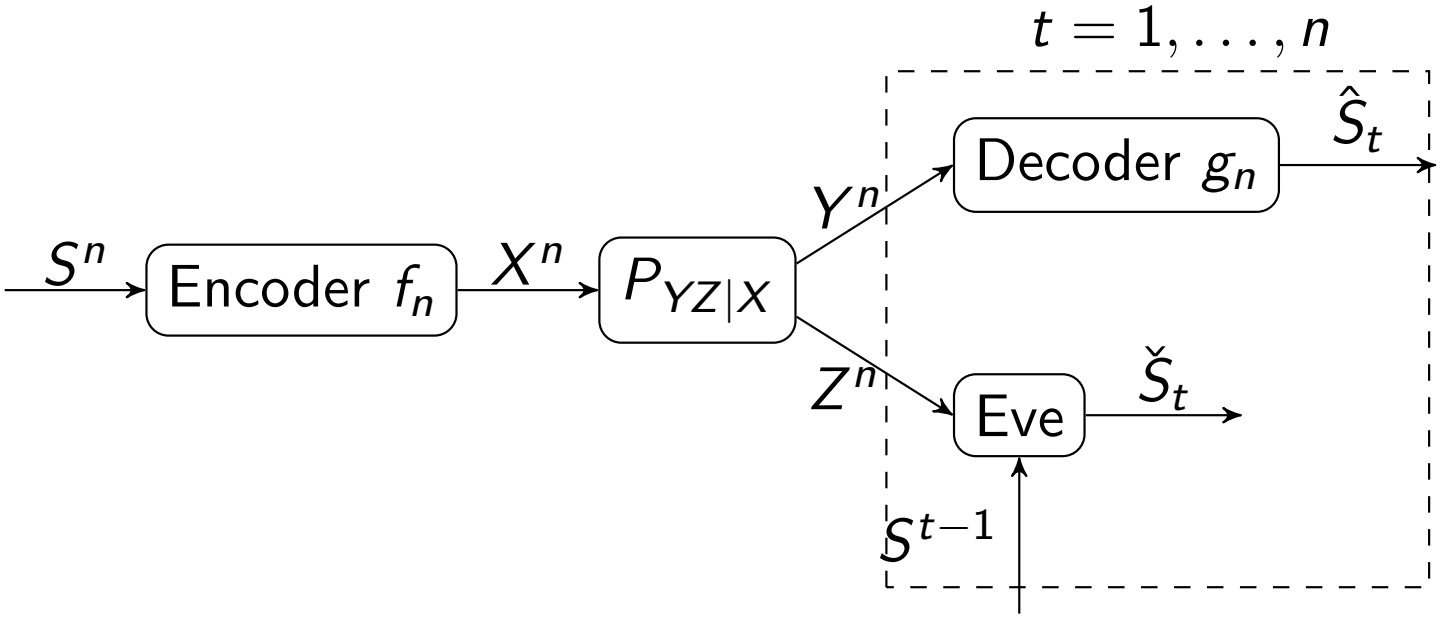
Joint Source-Channel Secrecy Using Hybrid Coding

