Secure Multiterminal Source Coding with Side Information at the Eavesdropper

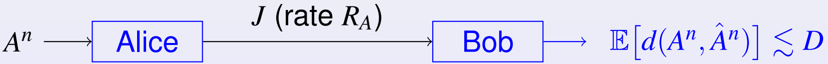
Joffrey Villard and Pablo Piantanida

SUPELEC, Dpt. of Telecommunications, Gif-sur-Yvette, France.

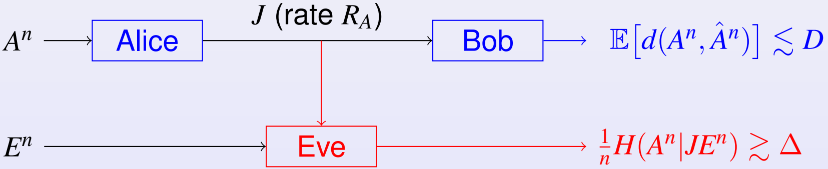
Email: {joffrey.villard, pablo.piantanida}@supelec.fr

1st International ICST Workshop on Secure Wireless Networks

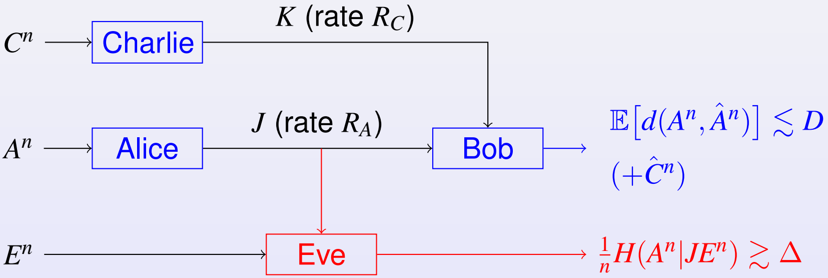
Context



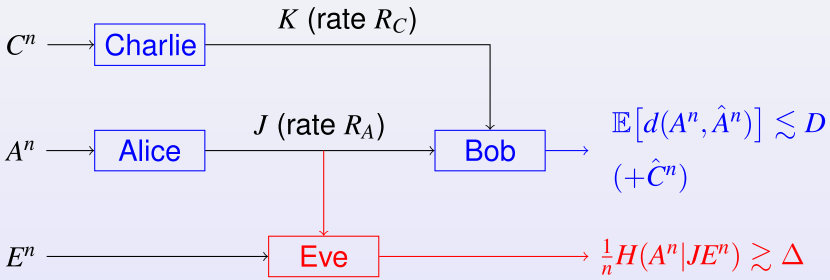
Context


A^n
Alice
J (rate R_A)
Bob
$\mathbb{E}\left[d(A^n, \hat{A}^n)\right] \lesssim D$
E^n
Eve
$\frac{1}{n}H(A^n|JE^n) \gtrsim \Delta$

Context


K (rate R_C)
C^n
Charlie
J (rate R_A)
A^n
Alice
Bob
$\mathbb{E}\left[d(A^n, \hat{A}^n)\right] \lesssim D$
$(+\hat{C}^n)$
E^n
Eve
$\frac{1}{n}H(A^n|JE^n) \gtrsim \Delta$

Context



Tradeoff: Min. rates + Min. distortion + Max. equivocation

Our Aim: Find all *achievable* tuples (R_A, R_C, D, Δ)

References

Multiterminal source coding.

D. Slepian and J. Wolf. Noiseless coding of correlated information sources. *IEEE Trans. IT*, 19(4):471–480, 1973.

T. Berger. Multiterminal source coding. in *The information theory approach to communications*, 1977.

Source coding with side-information.

A. Wyner and J. Ziv. The rate-distortion function for source coding with side information at the decoder. *IEEE Trans. IT*, 22(1):1–10, 1976.

Information-theoretic security.

C.E. Shannon. Communication theory of secrecy systems. *BSTJ*, 28:656–715, 1949.

A.D. Wyner. The wire-tap channel. *BSTJ*, 54(8):1355–1387, 1975.

I. Csiszar and J. Korner. Broadcast channels with confidential messages. , 24(3):339–348, 1978.

Y. Liang, H.V. Poor, and S. Shamai. *Information theoretic security*. Now Publishers, 2009.

Secure source coding.

