Define $\delta_{i,n}, i=3,4$ by

$$\delta_{3,n} := \frac{1}{n}\log\Big[\mathrm{e}(n+1)^{2|\mathcal{X}|} \times\{(n+1)^{|\mathcal{X}|}+(n+1)^{|\mathcal{X}||\mathcal{Z}|}\}\Big],$$

$$\delta_{4,n} := \frac{1}{n}\log\Big[(7nR)(n+1)^{3|\mathcal{X}||\mathcal{Z}|} \times\{(n+1)^{|\mathcal{X}|}+(n+1)^{|\mathcal{X}||\mathcal{Z}|}\}\Big].$$

Note that for $i=3,4$, $\delta_{i,n}\to 0$ as $n\to\infty$. Our main result is the following.

Theorem 2: For any $R_{\mathcal{A}}, R>0$, 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,p_K,W) with $(R_{\mathcal{A}},R)\in\mathcal{R}^{(\mathrm{in})}(p_X,p_K,W)$, we have that

$$p_{\mathrm{e}}(\phi^{(n)},\psi^{(n)}|p_X^n)\le \mathrm{e}^{-n[E(R|p_X)-\delta_{3,n}]} \tag{9}$$

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

$$\Delta^{(n)}(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_X^n,p_K^n,W^n) \le \mathrm{e}^{-n[G(R_{\mathcal{A}},R|p_K,W)-\delta_{4,n}]}. \tag{10}$$

By Theorem 2, under $(R_{\mathcal{A}},R)\in\mathcal{R}^{(\mathrm{in})}(p_X,\ p_K,W)$, we have the followings:

- On the reliability, $p_{\mathrm{e}}(\phi^{(n)},\psi^{(n)}|p_X^n)$ 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 $\varphi_{\mathcal{A}}$ satisfying $\varphi_{\mathcal{A}}^{(n)}\in\mathcal{F}_{\mathcal{A}}^{(n)}(R_{\mathcal{A}})$, $\Delta^{(n)}(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}\ |p_X^n,p_K^n,W^n)$ goes to zero exponentially as n tends to infinity, and its exponent is lower bounded by the function $G(R_{\mathcal{A}},\ R|p_K,W)$.
- The code that attains the exponent functions $E(\ R|p_X)$ and $G(R_{\mathcal{A}},R|p_K,W)$ is the universal code that depends only on $(R_{\mathcal{A}},R)$ not on the value of the distributions p_X, p_Z, and W.

V. Proof Outline of the Main Result

In this section we outline the proof of Theorem 2. We first present several definitions on the types. For any n-sequence $k^n=k_1k_2\cdots\ k_n\in\mathcal{X}^n$, $n(k|k^n)$ denotes the number of t such that $k_t=k$. The relative frequency $\{n(k|k^n)/n\}_{k\in\mathcal{X}}$ of the components of x^n is called the type of k^n denoted by P_{k^n}. The set that consists of all the types on $\mathcal{X}$ is denoted by $\mathcal{P}_n(\mathcal{X})$. For $p_{\overline{K}}\in\mathcal{P}_n(\mathcal{X})$, set

$$T_{\overline{K}}^n:=\{k^n: P_{k^n}=p_{\overline{K}}\}.$$

Similarly, for any two n-sequences $k^n=k_1\ k_2,\cdots,k_n\in\mathcal{X}^n$ and $z^n=z_1\ z_2,\cdots,z_n\in\mathcal{Z}^n$, $n(k,z|k^n,z^n)$ denotes the number of t such that $(k_t,\ z_t)=(k,\ z)$. The relative frequency $\{n(k,z|k^n,z^n)/n\ \}_{(k,z)\in\ \mathcal{X}\times\mathcal{Z}}$ of the components of (k^n,z^n) is called the joint type of (k^n,z^n) denoted by P_{k^n,z^n}. Furthermore, the set of all the joint type of $\mathcal{X}\times\mathcal{Z}$ is denoted by $\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})$. For $p_{\overline{K}\,\overline{Z}}\in\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})$, set

$$T_{\overline{K}\,\overline{Z}}^n:=\{(k^n,z^n): P_{k^n,z^n}=P_{\overline{K}\,\overline{Z}}\}.$$

Furthermore, for $p_{\overline{K}}\in\mathcal{P}_n\ (\mathcal{X})$ and $k^n\in T_{\overline{K}}^n$, set

$$T_{\overline{Z}|\overline{K}}^n(k^n):=\{z^n: P_{k^n,z^n}=p_{\overline{K}\,\overline{Z}}\}.$$

We next discuss upper bounds of

$$\Delta_n(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_X^n,p_K^n,W^n)=I(\widetilde{C}^m,M_{\mathcal{A}}^{(n)};X^n).$$

According to [5], on an upper bound of $I(\widetilde{C}^m,M_{\mathcal{A}}^{(n)};\ X^n)$, we have the following lemma.

