Joint Encryption Error Correction and Modulation (JEEM) Scheme

Oluwayomi Adamo, Eric Ayeh, & Murali Varanasi

IEEE CQR - June 26, 2012

Outline

- Motivation/Introduction
- Related Work
- Secure Communication System Model
- McEliece Cryptosystem
- JEEM Encryption Scheme
- Random Modulation Scheme (BPSK)
- Encryption Randomized Modulation Scheme (BPSK & QPSK)
- Evaluation of the Proposed Scheme
- Conclusions

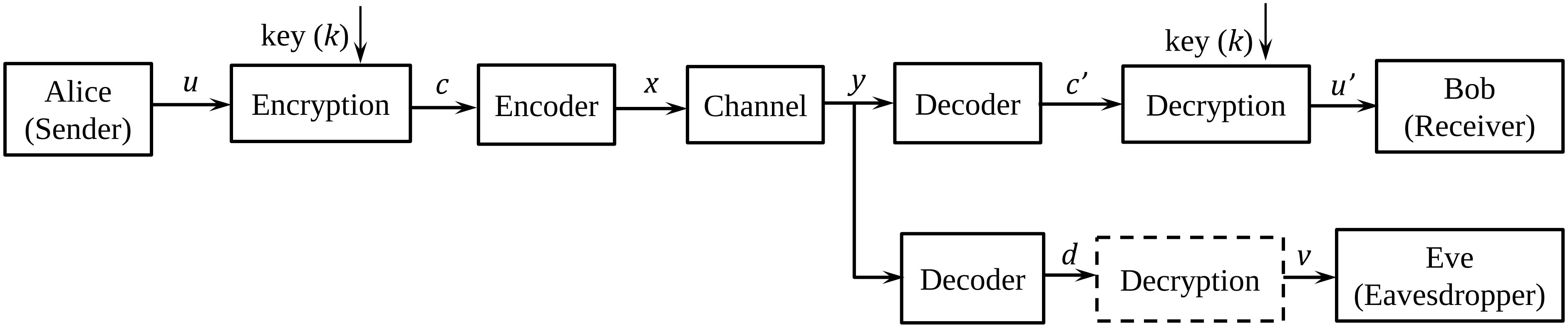
Motivation/Introduction

- Need for security, reliability and speed in wireless communication systems
- The best and often the only way to secure data in WN is to encrypt.
- Conventional modulation schemes are modified to provide random mapping of encoded information.
- JEEM - Physical layer encryption scheme to provide data reliability, secrecy and integrity

Related Work

- McEliece introduced the use of error correcting code as a public key cryptosystem.
  - Based on algebraic coding theory using t-error correcting Goppa code
  - Although very efficient, it has received little attention in practice because of the very large public keys.
- Rao proposed a private key cryptosystem based on algebraic-code using McEliece scheme.
  - Less computational intensive compared to McEliece scheme
  - Broken by a chosen-plaintext attack.
- Hwang et. Al proposed Secret Error Correcting Code (SECC) using preparata code
  - Did not use error vector originally introduced in the original McEliece scheme.

Secure Communication System Model



McEliece Cryptosystem

- Encryption of a plaintext $\boldsymbol{M}$ into a ciphertext $\boldsymbol{C}$

$$C = MG' + Z = MSGP + Z$$

C: cyphertext of length n,

M: plaintext of length k,

Z: random error vector of length n whose hamming weight $t' = t$,

$G' = SGP$: public key,

G: generator matrix of a t-error correction code (Goppa code for the McEliece's case),

S (scrambler) , G (generator matrix), P (permutation matrix) are private keys.

