN_F$$
$$\tilde{S} = [\tilde{B}_1, \tilde{B}_2, \dots, \tilde{B}_{N_bN_F}]$$

Notation

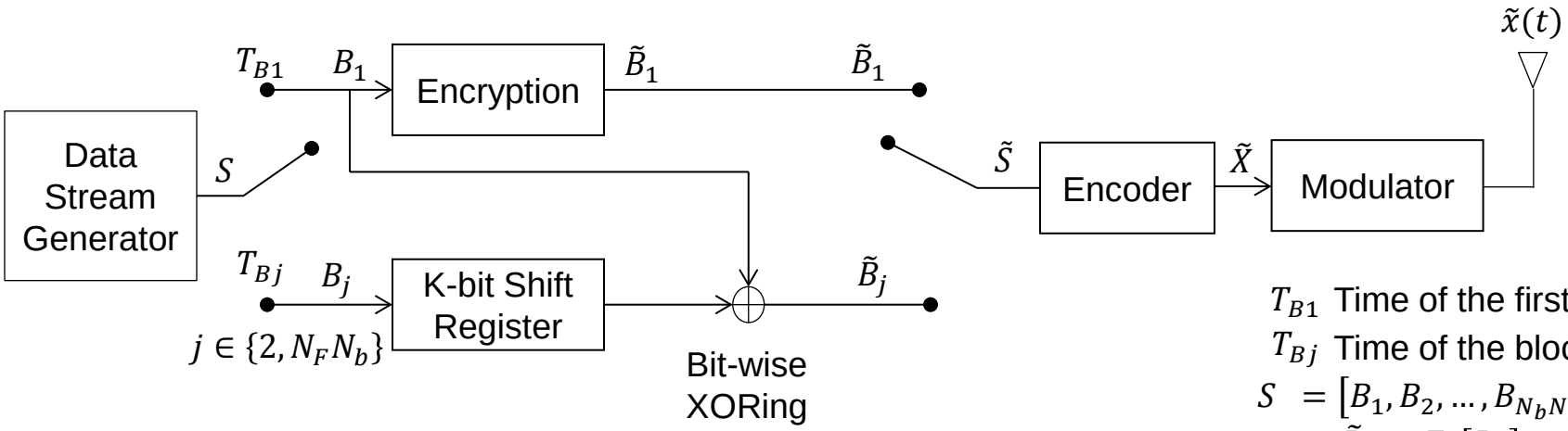


Receiver

Proposed Approach: Super-Frame Structure



Proposed Approach: Implementation Block Diagram



Transmitter

T_{B1} Time of the first block

T_{Bj} Time of the block B_j

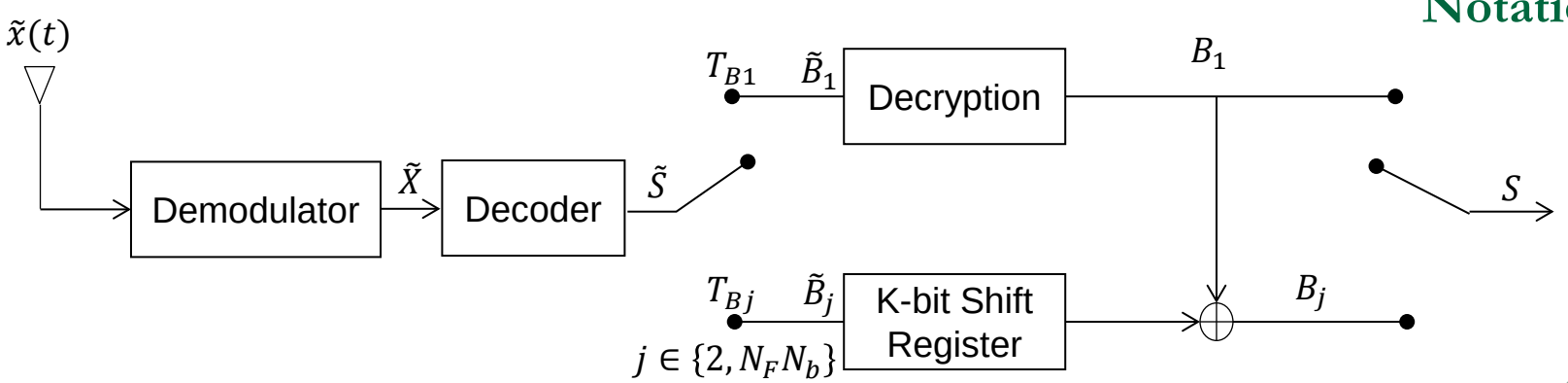
$$S = [B_1, B_2, \dots, B_{N_b N_F}]$$

$$\tilde{B}_1 = E_k[B_1]$$

$$\tilde{B}_k = B_1 \oplus B_k, \qquad k = 2, \dots, N_b N_F$$

$$\tilde{S} = [\tilde{B}_1, \tilde{B}_2, \dots, \tilde{B}_{N_b N_F}]$$

Notation



Receiver

Proposed Approach: Pseudo Code Structure

Algorithm 1: Generating secure encrypted-coded data using the proposed algorithm

Input: Data stream as plaintext
Output: Data stream as ciphertext
Divide the data sequence into N super frames;
for each N_i *superframe* (SF_i), $i = 1, \ldots, N$, *to be sent* **do**
    Divide each super frame into N_F frames;
    Divide the frame (F_k), $k = 1, \ldots, N_F$, into N_b blocks with block size of β_l;
    Encrypt the first block B_1 with an appropriate encryption algorithm, i.e., $\tilde{B}_1 = E_k[B_1]$
    for each *of the remaining blocks* B_j, $j \in \{2, N_F N_b\}$ **do**
        $\tilde{b}_{i,j} = b_{i,j} \oplus b_{i,1}, i \in \{1, \beta_l\}$;
        Generate the coded blocks as $\tilde{B}_j = [\tilde{b}_{1,j}, \ldots, \tilde{b}_{\beta_l,j}]$;
