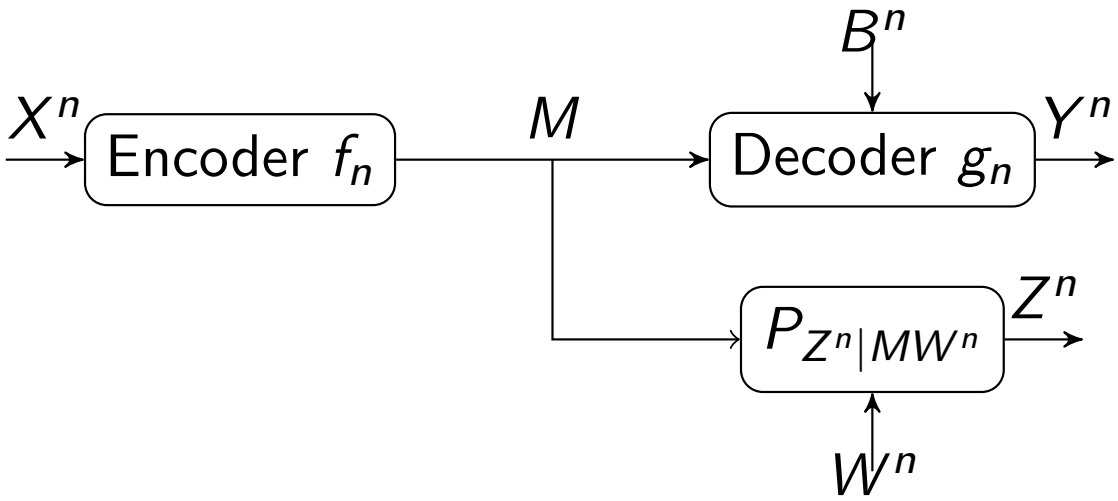
A Rate-Distortion Based Secrecy System with Side Information at the Decoders

Eva Song, Paul Cuff, and H. Vincent Poor

Department of Electrical Engineering
Princeton University

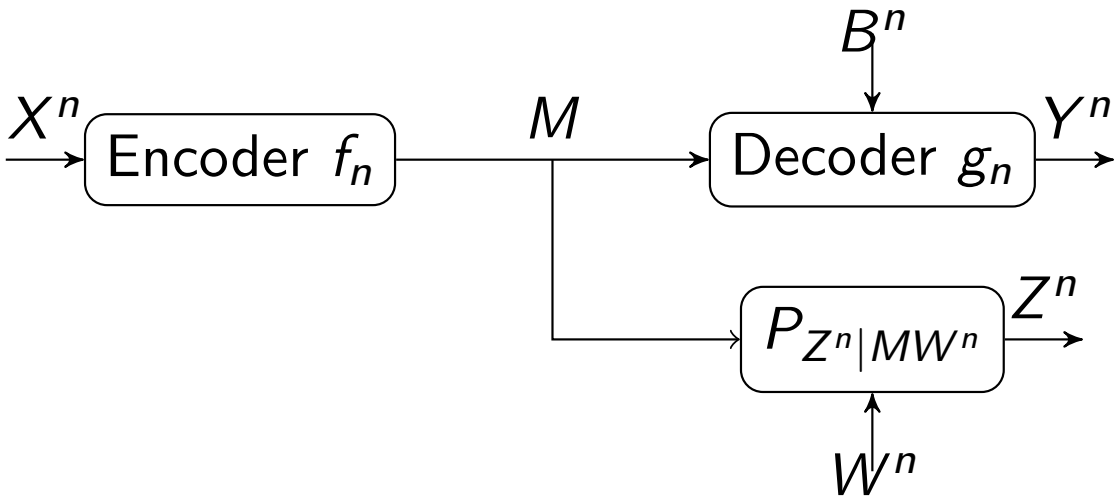
Oct 2, 2014

Related work



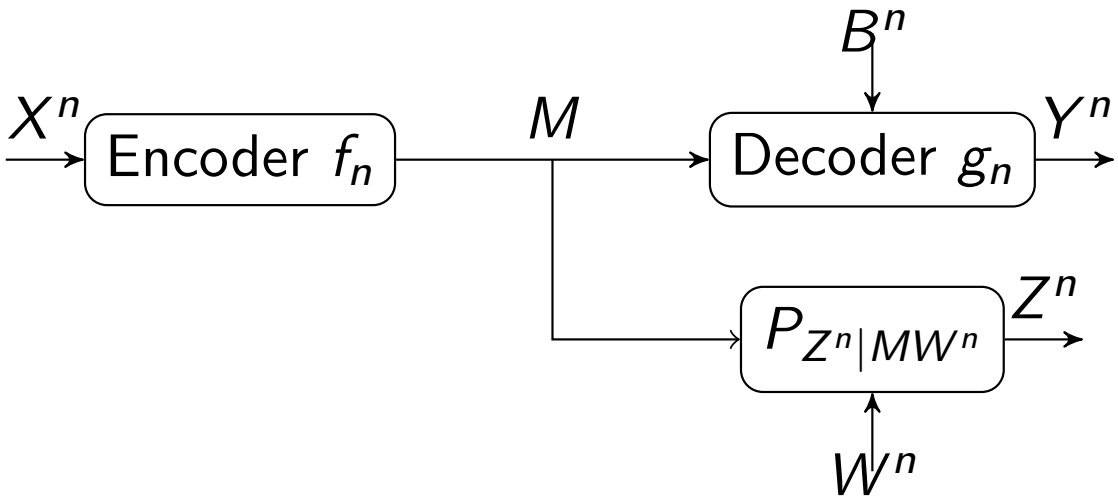
- average distortion $d(x^n, y^n) = \frac{1}{n}\sum_{t=1}^{n} d(x_t, y_t)$