H. Yamamoto. Rate-distortion theory for the Shannon cipher system. *IEEE Trans. IT*, 43(3):827–835, 1997.

V. Prabhakaran and K. Ramchandran. On secure distributed source coding. In *Proc. ITW*, p. 442–447, 2007.

D. Gunduz, E. Erkip, and H.V. Poor. Lossless compression with security constraints. In *Proc. ISIT*, p. 111–115, 2008.

R. Tandon, S. Ulukus, and K. Ramchandran. Secure source coding with a helper. In *Proc. Allerton*, p. 1061–1068, 2009.

N. Merhav. Shannon's secrecy system with informed receivers and its application to systematic coding for wiretapped channels. *IEEE Trans. IT*, 54(6):2723–2734, 2008.

Outline

Outline

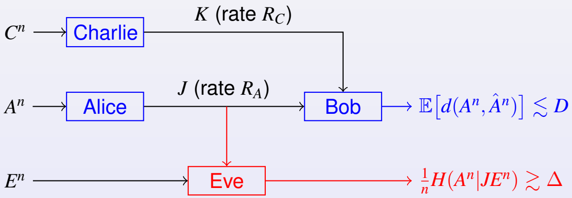
Definitions

- $\mathcal{A}$, $\mathcal{C}$ and $\mathcal{E}$: three finite sets
- $(A_i, C_i, E_i)_{i\geq 1}$: i.i.d random variables on $\mathcal{A} \times \mathcal{C} \times \mathcal{E}$
  with known joint distribution $p(a, b, e)$
- $d : \mathcal{A} \times \mathcal{A} \to [0\,; d_{max}]$: a finite distortion measure

An (n, R_A, R_C)-code for source coding in this setup is defined by

- Two encoding functions at Alice and Charlie
  $f_A : \mathcal{A}^n \to \{1, \ldots, 2^{nR_A}\}$ and $f_C : \mathcal{C}^n \to \{1, \ldots, 2^{nR_C}\}$, resp.
- A decoding function at Bob
  $g : \{1, \ldots, 2^{nR_A}\} \times \{1, \ldots, 2^{nR_C}\} \to \mathcal{A}^n$

Definitions (cont.)



A tuple $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if,

for any $\varepsilon > 0$, there exists an $(n, R_A + \varepsilon, R_C + \varepsilon)$-code (f_A, f_C, g) such that:

$$\mathbb{E}\left[d(A^n, g(f_A(A^n), f_C(C^n)))\right] \leq D + \varepsilon$$

$$\frac{1}{n} H(A^n | f_A(A^n), E^n) \geq \Delta - \varepsilon$$

Outline

Inner and Outer Bounds

Theorem (Inner bound)

$(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if there exist

- r.v. U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, resp., s.t.

$$p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace) \quad ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, s.t.

$$\begin{aligned} R_A &\geq I(V;A|W) \\ R_C &\geq I(W;C|V) \\ R_A + R_C &\geq I(VW;AC) \\ D &\geq \mathbb{E}\left[d(A,\hat{A}(V,W))\right] \\ \Delta &\leq H(A|UE) - I(V;A|UW) \\ \Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V) \end{aligned}$$

Inner and Outer Bounds

Theorem (Inner bound)

$(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if there exist

- r.v. U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, resp., s.t.

$$p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace) \quad ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, s.t.

$$\begin{aligned} R_A &\geq I(V;A|W) \\ R_C &\geq I(W;C|V) \\ R_A + R_C &\geq I(VW;AC) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V,W))\right] \\ \Delta &\leq H(A|UE) - I(V;A|UW) \\ \Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V) \end{aligned}$$

Inner and Outer Bounds

Theorem (Inner bound)

$(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if there exist

- r.v. U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, resp., s.t.

$$p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace) \quad ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, s.t.

$$\begin{aligned} R_A &\geq I(V;A|W) \\ R_C &\geq I(W;C|V) \\ R_A + R_C &\geq I(VW;AC) \\ D &\geq \mathbb{E}\left[d(A,\hat{A}(V,W))\right] \\ \Delta &\leq H(A|UE) - I(V;A|UW) \\ \Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V) \end{aligned}$$

Inner and Outer Bounds

Theorem (Inner bound)

$(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if there exist

- r.v. U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, resp., s.t.

$$p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace) \quad ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, s.t.

$$\begin{aligned} R_A &\geq I(V; A|W) \\ R_C &\geq I(W; C|V) \\ R_A + R_C &\geq I(VW; AC) \\ D &\geq \mathbb{E}\left[d(A, \hat{A}(V, W))\right] \\ \Delta &\leq H(A|UE) - I(V; A|UW) \\ \Delta - R_C &\leq H(A|V) - I(A; E|U) - I(W; C|V) \end{aligned}$$