    end
    Generate the encrypted-coded frame;
    Generate the encrypted-coded superframe;
end
Repeat for other superframes.

Encryption Ratio

- **A new figure of merit, defined as**

$$\beta_c = \frac{\text{Transformed text using the XOR}}{\text{Encrypted text using traditional algorithms}}$$

$$\beta_c = \frac{(N_F N_b - 1)\beta_l}{\beta_l} = (N_F N_b - 1)$$

- **It reveals the amount of overhead processing cycles reduction obtained when using the integrated encryption algorithm**

- **As the value of $\boldsymbol{\beta_c}$ increases, the encryption overhead as well as the avalanche effect decreases and hence the effective system throughput increases.**

Oak Ridge National Laboratory

BER Analysis

- **The BER for AWGN channel, BPSK modulation**

$$P_{e_G} = Q(\sqrt{2\gamma_b}) \ , \quad \gamma_b = \frac{E_b}{N_o}$$

- **The BER of the decrypted block**

$$P_{e_E} = 0.5(1 - [1 - P_{e_G}]^{\beta_l})$$

- **The BER of the XORed block**

$$P_{e_{XOR}} = P_{e_G} + P_{e_E} - 2P_{e_G}P_{e_E}$$

- **The BER of the proposed scheme**

$$P_{e_{proposed}} = \frac{P_{e_E} + \beta_c P_{e_{XOR}}}{\beta_c + 1}$$

OAK RIDGE National Laboratory

BER Analysis & ECC

- **The BER for AWGN channel, Error Correction Coding**

$$P_{e_G}^{encoding} = Q(\sqrt{2\gamma_c}), \quad \gamma_c = \frac{E_c}{N_o} \quad , E_c = R_c E_b$$

