Capacity of a Binary Channel with a Time-Bounded Adversary

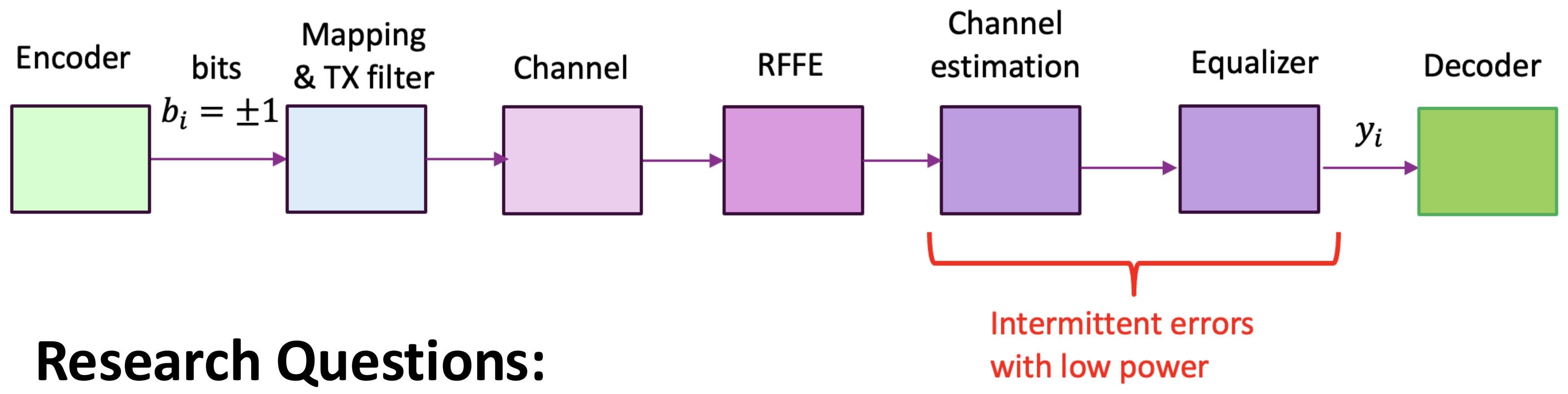
Mingjun Ying, Fatih Berkay Sarpkaya, Serhat Bakirtas, Elza Erkip, Theodore S. Rappaport, and Sundeep Rangan
{yingmingjun, f.sarpkaya, srangan}@nyu.edu
NYU Tandon School of Engineering · NYU WIRELESS

Asilomar Conference on Signals, Systems, and Computers 2024

1. Intermittent Wireless Vulnerabilities

- ❑ In adversarial scenarios, **the receiver's processing can be intermittently compromised**.
  - jamming, hardware Trojans, …
- ❑ This may happen due to:
  - **hardware errors**, **power-saving techniques**, …

Decoding with Intermittent Errors



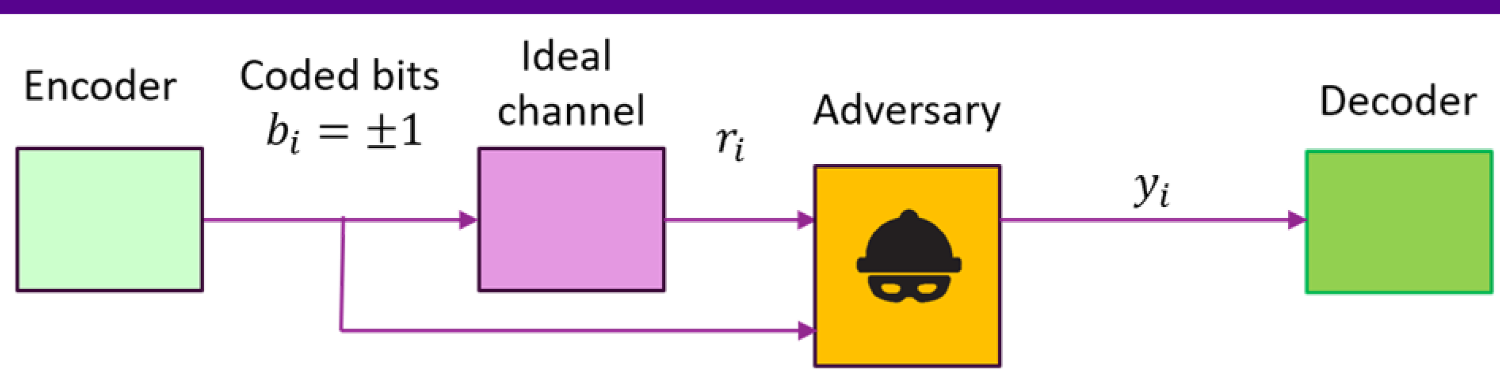
Research Questions:

→ What is the capacity under intermittent errors?

