Proof of the Converse

Pang-Chang Lan

I. Problem Statement and Assumptions

Let's consider a discrete memoryless wiretap channel with perfect CSIT but no CSIRE as shown in Fig. 1. The perfect CSIT is causally available to the transmitter. That is, the encoder knows S^i before transmission i occurs. Let the message set be $\mathcal{M} = \{1, 2, \cdots, 2^{nR}\}$. A $(2^{nR}, n)$ code is used for this setup. The encoder performs $x_i(m, s^i)$ for $i \in [1 : n]$, and the decoder performs $\hat{m}(y^n)$. Note that the function $x_i(\cdot, \cdot)$ is deterministic and fixed before the transmission begins.

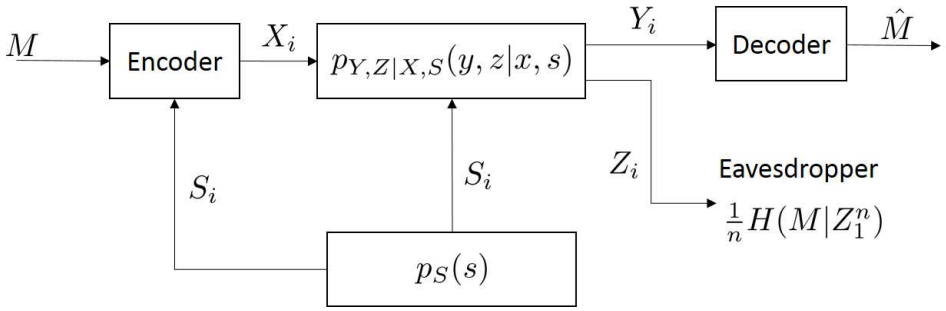

Fig. 1. Discrete memoryless wiretap channel with perfect CSIT but no CSIRE

II. Main Theorem

Theorem 1. *Suppose that the main channel is less noisy than the wiretap channel, i.e., $I(U;Y) \geqslant I(U;Z)$ for all U such that $(U, S) \to (X, S) \to (Y, Z)$ forms a Markov chain. The secrecy capacity of the discrete memoryless wiretap channel with perfect CSIT but no CSIRE is given by*

$$C_s = \max_{p(u)t(u,s),p(x|t,s)} I(T;Y) - I(T;Z) \tag{1}$$

where U is an auxiliary random variable independent of S, $t(\cdot, \cdot)$ is a deterministic function satisfying the Markov relation $U \to (T, S) \to (X, S) \to (Y, Z)$.

III. Achievability Proof

We first prove that the following rate is achievable in general, namely,

$$R_s = \max_{p(v)p(u|v)t(u,s),p(x|t,s)} I(V;Y) - I(V;Z). \tag{2}$$

where V is an auxiliary random variable.

We use multicoding and a three-step randomized encoding scheme.

Codebook generation. For each message $m \in \mathcal{M}$, generate a subcodebook $\mathcal{C}(m)$ consisting of $2^{n(\tilde{R}-R)}$ sequences $u^n(l)$ for $l \in [(m-1)2^{n(\tilde{R}-R)} + 1 : m2^{n(\tilde{R}-R)}]$ which is randomly and independently generated according to the distribution $\prod_{i=1}^{n} p_U(u_i)$. This codebook is revealed to all the nodes.

Encoding. To send message $m \in \mathcal{M}$, the encoder uniformly randomly chooses an index L from $\mathcal{C}(m)$. Given the function $t(\cdot, \cdot)$, the encoder generates $t^n(L)$ by $t_i = t(u_i(l), s_i)$. It then uses random coding to

generate the channel input x_i at time i according to the distribution $p_{X|T,S}(x_i|t_i, s_i)$.

Decoding. Given $Y^n = y^n$, find the unique $\hat{m}$ such that $(u^n(l), y^n) \in \mathcal{T}_\varepsilon^n(U, Y)$ for some $u^n(l) \in \mathcal{C}(\hat{m})$.