- **The BER for Hamming Code (HDD)**

$$P \approx P_{e_G}^{encoding} - P_{e_G}^{encoding}(1 - P_{e_G}^{encoding})^{n-1}$$

- **The BER for convolutional code (HDD)**

$$P \leq B_{d_{free}}[2\sqrt{P_{e_G}^{encoding}(1 - P_{e_G}^{encoding})}]^{d_{free}}$$

- **The BER for convolutional code (SDD)**

$$P \leq B_{d_{free}} Q(\sqrt{2 d_{free} \gamma_c})$$

OAK RIDGE National Laboratory

BER Analysis & ECC only the First (Encrypted) Block

- The BER for the ECC decrypted block

$$P_{e_E}^{encoding} = 0.5(1 - [1 - P]^{\beta_l})$$

- The BER for the XORed block

$$P_{e_{XOR}}^{first} = P_{e_E}^{encoding} + P_{e_G} - 2P_{e_G}P_{e_E}^{encoding}$$

- The BER for the proposed scheme

$$P_{e_{proposed}}^{first} = \frac{P_{e_E}^{encoding} + \beta_c P_{e_{XOR}}^{first}}{\beta_c + 1}$$

- The BER for the conventional scheme (AES)

$$P_{e_{conv}}^{first} = \frac{P_{e_E}^{encoding} + \beta_c P_{e_E}}{\beta_c + 1}$$

Oak Ridge National Laboratory

Throughput Analysis

- **In general, the throughput (T) is defined as the number of correctly received bits (carrying information) per second, which can be described in terms of the bit rate (R) as**

$$T = R(1 - P_e)^{\beta_l}$$

- **The average throughput for no encryption, conventional encryption, and the proposed scheme are**

$$T_{No_Enc} = R\left(1 - P_e^{No_Enc}\right)^{\beta_l}$$

$$T_{Conv} = \eta R(1 - P_e^{Conv})^{\beta_l}$$

$$T_{Prop} = R\left(\frac{\beta_c + \eta}{\beta_c + 1}\right)\left(1 - P_e^{Prop}\right)^{\beta_l}$$

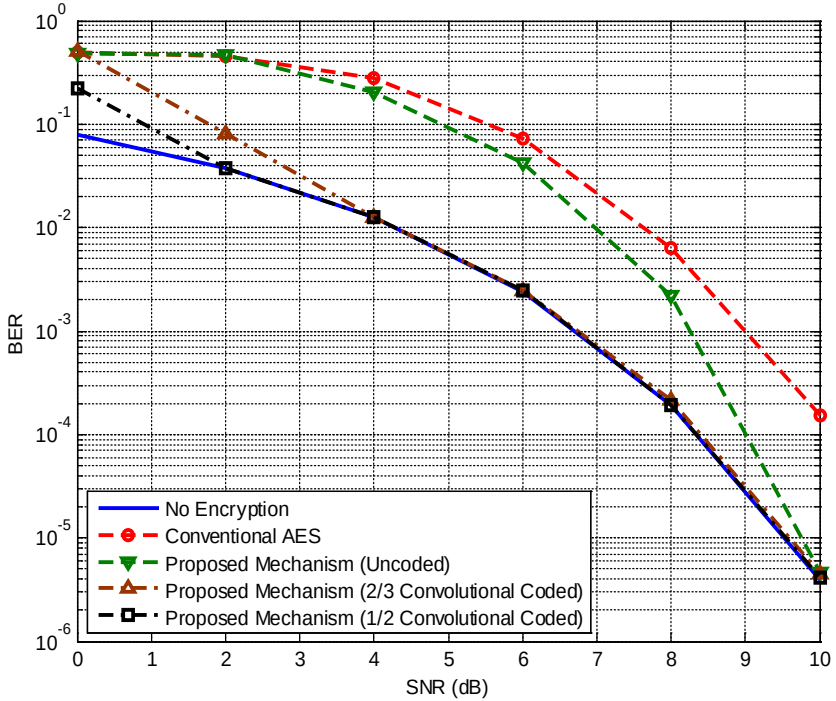
$$T_{Prop}^{Encoding} = R\left(\frac{\beta_c + \eta R_c}{\beta_c + 1}\right)\left(1 - P_e^{Prop_Encoding}\right)^{\beta_l}$$

