SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Secure Polar Coding for a Joint Source-Channel Model

Haowei WANG[1], Xiaofeng TAO[1*], Huici WU[1], Na LI[1] & Jin XU[1]

[1]*National Engineering Laboratory for Mobile Network Technologies, Beijing University of Posts and Telecommunications, Beijing* 100876*, China*

Appendix A Proof of Lemma 2

First, we have

$$\begin{aligned}|H(\tilde{A}_j^{1:n}[\mathcal{T}]|Z_{sj}^{1:n}) - H(A^{1:n}[\mathcal{T}]|Z_s^{1:n})| &\overset{(a)}{\leqslant} V(p_{\tilde{A}_j^{1:n}Z_{sj}^{1:n}}, p_{A^{1:n}Z_s^{1:n}}) \times \log \frac{2^n|\mathcal{Z}_s|^n}{V(p_{\tilde{A}_j^{1:n}Z_{sj}^{1:n}}, p_{A^{1:n}Z_s^{1:n}})} \\ &\leqslant V(p_{\tilde{A}_j^{1:n}Z_{sj}^{1:n}}, p_{A^{1:n}Z_s^{1:n}}) \times \left(n(1+\log|\mathcal{Z}_s|) - \log V(p_{\tilde{A}_j^{1:n}Z_{sj}^{1:n}}, p_{A^{1:n}Z_s^{1:n}})\right) \\ &\overset{(b)}{\leqslant} \sqrt{2\ln 2}\sqrt{n\delta_n}\left(n(1+\log|\mathcal{Z}_s|) - \log\left(\sqrt{2\ln 2}\sqrt{n\delta_n}\right)\right) = O(n\sqrt{n\delta_n}),\end{aligned} \tag{A1}$$

where (a) holds by [1, Theorem 17.3.3], (b) holds by Lemma 1 and the fact that $f(x) \triangleq x(a - \log_2 x)$ is increasing for x close enough to zero. Then, we have

$$\begin{aligned}|\mathcal{T}| - H(\tilde{A}_j^{1:n}[\mathcal{T}]|Z_{sj}^{1:n}) &\overset{(a)}{\leqslant} |\mathcal{T}| - H(A^{1:n}[\mathcal{T}]|Z_s^{1:n}) + O(n\sqrt{n\delta_n}) \\ &\overset{(b)}{\leqslant} |\mathcal{T}| - \sum_{i\in\mathcal{T}} H(A^i|A^{1:i-1}Z_s^{1:n}) + O(n\sqrt{n\delta_n}) \\ &\overset{(c)}{\leqslant} |\mathcal{T}| - \sum_{i\in\mathcal{T}}(1-\delta_n) + O(n\sqrt{n\delta_n}) \\ &= |\mathcal{T}|\delta_n + O(n\sqrt{n\delta_n}) = O(n\sqrt{n\delta_n}),\end{aligned} \tag{A2}$$

where (a) holds by (A1), (b) holds because conditioning reduces entropy, (c) holds by the definition of $\mathcal{V}_{U|Z_s}$.

Appendix B Proof of Lemma 3

Recall that $F_j \triangleq \tilde{A}_j^{1:n}[\mathcal{F}_a]$ in the encoding scheme. From Lemma 2, we know that

$$H(F_j) \geqslant H(F_j|Z_{sj}^{1:n}) \geqslant |\mathcal{F}_a| - O(n\sqrt{n\delta_n}). \tag{B1}$$

Since $M_j \triangleq (F_j, \bar{F}_j \oplus \bar{K}_{j-1})$, then we have

$$\begin{aligned}H(M_j) - H(F_j) &= H(\bar{F}_j \oplus \bar{K}_{j-1}|F_j) \\ &\geqslant H(\bar{F}_j \oplus \bar{K}_{j-1}|F_j\bar{F}_j\Phi) \\ &= H(\bar{K}_{j-1}|F_j\bar{F}_j\Phi) \\ &\overset{(a)}{=} H(\bar{K}_{j-1}|\Phi) \\ &= H(\bar{K}_{j-1}\Phi) - H(\Phi) \\ &\geqslant H(\bar{K}_{j-1}\Phi|Z_{s,j-1}^{1:n}) - H(\Phi) \\ &\overset{(b)}{\geqslant} |\mathcal{F}_b| + |\mathcal{V}_{U|X_s}| - O(n\sqrt{n\delta_n}) - H(\Phi) \\ &\overset{(c)}{=} |\mathcal{F}_b| - O(n\sqrt{n\delta_n}),\end{aligned} \tag{B2}$$

where (a) holds by the Markov chain $\bar{K}_{j-1} \to \Phi \to F_j\bar{F}_j$, (b) holds by the encoding scheme and Lemma 2, (c) holds by the uniformity of Φ, i.e., $H(\Phi) = |\mathcal{V}_{U|X_s}|$. Finally we conclude by combing (B1) and (B2).

