Encoding Individual Source Sequences for the Wiretap Channel

Neri Merhav

The Viterbi Faculty of Electrical and Computer Engineering

Technion – Israel Institute of Technology

Haifa 3200003, Israel

ISIT 2022, Aalto University, Espoo, Finland, June–July 2022

Objectives

- ♠ Fundamental limits for transmitting individual sequences over the WTC.
- ♠ Fundamental limits on the amount of local randomness at the encoder.
- ♠ Extension: side info at the decoder with leakage to the wiretapper.

Related Work

The WTC

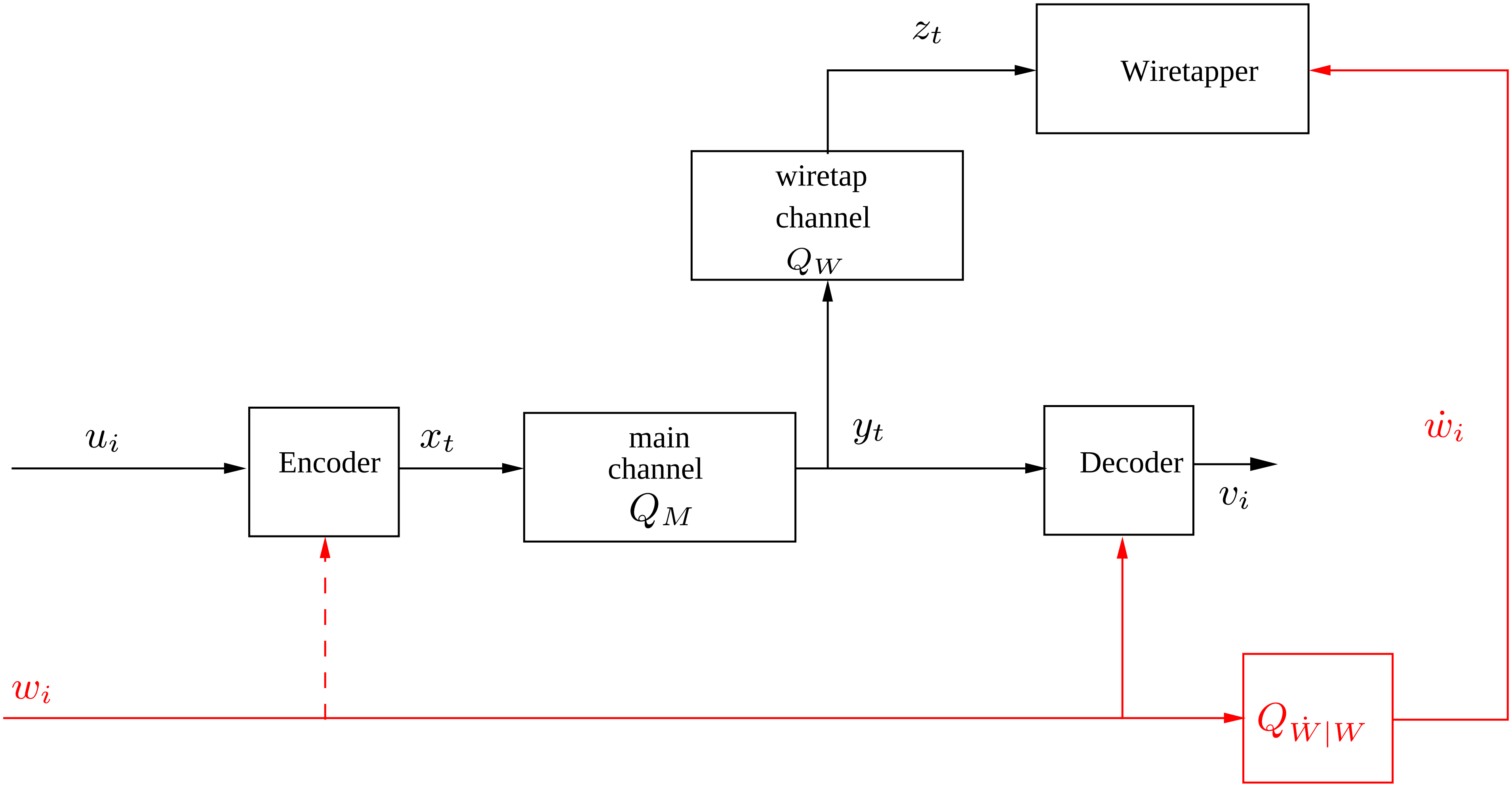
- ♣ Wyner (1975): degraded BC; secrecy capacity.
- ♣ Csiszár & Korner (1978): general broadcast channels.
- ♣ Leung-Yan-Cheong & Hellman (1978): The Gaussian WTC.
- ♣ Ozarow & Wyner (1985): WTC type II.
- ♣ Yamamoto (1989): secret sharing with two channels.
- ♣ Yamamoto (1997): rate–distortion + private key.

