

We can show that the above functions satisfy the following property.

Property 2:

- The cardinality bound $|\mathcal{U}| \leq |\mathcal{Z}|$ in $\mathcal{Q}(p_{K|Z})$ is sufficient to describe the quantity $\Omega^{(\mu,\alpha)}(p_K, W)$.
- Fix any $p = p_{UZK} \in \mathcal{P}_{\text{sh}}(p_K, W)$ and $\mu \in [0, 1]$. Define

$$\tilde{\omega}_p^{(\mu)}(z, k|u) := \mu \log \frac{p_{Z|U}(z|u)}{p_Z(z)} + \log \frac{1}{p_{K|U}(K|U)}.$$

For $\lambda \in [0, 1/2]$, we define a probability distribution $p^{(\lambda)} = p_{UZK}^{(\lambda)}$ by

$$p^{(\lambda)}(u, z, k) := \frac{p(u, z, k) \exp \left\{ -\lambda \tilde{\omega}_p^{(\mu)}(z, k|u) \right\}}{\mathbb{E}_p \left[\exp \left\{ -\lambda \tilde{\omega}_p^{(\mu)}(Z, K|U) \right\} \right]}.$$

For $(\mu, \lambda) \in [0, 1] \times [0, 1/2]$, define

$$\begin{aligned} \rho^{(\mu,\lambda)}(p_K, W) \\ := \max_{\substack{(\nu, p) \in [0, \lambda] \\ \times \mathcal{P}_{\text{sh}}(p_K, W): \\ \tilde{\Omega}^{(\mu,\lambda)}(p) \\ = \tilde{\Omega}^{(\mu,\lambda)}(p_K, W)}} \text{Var}_{p^{(\nu)}} \left[\tilde{\omega}_p^{(\mu)}(Z, K|U) \right], \end{aligned}$$

and set

$$\rho = \rho(p_K, W) := \max_{(\mu, \lambda) \in [0, 1] \times [0, 1/2]} \rho^{(\mu, \lambda)}(p_K, W).$$

Then we have $\rho(p_K, W) < \infty$. Furthermore, for every $\tau \in (0, (1/2)\rho(p_K, W))$, the condition $(R_A, R + \tau) \notin \mathcal{R}(p_K, W)$ implies

$$F(R_A, R|p_K, W) > \frac{\rho(p_K, W)}{4} \cdot g^2 \left(\frac{\tau}{\rho(p_K, W)} \right) > 0,$$

where g is the inverse function of $\vartheta(a) := a + (3/2)a^2, a \geq 0$.

Proof of this property is found in Oohama [6]. Define

$$\mathcal{R}^{(\text{in})}(p_X, p_K, W) := \{R > H(X)\} \cap \mathcal{R}^c(p_K, W).$$

The functions $E(R|p_X)$ and $F(R_A, R|p_K, W)$ take positive values if and only if (R_A, R) belongs to $\mathcal{R}_{\text{Sys}}^{(\text{in})}(p_X, p_K, W)$. Define $\delta_{i,n}, i = 1, 2$ by

$$\begin{aligned} \delta_{1,n} &:= \frac{1}{n} \log \left[e(n+1)^{2|\mathcal{X}|} \{ (n+1)^{|\mathcal{X}|} + 1 \} \right], \\ \delta_{2,n} &:= \frac{1}{n} \log \left[5nR \{ (n+1)^{|\mathcal{X}|} + 1 \} \right]. \end{aligned}$$

Note that for $i = 1, 2$, $\delta_{i,n} \rightarrow 0$ as $n \rightarrow \infty$. Santos and Oohama [5] proved the following result.

Theorem 1: For any $R_A, R > 0$, and any (p_K, W) with $(R_A, R) \in \mathcal{R}^c(p_Z, W)$, there exists a sequence of mappings $\{(\varphi^{(n)}, \psi^{(n)})\}_{n=1}^{\infty}$ satisfying

$$R - \frac{1}{n} \leq \frac{1}{n} \log |\mathcal{X}^m| = \frac{m}{n} \log |\mathcal{X}| \leq R$$

such that for any p_X with $R > H(X)$, we have that

$$p_e(\phi^{(n)}, \psi^{(n)}|p_X^n) \leq e^{-n[E(R|p_X) - \delta_{1,n}]} \quad (7)$$