* Corresponding author (email: taoxf@bupt.edu.cn)

Appendix C Proof of Lemma 4

We only prove the first inequality, the other one can be similarly obtained. First, we have

$$\begin{aligned} I(K_j\bar{K}_j; F_j\Phi Z_{sj}^{1:n}) &= H(K_j\bar{K}_j) - H(K_j\bar{K}_j|F_j\Phi Z_{sj}^{1:n}) \\ &= H(K_j\bar{K}_j) + H(F_j\Phi|Z_{sj}^{1:n}) - H(K_j\bar{K}_jF_j\Phi|Z_{sj}^{1:n}) \\ &\leqslant |K_j| + |\bar{K}_j| + |F_j| + |\Phi| - H(K_j\bar{K}_jF_j\Phi|Z_{sj}^{1:n}) \\ &\overset{(a)}{=} |\mathcal{V}_{U|Z_s}| - H(\tilde{A}_j^{1:n}[\mathcal{V}_{U|Z_s}]|Z_{sj}^{1:n}) \overset{(b)}{\leqslant} O(n\sqrt{n\delta_n}), \end{aligned} \tag{C1}$$

where (a) holds by the definition of $\{K_j, \bar{K}_j, F_j, \Phi\}$, (b) holds by Lemma 2.

Recall that $M_j \triangleq (F_j, \bar{F}_j \oplus K_{j-1})$. Then we continue as follows.

$$\begin{aligned} I(K_j\bar{K}_j; M_j\Phi Z_{sj}^{1:n}) - I(K_j\bar{K}_j; F_j\Phi Z_{sj}^{1:n}) &= I(K_j\bar{K}_j; \bar{F}_j \oplus \bar{K}_{j-1}|F_j\Phi Z_{sj}^{1:n}) \\ &\overset{(a)}{\leqslant} I(K_j\bar{K}_jF_j\Phi Z_{sj}^{1:n}; \bar{F}_j \oplus \bar{K}_{j-1}) \\ &= H(\bar{F}_j \oplus \bar{K}_{j-1}) - H(\bar{F}_j \oplus \bar{K}_{j-1}|K_j\bar{K}_jF_j\Phi Z_{sj}^{1:n}) \\ &\leqslant |\bar{K}_{j-1}| - H(\bar{F}_j \oplus \bar{K}_{j-1}|K_j\bar{K}_jF_j\Phi Z_{sj}^{1:n}) \\ &\leqslant |\bar{K}_{j-1}| - H(\bar{F}_j \oplus \bar{K}_{j-1}|K_j\bar{K}_jF_j\Phi Z_{sj}^{1:n}\bar{F}_j) \\ &= |\bar{K}_{j-1}| - H(\bar{K}_{j-1}|K_j\bar{K}_jF_j\Phi Z_{sj}^{1:n}\bar{F}_j) \\ &\overset{(b)}{=} |\bar{K}_{j-1}| - H(\bar{K}_{j-1}|\Phi) \\ &= |\bar{K}_{j-1}| + H(\Phi) - H(\bar{K}_{j-1}\Phi) \\ &= |\bar{K}_{j-1}| + |\Phi| - H(\bar{K}_{j-1}\Phi) \\ &\overset{(c)}{\leqslant} |\bar{K}_{j-1}| + |\Phi| - H(\bar{K}_{j-1}\Phi|Z_{sj}^{1:n}) \overset{(d)}{\leqslant} O(n\sqrt{n\delta_n}), \end{aligned} \tag{C2}$$

where (a) holds by the chain rule and positivity of mutual information, (b) holds because $\bar{K}_{j-1} \to \Phi \to K_j\bar{K}_jF_jZ_{sj}^{1:n}\bar{F}_j$, (c) holds by the definition of $\{\Phi, \bar{K}_{j-1}\}$, (d) holds by Lemma 2. The first inequality is obtained by combining (C1) and (C2).