Eva Song, Paul Cuff, and H. Vincent Poor

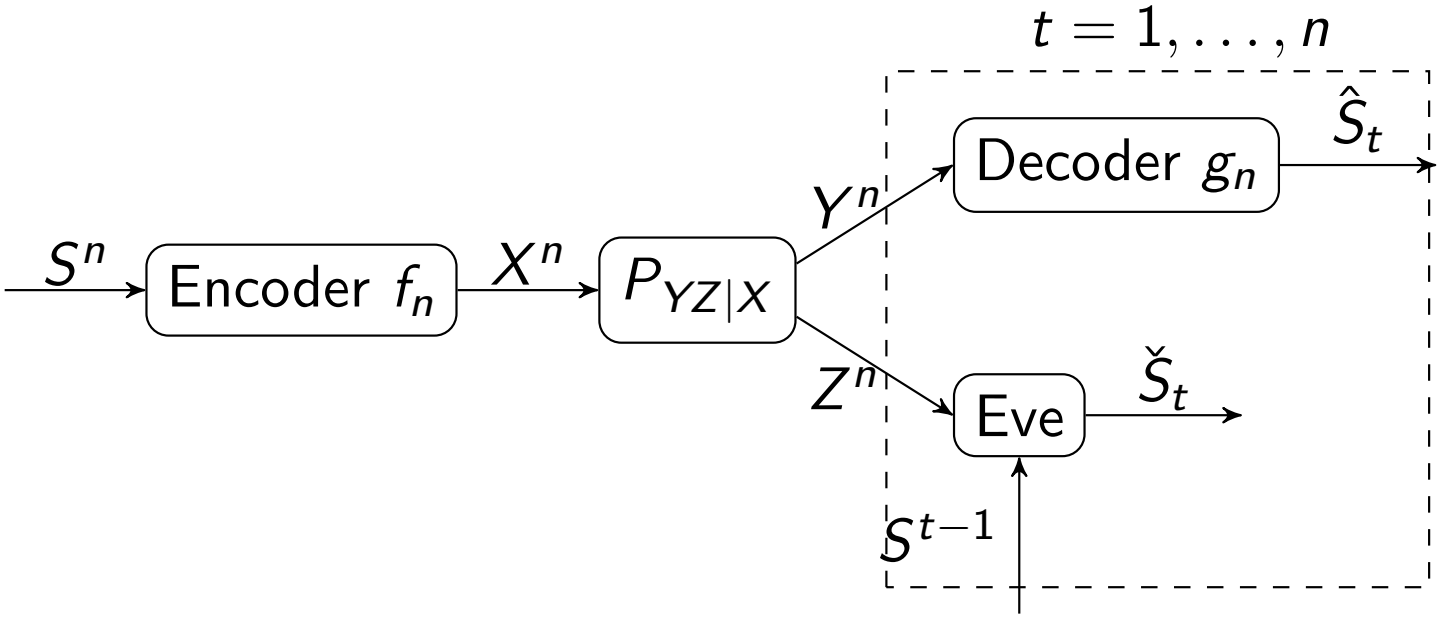
Department of Electrical Engineering
Princeton University