→ How do we design the decoder to make it robust to errors?

Main Contribution is the **derivation of the worst-case adversarial capacity** for a binary input memoryless channel **under the influence of such a time-bounded adversary.**

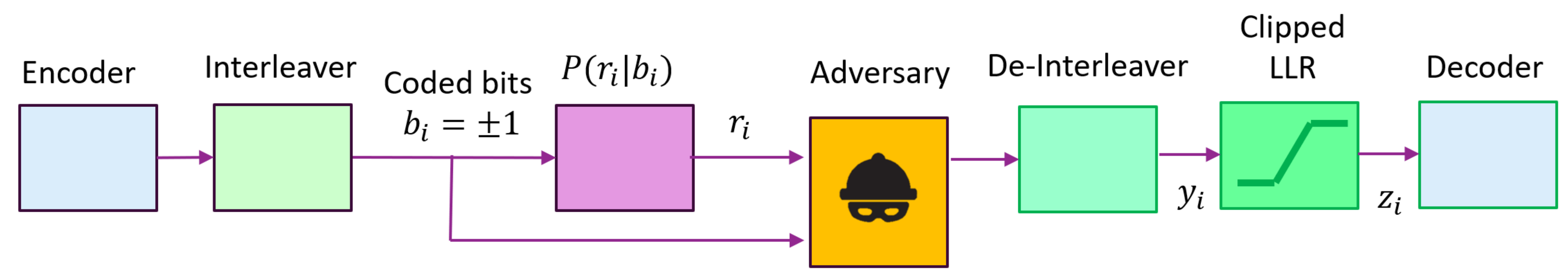
2. Worst-Case Adversarial Model



- $P(r_i|b_i)$: Known channel with no errors;
- Adversary $y_i = Q_i(\boldsymbol{r}, \boldsymbol{b})$ with $P(y_i \neq r_i) \leq \delta$:
  - Adversary is **arbitrary**, but **time-bounded**
  - Adversary is **not known** to the decoder
  - The adversary has knowledge of the transmitted codeword and received symbols, but **not the shared randomness** (the shared randomness [1] allows the transmitter and receiver to randomly interleave)

3. Main Idea

❑ **Interleave** + **LLR Clipping**



- **Randomly interleave** and de-interleave:
  - Unknown to adversary (i.e., shared randomness);
  - Compute LLR for ideal channel:

$$z_i' = \log \frac{P(y_i|b_i = 1)}{P(y_i|b_i = -1)}$$

- **Clip LLR**: $z_i = T_t(z_i')$ and decode as usual:

$$\widehat{\boldsymbol{b}} = \max_{\boldsymbol{b} \in \mathcal{C}} \sum_i b_i z_i$$

- **Intuition**: Clipping LLR limits damage from adversary:

$$\phi_t(y) = \begin{cases} t & z_i' > t \\ z_i' & -t \leq z_i' \leq t \\ -t & z_i' < -t \end{cases}$$

4. Minimax Optimality

Fix error rate δ and true channel $P(r|b)$

Achievability

❑ There exists a threshold t and C_0 such that:

