CIF: Small: Best wiretap codes for real-world information-theoretic security

Willie Harrison, Brigham Young University

https://icelab.byu.edu/research-projects

Scan for video presentation

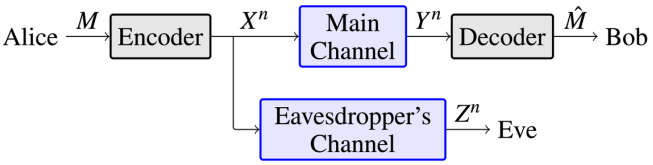


Figure 1: Wiretap channel model.

Table 1: Code table for $n = 4$, $n - k = 2$ secrecy code.

Coset		$M' = 0$	$M' = 1$	$M' = 2$	$M' = 3$
$\mathcal{C}_0$	$M = 0$	0000	0011	1101	1110
$\mathcal{C}_1$	$M = 1$	1000	1011	0101	0110
$\mathcal{C}_2$	$M = 2$	1001	1010	0100	0111
$\mathcal{C}_3$	$M = 3$	0001	0010	1100	1111

Problem Description:

- This project seeks to find/design best wiretap codes that provide reliable communications between Alice and Bob, and keep secrets as measured by the equivocation

$$\mathbb{H}(M|Z^n) = \sum_{z^n \in \mathcal{Z}^n} p(z^n)\mathbb{H}(M|Z^n = z^n)\,.$$

- Encoder function: $x = \begin{bmatrix} m' & m \end{bmatrix} \begin{bmatrix} G \\ G' \end{bmatrix}$.
- Decoder: recover the message.

- Equivocation is given by

$$\begin{aligned}\mathbb{H}(M|Z^n) &= \sum_{z^n \in \mathcal{Z}^n} p(z^n)\mathbb{H}(M|Z^n = z^n) \\ &= \sum_{z^n \in \mathcal{Z}^n} p(z^n)\left[\mathbb{H}(M) - \mu_z + \operatorname{rank}(G_{\mu_z})\right] \\ &= \sum_{\mu=0}^{n} \sum_{i^n \in \mathcal{I}_\mu} (1-\varepsilon)^{\mu}\varepsilon^{n-\mu}\left[k - \mu + \operatorname{rank}(G_{\mu_i})\right].\end{aligned}$$

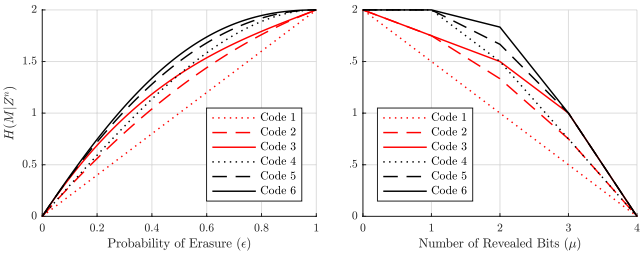
- Thus, we are looking for encoders that maximize

$$\sum_{i \in \mathcal{I}_\mu} \operatorname{rank}(G_{\mu_i})$$

for all μ.

Approach:

- Identify/prove characteristics of best codes.
- Classify families of codes.
- Improve code design to enhance security in wireless communication systems.
- Start with simple channel models and progress to more complex/real-world cases.



Broader Impact (technical):

- Wiretap coding could enhance secrecy in new telecommunications standards.
- Need to understand finite blocklength code limitations and benefits.
- Knowledge of best codes informs engineering design.

Broader impact (outreach):

- BYU IMMERSE
- Women in Engineering at BYU (WE@BYU)
- BYU Engineering Together (BE Together)
- Subgroup approach to including undergrads in information-theoretic research (REU).