June 19, 2015

A source-channel coding setting

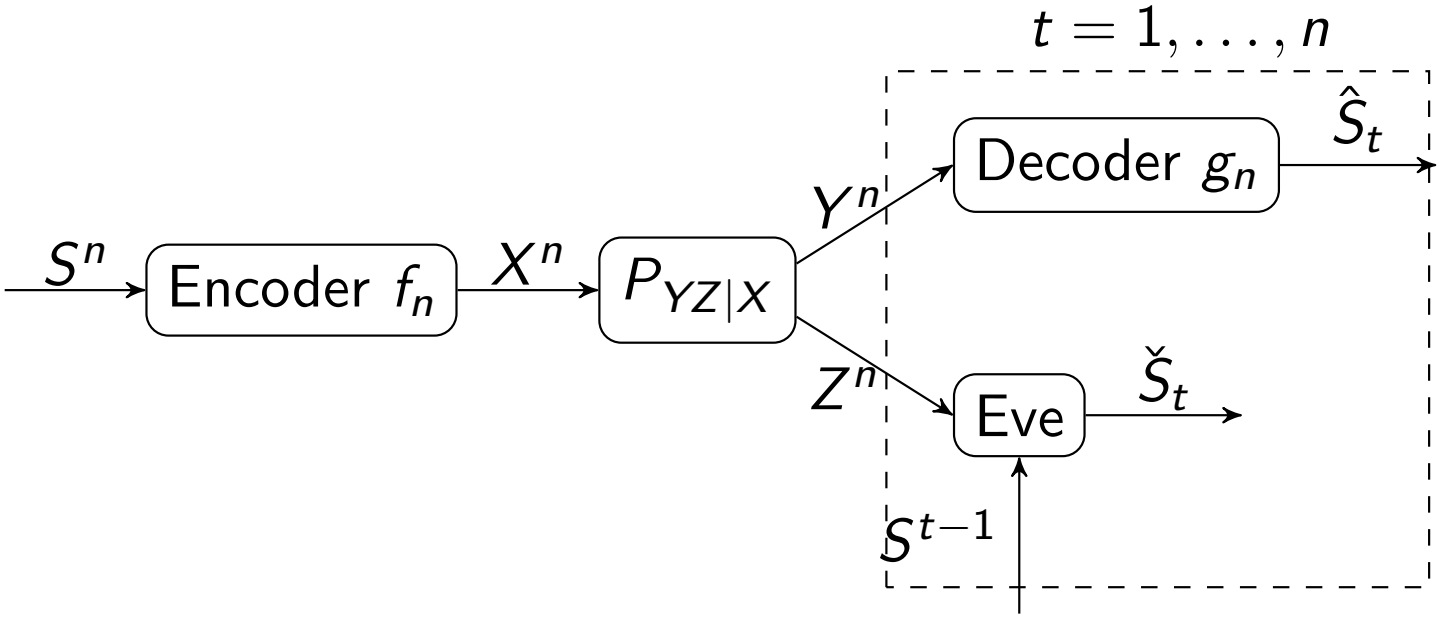


A source-channel coding setting



- Quality of reconstruction: $d(S^n, \hat{S}^n)$, $d(S^n, \check{S}^n)$

A source-channel coding setting



- Quality of reconstruction: $d(S^n, \hat{S}^n)$, $d(S^n, \check{S}^n)$
- Why causal disclosure?
  - Stronger formulation: to the favor of eavesdropper
  - Can generalize equivocation

In this talk...

In this talk...

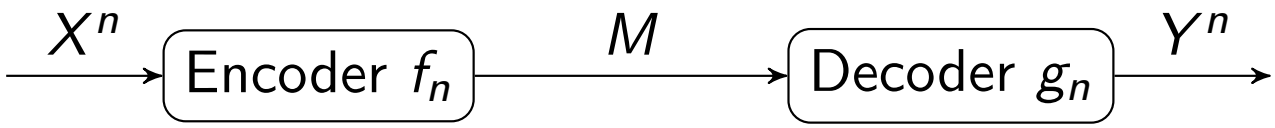
- Design source-channel coding schemes for (D_b, D_e) s.t.
  - $\mathbb{E}\left[d(S^n, \hat{S}^n)\right] \leq_n D_b$
  - $\min_{\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^n} \mathbb{E}[d(S^n, \check{S}^n)] \geq_n D_e$

In this talk...

- Design source-channel coding schemes for (D_b, D_e) s.t.
  - $\mathbb{E}\left[d(S^n, \hat{S}^n)\right] \leq_n D_b$
  - $\min_{\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^n} \mathbb{E}[d(S^n, \check{S}^n)] \geq_n D_e$
- Analysis uses The Likelihood Encoder
  - Total variation distance
  - Soft-covering lemma

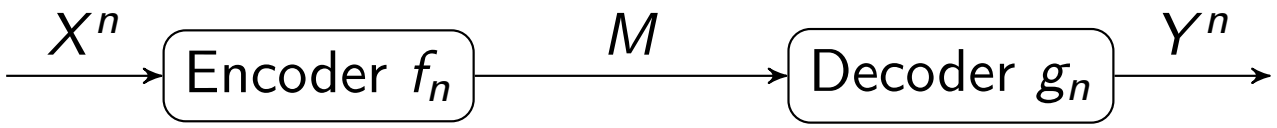
What is a likelihood encoder?

- a stochastic source encoder: $f_n : \mathcal{X}^n \mapsto \mathcal{M}$



What is a likelihood encoder?