Related work



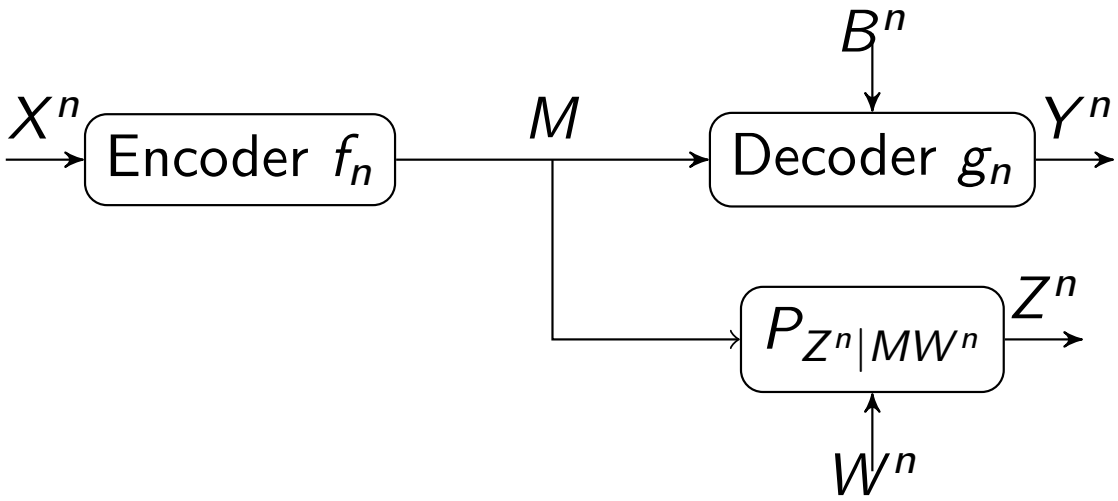
- average distortion $d(x^n, y^n) = \frac{1}{n}\sum_{t=1}^{n} d(x_t, y_t)$
- Secret key sharing [Schieler & Cuff ISIT '12] ✓

Related work



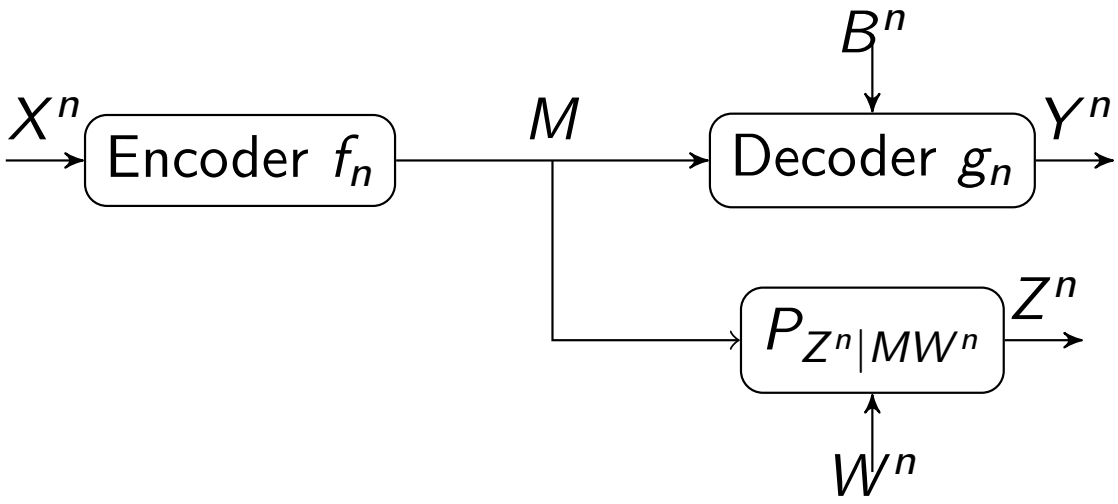
- average distortion $d(x^n, y^n) = \frac{1}{n}\sum_{t=1}^{n} d(x_t, y_t)$
- Secret key sharing [Schieler & Cuff ISIT '12] ✓
- RD-Equivocation [Villard & Piantanida Allerton '10] ✓
  - RD at legitimate receiver
  - Equivocation at eavesdropper

Related work



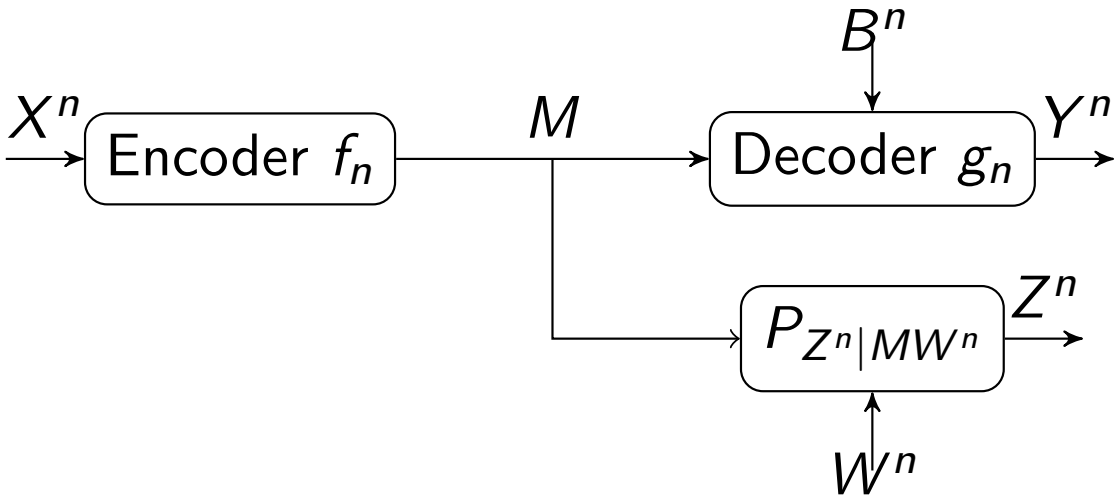
- average distortion $d(x^n, y^n) = \frac{1}{n}\sum_{t=1}^{n} d(x_t, y_t)$
- Secret key sharing [Schieler & Cuff ISIT '12] ✓
- RD-Equivocation [Villard & Piantanida Allerton '10] ✓
  - RD at legitimate receiver
  - Equivocation at eavesdropper
- RD-RD ⋆
  - RD at legitimate receiver
  - RD at eavesdropper