JEEM Encryption Scheme

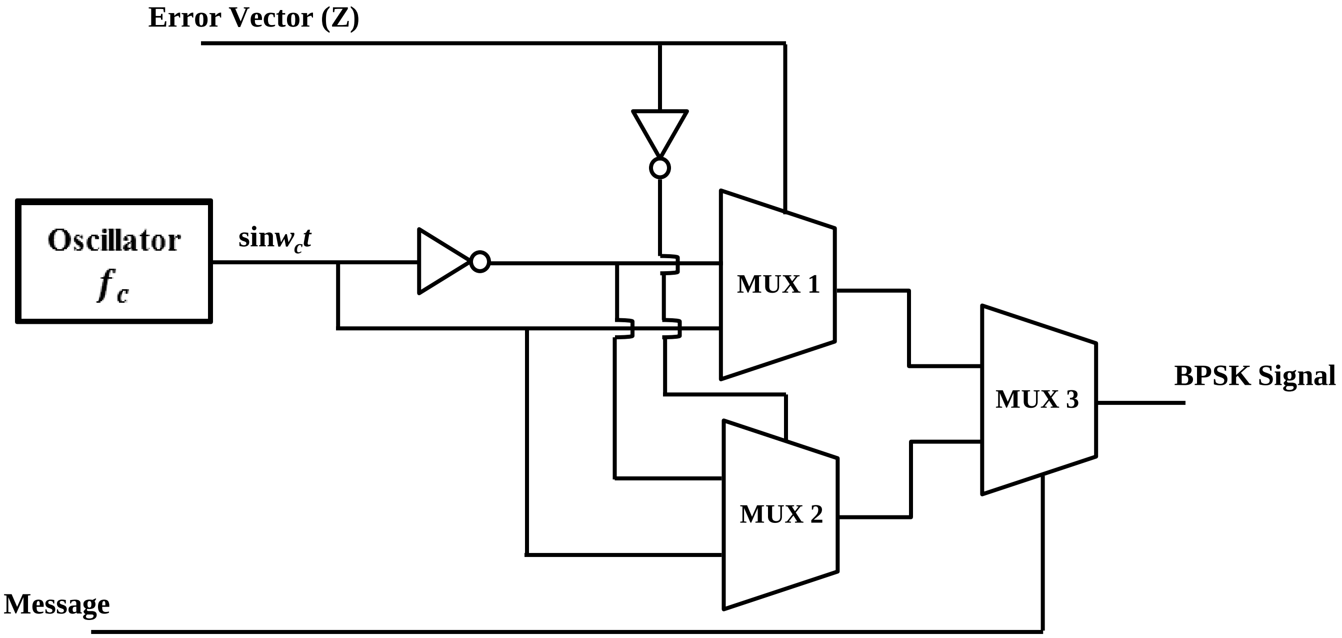
$$C' = MG' = MFGP$$

$$C = (MG')M_r = (MFGP)M_r$$

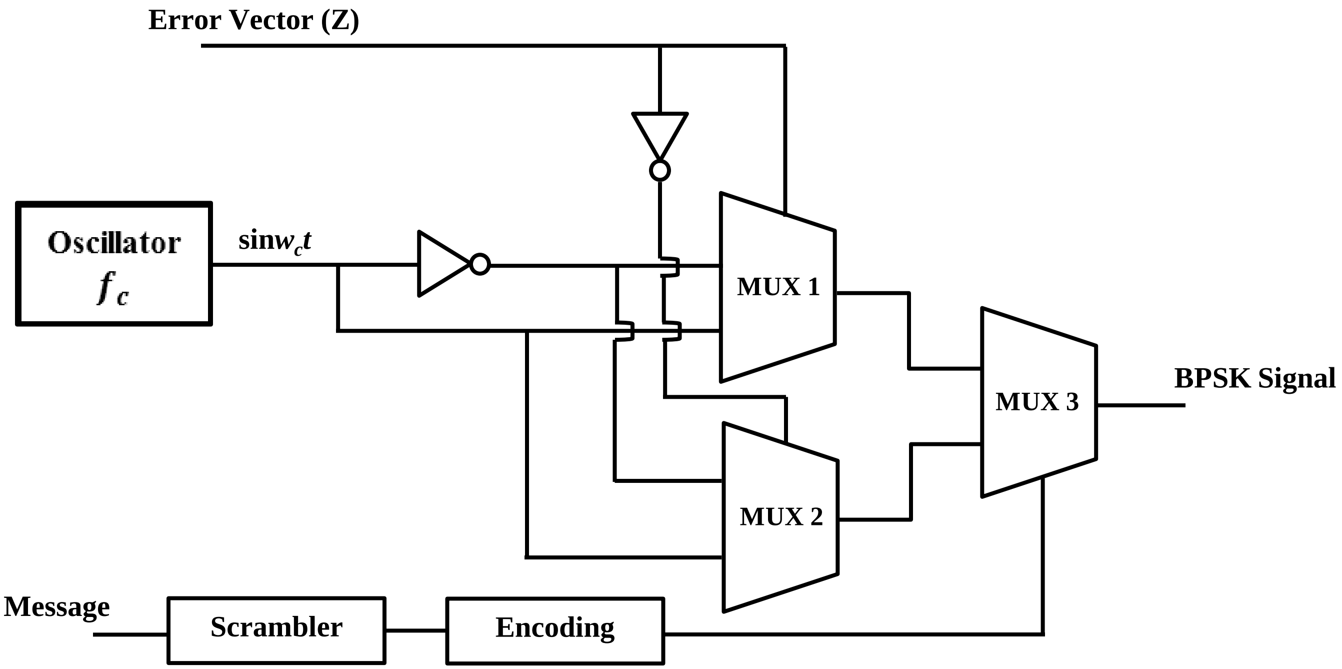
$$C = (MG')M_r = (MFGP)M_r \equiv MSGP + Z$$