- a stochastic source encoder: $f_n : \mathcal{X}^n \mapsto \mathcal{M}$



Given

- a codebook $\{y^n(m)\}_m$, $m \in [1 : 2^{nR}]$
- a joint distribution P_{XY}

the likelihood function for each codeword:

$$\mathcal{L}(m|x^n) \triangleq P_{X^n|Y^n}(x^n|y^n(m)) = \prod P_{X|Y}(x^n|y^n(m))$$

the likelihood encoder determines the message index according to:

$$P_{M|X^n}(m|x^n) = \frac{\mathcal{L}(m|x^n)}{\sum_{m' \in [1:2^{nR}]} \mathcal{L}(m'|x^n)} \propto \mathcal{L}(m|x^n).$$

Warm up – soft-covering lemma

Lemma

- *Given*
  1) $\overline{P}_{UXZ}$
  2) random $\mathcal{C}^{(n)}$ *of sequences* $U^n(m) \sim \prod_{t=1}^{n} \overline{P}_U(u_t)$, $m \in [1 : 2^{nR}]$

Warm up – soft-covering lemma

Lemma

- *Given*
  1) $\overline{P}_{UXZ}$
  2) random $\mathcal{C}^{(n)}$ *of sequences* $U^n(m) \sim \prod_{t=1}^{n} \overline{P}_U(u_t)$, $m \in [1 : 2^{nR}]$
- *Let*

$$\mathbf{P}_{MX^nZ^k}(m, x^n, z^k) \triangleq \frac{1}{2^{nR}} \prod_{t=1}^{n} \overline{P}_{X|U}(x_t|U_t(m)) \prod_{t=1}^{k} \overline{P}_{Z|XU}(z_t|x_t, U_t(m))$$

$$\overline{P}_{X^nZ^k} \triangleq \prod_{t=1}^{n} \overline{P}_X(x_t) \prod_{t=1}^{k} \overline{P}_{Z|X}(z_t|x_t)$$

Warm up – soft-covering lemma

Lemma

- *Given*
  1) $\overline{P}_{UXZ}$
  2) random $\mathcal{C}^{(n)}$ *of sequences* $U^n(m) \sim \prod_{t=1}^n \overline{P}_U(u_t)$, $m \in [1 : 2^{nR}]$
- *Let*

$$\mathbf{P}_{MX^nZ^k}(m, x^n, z^k) \triangleq \frac{1}{2^{nR}} \prod_{t=1}^{n} \overline{P}_{X|U}(x_t|U_t(m)) \prod_{t=1}^{k} \overline{P}_{Z|XU}(z_t|x_t, U_t(m))$$

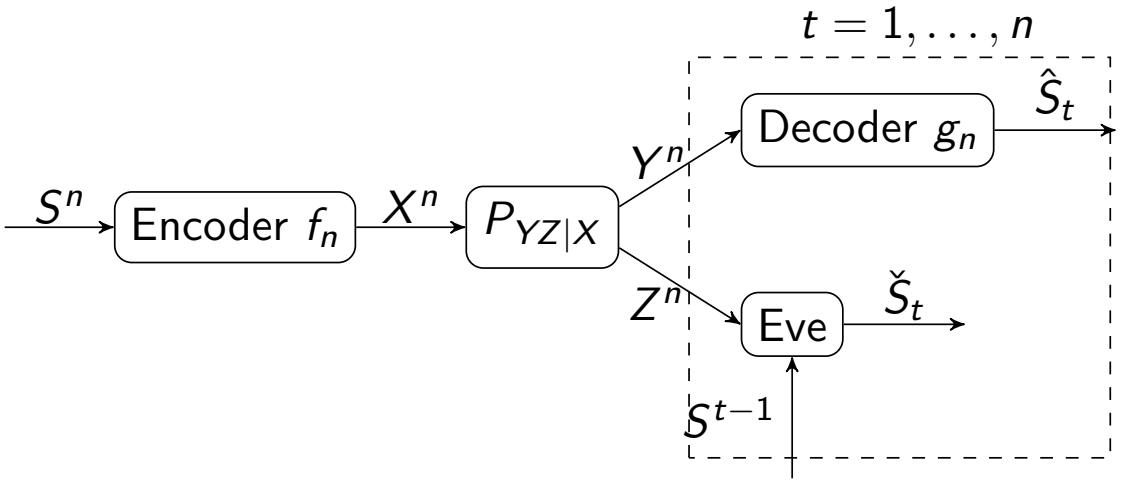
$$\overline{P}_{X^nZ^k} \triangleq \prod_{t=1}^{n} \overline{P}_X(x_t) \prod_{t=1}^{k} \overline{P}_{Z|X}(z_t|x_t)$$

