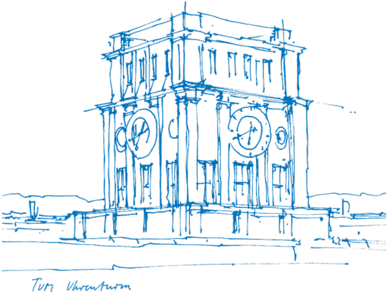
Polar Coding for Wire-Tap Channels

Peihong Yuan

Chair for Communications Engineering

Technical University of Munich

October 29, 2019, COCO 2019



Overview

Introduction

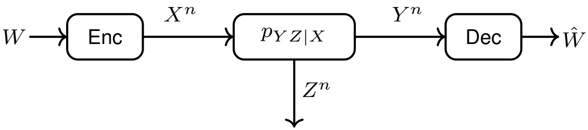
Polar Coding for Wire-Tap Channels

Simulation Results

Strong Secrecy with Polar Codes

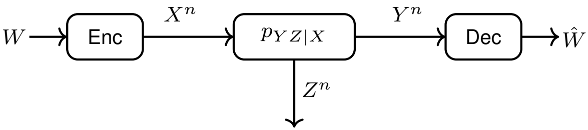
Conclusion and Future Work

Wire-Tap Channel[1]



[1] A. D. Wyner, "The Wire-Tap Channel." Bell system technical journal 54.8 (1975): 1355-1387.

Wire-Tap Channel[1]



- $p_{Z|X}$ is degraded w.r.t. $p_{Y|X}$
- Reliability: Pr $\left\{\hat{W} \neq W\right\}$
- Weak secrecy: $\lim_{n\to\infty} \frac{1}{n}\mathsf{I}\left(W, Z^n\right) = 0$
- Strong secrecy: $\lim_{n\to\infty} \mathsf{I}\left(W, Z^n\right) = 0$
- Secrecy capacity: $\max_{p_{UX}} \mathsf{I}(U,Y) - \mathsf{I}(U,Z)$

[1] A. D. Wyner, "The Wire-Tap Channel." Bell system technical journal 54.8 (1975): 1355-1387.

Polar Coding[2]

- Code length $n = 2^m$
- Polar transform: $b^n \mapsto x^n$ and BMS channel P: $p_{Y|X}$
- P_i denotes the sub-channel $p_{B_i|Y^n B^{i-1}}$
- $\mathcal{G}(P) = \left\{i : \mathsf{Z}(P_i) \leq 2^{-n\beta}\right\}$, $\mathcal{B}(P) = \left\{i : \mathsf{I}(P_i) \leq 2^{-n\beta}\right\}$

[2] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels." IEEE Transactions on information Theory 55.7 (2009): 3051-3073.

Polar Coding[2]

- Code length $n = 2^m$
- Polar transform: $b^n \mapsto x^n$ and BMS channel P: $p_{Y|X}$
- P_i denotes the sub-channel $p_{B_i|Y^n B^{i-1}}$
- $\mathcal{G}(P) = \left\{i : \mathsf{Z}(P_i) \leq 2^{-n\beta}\right\}$, $\mathcal{B}(P) = \left\{i : \mathsf{I}(P_i) \leq 2^{-n\beta}\right\}$

For all $0 < \beta < 1/2$:

$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P)| = \mathsf{C}(P)$$
$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{B}(P)| = 1 - \mathsf{C}(P)$$

[2] E. Arıkan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels." IEEE Transactions on information Theory 55.7 (2009): 3051-3073.

Introduction

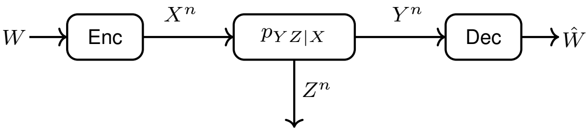
Polar Coding for Wire-Tap Channels

Simulation Results

Strong Secrecy with Polar Codes

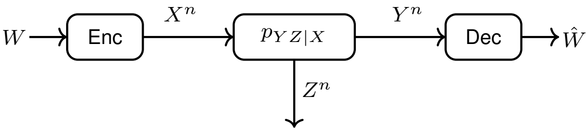
Conclusion and Future Work

Weak Secrecy[3]



[3] H. Mahdavifar and A. Vardy. "Achieving the secrecy capacity of wiretap channels using polar codes." IEEE Transactions on Information Theory 57.10 (2011): 6428-6443.