Analysis. We can obtain an equivalent wiretap channel described by

$$\begin{aligned} p_{Y,Z|U}(y,z|u) &= \sum_{x\in\mathcal{X},s\in\mathcal{S},t\in\mathcal{T}} P_{Y,Z,X,S,T|U}(y,z,x,s,t|u) \\ &= \sum_{x\in\mathcal{X},s\in\mathcal{S},t\in\mathcal{T}} P_{Y,Z|X,T,U,S}(y,z|x,t,u,s)p_{X|T,U,S}(x|t,u,s)p_{T|U,S}(t|u,s)p_S(s) \\ &= \sum_{x\in\mathcal{X},s\in\mathcal{S},t\in\mathcal{T}} P_{Y,Z|X,S}(y,z|x,s)p_{X|T,S}(x|t,s)1_{(t=t(u,s))}p_S(s) \\ &= \sum_{x\in\mathcal{X},s\in\mathcal{S}} P_{Y,Z|X,S}(y,z|x,s)p_{X|T,S}(x|t(u,s),s)p_S(s). \end{aligned}$$

The resulting equivalent DMC without CSI is shown in Figure 2. The rest of the analysis procedure

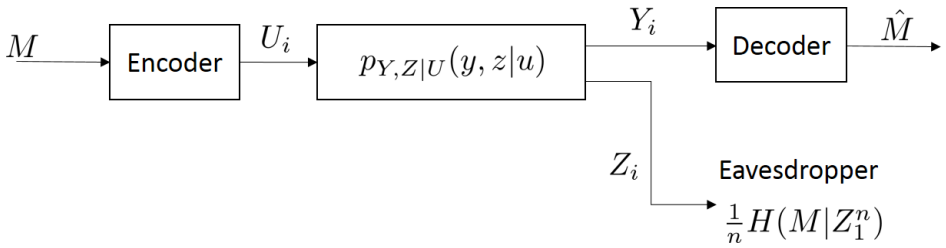

Fig. 2. Equivalent discrete memoryless wiretap channel with no CSI

follows that of the wiretap channel.

Let M be the transmitted message and L be the randomly picked index within codebook $\mathcal{C}(M)$. Let $\mathcal{E}$ be the event of error decoding. Let $\mathcal{E}_1 = \{(U^n(l), Y^n) \notin \mathcal{T}_\varepsilon^n(U, Y) \text{ for all } U^n(l) \in \mathcal{C}(m)\}$ and $\mathcal{E}_2 = \{(U^n(l), Y^n) \in \mathcal{T}_\varepsilon^n(U, Y) \text{ for some } l \neq L\}$. Then

$$P(\mathcal{E}) \leqslant P(\mathcal{E}_1 \cup \mathcal{E}_2) \leqslant P(\mathcal{E}_1) + P(\mathcal{E}_2)$$

By LLN, $P(\mathcal{E}_1) \to 0$ as $n \to \infty$. By the packing lemma, $P(\mathcal{E}_2) \to 0$ as $n \to \infty$ if $\tilde{R} < I(U;Y) - \delta(\varepsilon)$. Hence, the error probability diminishes as n goes to infinity.

By following the proof in the Network Information Theory book, the equivocation at the eavesdropper can also be shown to approach 0 as $n \to \infty$ if $\tilde{R} - R \geqslant I(U;Z)$. Hence, the achievable rate follows as (2).

Now, by the less noisy property, we have

$$\begin{aligned} R_s &= \max_{p(u)t(u,s),p(x|t,s)} I(U;Y) - I(U;Z) \\ &= \max_{p(u)t(u,s),p(x|t,s)} I(T,U;Y) - I(T,U;Z) - (I(T;Y|U) - I(T;Z|U)) \\ &= \max_{p(u)t(u,s),p(x|t,s)} I(T;Y) - I(T;Z) \end{aligned} \tag{3}$$

where the last equality follows since $I(T;Y|U) - I(T;Z|U) \geqslant 0$ and by letting $U = T$, it is made 0. Hence, the achievability follows.

IV. Converse Proof

Suppose there exists a code such that $R_e \leqslant \varepsilon_n$ where $\varepsilon_n \to 0$ as $n \to \infty$. Note that by Fano's inequality, $H(M|Y^n) \leqslant n\varepsilon'_n$ where $\varepsilon'_n \to 0$ as $n \to \infty$. We have