OAK RIDGE National Laboratory

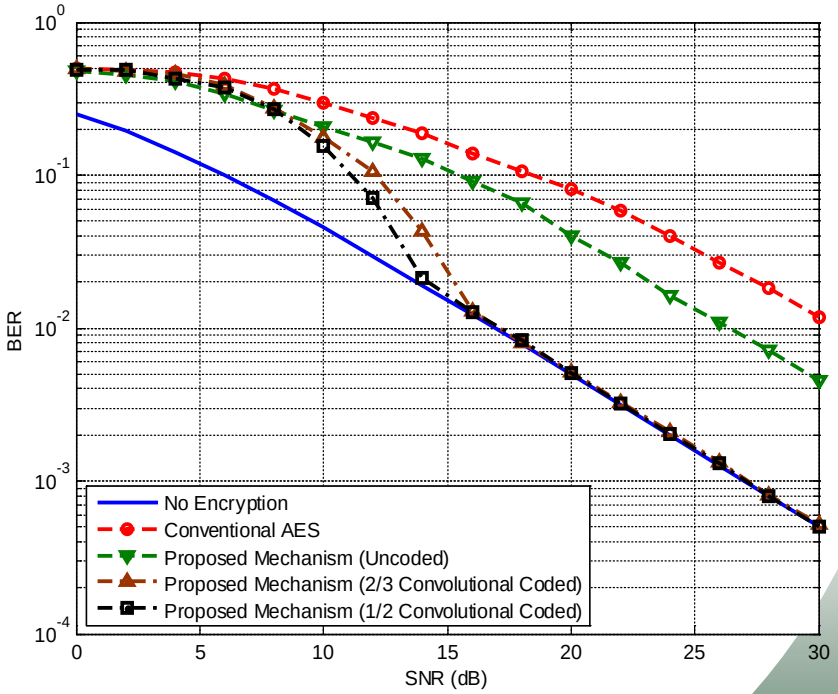
Performance Evaluation and Comparison: BER Analysis

- The Convolutional code in only applied to the first AES-encrypted block of each superframe
- The block size is 128 bits and superframe size is 1000 blocks.