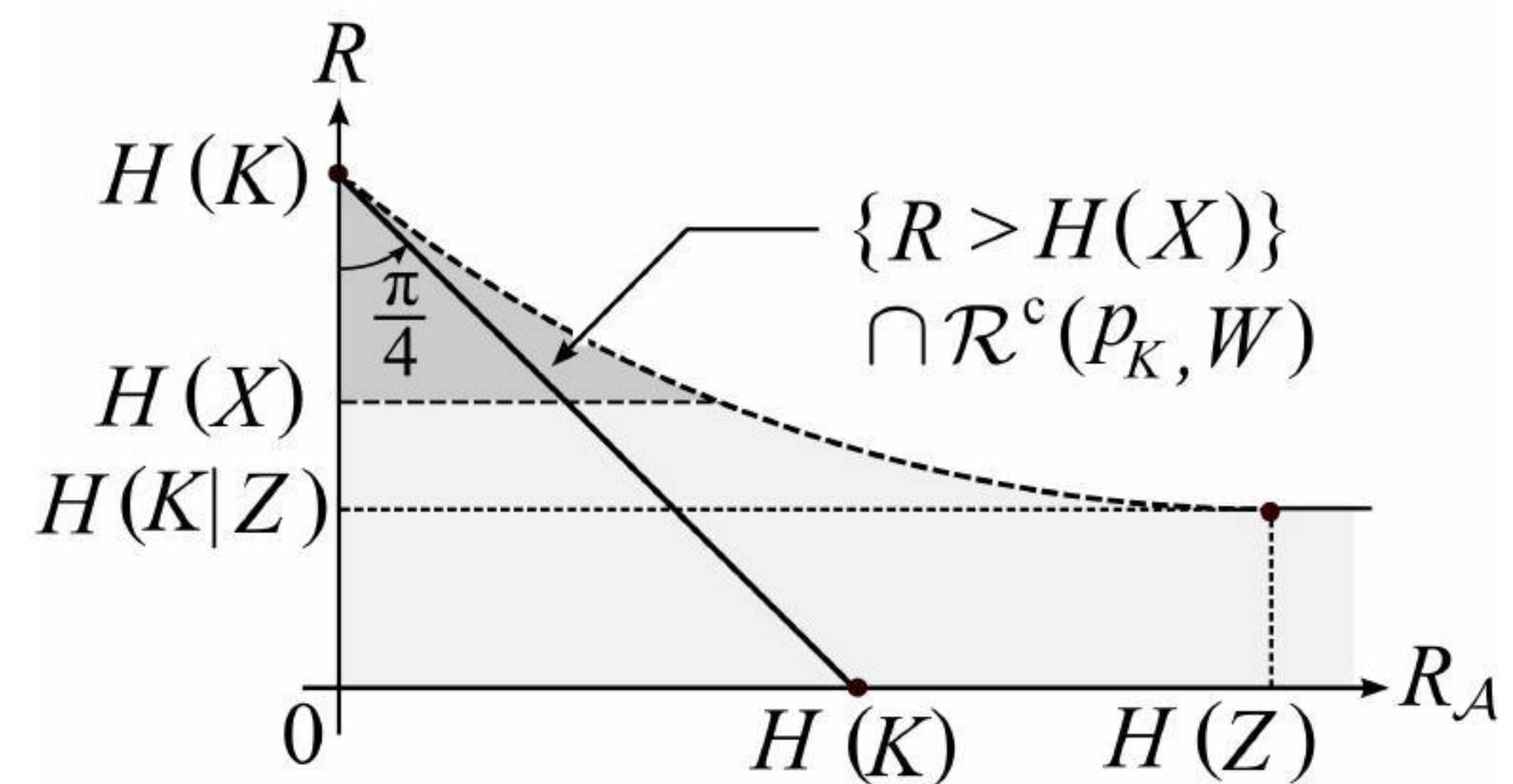


Fig. 3. The inner bound $\mathcal{R}^{(\text{in})}(p_X, p_K, W)$ of the reliable and secure rate region $\mathcal{R}_{\text{Sys}}(p_X, p_K, W)$.

and that for any eavesdropper \mathcal{A} with $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)} \in \mathcal{F}_{\mathcal{A}}^{(n)}(R_A)$,

$$\begin{aligned} \Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n) \\ \leq e^{-n[F(R_A, R|p_K, W) - \delta_{2,n}]}. \end{aligned} \quad (8)$$

By Theorem 1 under $(R_A, R) \in \mathcal{R}^{(\text{in})}(p_X, p_K, W)$, we have the followings:

- On the reliability, $p_e(\phi^{(n)}, \psi^{(n)}|p_X^n)$ goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $E(R|p_X)$.
- On the security, for any $\varphi_{\mathcal{A}}^{(n)}$ belonging to $\mathcal{F}_{\mathcal{A}}^{(n)}(R_A)$, the information leakage $\Delta^{(n)}(\varphi^{(n)}, \varphi_{\mathcal{A}}^{(n)}|p_X^n, p_K^n, W^n)$ goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $F(R_A, R|p_K, W)$.
- The code that attains the exponent functions $E(R|p_X)$ is the universal code that depends only on R not on the value of the distribution p_X .

From Theorem 1 we have the following corollary.

Corollary 1:

$$\mathcal{R}^{(\text{in})}(p_X, p_K, W) \subseteq \mathcal{R}_{\text{Sys}}(p_X, p_K, W).$$

A typical shape of the region $\mathcal{R}^{(\text{in})}(p_X, p_K, W)$ is shown in Fig. 3.

IV. MAIN RESULT

To describe our main result we define several quantities. For $p_{\overline{K}\overline{Z}} \in \mathcal{P}(\mathcal{X} \times \mathcal{Z})$, define

$$\begin{aligned} G^{(\mu,\alpha)}(\mu R_A + \bar{\mu} R|p_{\overline{K}\overline{Z}}) \\ := \frac{\Omega^{(\mu,\alpha)}(p_{\overline{K}\overline{Z}}) - \alpha(\mu R_A + \bar{\mu} R)}{2 + 3\alpha\bar{\mu}}, \\ G(R_A, R|p_{\overline{K}\overline{Z}}) := \sup_{\substack{(\mu,\alpha) \\ \in [0,1]^2}} G^{(\mu,\alpha)}(\mu R_A + \bar{\mu} R|p_{\overline{K}\overline{Z}}). \end{aligned}$$

By simple computation we can show that

$$G(R_A, R|p_{\overline{K}\overline{Z}}) \geq (1/3)F(R_A, R|p_{\overline{K}\overline{Z}}).$$

Set

$$\begin{aligned} G(R_A, R|p_K, W) \\ := \min_{p_{\overline{K}\overline{Z}} \in \mathcal{P}(\mathcal{K} \times \mathcal{Z})} \{G(R_A, R|p_{\overline{K}\overline{Z}}) + D(p_{\overline{K}\overline{Z}}||p_X, W)\}. \end{aligned}$$