- $\boldsymbol{F}$ is a non-linear function instead of scrambler in the McEliece scheme.
- $\boldsymbol{G'}$ is generator matrix of low-density parity-check code (LDPC)
- Random modulation using $\boldsymbol{M_r}$ instead of modulo-2 addition of $\boldsymbol{C'}$ with $\boldsymbol{Z}$
- The modulation is controlled by the error vectors.
- Provides both randomization and modulation without compromising the structure of the McEliece-like scheme.

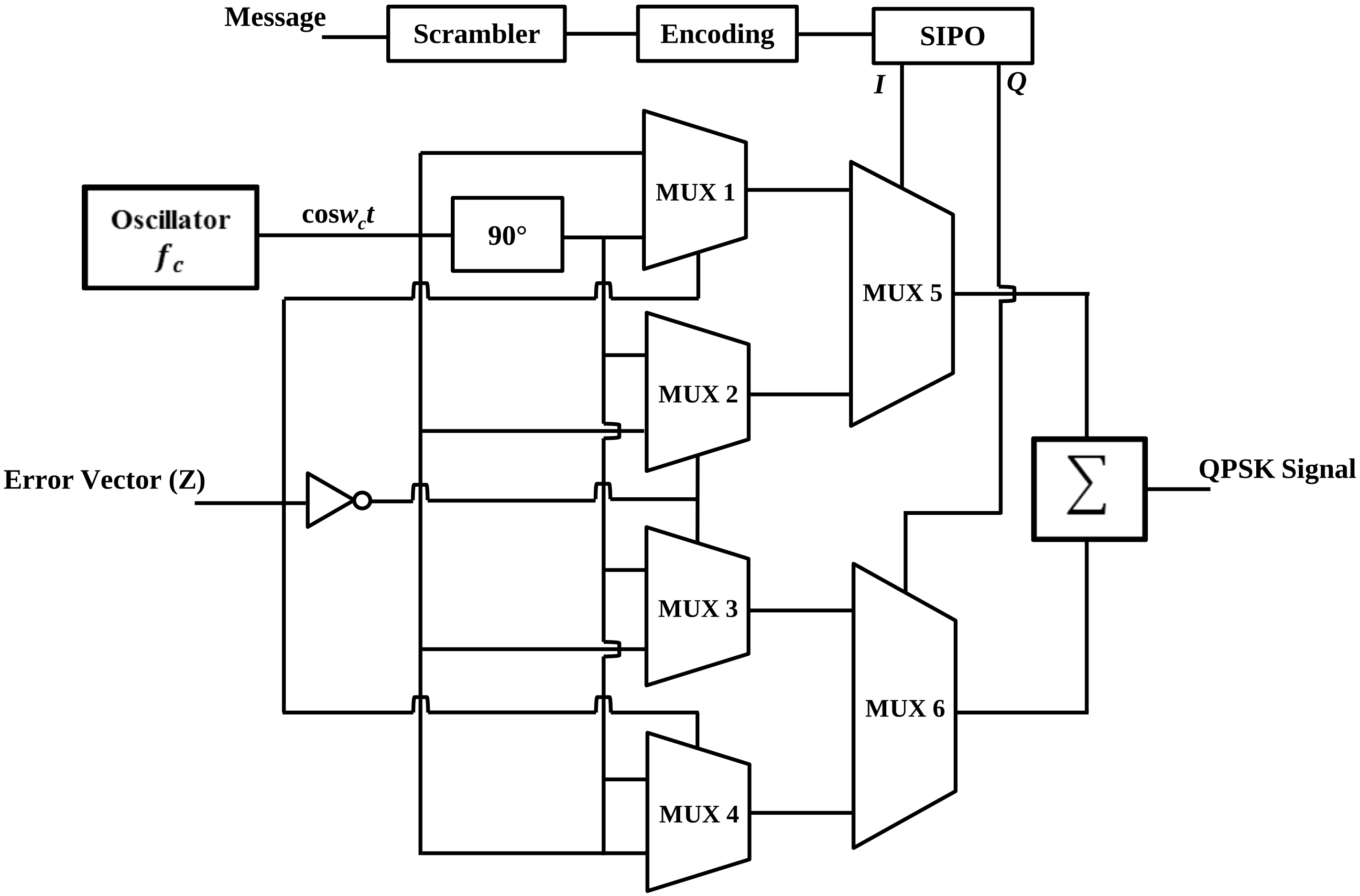
Random Modulation Scheme - BPSK



Encryption Randomized Modulation Scheme - BPSK



Encryption Randomized Modulation Scheme - QPSK

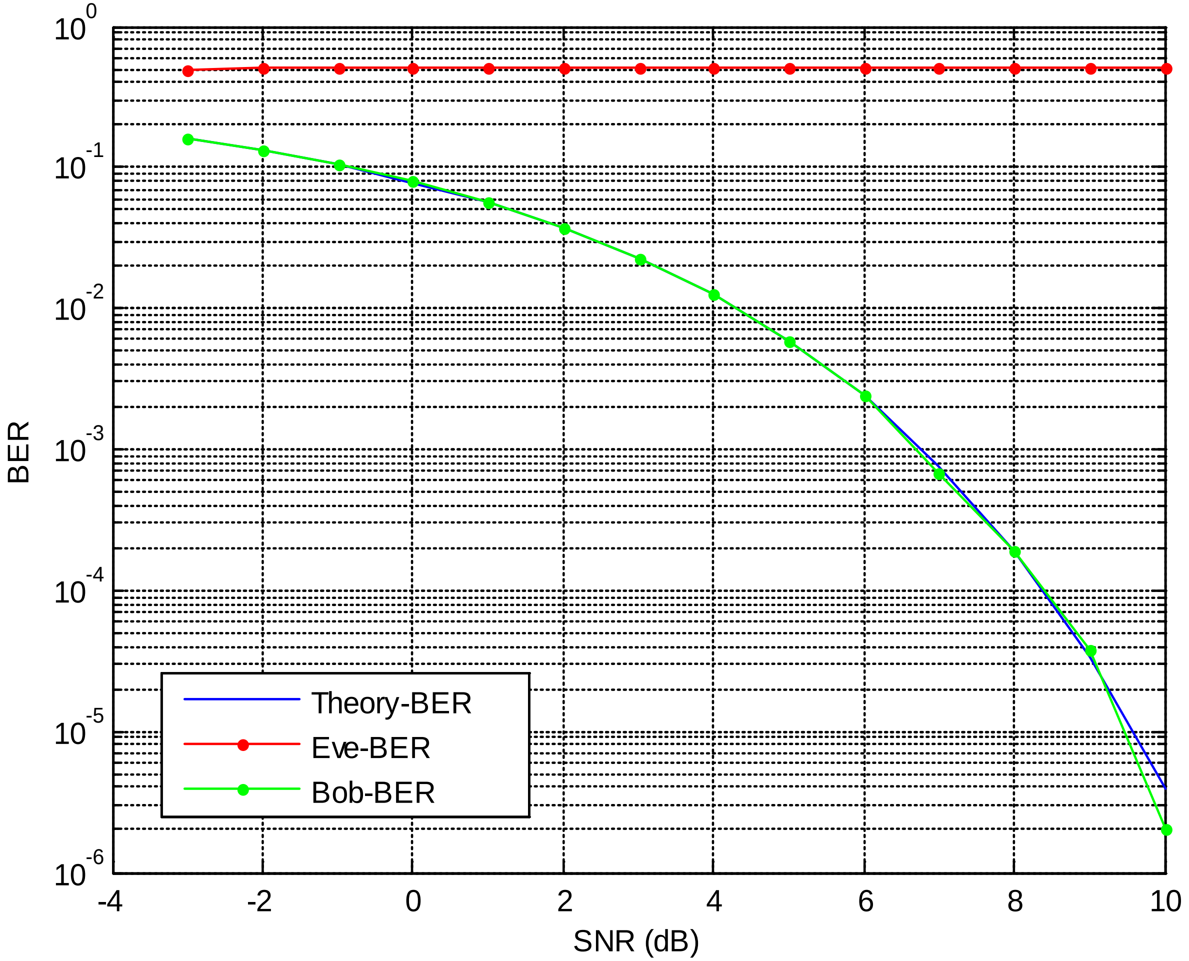


*Serial-in parallel-out (SIPO)