Problem setup

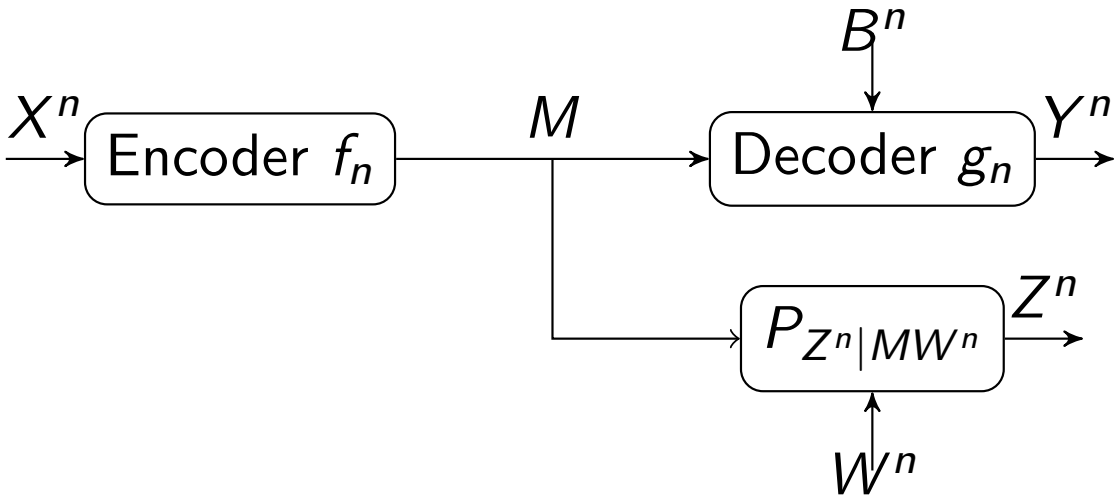


- i.i.d. source and correlated side info $X^n B^n W^n \sim \prod \overline{P}_{XBW}$
- Encoder $f_n : \mathcal{X}^n \mapsto \mathcal{M}$ (possibly stochastic)
- Legitimate receiver decoder $g_n : \mathcal{M} \times \mathcal{B}^n \mapsto \mathcal{Y}^n$ (possibly stochastic)
- Eavesdropper decoder $P_{Z^n|MW^n}$
- Compression rate: R, i.e. $|\mathcal{M}| = 2^{nR}$

Problem setup – continued



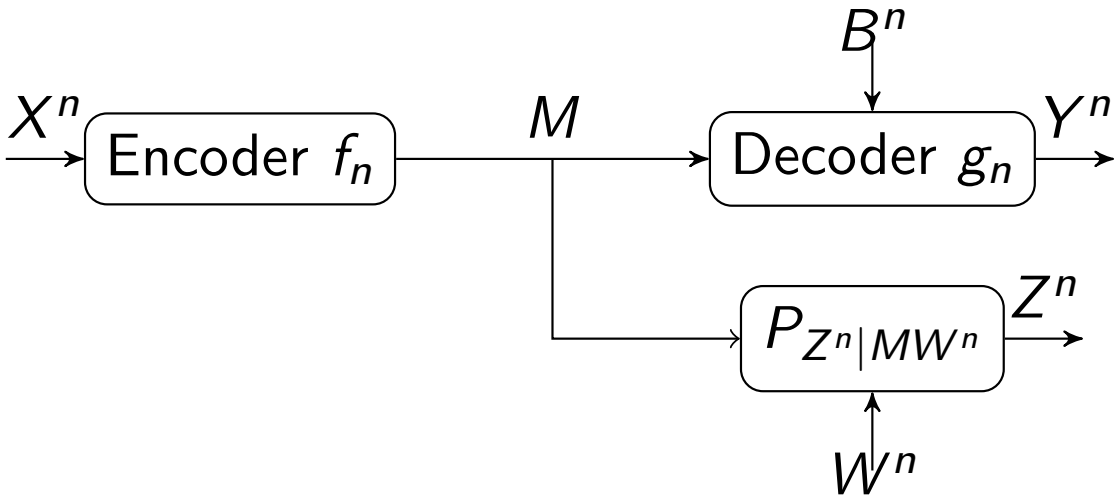
Problem setup – continued



- Average distortion for the legitimate receiver:

$$\mathbb{E}[d_b(X^n, Y^n)] \leq_n D_b$$

Problem setup – continued



- Average distortion for the legitimate receiver:

$$\mathbb{E}[d_b(X^n, Y^n)] \leq_n D_b$$

- Minimum average distortion for the eavesdropper:

$$\min_{P_{Z^n|MW^n}} \mathbb{E}[d_w(X^n, Z^n)] \geq_n D_w$$

Lossy compression

Definition

The rate-distortion triple (R, D_b, D_w) *is achievable if there exists a sequence of rate* R *encoders and decoders* (f_n, g_n) *such that*

$$\mathbb{E}[d_b(X^n, Y^n)] \leq_n D_b$$

and

$$\min_{P_{Z^n|MW^n}} \mathbb{E}[d_w(X^n, Z^n)] \geq_n D_w.$$

Inner bound

Theorem

A rate-distortion triple (R, D_b, D_w) *is achievable if*

$$R > I(V;X|B)$$
$$D_b \geq \mathbb{E}[d_b(X,Y)]$$
$$D_w \leq \min_{z(u,w)} \mathbb{E}[d_w(X, Z(U,W))]$$
$$I(V;B|U) > I(V;W|U)$$

for some $\overline{P}_{UVXBW} = \overline{P}_{XBW}\overline{P}_{V|X}\overline{P}_{U|V}$, *where* $Y = \phi(V,B)$ *for some function* $\phi(\cdot,\cdot)$.

Outer bound

Theorem

If a rate-distortion triple (R, D_b, D_w) *is achievable, then*

$$R \geq I(V; X|B)$$
$$D_b \geq \mathbb{E}[d_b(X, Y)]$$
$$D_w \leq \min_{z(w)} \mathbb{E}[d_w(X, Z(W))]$$

for some $\overline{P}_{VXBW} = \overline{P}_{XBW}\overline{P}_{V|X}$, *where* $Y = \phi(V, B)$ *for some function* $\phi(\cdot, \cdot)$ *and all the quantities are with respect to* $\overline{P}_{XBW}$.