AWGN



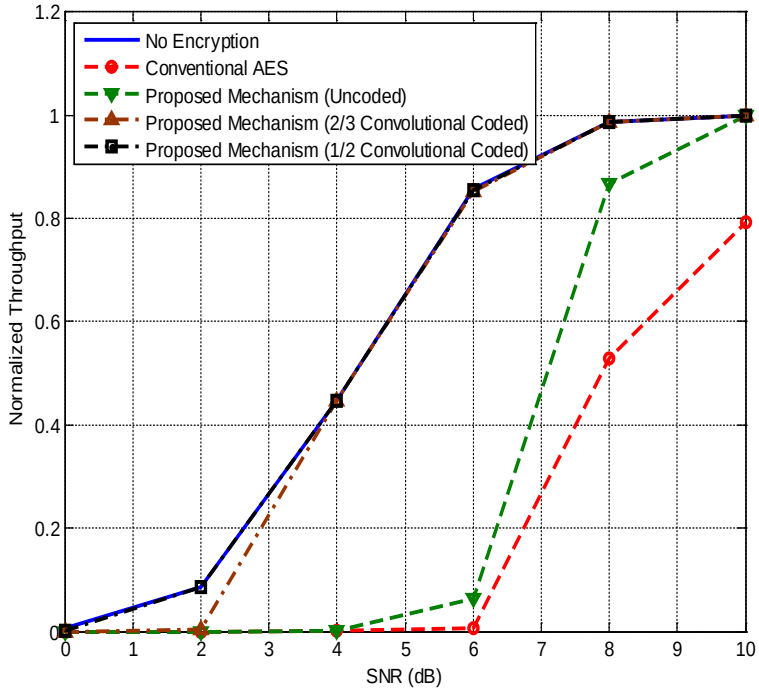
Rayleigh



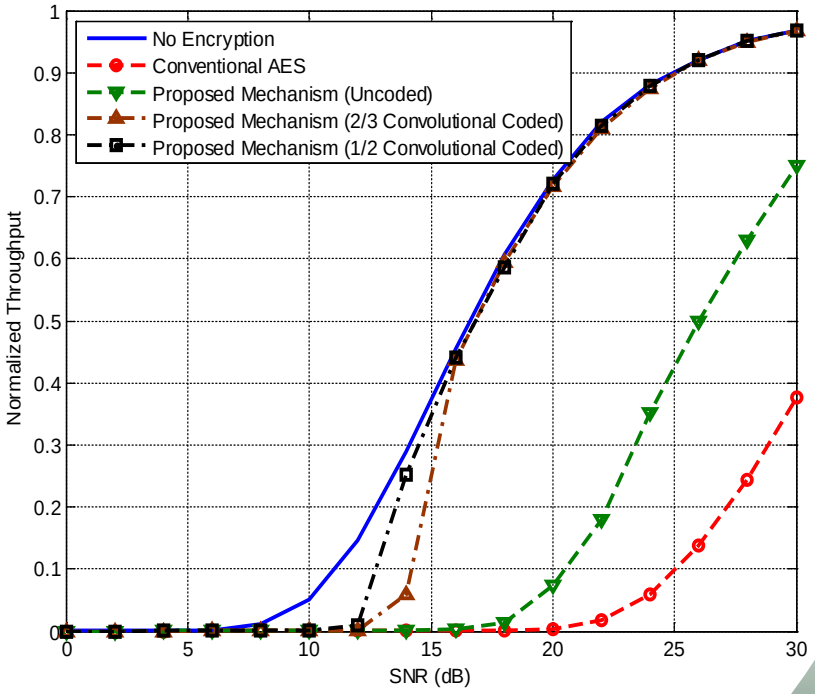
Performance Evaluation and Comparison: Throughput Analysis

- Throughput is defined as the number of correctly received bits (carrying information) per second