Weak Secrecy[3]



- Main channel P: $p_{Y|X}$
- Wire-Tap channel Q: $p_{Z|X}$
- $Q \preceq P$

[3] H. Mahdavifar and A. Vardy. "Achieving the secrecy capacity of wiretap channels using polar codes." IEEE Transactions on Information Theory 57.10 (2011): 6428-6443.

Weak Secrecy (Cont'd)

$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P) \cap \mathcal{B}(Q)| = \mathsf{C}(P) - \mathsf{C}(Q)$$
$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P)^c \cap \mathcal{B}(Q)^c| = 0$$

Weak Secrecy (Cont'd)

$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P) \cap \mathcal{B}(Q)| = \mathsf{C}(P) - \mathsf{C}(Q)$$
$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P)^c \cap \mathcal{B}(Q)^c| = 0$$

$$\mathcal{M} = \mathcal{G}(P) \cap \mathcal{B}(Q)$$
$$\mathcal{R} = \mathcal{G}(P) \cap \mathcal{B}(Q)^c$$
$$\mathcal{F} = \mathcal{G}(P)^c \cap \mathcal{B}(Q)$$
$$\mathcal{D} = \mathcal{G}(P)^c \cap \mathcal{B}(Q)^c$$

Weak Secrecy (Cont'd)

$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P) \cap \mathcal{B}(Q)| = \mathsf{C}(P) - \mathsf{C}(Q)$$

$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{G}(P)^c \cap \mathcal{B}(Q)^c| = 0$$

$$\mathcal{M} = \mathcal{G}(P) \cap \mathcal{B}(Q)$$

$$\mathcal{R} = \mathcal{G}(P) \cap \mathcal{B}(Q)^c$$

$$\mathcal{F} = \mathcal{G}(P)^c \cap \mathcal{B}(Q)$$

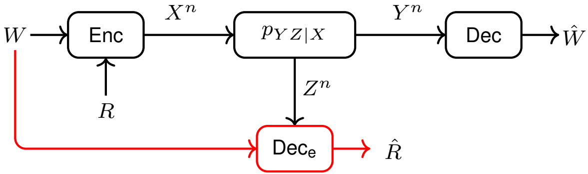
$$\mathcal{D} = \mathcal{G}(P)^c \cap \mathcal{B}(Q)^c$$

$$\lim_{n\to\infty} \frac{1}{n}\mathsf{I}(W, Z^n) = 0$$

Information Leakage

$$\begin{aligned} \mathsf{I}(W, Z^n) &= \mathsf{H}(W) - \mathsf{H}(W|Z^n) \\ &= \mathsf{H}(W) - \mathsf{H}(X^n|Z^n) + \mathsf{H}(X^n|Z^nW) \\ &= \mathsf{H}(W) - \mathsf{H}(X^n) + \mathsf{I}(X^n; Z^n) + \mathsf{H}(X^n|Z^nW) \end{aligned}$$

Information Leakage (Cont'd)



$$\mathsf{H}(X^n|Z^nW) = \mathsf{H}(R|Z^nW) \leq \mathsf{H}_2(P_e) + P_e \log_2(|R|-1),$$
$$P_e = \Pr\left\{\hat{R} \neq R\right\}$$

Information Leakage (Cont'd)

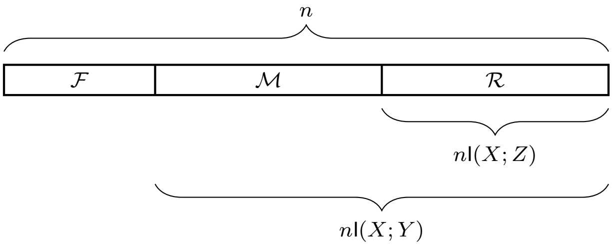
$$\mathsf{I}\,(W, Z^n) < k_M - (k_M + k_R) + n\mathsf{I}(X;Z) + \mathsf{H}_2(P_e) + P_e k_R$$

$$\frac{1}{n}\mathsf{I}\,(W, Z^n) < \mathsf{I}(X;Z) - \frac{k_R}{n} + \mathsf{H}_2(P_e) + P_e\frac{k_R}{n}$$

Information Leakage (Cont'd)

$$\mathsf{I}(W, Z^n) < k_M - (k_M + k_R) + n\mathsf{I}(X;Z) + \mathsf{H}_2(P_e) + P_e k_R$$

$$\frac{1}{n}\mathsf{I}(W, Z^n) < \mathsf{I}(X;Z) - \frac{k_R}{n} + \mathsf{H}_2(P_e) + P_e \frac{k_R}{n}$$