Outer bound

Theorem

If a rate-distortion triple (R, D_b, D_w) *is achievable, then*

$$R \geq I(V; X|B)$$
$$D_b \geq \mathbb{E}[d_b(X, Y)]$$
$$D_w \leq \min_{z(w)} \mathbb{E}[d_w(X, Z(W))]$$

for some $\overline{P}_{VXBW} = \overline{P}_{XBW}\overline{P}_{V|X}$, *where* $Y = \phi(V, B)$ *for some function* $\phi(\cdot, \cdot)$ *and all the quantities are with respect to* $\overline{P}_{XBW}$.

- proof:
  - $R - D_b$: Wyner-Ziv converse
  - D_w: cannot be worse than symbol-by-symbol estimation of X^n from W^n without M

Less noisy side info

Definition

The side information B is **strictly** *less noisy than the side information W with respect to X if*

$$I(V;B) > I(V;W)$$

for all V such that $V - X - (B, W)$ and $I(V;B) > 0$.

Less noisy side info

Definition

The side information B is **strictly** *less noisy than the side information W with respect to X if*

$$I(V;B) > I(V;W)$$

for all V such that $V - X - (B, W)$ and $I(V;B) > 0$.

Corollary

If the legitimate receiver has **strictly** *less noisy side information than the eavesdropper, Inner and Outer bounds match.*

secrecy is FREE

Lossless compression

Definition

A rate-distortion pair (R, D_w) is achievable if there exists a sequence of encoders and decoders (f_n, g_n) such that

$$\lim_{n\to\infty} \mathbb{P}\left[X^n \neq Y^n\right] = 0$$

and

$$\min_{P_{Z^n|M,W^n}} \mathbb{E}[d_w(X^n, Z^n)] \geq_n D_w.$$

Lossless compression – achievability

Corollary

(R, D_w) is achievable if

$$R > H(X|B)$$
$$D_w \leq \min_{z(u,w)} \mathbb{E}[d_w(X, z(U, W))]$$
$$I(X; B|U) > I(X; W|U)$$

for some $\overline{P}_{UXBW} = \overline{P}_{XBW}\overline{P}_{U|X}$.

More capable side info

Definition

The side information B is **strictly** *more capable than the side information W with respect to X if*

$$I(X;B) > I(X;W).$$

More capable side info

Definition

The side information B is **strictly** *more capable than the side information W with respect to X if*

$$I(X;B) > I(X;W).$$

Corollary

If the legitimate receiver has strictly more capable side information than the eavesdropper with respect to the source, then the rate-distortion pair (R, D_w) is achievable if and only if

$$R \geq H(X|B)$$
$$D_w \leq \min_{z(w)} \mathbb{E}[d_w(X, z(W))].$$

secrecy is FREE

Proof of Inner bound

Proof of Inner bound

- Fix $\overline{P}_{UVXBW} = \overline{P}_X \overline{P}_{BW|X} \overline{P}_{V|X} \overline{P}_{U|V}$ s.t.
  - $I_{\overline{P}}(V; B|U) > I_{\overline{P}}(V; W|U)$
  - $\mathbb{E}_{\overline{P}}[d_b(X, \phi(V, B))] \leq D_b$
  - $\min_{z(u,w)} \mathbb{E}_{\overline{P}}[d_w(X, Z(U, W))] \geq D_w$

Proof of Inner bound

- Fix $\overline{P}_{UVXBW} = \overline{P}_X \overline{P}_{BW|X} \overline{P}_{V|X} \overline{P}_{U|V}$ s.t.
  - $I_{\overline{P}}(V; B|U) > I_{\overline{P}}(V; W|U)$
  - $\mathbb{E}_{\overline{P}}[d_b(X, \phi(V, B))] \leq D_b$
  - $\min_{z(u,w)} \mathbb{E}_{\overline{P}}[d_w(X, Z(U, W))] \geq D_w$
- Fix rates R_p, R'_p, R_s, R'_s
  - $R_p + R'_p > I_{\overline{P}}(U; X)$
  - $R'_p < I_{\overline{P}}(U; B)$
  - $R_s + R'_s > I_{\overline{P}}(X; V|U)$
  - $I_{\overline{P}}(V; W|U) < R'_s < I_{\overline{P}}(V; B|U)$

Proof of Inner bound

- Fix $\overline{P}_{UVXBW} = \overline{P}_X \overline{P}_{BW|X} \overline{P}_{V|X} \overline{P}_{U|V}$ s.t.
  - $I_{\overline{P}}(V; B|U) > I_{\overline{P}}(V; W|U)$
  - $\mathbb{E}_{\overline{P}}[d_b(X, \phi(V, B))] \leq D_b$
  - $\min_{z(u,w)} \mathbb{E}_{\overline{P}}[d_w(X, Z(U, W))] \geq D_w$
- Fix rates R_p, R'_p, R_s, R'_s
  - $R_p + R'_p > I_{\overline{P}}(U; X)$
  - $R'_p < I_{\overline{P}}(U; B)$
  - $R_s + R'_s > I_{\overline{P}}(X; V|U)$
  - $I_{\overline{P}}(V; W|U) < R'_s < I_{\overline{P}}(V; B|U)$
- Main tool:
  - soft-covering lemmas
  - likelihood encoder

Codebook generation

Codebook generation

- $\mathcal{C}_U^{(n)}$
  - independently generate $2^{n(R_p+R_p')}$ sequences in $\mathcal{U}^n \sim \prod_{t=1}^n \overline{P}_U(u_t)$
  - index by (m_p, m_p')

Codebook generation

- $\mathcal{C}_U^{(n)}$
  - independently generate $2^{n(R_p+R_p')}$ sequences in $\mathcal{U}^n \sim \prod_{t=1}^n \overline{P}_U(u_t)$
  - index by (m_p, m_p')
- $\mathcal{C}_V^{(n)}(m_p, m_p')$
  - independently generate $2^{n(R_s+R_s')}$ sequences in $\mathcal{V}^n \sim \prod_{t=1}^n \overline{P}_{V|U}(v_t|u_t(m_p, m_p'))$
  - index by (m_p, m_p', m_s, m_s')