Appendix D Proof of Lemma 5

Consider a sequence $\bar{B}_2^{1:n}$, where $\bar{B}_2^{1:n}[\mathcal{V}_{V_2}]$ carry uniformly distributed bits and the remaining bits are successively determined by the conditional probability $p_{B_2^i|B_2^{1:i-1}}(b_2^i|\bar{B}_2^{1:i-1})$, for $i \in (\mathcal{V}_{V_2})^c$. Let $\bar{V}_2^{1:n} = \bar{B}_2^{1:n}G_n$. Further, consider a sequence $\bar{B}_1^{1:n}$, where $\bar{B}_1^{1:n}[\mathcal{V}_{V_1|V_2}]$ carry uniformly distributed bits and the remaining bits are successively determined by the conditional probability $p_{B_1^i|B_1^{1:i-1}V_2^{1:n}}(b_1^i|\bar{B}_1^{1:i-1}\bar{V}_2^{1:n})$, for $i \in (\mathcal{V}_{V_1|V_2})^c$. Let $\bar{V}_1^{1:n} = \bar{B}_1^{1:n}G_n$. Similar to the proof of [2, Lemma 5], we have

$$\begin{aligned} D(p_{V_2^{1:n}}||p_{\bar{V}_2^{1:n}}) &\leqslant n\delta_n, \\ D(p_{V_1^{1:n}|V_2^{1:n}}||p_{\bar{V}_1^{1:n}|\bar{V}_2^{1:n}}) &\leqslant n\delta_n. \end{aligned} \tag{D1}$$

Then by the chain rule for divergence [1], we have

$$D(p_{V_1^{1:n}V_2^{1:n}}||p_{\bar{V}_1^{1:n}\bar{V}_2^{1:n}}) = D(p_{V_2^{1:n}}||p_{\bar{V}_2^{1:n}}) + D(p_{V_1^{1:n}|V_2^{1:n}}||p_{\bar{V}_1^{1:n}|\bar{V}_2^{1:n}}) \leqslant 2n\delta_n. \tag{D2}$$

In the encoding scheme, $(\bar{S}_j^2, M_j^2)$ are carried by $\tilde{B}_{2j}^{1:n}[\mathcal{I}_2]$. Notice that, $\bar{S}_j^2$ is uniformly distributed because

$$H(\bar{S}_j^2) = H(S_j^2 \oplus K_j^2) \geqslant H(S_j^2 \oplus K_j^2|K_j^2) = H(S_j^2|K_j^2) = H(S_j^2), \tag{D3}$$

where the last equality holds by the independence between S_j and K_j. Note that M_j^2 is a subvector of M_j. Similar to (D1), we have by Lemma 3

$$D(p_{\bar{V}_{2j}^{1:n}}||p_{\bar{V}_2^{1:n}}) \leqslant |M_j^2| - H(M_j^2) \leqslant O(n\sqrt{n\delta_n}). \tag{D4}$$

In the encoding scheme, $(S_j^1, \bar{S}_j^{1a}, M_j^{1a})$ and $(\bar{S}_j^{1b}, M_j^{1b})$ are carried by $\tilde{B}_{1j}^{1:n}[\mathcal{I}_{1a}\backslash\mathcal{R}'_{1b}]$ and $\tilde{B}_{1j}^{1:n}[\mathcal{I}_{1b} \cup \mathcal{R}'_{1b}]$, respectively. Moreover, $R_{j-1} \triangleq \tilde{B}_{1,j-1}^{1:n}[\mathcal{R}'_{1b}]$ is repeated in $\tilde{B}_{1j}^{1:n}[\mathcal{R}_{1b}]$. Let $R_{j-1} \triangleq (R_{j-1}^s, R_{j-1}^m)$, where R_{j-1}^s and R_{j-1}^m are the subvecotr of $\bar{S}_{j-1}^{1b}$ and M_{j-1}^{1b}, respectively. Similar to (D3), it is easy to see that $\{\bar{S}_j^1, \bar{S}_j^{1a}, \bar{S}_j^{1b}\}$ are uniformly distributed. Let $M_j^1 \triangleq (M_j^{1a}, M_j^{1b})$.

Then we have

$$\begin{aligned} D(p_{\bar{V}_{1j}^{1:n}|\bar{V}_{2j}^{1:n}}||p_{\bar{V}_1^{1:n}|\bar{V}_2^{1:n}}) &\leqslant |M_j^1| + |R_{j-1}^m| - H(M_j^1 R_{j-1}^m) \\ &= |M_j^1| + |R_{j-1}^m| - H(M_j^1) - H(R_{j-1}^m) + I(M_j^1; R_{j-1}^m) \\ &\overset{(a)}{\leqslant} O(n\sqrt{n\delta_n}) + I(M_j^1; R_{j-1}^m) \\ &\leqslant O(n\sqrt{n\delta_n}) + I(M_j^1 \Phi \bar{K}_{j-1}; R_{j-1}^m) \\ &= O(n\sqrt{n\delta_n}) + I(\Phi\bar{K}_{j-1}; R_{j-1}^m) + I(M_j^1; R_{j-1}^m|\Psi\bar{K}_{j-1}) \\ &\overset{(b)}{=} O(n\sqrt{n\delta_n}) + I(\Phi\bar{K}_{j-1}; R_{j-1}^m) \overset{(c)}{=} O(n\sqrt{n\delta_n}), \end{aligned} \tag{D5}$$