. . . .

Individual Sequences

- ♣ Ziv (1978): coding thms for individual sequences.
- ♣ Ziv (1980): rate-distortion for individual sequences.
- ♣ Ziv (1984): same + side info.
- ♣ Merhav (2013): encryption for individual sequences.
- ♣ Merhav (2014): data processing thms for individual sequences.

The Model


z_t
Wiretapper
wiretap
channel
Q_W
u_i
Encoder
x_t
main
channel
Q_M
y_t
Decoder
v_i
$\dot{w}_i$
w_i
$Q_{\dot{W}|W}$

The Model (Cont'd)

Finite–state stochastic encoder

$$\Pr\{X_{im+1}^{im+m} = x^m | u_{ik+1}^{ik+k} = u^k,\ s_i^e = s\} = P(x^m|u^k, s), \quad i = 0, 1, 2, \ldots$$

$$s_{i+1}^e = h(u_{ik+1}^{ik+k}, s_i^e) \quad i = 0, 1, 2, \ldots$$

Finite–state decoder

$$\begin{aligned} v_{ik+1}^{ik+k} &= f(y_{im+1}^{im+m}, s_i^d) \\ s_{i+1}^d &= g(y_{im+1}^{im+m}, s_i^d). \end{aligned}$$

$$|\mathcal{S}^e| = q_e, \quad |\mathcal{S}^d| = q_d$$

The bandwidth expansion factor (BEF):

$$\lambda = \frac{m}{k}.$$

System Requirements

Reliability

$$P_b \triangleq \frac{1}{k}\sum_{i=1}^{k} \mathrm{Pr}\{V_i \neq u_i\} \leq \epsilon_r$$

Security

$$\max_{\mu} I_{\mu}(U^n; Z^N) \leq n\epsilon_s, \qquad N = n\lambda$$

Lempel-Ziv (LZ) Complexity

The incremental parsing procedure sequentially parses u^n into distinct phrases, such that each new phrase is the shortest string that has not been obtained before as a phrase.

Let $c(u^n)$ denote the number of resulting phrases. For example, if

$$u^{10} = (0000110110)$$

then incremental parsing yields

$$(0, 00, 01, 1, 011, 0)$$

and so, $c(u^{10}) = 6$.

We define the LZ complexity of u^n, as

$$\rho_{LZ}(u^n) \triangleq \frac{c(u^n) \log c(u^n)}{n}$$

Converse Bound

Theorem: If $\exists$ stochastic encoder with q_e states and a decoder with q_d states that satisfy the reliability constraint and the security constraint, then

$$\lambda \geq \frac{\rho_{LZ}(u^n) - \Delta(\epsilon_r) - \epsilon_s - \zeta_n(q_d, k)}{C_s}, \tag{1}$$

where

$$\Delta(\epsilon_r) \stackrel{\triangle}{=} h_2(\epsilon_r) + \epsilon_r \cdot \log(\alpha - 1), \tag{2}$$

and

$$\zeta_n(q_d, k) \to 0$$

for fixed q_d and k.

Discussion

- Irrelevance of q_e.
- Decay rate of $\zeta_n(q_d, k)$ is slow.
- Achievability: V-F LZ compression + channel coding for the WTC.

Minimum Local Randomness

Consider the following representation of the encoder

$$x_{im+1}^{im+m} = a(u_{ik+1}^{ik+k}, s_i^{\mathsf{e}}, b_{ij+1}^{ij+j}),$$

where the b's are purely random bits.