Encoder

- System induced distribution

$$\begin{aligned} & \mathbf{P}(x^n, b^n, w^n, m_p, m'_p, m_s, m'_s, \hat{m}'_p, \hat{m}'_s, y^n) \\ \triangleq \; & \overline{P}_{X^n B^n W^n}(x^n, b^n, w^n)\mathbf{P}_E(m_p, m'_p, m_s, m'_s|x^n) \\ & \mathbf{P}_D(\hat{m}'_p, \hat{m}'_s|m_p, m_s, b^n)\mathbf{P}_\Phi(y^n|m_p, \hat{m}'_p, m_s, \hat{m}'_s, b^n) \end{aligned}$$

Encoder

- System induced distribution

$$\begin{aligned} & \mathbf{P}(x^n, b^n, w^n, m_p, m_p', m_s, m_s', \hat{m}_p', \hat{m}_s', y^n) \\ \triangleq\ & \overline{P}_{X^n B^n W^n}(x^n, b^n, w^n)\mathbf{P}_E(m_p, m_p', m_s, m_s'|x^n) \\ & \mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)\mathbf{P}_\Phi(y^n|m_p, \hat{m}_p', m_s, \hat{m}_s', b^n) \end{aligned}$$

- Encoder: the likelihood encoder

$$\mathbf{P}_E(m|x^n) = \frac{\mathcal{L}(m|x^n)}{\sum_{\bar{m}\in\mathcal{M}} \mathcal{L}(\bar{m}|x^n)},$$

$$\mathcal{L}(m|x^n) = \overline{P}_{X^n|V^n}(x^n|v^n(m))$$

Decoder

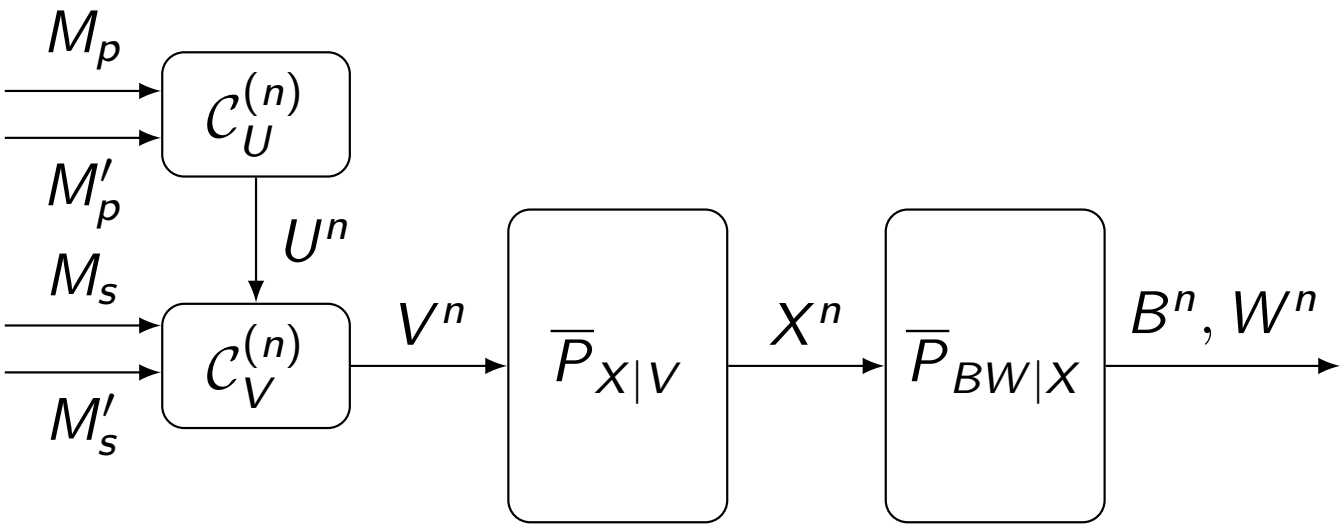
Decoder

- $\mathbf{P}_D(\hat{m}'_p, \hat{m}'_s | m_p, m_s, b^n)$ a good channel decoder w.r.t.
  - superposition sub-codebook $\{v^n(m_p, a_p, m_s, a_s)\}_{a_p, a_s}$
  - memoryless channel $\overline{P}_{B|V}$