where (a) holds by Lemma 3, i.e., $|M_j^1| - H(M_j^1) \leqslant O(n\sqrt{n\delta_n})$, $|R_{j-1}^m| - H(R_{j-1}^m) \leqslant O(n\sqrt{n\delta_n})$, (b) holds because $R_{j-1}^m \to \Psi\bar{K}_{j-1} \to M_j^1$, (c) holds by Lemma 4. Then by the chain rule for divergence [1], we have

$$D(p_{\bar{V}_{1j}^{1:n}\bar{V}_{2j}^{1:n}}||p_{\bar{V}_1^{1:n}\bar{V}_2^{1:n}}) = D(p_{\bar{V}_{2j}^{1:n}}||p_{\bar{V}_2^{1:n}}) + D(p_{\bar{V}_{1j}^{1:n}|\bar{V}_{2j}^{1:n}}||p_{\bar{V}_1^{1:n}|\bar{V}_2^{1:n}}) \leqslant O(n\sqrt{n\delta_n}). \tag{D6}$$

Since $V_2 \to V_1 \to X_c \to Y_c Z_c$, we can factorize the joint distributions as

$$\begin{aligned} p_{V_2^{1:n}V_1^{1:n}X_c^{1:n}Y_c^{1:n}Z_c^{1:n}} &= p_{V_2^{1:n}V_1^{1:n}} p_{X_c^{1:n}|V_1^{1:n}} p_{Y_c^{1:n}Z_c^{1:n}|X_c^{1:n}}, \\ p_{\bar{V}_{2j}^{1:n}\bar{V}_{2j}^{1:n}\tilde{X}_{cj}^{1:n}\tilde{Y}_{cj}^{1:n}\tilde{Z}_{cj}^{1:n}} &= p_{\bar{V}_{2j}^{1:n}\bar{V}_{1j}^{1:n}} p_{\tilde{X}_{cj}^{1:n}|\bar{V}_{1j}^{1:n}} p_{\tilde{Y}_{cj}^{1:n}\tilde{Z}_{cj}^{1:n}|\tilde{X}_{cj}^{1:n}}. \end{aligned} \tag{D7}$$

Note that, $p_{X_c^{1:n}|V_1^{1:n}} = p_{\tilde{X}_{cj}^{1:n}|\bar{V}_{1j}^{1:n}}$ and $p_{Y_c^{1:n}Z_c^{1:n}|X_c^{1:n}} = p_{\tilde{Y}_{cj}^{1:n}\tilde{Z}_{cj}^{1:n}|\tilde{X}_{cj}^{1:n}}$. Finally we have

$$\begin{aligned} V(p_{\bar{V}_{2j}^{1:n}\bar{V}_{1j}^{1:n}\tilde{X}_{cj}^{1:n}\tilde{Y}_{cj}^{1:n}\tilde{Z}_{cj}^{1:n}}, p_{V_2^{1:n}V_1^{1:n}X_c^{1:n}Y_c^{1:n}Z_c^{1:n}}) &\overset{(a)}{=} V(p_{\bar{V}_{1j}^{1:n}\bar{V}_{2j}^{1:n}}, p_{V_1^{1:n}V_2^{1:n}}) \\ &\overset{(b)}{\leqslant} V(p_{\bar{V}_{1j}^{1:n}\bar{V}_{2j}^{1:n}}, p_{\bar{V}_1^{1:n}\bar{V}_2^{1:n}}) + V(p_{\bar{V}_1^{1:n}\bar{V}_2^{1:n}}, p_{V_1^{1:n}V_2^{1:n}}) \\ &\overset{(c)}{\leqslant} \sqrt{2\ln 2}\left(\sqrt{2n\delta_n} + \sqrt{O(n\sqrt{n\delta_n})}\right) \\ &= O\left(\sqrt{n\sqrt{n\delta_n}}\right), \end{aligned} \tag{D8}$$

where (a) holds by [3, Lemma 17], (b) holds by the triangle inequality, (c) holds by (D2), (D6) and Pinsker's inequality.

References

1 Cover, T M, Thomas, J A, Wiley, J. Elements of information theory. Tsinghua University Press, 2003
2 Chou R A, Bloch M R. Polar coding for the broadcast channel with confidential messages: A random binning analogy. IEEE Trans. Inf. Theory, 2016, 62: 2410-2429
3 Cuff P W. Communication in networks for coordinating behavior. Stanford University, 2009