- *If* $R > I(X;U)$, *then*

$$\mathbb{E}_{\mathcal{C}^n}\left[\left\|\mathbf{P}_{X^nZ^k} - \overline{P}_{X^nZ^k}\right\|_{TV}\right] \leq \exp(-\gamma n) \to_n 0,$$

for any $\beta < \frac{R - I(X;U)}{I(Z;U|X)}$, $k \leq \beta n$, $\gamma > 0$ *depending on this gap.*

Problem setup



- i.i.d. source $S^n \sim \prod_{t=1}^n \overline{P}_S(s_t)$
- memoryless broadcast channel $\prod_{t=1}^n \overline{P}_{YZ|X}(y_t, z_t|x_t)$
- Encoder $f_n : \mathcal{S}^n \mapsto \mathcal{X}^n$ (possibly stochastic)
- Legitimate receiver decoder $g_n : \mathcal{Y}^n \mapsto \hat{\mathcal{S}}^n$ (possibly stochastic)
- Eavesdropper decoders $\left\{P_{\check{S}_t|Z^n S^{t-1}}\right\}_{t=1}^n$

Definition

Definition

A distortion pair (D_b, D_e) is achievable if there exists a sequence of source-channel encoders and decoders (f_n, g_n) such that

$$\mathbb{E}[d(S^n, \hat{S}^n)] \leq_n D_b$$

and

$$\min_{\{P_{\check{S}_t|Z^n S^{t-1}}\}_{t=1}^n} \mathbb{E}[d(S^n, \check{S}^n)] \geq_n D_e.$$

We consider

- Scheme O – Operationally separate SC coding [Schieler et al. Allerton 2012]
- Scheme I – Joint SC coding using Hybrid Coding
- Scheme II – Joint SC coding using superposition Hybrid Coding

Scheme O – operational separate

Theorem

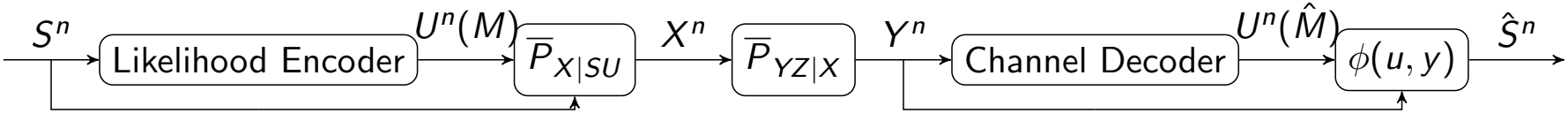
A distortion pair (D_b, D_e) *is achievable if*

$$I(S;U_1) < I(U_2;Y)$$
$$I(S;\hat{S}|U_1) < I(V_2;Y|U_2) - I(V_2;Z|U_2)$$
$$D_b \geq \mathbb{E}\left[d(S,\hat{S})\right]$$
$$D_e \leq \eta \min_{a\in\hat{\mathcal{S}}} \mathbb{E}[d(S,a)] + (1-\eta) \min_{t(u_1)} \mathbb{E}[d(S,t(U_1))]$$

for some distribution $\overline{P}_S \overline{P}_{\hat{S}|S} \overline{P}_{U_1|\hat{S}} \overline{P}_{U_2} \overline{P}_{V_2|U_2} \overline{P}_{X|V_2} \overline{P}_{YZ|X}$, *where*

$$\eta = \frac{[I(U_2;Y) - I(U_2;Z)]^+}{I(S;U_1)}.$$

Hybrid coding



- at least optimal for P2P communication [Minero et al.]
- achieves best known bounds in multiuser settings
- Secrecy: need *stochastic symbol-by-symbol mapping*