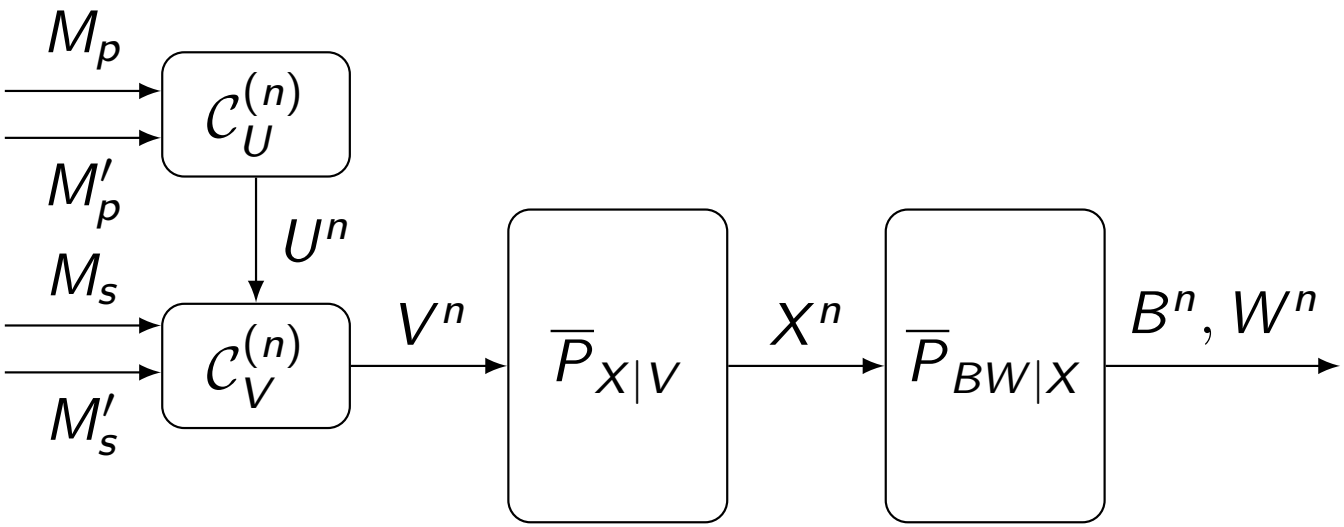
Decoder

- $\mathbf{P}_D(\hat{m}'_p, \hat{m}'_s | m_p, m_s, b^n)$ a good channel decoder w.r.t.
  - superposition sub-codebook $\{v^n(m_p, a_p, m_s, a_s)\}_{a_p, a_s}$
  - memoryless channel $\overline{P}_{B|V}$
- $\mathbf{P}_\Phi(y^n | m_p, \hat{m}'_p, m_s, \hat{m}'_s, b^n)$ deterministic function
  - fix a function $\phi^n(v^n, b^n)$
  - define $\phi^n(v^n, b^n)$ as the concatenation $\{\phi(v_t, b_t)\}_{t=1}^n$
  - $\mathbb{1}\{y^n = \phi^n(v^n(m_p, \hat{m}'_p, m_s, \hat{m}'_s), b^n)\}$

Distortion at the legitimate receiver

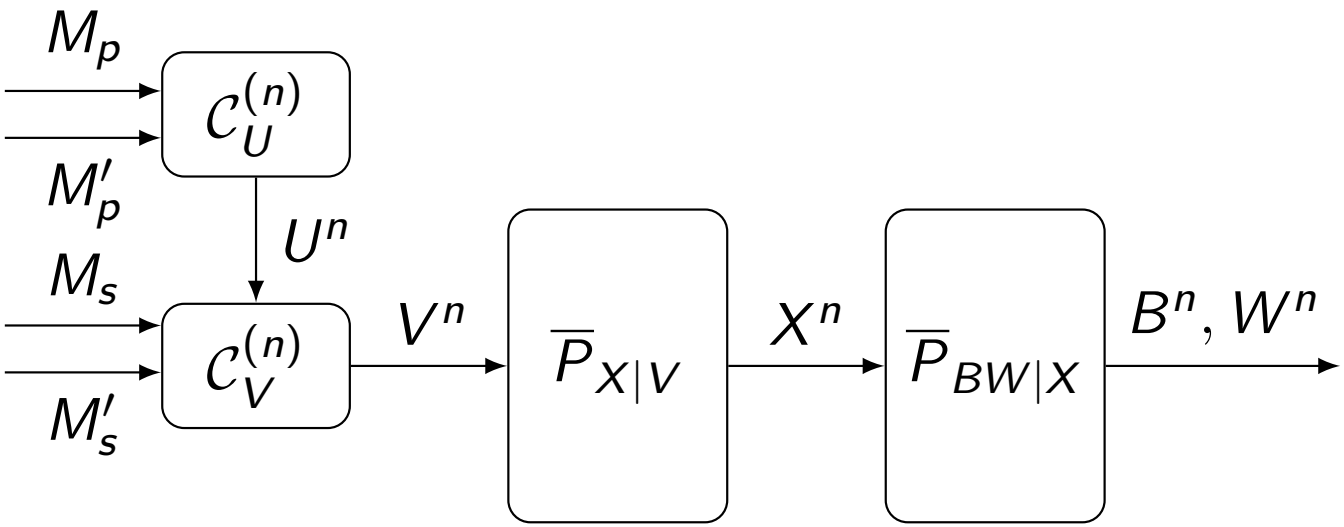


Distortion at the legitimate receiver



- $\mathbf{P}_E(m_p, m'_p, m_s, m'_s|x^n) = \mathbf{Q}(m_p, m'_p, m_s, m'_s|x^n)$

Distortion at the legitimate receiver



- $\mathbf{P}_E(m_p, m_p', m_s, m_s'|x^n) = \mathbf{Q}(m_p, m_p', m_s, m_s'|x^n)$
- $\mathbf{Q}^{(1)}(x^n, b^n, w^n, u^n, v^n, m_p, m_p', m_s, m_s', \hat{m}_p', \hat{m}_s') \triangleq$
  $\mathbf{Q}(\ldots)\mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)\mathbf{P}_\Phi(y^n|m_p, \hat{m}_p', m_s, \hat{m}_s')$
- $\mathbf{Q}^{(2)}(x^n, b^n, w^n, u^n, v^n, m_p, m_p', m_s, m_s', \hat{m}_p', \hat{m}_s') \triangleq$
  $\mathbf{Q}(\ldots)\mathbf{P}_D(\hat{m}_p', \hat{m}_s'|m_p, m_s, b^n)\mathbf{P}_\Phi(y^n|m_p, m_p', m_s, m_s')$

Distortion at the legitimate receiver – continued

- $\mathbf{P} \approx_n \mathbf{Q}^{(1)}$
- $\mathbf{Q}^{(1)} \approx_n \mathbf{Q}^{(2)}$
- $\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{Q}^{(2)}}[d_b(X^n, Y^n)]\right] = \mathbb{E}_{\overline{P}}[d_b(X, Y)]$
- $\mathbb{E}_{\mathcal{C}^{(n)}}\left[\mathbb{E}_{\mathbf{P}}[d_b(X^n, Y^n)]\right] \leq_n \mathbb{E}_{\overline{P}}[d_b(X, Y)]$

Distortion at the eavesdropper

Distortion at the eavesdropper

- Auxiliary distribution $\tilde{\mathbf{Q}}^{(i)}$

$$\begin{aligned}
&\tilde{\mathbf{Q}}^{(i)}(m_p, m_p', m_s, m_s', u^n, x, w^n) \\
\triangleq\ &\frac{1}{2^{n(R_p+R_p'+R_s+R_s')}} \mathbb{1}\{u^n = U^n(m_p, m_p')\} \\
&\prod_{t=1}^{n} \overline{P}_{W|U}(w_t|U_t(m_p, m_p'))\overline{P}_{X|WU}(x|w_i, U_i(m_p, m_p')).
\end{aligned}$$

