Wyner’s Wiretap Channel [1]

\[
S_x \in S, \\
|S| = 2^N
\]

Alice Encoder

\[
W_{ki}: X \rightarrow Y
\]

Bob’s Decoder

\[
W_k: X \rightarrow Z
\]

\begin{itemize}
  \item Alice wants to communicate \(nR\) bits of secret message \(S_x\) to Bob, reliably through the communication channel \(W_{ki}: X \rightarrow Y\), while concealing the message from Eve using i.i.d. random codes for the wiretap channel \(W_k: X \rightarrow Z\), where
  \[\lim_{n \to \infty} \Pr(S_x \neq S_y) = 0,\]
  
  \item For any input distribution \(P_x\), any message rate \(R < I(X;Y) - I(X;Z)\) is achievable under weak [1, 2] or strong [3] secrecy criteria.
\end{itemize}

Achievability via Random Binning and Channel Resolvability

\begin{itemize}
  \item Divide a (random) code of rate \(R + R_i\) into \(2^{nR_i}\) bins of size \(2^{nR_i}\).
  \item To communicate \(x_s\), transmit a randomly chosen codeword from the \(s^{th}\) row.
  \item Reliability: If \(R + R_i < I(X;Y)\), Bob can decode the sent codeword (hence the bin index).
  \item Secrecy via Channel Resolvability: For any distribution \(\Phi_0\) on \(Z^0\),
  \[I(S_x;Z^0) = D(P_{Z|X}(x)\Phi_0|P_{Z|X}|D(P_{Z|X}(x)\Phi_0|P_{Z|X}) \leq D(P_{Z|X}(x)\Phi_0|P_{Z|X}).\]
  
  (1)
  
  Once \(R > I(X;Z)\),
  \[D(P_{Z|X}(x)\Phi_0|P_{Z|X}) = 0\]
  
  (2)
  
  Where \(\Phi_0(x) = \sum P_{Z|X}(z|x)W^0_k(z|x)\) with \(P_{x}\) being the code sampling distribution [4, 5].
  
  Hence, \(Z^0\) is almost independent of \(S_x\).
  
  Intuitive Reason:
  \[P_{Z|x}(z|x) = \frac{1}{2^n} \sum_{s=1}^{2^n} W^0_k(z|x)\]
  \[\text{an i.i.d. sum}\]
  
  So \(P_{Z|x}(z|x) = \Pr(W^0_k(z|x)) = \Phi_0(z)\text{ as } n \to \infty.\]
\end{itemize}

\textbf{How fast \(I(S_x;Z^0)\) vanishes?}

\begin{itemize}
  \item Using i.i.d. random codes for the wiretap channel \(I(S_x;Z^0)\) decays exponentially fast in \(n\).
  \item Indeed (see [6, 7]), for every \(x\),
  \[\lim_{n \to \infty} \frac{1}{n} \log D(P_{Z|x}(x)\Phi_0) \geq \epsilon^{I(k)}(P_x, W_k, R)\]
  
  where \(\epsilon(I)\) is over the random coding ensemble and
  \[E^{I(k)}(P_x, W_k, R) = \min \{D(\epsilon|x)\Phi_0|P_{Z|x})\}
  
  and
  \[\epsilon|x) := \frac{1}{n} \log \frac{W_{ki}(x)}{P_{ki}(x)}\]
  
  Hence, (1) (together with the linearity of expectation) yields
  \[\lim_{n \to \infty} \frac{1}{n} \log D(P_{Z|x}(x)\Phi_0) \geq \epsilon^{I(k)}(P_x, W_k, R).
  \]
  \[E^{I(k)}\text{ is an achievable secrecy exponent.}\]
  \end{itemize}

\textbf{Exact Secrecy Exponent [9]}

\begin{itemize}
  \item The exponent of (3) is the \textit{exact} random coding secrecy exponent for the ensemble, \[\lim_{n \to \infty} \frac{1}{n} \log D(P_{Z|x}(x)\Phi_0) = E^{I(k)}(P_x, W_k, R).
  \]
  \item In other words, \(E^{I(k)}\) characterizes the exact exponential decay rate of \(I(S_x;Z^0)\) when an average code in the ensemble is used for communication.
\end{itemize}