Scheme I – basic hybrid coding

Theorem

A distortion pair (D_b, D_e) is achievable if

$$\begin{aligned} I(U;S) &< I(U;Y) \\ D_b &\geq \mathbb{E}[d(S,\phi(U,Y))] \\ D_e &\leq \beta \min_{\psi_0(z)} \mathbb{E}[d(S,\psi_0(Z))] \\ &\quad +(1-\beta) \min_{\psi_1(u,z)} \mathbb{E}[d(S,\psi_1(U,Z))] \end{aligned}$$

where

$$\beta = \min\left\{\frac{[I(U;Y)-I(U;Z)]^+}{I(S;U|Z)}, 1\right\}$$

for some distribution $\overline{P}_S\overline{P}_{U|S}\overline{P}_{X|SU}\overline{P}_{YZ|X}$ and function $\phi(\cdot,\cdot)$.

Scheme I – achievability scheme

- Fix distribution $\overline{P}_S \overline{P}_{U|S} \overline{P}_{X|SU} \overline{P}_{YZ|X}$
- Codebook generation: Independently generate 2^{nR} sequences in $\mathcal{U}^n$ according to $\prod_{t=1}^{n} \overline{P}_U(u_t)$ and index by $m \in [1 : 2^{nR}]$

Scheme I – achievability scheme – continued

- Encoder
  - likelihood encoder $\mathbf{P}_{LE}(m|s^n)$ with

$$\mathcal{L}(m|s^n) = \overline{P}_{S^n|U^n}(s^n|u^n(m))$$

  - produces channel input through a random transformation: $\prod_{t=1}^{n} \overline{P}_{X|SU}(x_t|s_t, U_t(m))$

Scheme I – achievability scheme – continued

- Encoder
  - likelihood encoder $\mathbf{P}_{LE}(m|s^n)$ with

$$\mathcal{L}(m|s^n) = \overline{P}_{S^n|U^n}(s^n|u^n(m))$$

  - produces channel input through a random transformation: $\prod_{t=1}^{n} \overline{P}_{X|SU}(x_t|s_t, U_t(m))$
- Decoder
  - good channel decoder $\mathbf{P}_{D1}(\hat{m}|y^n)$ w.r.t. codebook $\{u^n(a)\}_a$ and memoryless channel $\overline{P}_{Y|U}$
  - deterministic mapping $\phi^n(u^n, y^n)$ is the concatenation of $\{\phi(u_t, y_t)\}_{t=1}^{n}$:

$$\mathbf{P}_{D2}(\hat{s}^n|\hat{m}, y^n) \triangleq \mathbb{1}\{\hat{s}^n = \phi^n(u^n(\hat{m}), y^n)\}$$

Analysis outline – at legitimate receiver

- System induced distribution $\mathbf{P}$
- Idealized distribution $\mathbf{Q}$

$$\begin{aligned}
&\mathbf{Q}_{MU^nS^nX^nY^nZ^n}(m, u^n, s^n, x^n, y^n, z^n) \\
\triangleq\ &\frac{1}{2^{nR}} \mathbb{1}\{u^n = U^n(m)\} \prod_{t=1}^{n} \overline{P}_{S|U}(s_t|u_t) \\
&\prod_{t=1}^{n} \overline{P}_{X|SU}(x_t|s_t, u_t) \prod_{t=1}^{n} \overline{P}_{YZ|X}(y_t, z_t|x_t).
\end{aligned}$$

- soft-covering: $R > I(U;S) \Rightarrow \mathbf{P} \approx \mathbf{Q}$
- channel coding: $R \leq I(U;Y) \Rightarrow$

$$\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}\left[d(S^n, \hat{S}^n)\right]\right] \leq \mathbb{E}_{\overline{P}}[d(S, \phi(U, Y))] + \delta_n$$

Analysis outline – at eavesdropper

- auxiliary distribution

$$\check{\mathbf{Q}}^{(i)}_{S^i Z^n}(s^i, z^n) \triangleq \prod_{t=1}^{n} \overline{P}_Z(z_t) \prod_{j=1}^{i} \overline{P}_{S|Z}(s_j|z_j)$$