Introduction

Polar Coding for Wire-Tap Channels

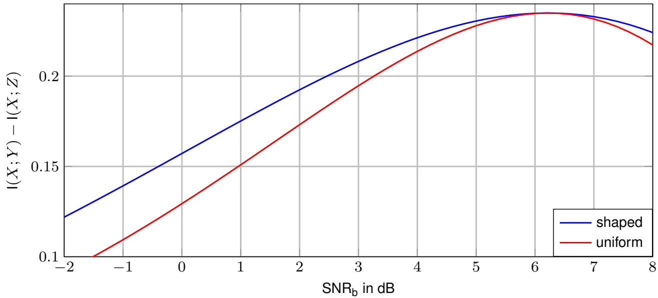
Simulation Results

Strong Secrecy with Polar Codes

Conclusion and Future Work

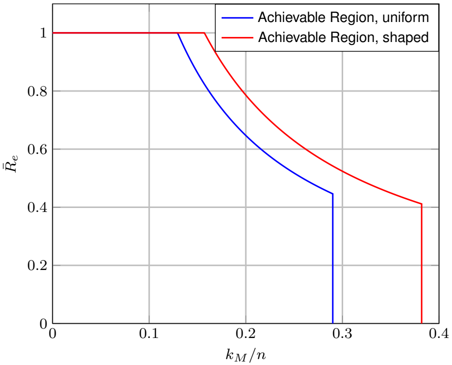
Secrecy Capacity of AWGN with On-Off Keying

- 3 dB degradation: $\mathsf{SNR_b} - \mathsf{SNR_e} = 3$ dB
- $p_X = \arg\max \mathsf{I}(X;Y) - \mathsf{I}(X;Z)$



Secrecy Capacity Region

- $\text{SNR}_\text{b} = 0$ dB, $\text{SNR}_\text{e} = -3$ dB
- Normalized equivocation rate: $\bar{R}_e = \mathsf{H}(W|Z^n)/k_M$



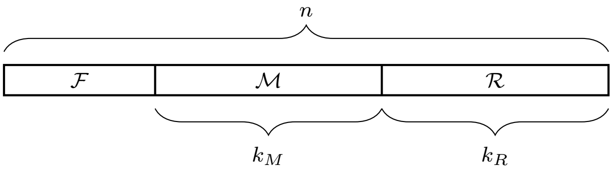
Code Design[4]

- Nested polar codes: (n, k_R), $(n, k_R + k_M)$

[4] T. Wiegart *et al.* "Shaped On-Off Keying Using Polar Codes." IEEE Communications Letters (2019).

Code Design[4]

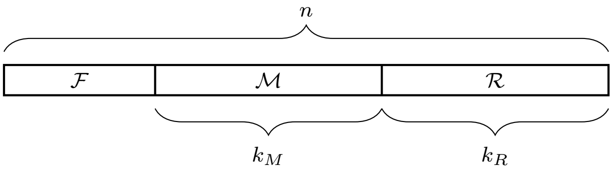
- Nested polar codes: (n, k_R), $(n, k_R + k_M)$



[4] T. Wiegart *et al.* "Shaped On-Off Keying Using Polar Codes." IEEE Communications Letters (2019).

Code Design[4]

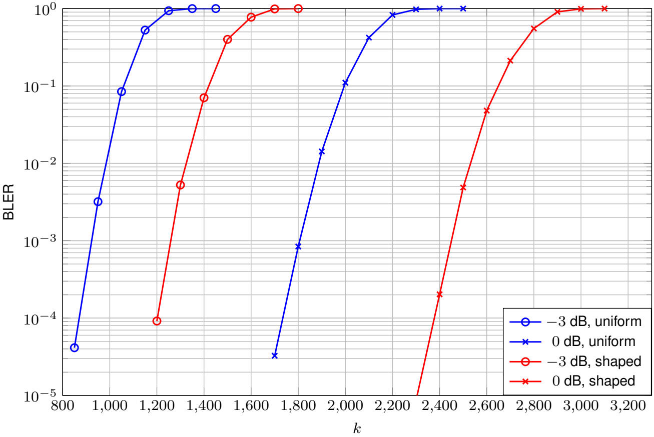
- Nested polar codes: (n, k_R), $(n, k_R + k_M)$



