Exact Random Coding Exponents for the Wiretap Channel Model: Authorized Decoder and Wiretapper

Neri Merhav

Department of Electrical Engineering

Technion—Israel Institute of Technology

Haifa 32000, Israel

ITA 2015, La Jolla, California, February 1–6, 2015.

Background

- Wyner (1975): the wire-tap channel – rate/equivocation tradeff.
- Extended/modified in many ways (tutorial: Liang–Poor–Shamai, 2009).
- Reliability/secrecy exponents (Chou, Tan, Draper, Hayashi, Matsumoto).
- Constructive coding schemes (Bellare, Tessaro, Vardy, Mahdavifar).
- No earlier work on decoding reliability @ authorized user and wiretapper.

In This Work

- Exact random coding exponents of Wyner's achievability scheme:
  - Wiretapper: correct–decoding exponent.
  - Legitimate user: error exponent.
- Both decoders use optimal bin–index decoding (bin level ML).
- Motivation for studying P_e and P_c:
  - Ordinary performance criterion in communication in general.
  - Wiretapper: secrecy metric for sensitive info (password, acct. #).
  - Legit. user: relevant to superposition coding (GP, relay, IFC, MAC).
  - Extension to the broadcast channel.
- Exact analysis – challenge due to the complicated likelihood score.

Wyner's Achievability Scheme

Given:

- A cascade of two DMC's $P_{Y|X}$ and $P_{Z|Y}$,
- An input assignment P_X,
- A coding rate R,
- A block length n.

Wyner's Achievability Scheme (Cont'd)

Do as follows:

- Select $M_1 = e^{nR_1}$ ($R_1 < I(X;Y)$) codewords $\boldsymbol{X}_m \sim \mathcal{T}(P_X)$.
- Partition to $M = e^{nR}$ bins $\{\mathcal{C}_w\}_{w=0}^{M-1}$ of size $M_2 = e^{nR_2}$, $R_2 = R_1 - R$.
- Reveal all this to all parties.
- For message $0 \leq w < M$, send $\boldsymbol{x}_{wM_2+U}$, $0 \leq U < M_2$ – random.
- Legitimate decoder: $w^*(\boldsymbol{y}) = \arg\max_w P(\boldsymbol{y}|\mathcal{C}_w)$, where

$$P(\boldsymbol{y}|\mathcal{C}_w) = \frac{1}{M_2}\sum_{u=0}^{M_2-1} P(\boldsymbol{y}|\boldsymbol{x}_{wM_2+u}).$$

- Wiretapper: $w^*(\boldsymbol{z}) = \arg\max_w P(\boldsymbol{z}|\mathcal{C}_w)$.

Our goal: evaluating $P_e = \overline{\text{Pr}}\{w^*(\boldsymbol{Y}) \neq W\}$ and $P_c = \overline{\text{Pr}}\{w^*(\boldsymbol{Z}) = W\}$.

The Legitimate User

Main Result for the Legitimate User

Let

$$E_{\mathsf{L}}^*(R_1, R_2) \stackrel{\triangle}{=} -\lim_{n\to\infty} \frac{\ln \Pr\{w^*(\boldsymbol{Y}) \neq W\}}{n}$$

We also consider $\hat{w}(\boldsymbol{Y}) \stackrel{\triangle}{=}$ bin index of $\arg\max_m P(\boldsymbol{y}|\boldsymbol{x}_m)$, and define

$$\hat{E}_{\mathsf{L}}(R_1, R_2) \stackrel{\triangle}{=} -\lim_{n\to\infty} \frac{\ln \Pr\{\hat{w}(\boldsymbol{Y}) \neq W\}}{n}.$$

Our main result on this is the following:

Theorem: $E_{\mathsf{L}}^*(R_1, R_2) = \hat{E}_{\mathsf{L}}(R_1, R_2) = E_{\mathsf{r}}(R_1)$, where $E_{\mathsf{r}}(R_1)$ is the ordinary random coding error exponent

$$E_{\mathsf{r}}(R_1) = \min_{Q_{XY}:\, Q_X = P_X} \{D(Q_{Y|X} \| P_{Y|X} | P_X) + [I_Q(X;Y) - R_1]_+\}.$$

Just a Few Hints on the Proof

Assume $\boldsymbol{x}_0$ was transmitted: $P_e \doteq \mathbf{E}\min\{1, M \cdot \mathrm{Pr}\{P(\boldsymbol{Y}|\mathcal{C}_1) \geq P(\boldsymbol{Y}|\mathcal{C}_0)\}\}$.

$$P(\boldsymbol{y}|\mathcal{C}_w) = \frac{1}{M_2}\sum_{u=0}^{M_2-1} P(\boldsymbol{y}|\boldsymbol{x}_{wM_2+u}) = \frac{1}{M_2}\sum_{Q_{XY}} N_w(Q_{XY})e^{nf(Q_{XY})}.$$