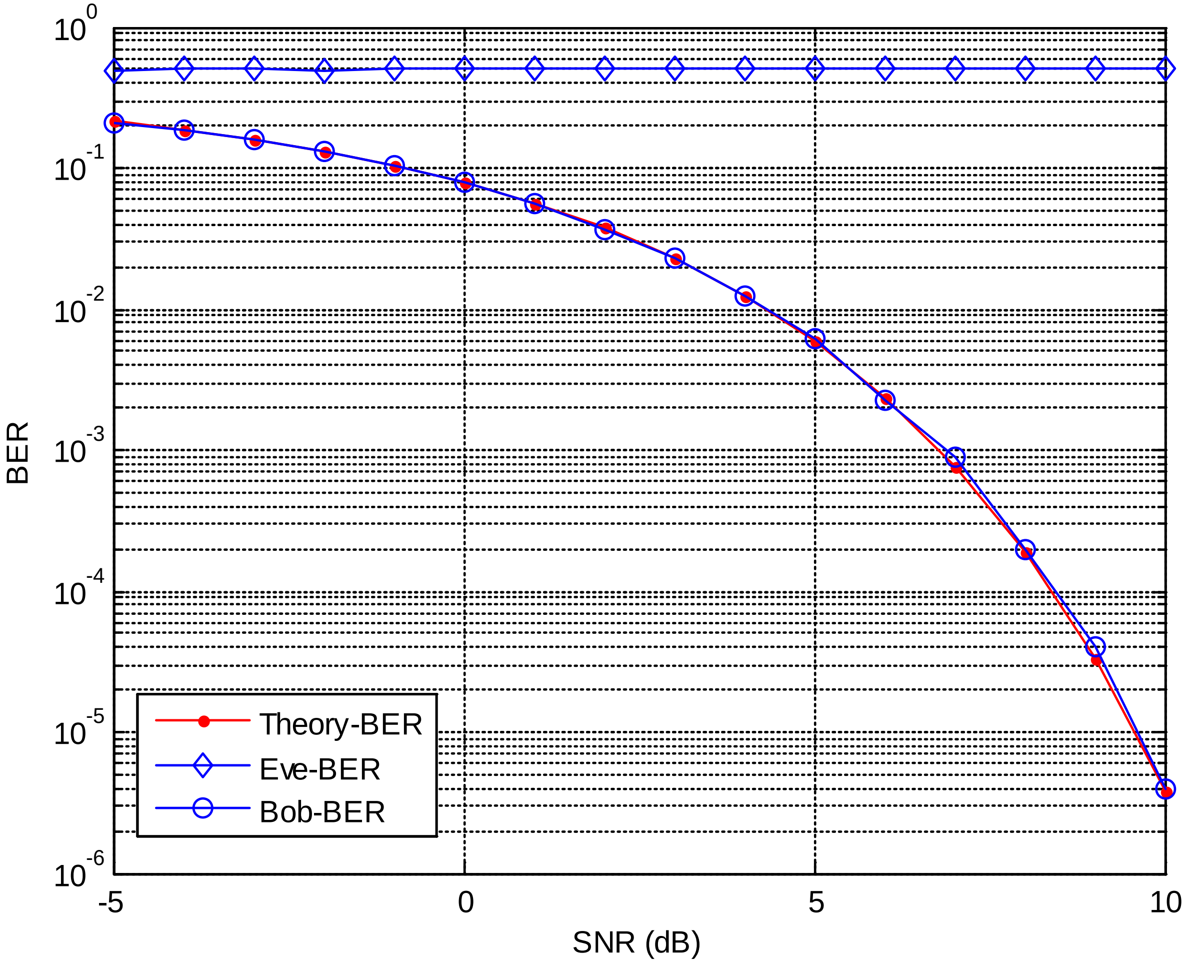
Evaluation of JEEM

- Bit error rate (BER), symbol error rate (SER) used as a measure of security
- High BER/SER at Eve can deliver improved resilience against eavesdropping
- Simulated performance of the communication channels for Bob and Eve for BPSK and QPSK modulation schemes
- Communication through an additive white Gaussian noise channel