- soft-covering: $R > I(Z;U) \Rightarrow \check{\mathbf{Q}}^{(i)}_{Z^n S^i} \approx \mathbf{Q}_{Z^n S^i}$
- i can go up to βn, for any $\beta < \frac{R - I(U;Z)}{I(S;U|Z)}$
- phase transition in distortion
  - before βn:
  - $\min_{\{\psi_{0i}(s^{i-1}, z^n)\}_i} \mathbb{E}_P \left[\frac{1}{k} \sum_{i=1}^{k} d(S_i, \psi_{0i}(S^{i-1}, Z^n)) \right] \geq \min_{\psi_0(z)} \mathbb{E}_{\overline{P}} [d(S, \psi_0(Z))] - \epsilon_n$
  - after βn:
  - $\min_{\{\psi_{1i}(s^{i-1}, z^n)\}} \mathbb{E}_P \left[\frac{1}{k} \sum_{i=j}^{n} d(S_i, \psi_{1i}(S^{i-1}, Z^n)) \right] \geq \min_{\psi_1(u,z)} \mathbb{E}_{\overline{P}} [d(S, \psi_1(U, Z))] - \epsilon_n$

Scheme II – superposition hybrid coding

Theorem

A distortion pair (D_b, D_e) *is achievable if*

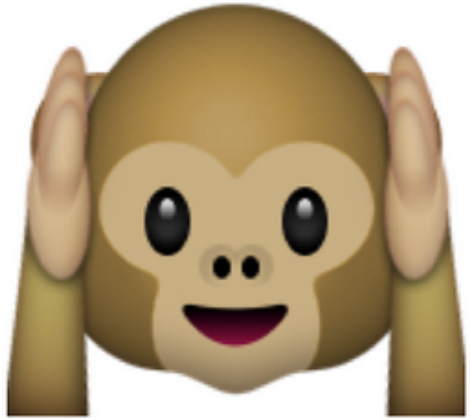
$$\begin{aligned} I(V;S) &< I(UV;Y) \\ D_b &\geq \mathbb{E}\left[d(S,\phi(V,Y))\right] \\ D_e &\leq \min\{\beta,\alpha\} \min_{\psi_0(z)} \mathbb{E}\left[d(S,\psi_0(Z))\right] \\ &\quad + (\alpha - \min\{\beta,\alpha\}) \min_{\psi_1(u,z)} \mathbb{E}\left[d(S,\psi_1(U,Z))\right] \\ &\quad + (1-\alpha) \min_{\psi_2(v,z)} \mathbb{E}\left[d(S,\psi_2(V,Z))\right] \end{aligned}$$

for some distribution $\overline{P}_S \overline{P}_{V|S} \overline{P}_{U|V} \overline{P}_{X|SUV} \overline{P}_{YZ|X}$ *and function* $\phi(\cdot,\cdot)$.

Scheme II – achievability proof

Scheme II – achievability proof





Relations among schemes

- Scheme II generalizes Scheme I
- Scheme II generalizes Scheme O

Perfect secrecy outer bound

Theorem

If (D_b, D_e) *is achievable, then*

$$\begin{aligned} I(S;U) &\leq I(U;Y) \\ D_b &\geq \mathbb{E}[d(S,\phi(U,Y))] \\ D_e &\leq \min_{a\in\hat{\mathcal{S}}} \mathbb{E}[d(S,a)] \end{aligned}$$

for some distribution $\overline{P}_S\overline{P}_{U|S}\overline{P}_{X|SU}\overline{P}_{YZ|X}$ *and function* $\phi(\cdot,\cdot)$.