The rest is based on large deviations of the binomial RV's $\{N_w(Q_{XY})\}$:

$$\mathrm{Pr}\left\{\sum_{Q_{XY}} N_w(Q_{XY})e^{nf(Q_{XY})} \geq e^{ns}\right\} \doteq \mathrm{Pr}\left\{\max_{Q_{XY}} N_w(Q_{XY})e^{nf(Q_{XY})} \geq e^{ns}\right\}$$

$$= \mathrm{Pr}\bigcup_{Q_{XY}}\left\{N_w(Q_{XY})e^{nf(Q_{XY})} \geq e^{ns}\right\} \doteq \sum_{Q_{XY}} \mathrm{Pr}\left\{N_w(Q_{XY})e^{nf(Q_{XY})} \geq e^{ns}\right\}$$

$$\doteq \max_{Q_{XY}} \mathrm{Pr}\left\{N_w(Q_{XY}) \geq e^{n[s-f(Q_{XY})]}\right\}$$

Discussion

- Meaning: decoding part of w is as reliable as decoding it completely.
- Expected when $R \approx 0$: bit error exponent = block error exponent.
- Also, for $R \approx 0$, $P(\boldsymbol{y}|\mathcal{C}_w)$ is approx. equivalent to $\max_{\boldsymbol{x}\in\mathcal{C}_w} P(\boldsymbol{y}|\boldsymbol{x})$.
- Not quite trivial for $R > 0$.
- Intuition: fluctuations – more likely to come from few codewords.
- Good news since $\hat{w}$ is easier to implement.
- Universal version: bin index of the MMI message estimator.
- Mismatch: mismatched version of $\hat{w}$ is never worse than that of w^*.
- Extendable to hierarchical ensembles – BC's.

The Wiretapper

Main Result for the Wiretapper

Let $E_{\mathsf{W}}(R_1, R_2)$ denote the correct–decoding exponent of $w^*(\boldsymbol{Z})$.

Theorem:

$$E_{\mathsf{W}}(R_1, R_2) = \min\{E_1, E_2, E_3\},$$

where

$$\begin{aligned}
E_1 &= R_1 - R_2 + \min_{Q_{Z|X}} \{D(Q_{Z|X} \| P_{Z|X} | P_X) : \; I_Q(X;Z) \le R_2\} \\
E_2 &= R_1 + \min_{Q_{Z|X}} \{D(Q_{Z|X} \| P_{Z|X} | P_X) - I_Q(X;Z) : \; R_2 \le I_Q(X;Z) \le R_1\} \\
E_3 &= \min_{Q_{Z|X}} \{D(Q_{Z|X} \| P_{Z|X} | P_X) : \; I_Q(X;Z) \ge R_1\},
\end{aligned}$$

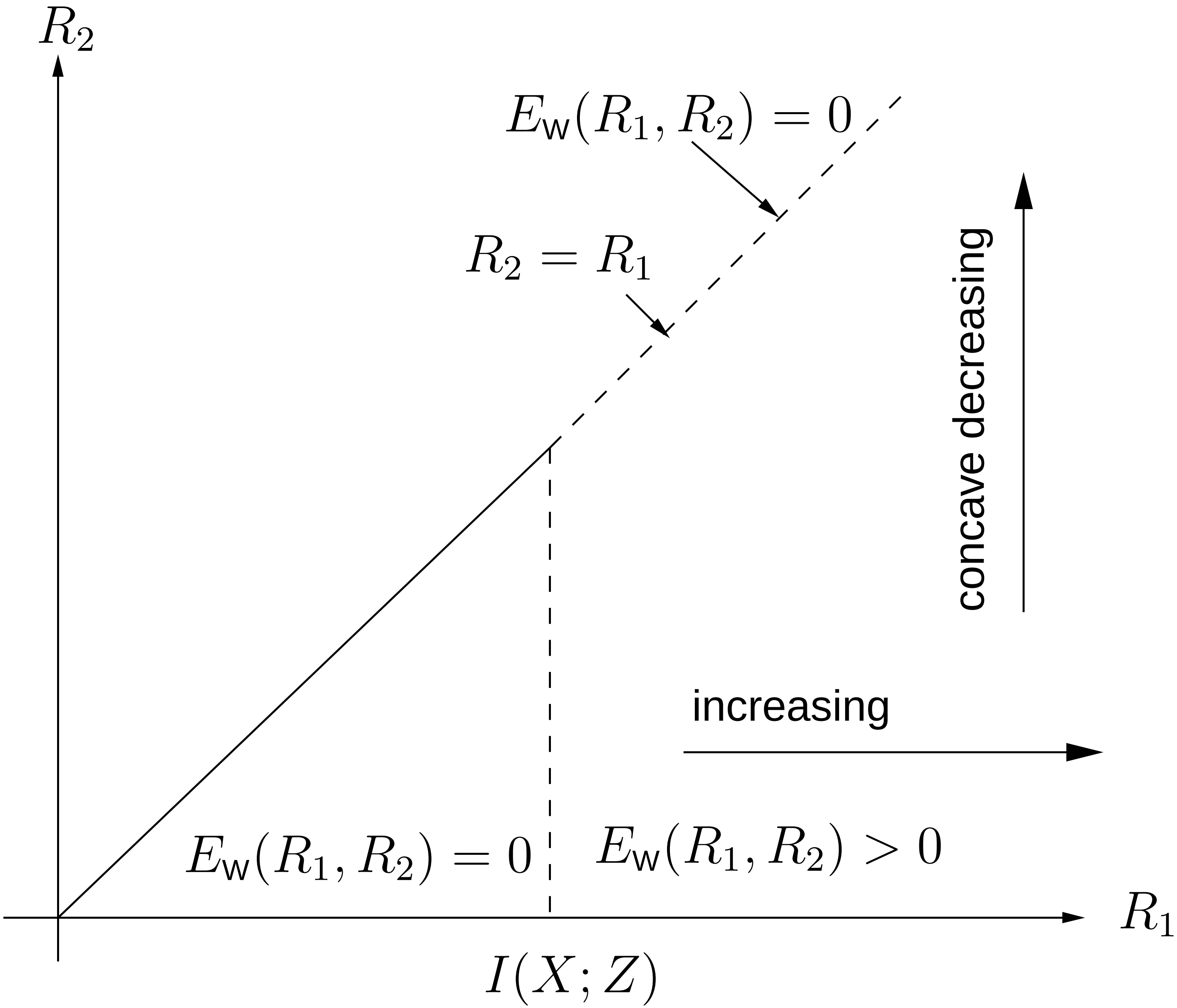
where $Q = Q_{XZ}$ must satisfy the constraint $Q_X = P_X$.

