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

Property 2:

a) The cardinality bound $|\mathcal{U}| \le |\mathcal{Z}|$ in $\mathcal{Q}(p_{K|Z})$ is sufficient to describe the quantity $\Omega^{(\mu,\alpha)}(p_K, W)$.

b) Fix any $p = p_{UZK} \in \mathcal{P}_{\rm sh}(p_K, W)$ 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

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

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

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

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 $(R_{\mathcal{A}}, R+\tau) \notin \mathcal{R}(p_K,W)$ implies

$$F(R_{\mathcal{A}},R|p_K,W) > \tfrac{\rho(p_K,W)}{4} \cdot g^2\left(\tfrac{\tau}{\rho(p_K,W)}\right) > 0,$$

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

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

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

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

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

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

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

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

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

$$p_{\rm e}(\phi^{(n)},\psi^{(n)}|p_X^n) \le \mathrm{e}^{-n[E(R|p_X)-\delta_{1,n}]} \tag{7}$$

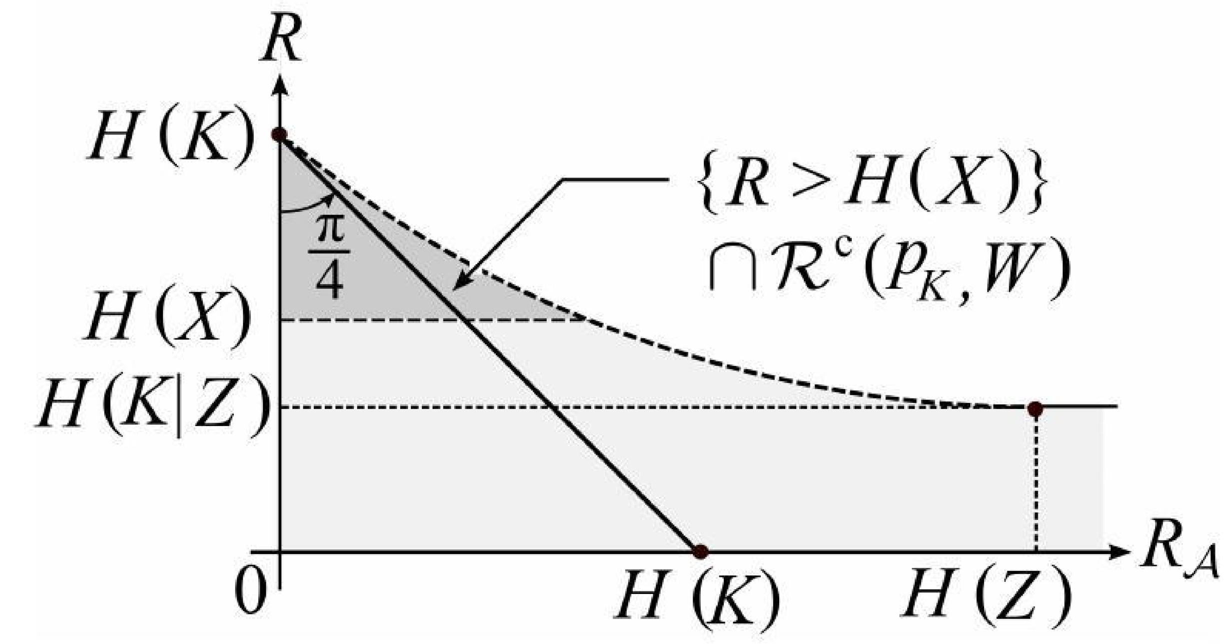

Fig. 3. The inner bound $\mathcal{R}^{(\rm in)}(p_X,p_K,W)$ of the reliable and secure rate region $\mathcal{R}_{\rm Sys}(p_X,p_K\ W)$.

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

$$\begin{aligned}&\Delta^{(n)}(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_X^n,p_K^n,W^n) \\ &\le \mathrm{e}^{-n[F(R_{\mathcal{A}},R|p_K,W)-\delta_{2,n}]}.\end{aligned} \tag{8}$$

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

- On the reliability, $p_{\rm e}(\phi^{(n)},\psi^{(n)}|p_X^n)$ 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 $\mathcal{F}_{\mathcal{A}}^{(n)}(\ R_{\mathcal{A}})$, 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 $F(R_{\mathcal{A}},R|p_K,W)$.
- 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:

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

A typical shape of the region $\mathcal{R}^{(\rm in)}(p_X,p_K,W)$ 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

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

By simple computation we can show that

$$G(R_{\mathcal{A}},R|p_{\overline{K}\,\overline{Z}}) \ge (1/3)F(R_{\mathcal{A}},R|p_{\overline{K}\,\overline{Z}}).$$

Set

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