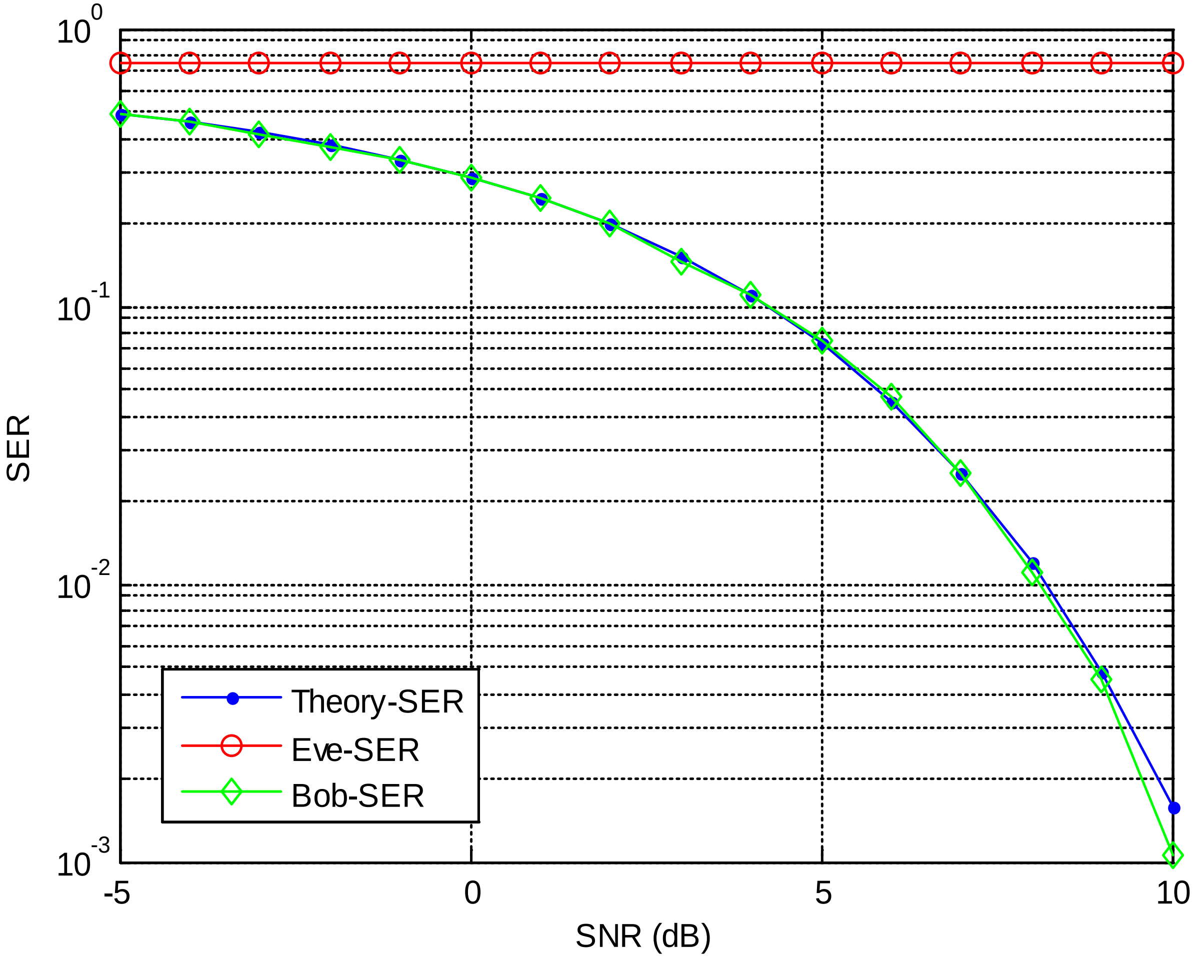
BER vs. SNR for BPSK



BER vs. SNR for QPSK

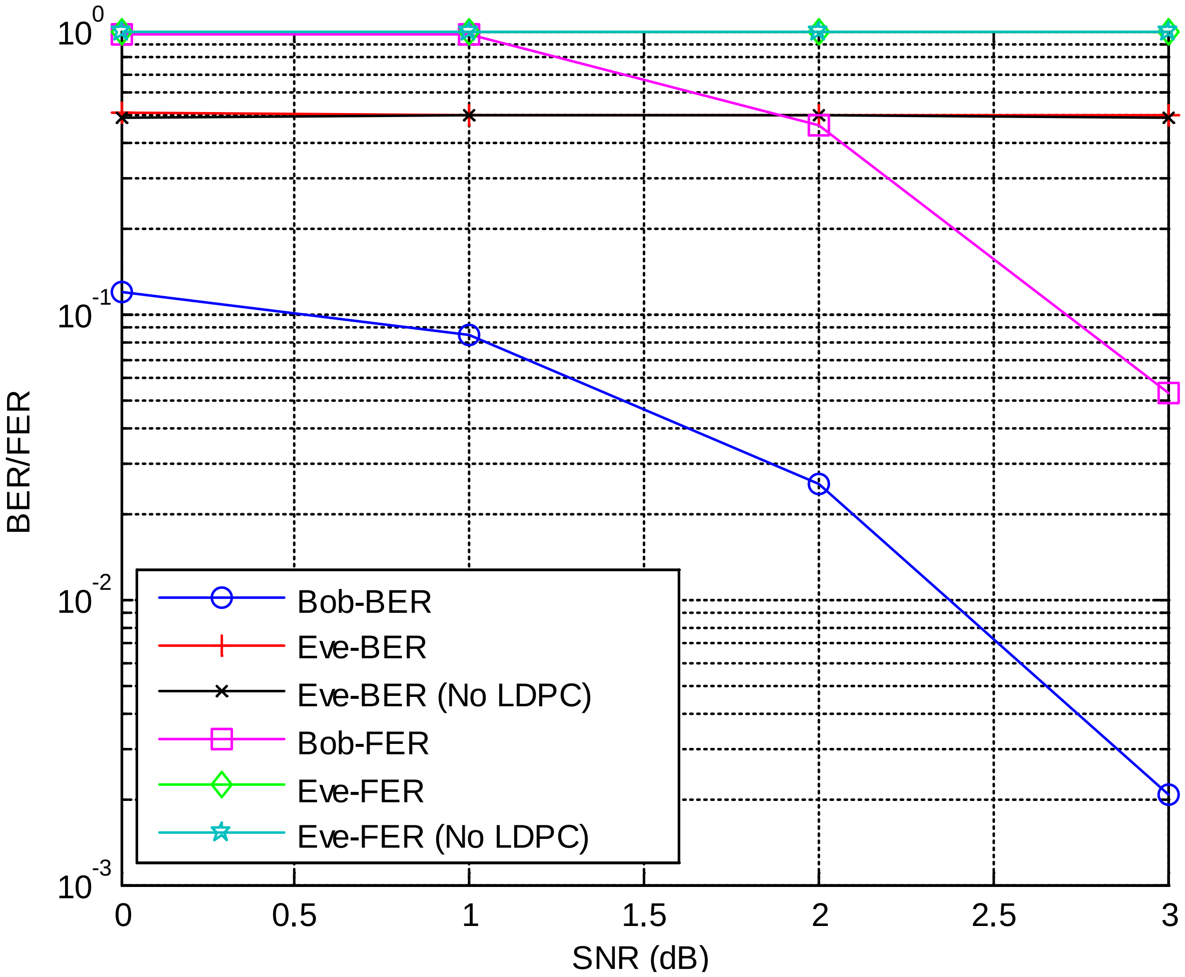


SER vs. SNR for QPSK



BER/FER vs. SNR

*Assumed Eve uses a LDPC decoder

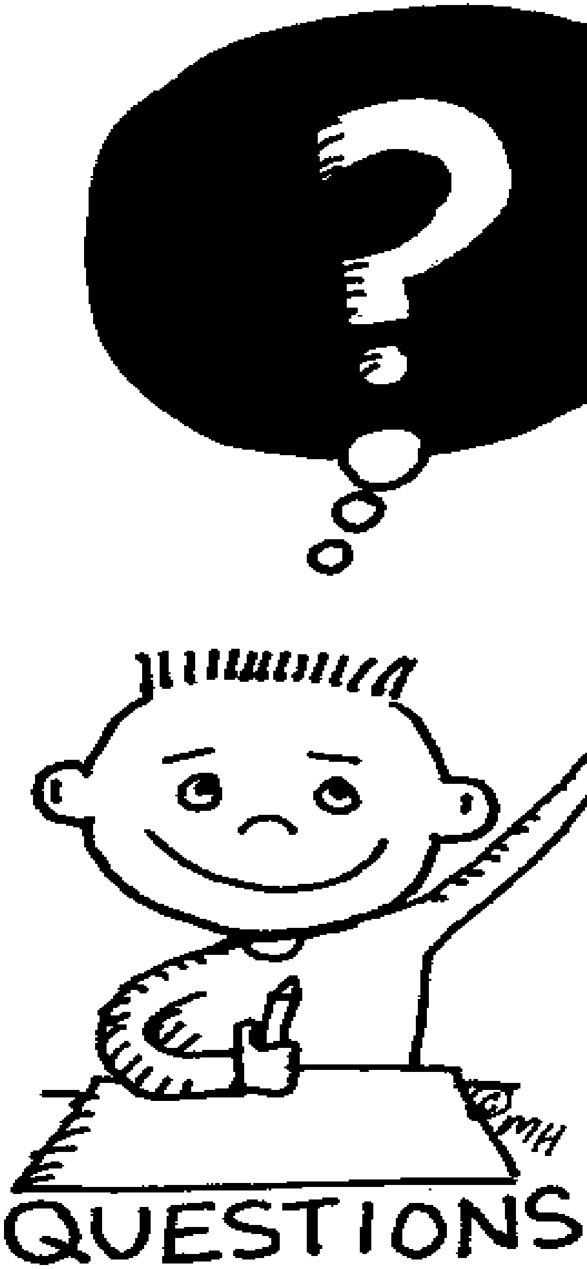


Conclusions

- We proposed a joint encryption, error correction and modulation scheme.
- It provides security and error correction at the physical layer.
- It utilizes a random mapping scheme in order to degrade Eve’s communication channel.
- It does not compromise the full error correcting capability.
- It has the potential of reducing the key size of McEliece-like schemes.

References

[1] M. Healy, T. Newe, and E. Lewis, “Analysis of hardware encryption versus software encryption on wireless sensor network motes,” in *Smart Sensors and Sensing Technology*, ser. Lecture Notes in Electrical Engineering, vol. 20. Springer Berlin Heidelberg, 2008, pp. 3–14.