An Alternative Representation of $E_{\mathsf{W}}(R_1, R_2)$

$$E_{\mathsf{W}}(R_1,R_2) = \min_{\lambda_2\in[0,1]} \max_{\lambda_1\in[0,1]} \min_{Q_{Z|X}} \Big\{ D(Q_{Z|X}\|P_{Z|X}|Q_X) + (\lambda_1+\lambda_2-1)I_Q(X;Z) + (1-\lambda_1)R_1 - \lambda_2 R_2 \Big\}$$

A few properties:

- $E_{\mathsf{W}}(R_1, R_2) = 0$ iff $I(X;Z) \geq R_1$ or $R_1 = R_2$.
- Non–decreasing in R_1.
- Non–increasing in R_2.
- Concave in R_2.


R_2
$E_{\mathsf{w}}(R_1, R_2) = 0$
$R_2 = R_1$
concave decreasing
increasing
$E_{\mathsf{w}}(R_1, R_2) = 0$
$E_{\mathsf{w}}(R_1, R_2) > 0$
R_1
$I(X; Z)$

Maximum Secrecy

There exists a region of maximum secrecy, where

$$E_{\mathsf{W}}(R_1, R_2) = E_{\mathsf{blind}}(R_1, R_2) \stackrel{\triangle}{=} R = R_1 - R_2.$$

This region is characterized as follows: Let

$$Q^*_{Z|X} = \text{argmin}[D(Q_{Z|X} \| P_{Z|X} | P_X) - I_Q(X;Z)].$$

Then, maximum secrecy is attained for all (R_1, R_2) such that

$$\max\{I_{Q^*}(X;Z) - D(Q^*_{Z|X} \| P_{Z|X} | P_X), R_1 - E_3(R_1)\} \le R_2 \le I_{Q^*}(X;Z) \le R_1.$$

Comment: At least in this region, $E_{\mathsf{W}}(R_1, R_2)$ is the best exponent as there is an obvious matching converse.

Example

$$E_{\mathsf{W}}(R_1,R_2) = \min_{\lambda_2\in[0,1]}\max_{\lambda_1\in[0,1]}\min_{Q_{Z|X}}\Big\{D(Q_{Z|X}\|P_{Z|X}|Q_X)+$$
$$(\lambda_1+\lambda_2-1)I_Q(X;Z)+(1-\lambda_1)R_1-\lambda_2 R_2\Big\}$$

Let $P_{Z|X}$ be a BSC with crossover probability p and $P_X=(\frac{1}{2},\frac{1}{2})$.

The minimization over $Q_{Z|X}$ can be confined to BSC's as well, and one obtains a Gallager–like expression:

$$E_{\mathsf{W}}(R_1,R_2) = \min_{\lambda_2\in[0,1]}\max_{\lambda_1\in[0,1]}\{(\lambda_1+\lambda_2-1)\ln 2-$$
$$(\lambda_1+\lambda_2)\ln\left[p^{1/(\lambda_1+\lambda_2)}+(1-p)^{1/(\lambda_1+\lambda_2)}\right]+$$
$$(1-\lambda_1)R_1-\lambda_2 R_2\}\,.$$

Summary

- The wiretap channel model from the viewpoint of error exponents.
- Exact analysis for both legitimate user and wiretapper.
- Legitimate user:
  - Same as ordinary random coding exponent at rate R_1.
  - Method: extendable to BC, MAC, IFC (with W. Huleihel), etc.
- Wiretapper:
  - Two representations.
  - Properties.
  - Maximum secrecy.
  - Same analysis method – applicable also to the secrecy exponent.

Thank You!