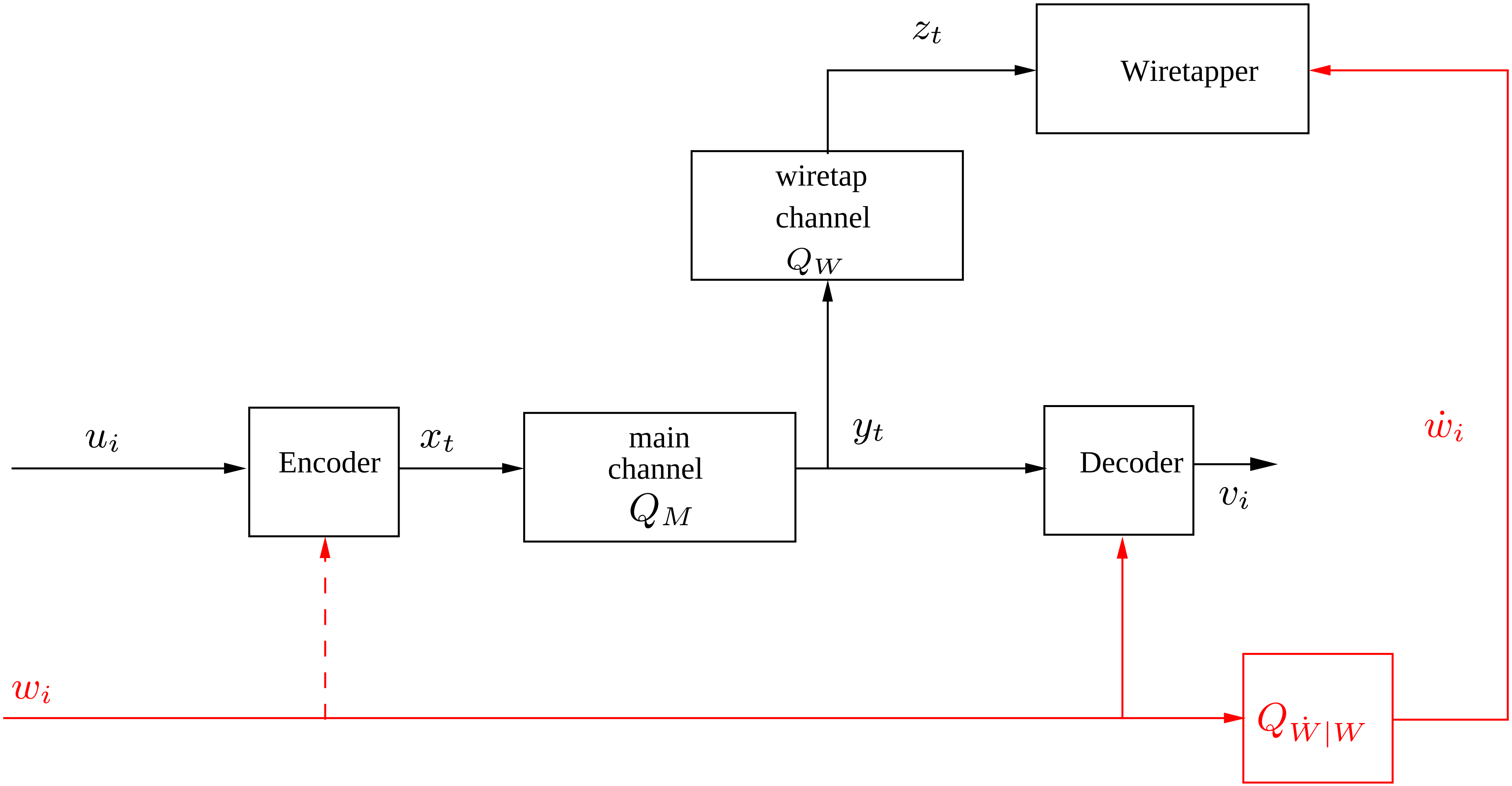
Theorem: Let λ meet the lower bound above. If $\exists$ encoder with q_e states and a decoder with q_d states that satisfy the reliability constraint and the security constraint, then

$$j \geq mI(X^*; Z^*) - k\epsilon_s - \frac{\log q_e}{\ell}$$

where X^* is the random variable that achieves C_s and ℓ is the achiever of $\zeta_n(q_d, k)$.

Wyner's coding scheme achieves this lower bound.

Side Information



Conditional LZ Complexity

$c(u^n, w^n) =$ number of distinct phrases of (u^n, w^n).

$c(w^n) =$ resulting number of distinct phrases of w^n,

$w(l) =$ the l-th distinct w–phrase, $l = 1, 2, ..., c(w^n)$.

$c_l(u^n|w^n) =$ number of distinct u-phrases that jointly appear with $w(l)$.

$$\rho_{LZ}(u^n|w^n) \stackrel{\triangle}{=} \frac{1}{n} \sum_{l=1}^{c(w^n)} c_l(u^n|w^n) \log c_l(u^n|w^n).$$

Achievable Lower Bound

Theorem: If $\exists$ a stochastic encoder with q_e states and a decoder with q_d states that satisfy the reliability constraint and the security constraint, then

$$\lambda \geq \frac{\rho_{LZ}(u^n|w^n) - \Delta(\epsilon_r) - \epsilon_s - \eta_n(q_e \cdot q_d, k)}{C_{\mathsf{s}}}.$$

Discussion

- ♣ Irrelevance of the SI channel $Q_{\dot{W}|W}$. Same as if $\dot{w} = w$.
- ♣ Now depends on q_e too (unless $\dot{w} = w$).
- ♣ Achievability: if $\dot{w}$ is available to the encoder - LZ with SI. Otherwise, needs a little feedback.