CERIAS 2020
Annual Security Symposium ★ September 29 & 30
Purdue University, West Lafayette, Indiana

PURDUE UNIVERSITY Discovery Park

A Characterization of the Deterministic Capacity of a Channel with an Active Eavesdropper

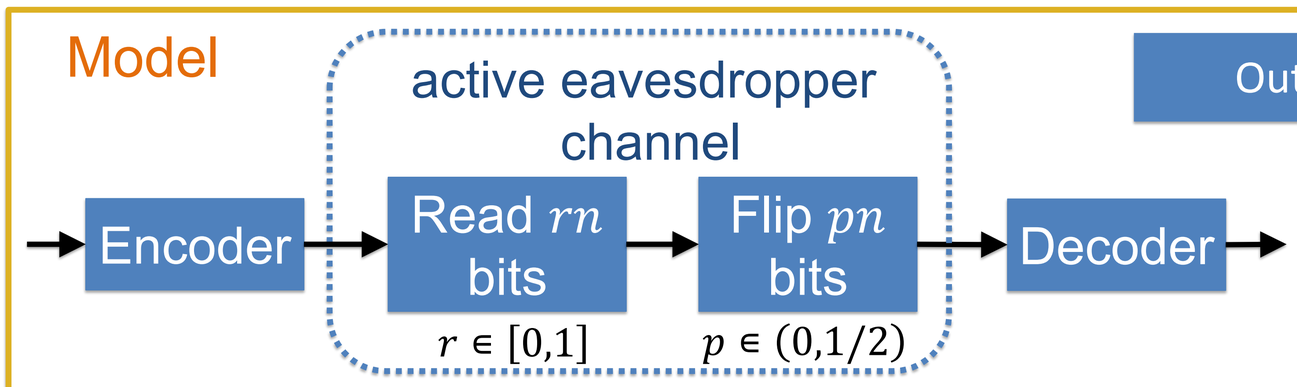
Eric Ruzomberka and David J. Love

School of Electrical and Computer Engineering, Purdue University

Overview

We investigate a family of channels in which an active eavesdropper may read and flip a fraction of transmitted bits. This active eavesdropper channel is sometimes referred to as a limited view (LV) adversarial channel [1]. We characterize the capacity of the channel family in a *deterministic* setting, i.e., when no private randomness is shared between the encoder and decoder.

Model



Outline

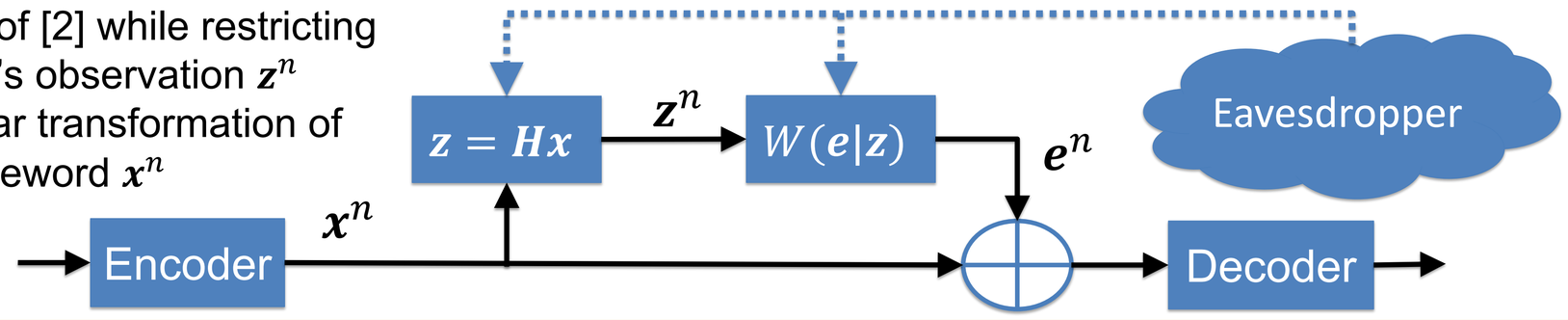
1. Encoder transmits codeword of n bits
2. Eavesdropper chooses rn bits to read
3. Eavesdropper chooses pn bits to flip based on read bits

- **Deterministic**: Eavesdropper knows encoder's codebook

Method

Goal: Find capacity C_r of active eavesdropper channel

Apply the method of [2] while restricting eavesdropper's observation $\boldsymbol{z}^n$ to a rank rn linear transformation of of codeword $\boldsymbol{x}^n$