AWGN



Rayleigh

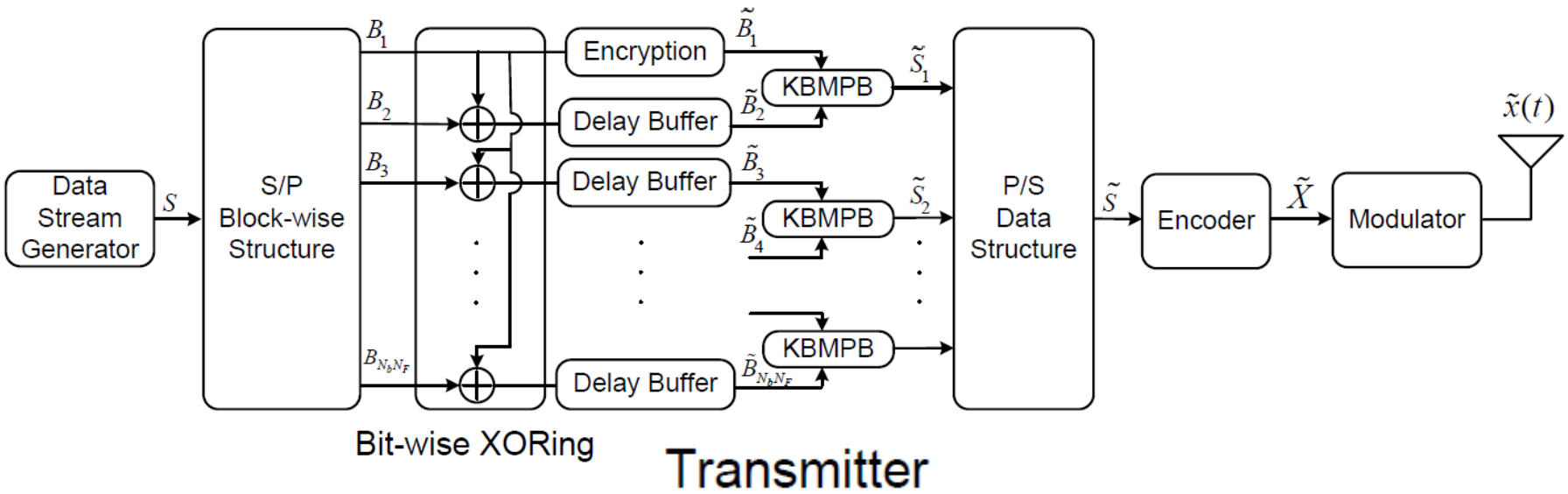


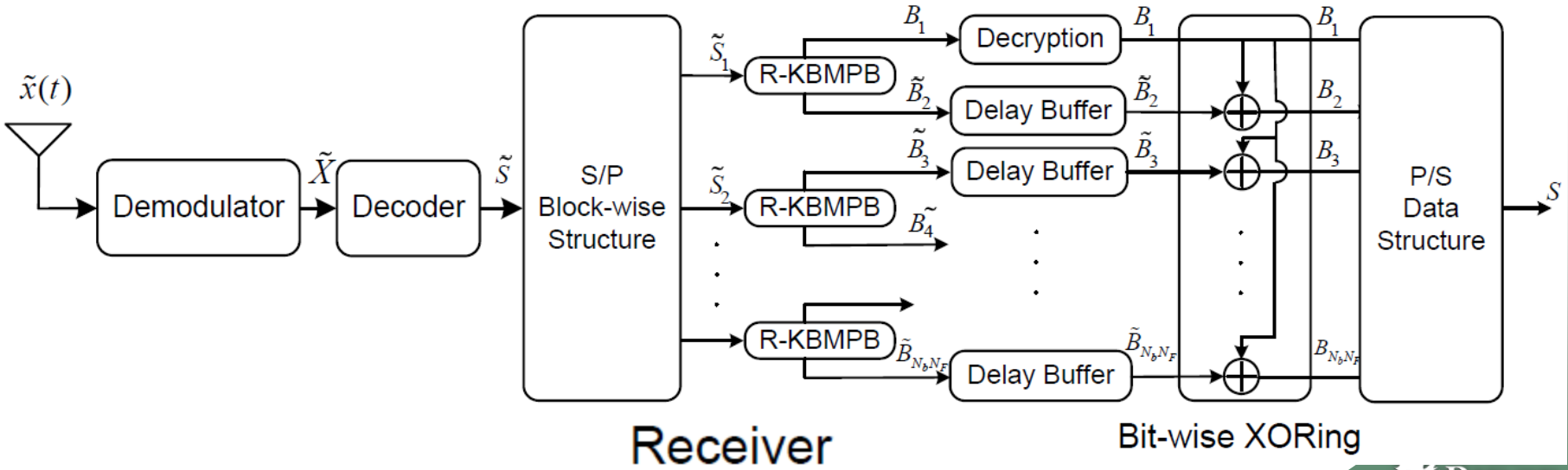
Conclusion

- **Performance evaluation analyses have been conducted for the integrated signaling-encryption mechanism in terms of BER and throughput in wireless channels**
- **We considered error correction encoding only the first encrypted block in order to achieve higher data throughput**
- **Numerical results show that the BER performance and throughput of the integrated mechanism are superior to those of the conventional AES over standard Gaussian and Rayleigh fading-type channels**
- **On going work is to investigate the security aspect of the proposed scheme**

Oak Ridge National Laboratory

Enhancing the Security of the Proposed Scheme





Thank you

Questions?