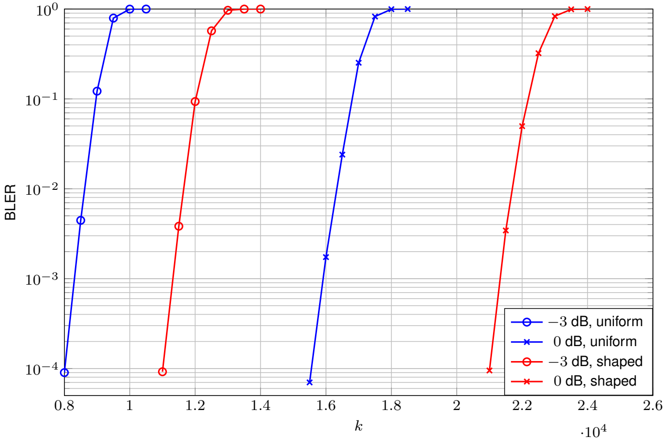
- $n = 8192$, $\ell_{\text{CRC}} = 16$, $L = 32$
- $n = 65536$, $\ell_{\text{CRC}} = 32$, $L = 64$

[4] T. Wiegart *et al.* "Shaped On-Off Keying Using Polar Codes." IEEE Communications Letters (2019).

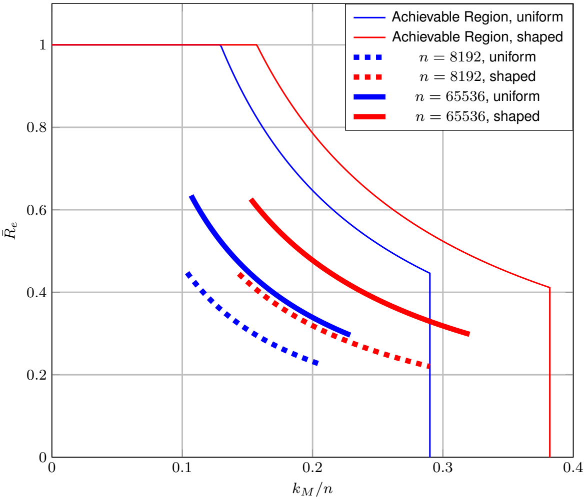
Finite Length Results, $n = 2^{13}$



Finite Length Results, $n = 2^{16}$



Secrecy Capacity Region



Review the Proof of Weak Secrecy

The unreliable and insecure bits in set $\mathcal{D}$.

$$\mathcal{D} = \mathcal{G}(P)^c \cap \mathcal{B}(Q)^c$$

$$\lim_{n\to\infty} \frac{1}{n}|\mathcal{D}| = 0$$

$$\lim_{n\to\infty} \frac{1}{n}\mathsf{I}(W, Z^n) = 0$$

Review the Proof of Weak Secrecy

The unreliable and insecure bits in set $\mathcal{D}$.

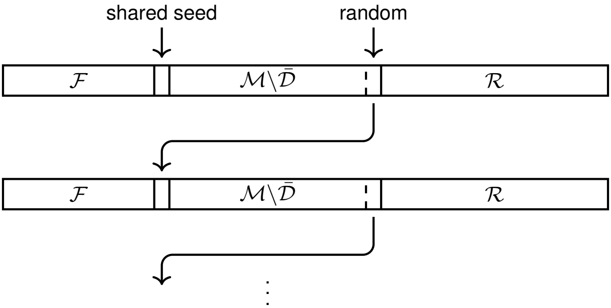
$$\mathcal{D} = \mathcal{G}(P)^c \cap \mathcal{B}(Q)^c$$

$$\lim_{n\to\infty} \frac{1}{n} |\mathcal{D}| = 0$$

$$\lim_{n\to\infty} \frac{1}{n} \mathsf{I}(W, Z^n) = 0$$

$|\mathcal{D}| = o(n) \neq 0$.

Strong Secrecy with Polar Codes[5]



[5] E. Şaşoğlu and A. Vardy. "A new polar coding scheme for strong security on wiretap channels." 2013 IEEE International Symposium on Information Theory. IEEE, 2013.

Introduction

Polar Coding for Wire-Tap Channels

Simulation Results

Strong Secrecy with Polar Codes

Conclusion and Future Work

Conclusion and Future Work

- Higher order modulation
- Other metrics for secrecy
- MAC/BC