Results & Conclusions

Capacity

Consider values of $r \in [0,1]$ partitioned into 3 regions

Key

C_r := capacity of active eavesdropper channel

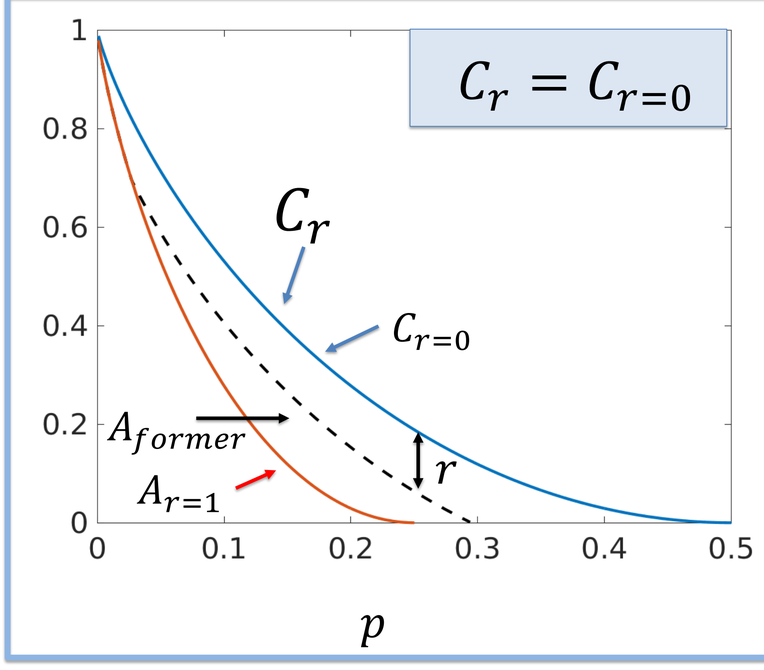
A_r := lower bound on achievable rate of eavesdropper channel

A_{former} := former largest known lower bound on achievable rate [2]

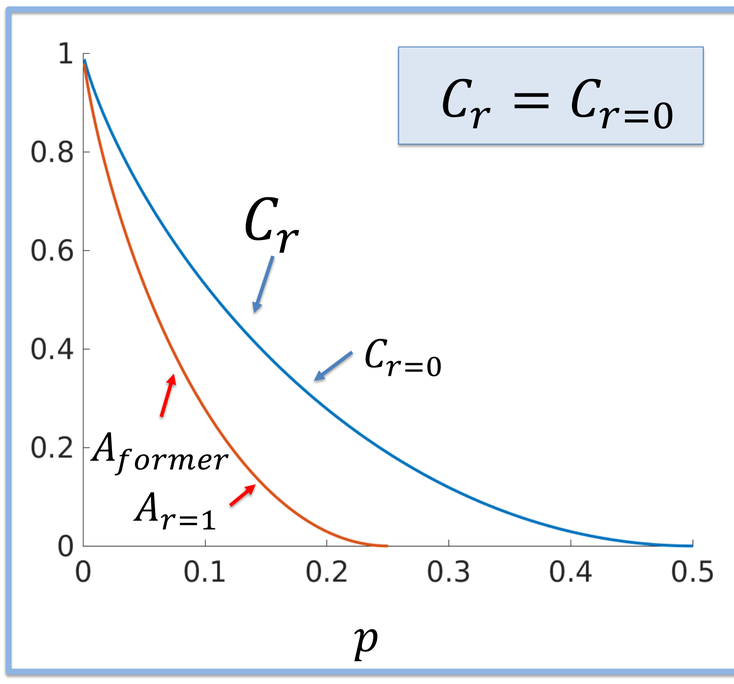
Capacity $C_{BSC(p)}$ of binary symmetric channel (w/ parameter p)

Gilbert-Varshamov Bound

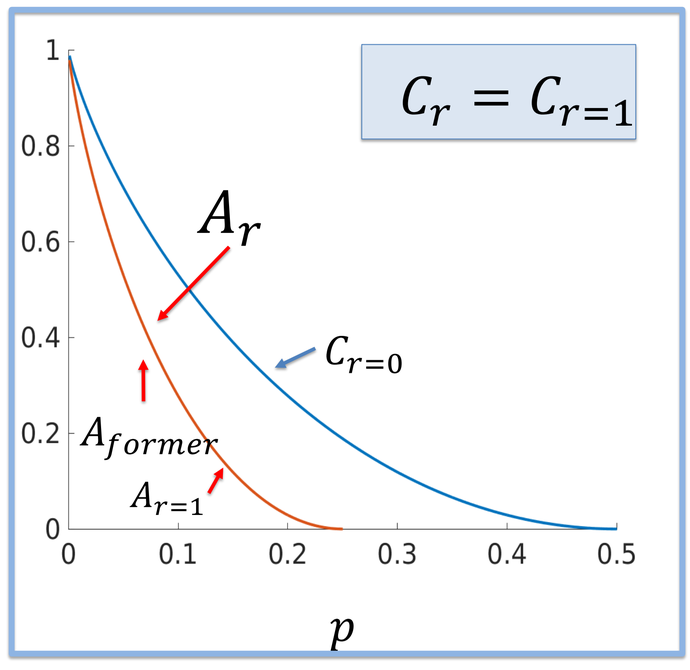
If $r \in [0, C_{BSC(p)}/3)$



If $r \in [C_{BSC(p)}/3, C_{BSC(p)})$



If $r \in [C_{BSC(p)}, 1]$



Eavesdropper's Optimal Strategy

- When r is large, decode codeword and push to nearest neighbor
- When r is small, pick flipped bits randomly (independent of codebook/codeword)
- Always pick readable bits randomly (independent of codebook)

Takeaway

A little eavesdropper uncertainty (i.e., $r < 1$) can dramatically expand the achievable rate region

Ref

[1] Wang and Safavi-Naini, "Limited view adversary codes: bounds, constructions and applications" ICITS 2015
[2] Langberg, "Oblivious communication channels and their capacity", IEEE TOIT 2008

This work was supported by Sandia National Laboratories. Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia LLC, a wholly owned subsidiary of Honeywell International Inc. for the U.S. Department of Energy National Nuclear Security Administration under contract DE-NA0003525. SAND2020-10202 C