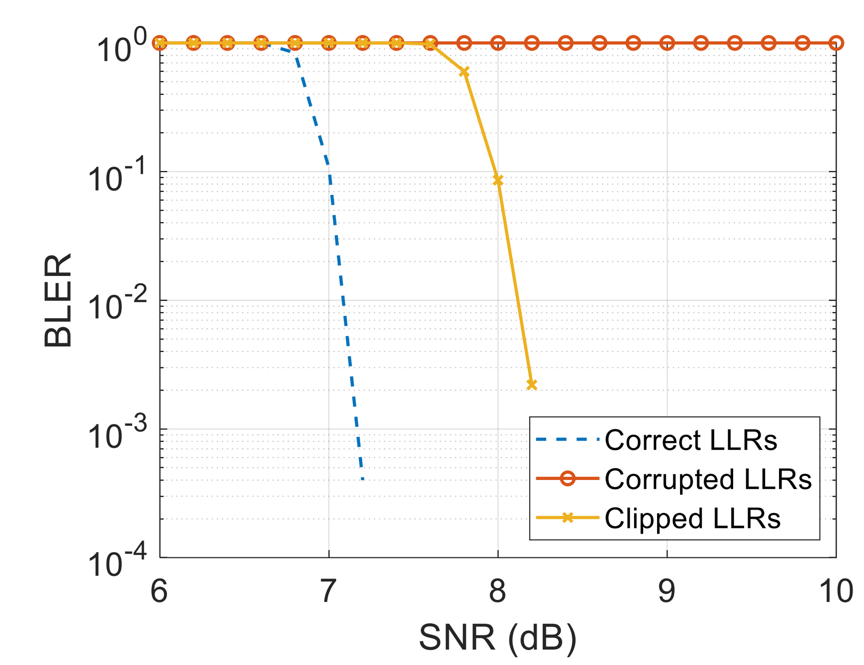
- Any rate $R < C_0$ is achievable for all adversaries;
- Adversary may be any, even non-causal, function;
- Can be achieved with LLR clipping and interleaving;
- Idea is readily implementable with existing decoders.

Converse

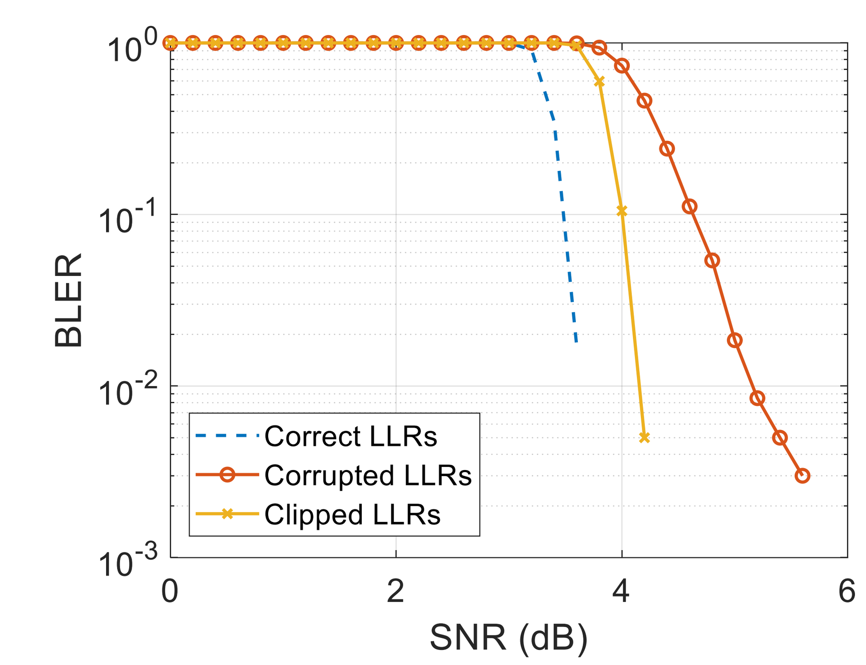
❑ There exists a memoryless adversary s.t. capacity $= C_0$.

5. Simulation Results

- ❑ **BLER for LDPC code [2]** (Code rate 1/3, 64 QAM)
  - Correct LLRs (i.e., no adversary)
  - Corrupted LLRs (worst-case adversary, no thresholding)
  - Clipped LLRs (minimax optimum)
- ❑ 5% corruption is assumed. (δ = 0.05)
- ❑ **Clipping the LLRs provides improved robustness.**



5G NR LDPC BG1 (K =8448)



5G NR LDPC BG2 (K =3840)

6. Conclusions

- ❑ Our work provide an **exact characterization** of the capacity **in the presence of a time-bounded adversary.**
- ❑ Optimal capacity achievable with simple modifications to existing decoders (clipped LLRs + interleaving)
- ❑ Shared randomness is essential
- ❑ Simulations on a real LDPC code
- ❑ Future applications:
  - Jammers with frequency hopping
  - Low-power circuits with intermittent errors

7. References

[1] A. D. Sarwate, "Coding against myopic adversaries," in 2010 IEEE Information Theory Workshop. IEEE, 2010, pp. 1–5.

[2] 3GPP, "Multiplexing and channel coding (Release 15)," 3GPP TR 38.212 V15.2.0 (2018-07), pp. 1 –101, July 2018.