$$\begin{aligned}
nR_s &= H(M) - H(M|Y^n) + H(M|Y^n) \\
&\leqslant I(M;Y^n) + n\varepsilon'_n \\
&= I(M;Y^n) - I(M;Z^n) + nR_e + n\varepsilon'_n \\
&\leqslant I(M;Y^n) - I(M;Z^n) + n(\varepsilon'_n + \varepsilon_n) \\
&= \sum_{i=1}^{n} \left[I(M;Y_i|Y_1^{i-1}) - I(M;Z_i|Z_{i+1}^n) \right] + n(\varepsilon'_n + \varepsilon_n) \\
&= \sum_{i=1}^{n} \left[I(M, Z_{i+1}^n; Y_i|Y_1^{i-1}) - I(Z_{i+1}^n; Y_i|Y_1^{i-1}, M) - I(M, Y_1^{i-1}; Z_i|Z_{i+1}^n) + I(Y_1^{i-1}; Z_i|Z_{i+1}^n, M) \right] \\
&\quad + n(\varepsilon'_n + \varepsilon_n) \\
&= \sum_{i=1}^{n} \left[I(M, Z_{i+1}^n; Y_i|Y_1^{i-1}) - I(M, Y_1^{i-1}; Z_i|Z_{i+1}^n) \right] + n(\varepsilon'_n + \varepsilon_n) \qquad (4) \\
&= \sum_{i=1}^{n} \left[I(M; Y_i|Y_1^{i-1}, Z_{i+1}^n) + I(Z_{i+1}^n; Y_i|Y_1^{i-1}) - I(M; Z_i|Z_{i+1}^n, Y_1^{i-1}) - I(Y_1^{i-1}; Z_i|Z_{i+1}^n) \right] \\
&\quad + n(\varepsilon'_n + \varepsilon_n) \\
&= \sum_{i=1}^{n} \left[I(M; Y_i|Y_1^{i-1}, Z_{i+1}^n) - I(M; Z_i|Y_1^{i-1}, Z_{i+1}^n) \right] + n(\varepsilon'_n + \varepsilon_n) \qquad (5) \\
&= \sum_{i=1}^{n} \left[I(T_i; Y_i|V_i) - I(T_i; Z_i|V_i) \right] + n(\varepsilon'_n + \varepsilon_n) \qquad (6)
\end{aligned}$$

where (4) and (5) are due to Csiszar sum identity, and in (6) auxiliary random variables $V_i = (Y_1^{i-1}, Z_{i+1}^n)$ and $T_i = (M, V_i)$ are introduced such that $(V_i, S_i) \to (T_i, S_i) \to (X_i, S_i) \to (Y_i, Z_i)$ forms a Markov chain. Note that here V_i and T_i are dependent on S_i.

Hence,

$$\begin{aligned}
(6) &= \left[I(T_Q; Y_Q|V_Q, Q) - I(T_Q; Z_Q|V_Q, Q) \right] + n(\varepsilon'_n + \varepsilon_n) \qquad (7) \\
&= \left[I(T; Y|V) - I(T; Z|V) \right] + n(\varepsilon'_n + \varepsilon_n) \qquad (8) \\
&= \sum_{v \in \mathcal{V}} p(v) \left[I(T; Y|V = v) - I(T; Z|V = v) \right] + n(\varepsilon'_n + \varepsilon_n) \\
&\leqslant \max_v \left[I(T; Y|V = v) - I(T; Z|V = v) \right] + n(\varepsilon'_n + \varepsilon_n) \\
&= n \max_{p(t|s)p(x|t,s)} \left[I(T; Y) - I(T; Z) \right] + n(\varepsilon'_n + \varepsilon_n) \\
&= n \max_{p(u)t(u,s),p(x|t,s)} \left[I(T; Y) - I(T; Z) \right] + n(\varepsilon'_n + \varepsilon_n) \qquad (9)
\end{aligned}$$

where in (7) a time-sharing random variable Q is introduced, (8) holds by letting $V = (V_Q, Q)$, $U = (U_Q, Q)$, $Y = Y_Q$, and $Z = Z_Q$, (9) is because of the Markov chain $(T, S) \to (X, S) \to (Y, Z)$ and the functional representation lemma, and $t(\cdot, \cdot)$ is a deterministic function.

Lemma 1 (functional representation)**.** *Let $(S, T, X) \sim p(s, t, x)$. Then T can be represented as a function of (S, U) for some random variable U of cardinality $|\mathcal{U}| \leqslant |\mathcal{S}|(|\mathcal{T}| - 1) + 1$ such that U is independent of S and $U \to (T, S) \to X$ forms a Markov chain.*