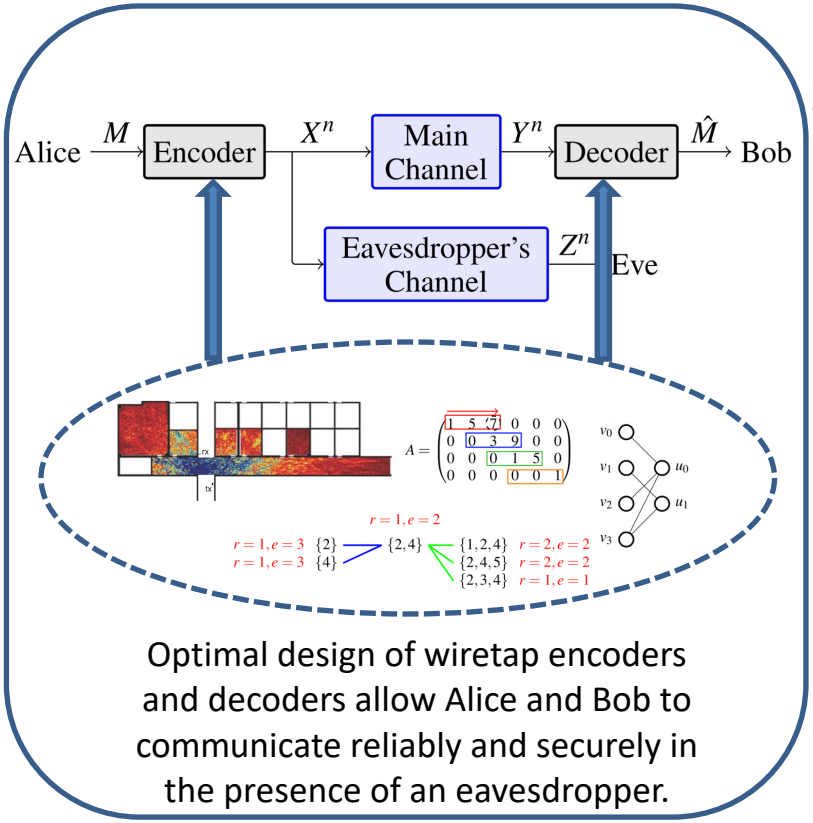
CIF: Small: Best Wiretap Codes for Real-world Physical-layer Security

Challenge:

- Find and design new *optimal* wiretap coding structures for discrete memoryless communication models and more realistic models of communication channels (e.g., Gaussian and fading).



Optimal design of wiretap encoders and decoders allow Alice and Bob to communicate reliably and securely in the presence of an eavesdropper.

Solution:

- Technical Approach: find best codes for various channels, categorize codes according to security/reliability measures, investigate the effects of practical elements.
- Key Innovations: coset codes from Hamming/simplex families are locally optimal, dual codes have strong relationships, scatterers such as pedestrian traffic can help.

Award #1910812, PI: Willie Harrison, Brigham Young University

Scientific Impact:

- Wiretap codes achieve security through the physical layer of a communications system and can enhance existing systems.
- Currently known code constructions satisfy information theoretic security measures as blocklength tends to infinity in the code design. The results from this project deal with finite blocklength codes.

Broader Impact and Broader Participation:

- All wireless communication systems can be strengthened by application of optimal wiretap codes.
- Wiretap codes could be included in future wireless standards.
- The project recruits women undergraduate researchers through WE@BYU (Women in Engineering at BYU) and BYU IMMERSE programs.