Lemma 1: [5]

$$I(\widetilde{C}^m,M_{\mathcal{A}}^{(n)};X^n)\le D\left(p_{\widetilde{K}^m|M_{\mathcal{A}}^{(n)}}\middle|\middle|\,p_{V^m}\middle|\,p_{M_{\mathcal{A}}^{(n)}}\right), \tag{11}$$

where p_{V^m} is the uniform distribution over $\mathcal{X}^m$.

Set $M^{(n)}:=P_{K^n,Z^n}$. Then we have the folllowing:

$$D\left(p_{\widetilde{K}^m|M_{\mathcal{A}}^{(n)}}\middle|\middle|\,p_{V^m}\middle|\,p_{M_{\mathcal{A}}^{(n)}}\right) \le\ D\left(p_{\widetilde{K}^m|M_{\mathcal{A}}^{(n)}M^{(n)}}\middle|\middle|\,p_{V^m}\middle|\,p_{M_{\mathcal{A}}^{(n)}M^{(n)}}\right). \tag{12}$$

For $p_{\overline{K}\,\overline{Z}}\in\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})$, set

$$D\left(p_{\widetilde{K}^m|M_{\mathcal{A}}^{(n)}M^{(n)}=p_{\overline{K}\,\overline{Z}}}\middle|\middle|\,p_{V^m}\middle|\,p_{M_{\mathcal{A}}^{(n)}M^{(n)}=p_{\overline{K}\,\overline{Z}}}\right) := \zeta(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_{\overline{K}\,\overline{Z}}). \tag{13}$$

From (11),(12), and (13), we have

$$\Delta_n(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_X^n,p_K^n,W^n)\le \sum_{\substack{p_{\overline{K}\,\overline{Z}}\\ \in\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})}} 1 \times\Pr\{M^{(n)}=p_{\overline{K}\,\overline{Z}}\}\zeta(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_{\overline{K}\,\overline{Z}}). \tag{14}$$

For $p_{\overline{K}\,\overline{Z}}\in\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})$, define

$$\Upsilon(R,\varphi_{\mathcal{A}}^{(n)}|p_{\overline{K}\,\overline{Z}}):=\sum_{\substack{(a,k^n)\\ \in\mathcal{M}_{\mathcal{A}}^{(n)}\times T_{\overline{K}}^n}}\frac{\left|\left(\varphi_{\mathcal{A}}^{(n)}\right)^{-1}(a)\cap T_{\overline{Z}|\overline{K}}^n(k^n)\right|}{\left|T_{\overline{K}\,\overline{Z}}^n\right|} \times\log\left[1+(\mathrm{e}^{nR}-1)\frac{\left|\left(\varphi_{\mathcal{A}}^{(n)}\right)^{-1}(a)\cap T_{\overline{Z}|\overline{K}}^n(k^n)\right|\left|T_{\overline{K}}^n\right|}{\left|\left(\varphi_{\mathcal{A}}^{(n)}\right)^{-1}(a)\cap T_{\overline{Z}}^n\right|\left|T_{\overline{K}\,\overline{Z}}^n\right|}\right].$$

On $\zeta(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_{\overline{K}\,\overline{Z}})$ for $p_{\overline{K}\,\overline{Z}}\in\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})$, we have the following lemma.

Lemma 2: For any $p_{\overline{K}\,\overline{Z}}\in\mathcal{P}_n(\mathcal{X}\times\mathcal{Z})$,

$$\mathbf{E}\left[\zeta(\varphi^{(n)},\varphi_{\mathcal{A}}^{(n)}|p_{\overline{K}\,\overline{Z}})\right]\le\Upsilon(R,\varphi_{\mathcal{A}}^{(n)}|p_{\overline{K}\,\overline{Z}}), \tag{15}$$

where $\mathbf{E}[\cdot]$ is an expectation based on the random choice of $\varphi^{(n)}$.

To prove the above lemma we use a technique quite similar to that of Hayashi [7] used for an ensemble of universal$_2$ functions. The following proposition is a key result for the proof of Theorem 1.

Proposition 1: For any $R_{\mathcal{A}},R>0$, there exists a sequence of mappings $\{(\varphi^{(n)},\psi^{(n)})\}_{n=1}^{\infty}$ satisfying

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