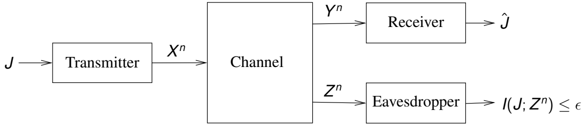
Strong Secrecy in Arbitrarily Varying Wiretap Channels

I. Bjelaković, H. Boche and J. Sommerfeld

Lehrstuhl für theoretische Informationstechnik
Technische Universität München

September 7, 2012

Wiretap channel - Basic Model



input alphabet A, output alphabets B, C (finite sets)

two communication links:

- channel to the legitimate receiver: $W : A \to \mathcal{P}(B)$
- channel to the eavesdropper: $V : A \to \mathcal{P}(C)$

wiretap channel $\mathfrak{W} := (W, V)$

a (n, J_n) wiretap code $\mathcal{C}_n$

- message set $\mathcal{J}_n = \{1, \ldots, J_n\}$, $|\mathcal{J}_n| = J_n$
- stochastic encoder E: $\mathcal{J}_n \to \mathcal{P}(A^n)$
- disjunct decoding sets $\{D_j \subset B^n : j \in \mathcal{J}_n\}$ at the legitimate receiver

Secure Transmission

Achievable secrecy rates R_S

$$\liminf_{n\to\infty} \frac{1}{n} \log J_n \geq R_S \quad ,$$

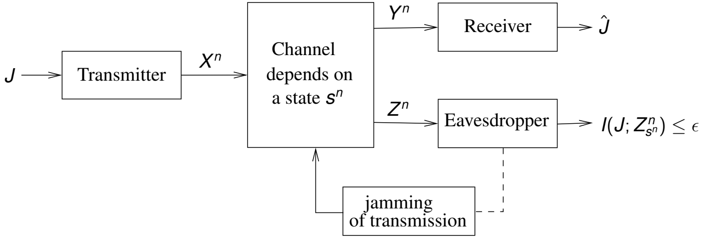
$$\lim_{n\to\infty} e(\mathcal{C}_n) = 0 \quad \text{and} \quad \lim_{n\to\infty} I(J; Z^n) = 0$$

with

- $e(\mathcal{C}_n)$ the average error probability of the channel to the legitimate receiver W^n
- $I(J; Z^n)$ as a measure of (strong) secrecy against the eavesdropper.

Strong secrecy guarantees that the average error probability of every decoding strategy at the eavesdropper tends to one.

Arbitrarily Varying Wiretap Channels



Arbitrary and unknown channel fluctuations described by an AVC

Arbitrarily varying wiretap channels AVWC modelling certain attach classes (eavesdropping, jamming)

AVWC $\mathfrak{W} := \{(W^n_{s^n}, V^n_{s^n}) : s^n \in S^n\}$, $s \in S$ denotes the channel state.

Common randomness assisted wiretap codes results in a dichotomy similar to Ahlswede's dichotomy for ordinary AVCs.

Theorem

1. *Assume that for the AVWC $\mathfrak{W}$ it holds that $C_{S,\mathrm{ran}}(\mathfrak{W}) > 0$. Then the secrecy capacity $C_S(\mathfrak{W})$ equals its random code secrecy capacity $C_{S,\mathrm{ran}}(\mathfrak{W})$,*

$$C_S(\mathfrak{W}) = C_{S,\mathrm{ran}}(\mathfrak{W}), \tag{1}$$

   if and only if the channel to the legitimate receiver is non-symmetrisable.
2. *If $C_{S,\mathrm{ran}}(\mathfrak{W}) = 0$ it always holds that $C_S(\mathfrak{W}) = 0$.*

$\longrightarrow$ Importance of characterization of $C_{S,\mathrm{ran}}(\mathfrak{W})$ under a strong secrecy constraint