Distortion at the eavesdropper

- Auxiliary distribution $\tilde{\mathbf{Q}}^{(i)}$

$$\begin{aligned}
&\tilde{\mathbf{Q}}^{(i)}(m_p, m_p', m_s, m_s', u^n, x, w^n) \\
\triangleq\ &\frac{1}{2^{n(R_p+R_p'+R_s+R_s')}} \mathbb{1}\{u^n = U^n(m_p, m_p')\} \\
&\prod_{t=1}^{n} \overline{P}_{W|U}(w_t|U_t(m_p, m_p'))\overline{P}_{X|WU}(x|w_i, U_i(m_p, m_p')).
\end{aligned}$$

- Markov chain: $X - U_i(M_p, M_p')W_i - M_pM_p'M_sM_s'W^n$

Distortion at the eavesdropper–continued

Distortion at the eavesdropper–continued

- exists code under which
  - $\sum_{i=1}^{n} \left\| P_{M_p M_p' M_s W^n X_i} - \tilde{Q}^{(i)}_{M_p M_p' M_s W^n X} \right\|_{TV} \leq \epsilon_n$
  - $\sum_{i=1}^{n} \left\| \tilde{Q}^{(i)}_{u_i(M_p, M_p')} - \overline{P}_U \right\|_{TV} \leq \epsilon_n$
  - $\mathbb{E}_P[d_b(X^n, Y^n)] \leq D_b + \epsilon_n$

Distortion at the eavesdropper–continued

- exists code under which
  - $\sum_{i=1}^{n} \left\| P_{M_p M_p' M_s W^n X_i} - \tilde{Q}^{(i)}_{M_p M_p' M_s W^n X} \right\|_{TV} \leq \epsilon_n$
  - $\sum_{i=1}^{n} \left\| \tilde{Q}^{(i)}_{u_i(M_p, M_p')} - \overline{P}_U \right\|_{TV} \leq \epsilon_n$
  - $\mathbb{E}_P[d_b(X^n, Y^n)] \leq D_b + \epsilon_n$
- Lower bound on the distortion

$$\begin{aligned} & \min_{z^n(m_p, m_s, w^n)} \mathbb{E}_P \left[d_w(X^n, z^n(M_p, M_s, W^n)) \right] \\ \geq \quad & \frac{1}{n} \sum_{i=1}^{n} \min_{z(u,w)} \mathbb{E}_{\overline{P}} \left[d_w(X, z(U, W)) \right] - 2\epsilon_n d_{w\,max} \end{aligned}$$

Example

Example

- Lossless compression at legitimate receiver

Example

- Lossless compression at legitimate receiver
- Hamming distortion

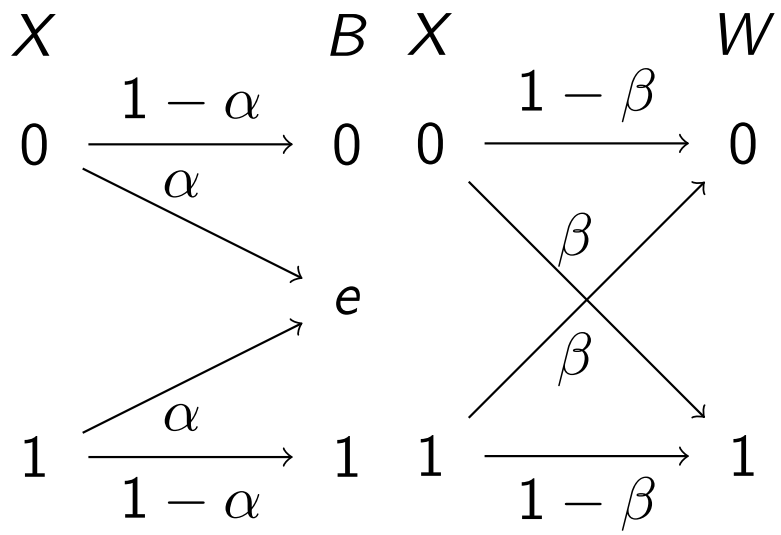
$$d(x,y) = \begin{cases} 0, & x = y \\ 1, & \text{otherwise.} \end{cases}$$