[2] O. Adamo and M. R. Varanasi, “Joint scheme for physical layer error correction and security,” in *ISRN Journal of Communications and Networking*, 2011.
[3] R. J. McEliece, “A public-key cryptosystem based on algebraic coding theory,” DSN Progress Rep., Jet Propulsion Laboratory, Pasadena,CA, Tech. Rep., 1978.
[4] T. Hwang and T. R. N. Rao, “Secret error-correcting codes (secc),” in *Proc. of Crpto’88*, 1988, pp. 540–563.
[5] M. Baldi and F. Chiaraluce, “Cryptanalysis of a new instance of McEliece cryptosystem based on QC-LDPC codes,” in *IEEE ISIT*, pp. 2591-2595, 2007.
[6] C. Park, “Improving code rate of McEliece’s public-key cryptosystem,” in *Electron Letter*, vol. 25, 1989, pp. 1466–1467.
[7] A. D. Wyner, “The wire-tap channel,” *Bell System Technical Journal*, vol. 54, pp. 1355–1387, 1975.
[8] W. Leng, L. S. C. Xu, and X. Zhang, “Applications of modulation in a McEliece-like symmetric-key scheme,” in *IEEE 71st Vehicular Technology Conference (VTC 2010-Spring*, ser. Lecture Notes in Computer Science, Springer-Verlag, 2010, pp. 1–4.
[9] L. Ozarow and A. D. Wyner, “Wire-tap channel II,” *ATT Bell Laboratories technical journal*, vol. 63, pp. 2135-2157, 1984.
[10] I. Csiszar and J. Korner, “Broadcast channels with confidential messages,” *IEEE Trans. on Info. Theory*, vol. 24, no. 3, pp. 339–348, 1978.
[11] S. K. Leung-Yan-Cheong and M. E. Hellman, “The Gaussian wire-tap channel,” in *IEEE Transactions on Information Theory*, vol. 24, no. 4, pp. 451-456, 1978.
[12] M. Baldi, F. Chiaraluce, R. Garello, and F. Mininni, “Quasi-cyclic lowdensity parity-check codes in the McEliece cryptosystem,” *IEEE ICC*, pp. 951-956, 2007.
[13] A. A. S. Afshar, T. Eghlidos, and M. R. Aref, “Efficient secure channel coding based on quasi-cyclic low-density parity-check codes,” in *IET Communications*, vol. 3, no. 2, 2009, pp. 279-292.



THANKS!