Numerical example

- Source: i.i.d. $Bern(p)$
- Channels: BSC with crossover probabilities p_1, p_2
- Legitimate receiver: lossless decoding
- Eavesdropper: Hamming distortion

Numerical example

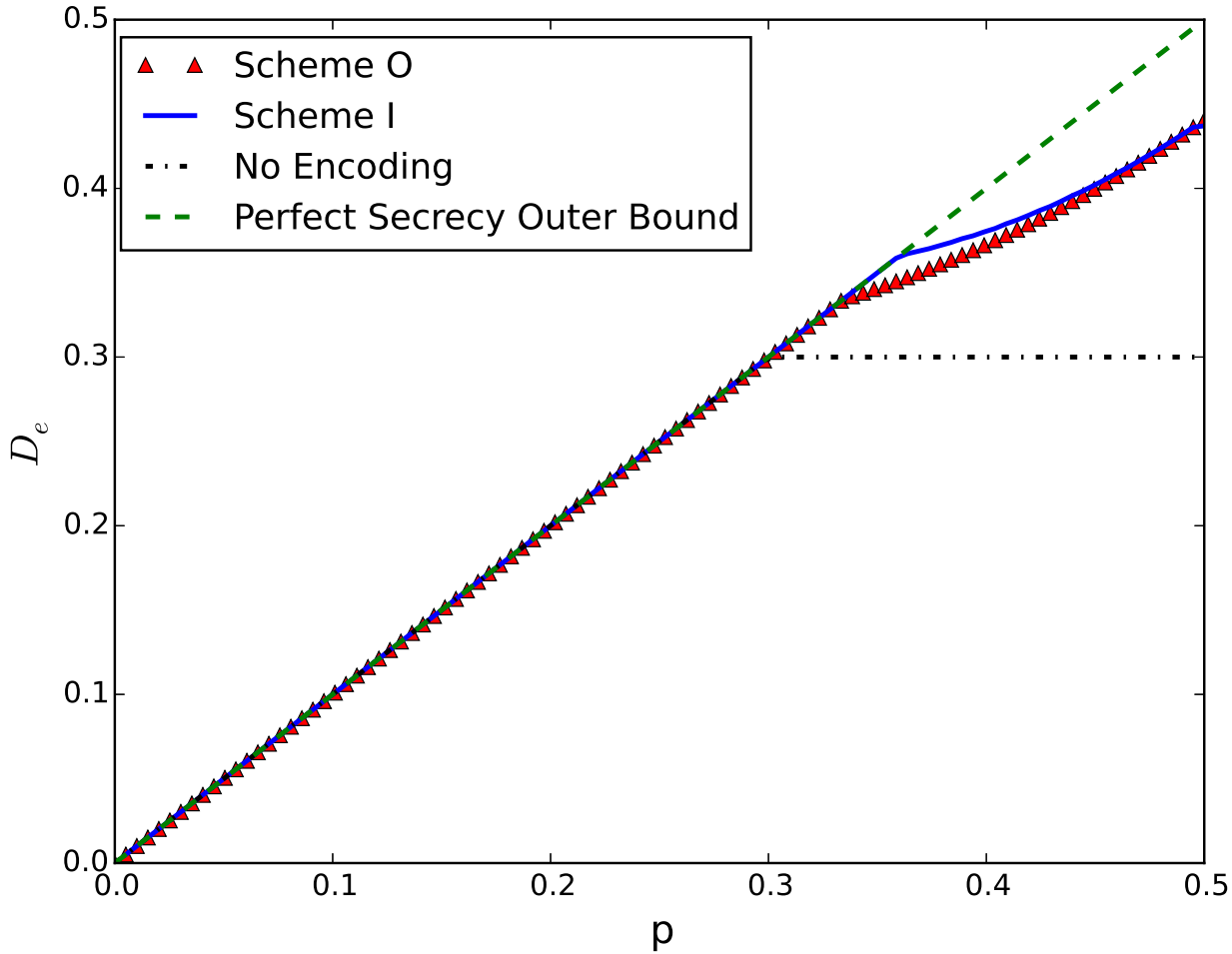


Figure: Distortion at the eavesdropper as a function of source distribution p with $p_1 = 0$, $p_2 = 0.3$

Summary

- have done:
  - achieved better performance in joint source-channel secrecy with hybrid coding
  - superposition hybrid coding (II) fully generalizes basic hybrid coding (I) and operationally separate SC coding (O)
- have not done:
  - Can I outperform O?
  - Is II strictly better than I?
  - non-trivial outer bound?