Example

- Lossless compression at legitimate receiver
- Hamming distortion

$$d(x,y) = \begin{cases} 0, & x = y \\ 1, & \text{otherwise.} \end{cases}$$

- i.i.d. $Bern(p)$ source



Example–continued

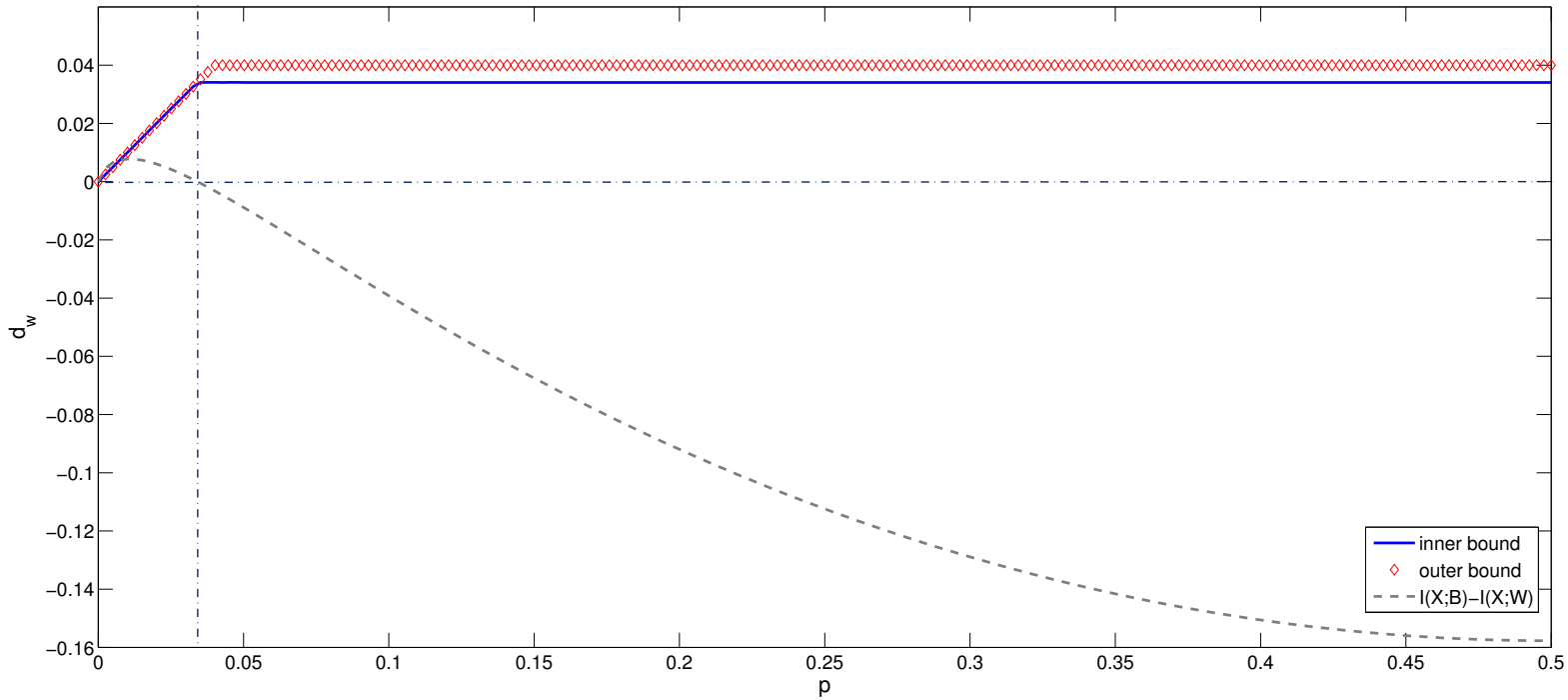


Figure: Distortion at the eavesdropper as a function of source distribution p with $\alpha = 0.4$, $\beta = 0.04$

Example–continued

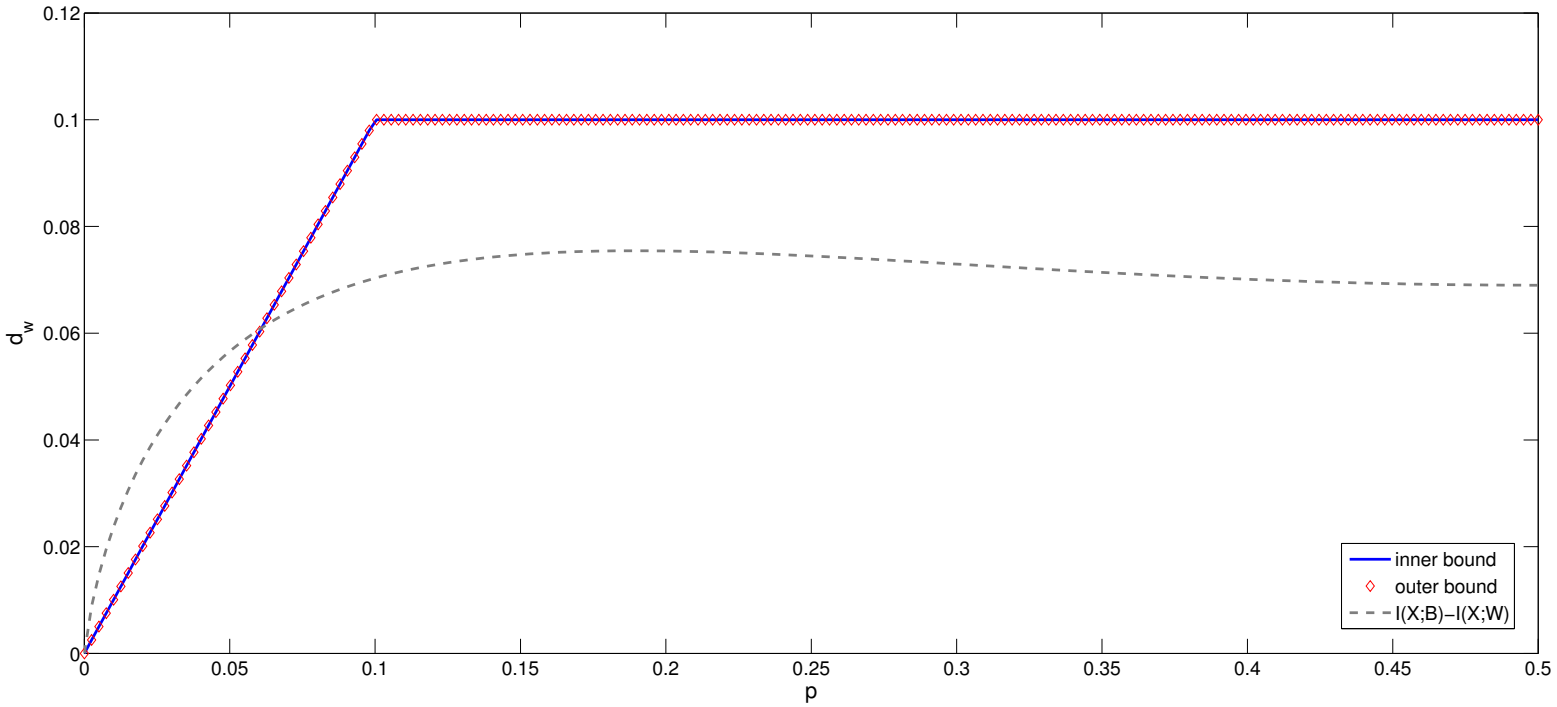


Figure: Distortion at the eavesdropper as a function of source distribution p with $\alpha = 0.4$, $\beta = 0.1$

Conclusion

- Positive distortion is achievable even if eavesdropper has stronger side info
- Exact bounds obtained for several special cases
- Outer bound is not tight for the general case