Inner and Outer Bounds

Theorem (Inner bound)

$(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable if there exist

- r.v. U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, resp., s.t.

$$p(uvwace) = p(u|v)p(v|a)p(w|c)p(ace) \quad ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, s.t.

$$\begin{aligned}
R_A &\geq I(V;A|W) \\
R_C &\geq I(W;C|V) \\
R_A + R_C &\geq I(VW;AC) \\
D &\geq \mathbb{E}\left[d(A,\hat{A}(V,W))\right] \\
\Delta &\leq H(A|UE) - I(V;A|UW) \\
\Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V)
\end{aligned}$$

Inner and Outer Bounds

Theorem (Outer bound)

If $(R_A, R_C, D, \Delta) \in \mathbb{R}_+^4$ is achievable, then there exist

- r.v. U, V, W on some finite sets $\mathcal{U}$, $\mathcal{V}$, $\mathcal{W}$, resp., s.t.

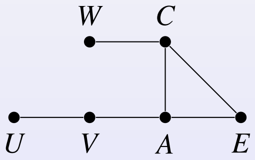
$$p(wace) = p(w|c)p(ace), \; p(uvace) = p(u|v)p(v|a)p(ace) \quad ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{W} \to \mathcal{A}$, s.t.

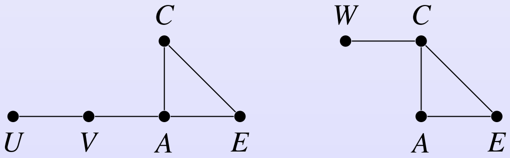
$$\begin{aligned} R_A &\geq I(V;A|W) \\ R_C &\geq I(W;C|V) \\ R_A + R_C &\geq I(VW;AC) \\ D &\geq \mathbb{E}\left[d(A,\hat{A}(V,W))\right] \\ \Delta &\leq H(A|UE) - I(V;A|UW) \\ \Delta - R_C &\leq H(A|V) - I(A;E|U) - I(W;C|V) \end{aligned}$$

Auxiliary Variables

Inner Bound



Outer Bound



Outline

Three Corner Points

3 three-step schemes to deliver (U, V) and W, using

- superposition coding $(U - V - A - C - W)$
- previously received information used as side information
- random binning
- time-sharing

Corner point	(I)
Comm. order	$W,\ U,\ V$
R_A	$I(V;A\|W)$
R_C	$I(W;C)$
D	$\mathbb{E}\left[d(A,\hat{A}(V,W))\right]$
Δ	$H(A\|UE) - I(V;A\|UW)$

Three Corner Points

3 three-step schemes to deliver (U, V) and W, using

- superposition coding ($U - V - A - C - W$)
- previously received information used as side information
- random binning
- time-sharing

Corner point	(I)	(II)
Comm. order	$W,\ U,\ V$	$U,\ W,\ V$
R_A	$I(V;A\|W)$	$I(U;A) + I(V;A\|UW)$
R_C	$I(W;C)$	$I(W;C\|U)$
D	$\mathbb{E}\left[d(A,\hat{A}(V,W))\right]$	—
Δ	$H(A\|UE) - I(V;A\|UW)$	$H(A\|UE) - I(V;A\|UW)$

Three Corner Points

3 three-step schemes to deliver (U,V) and W, using

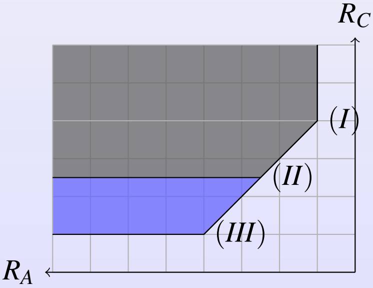
- superposition coding ($U - V - A - C - W$)
- previously received information used as side information
- random binning
- time-sharing

Corner point	(I)	(II)	(III)
Comm. order	$W,\ U,\ V$	$U,\ W,\ V$	$U,\ V,\ W$
R_A	$I(V;A\|W)$	$I(U;A)+I(V;A\|UW)$	$I(V;A)$
R_C	$I(W;C)$	$I(W;C\|U)$	$I(W;C\|V)$
D	$\mathbb{E}\left[d(A,\hat{A}(V,W))\right]$	—	—
Δ	$H(A\|UE)-I(V;A\|UW)$	$H(A\|UE)-I(V;A\|UW)$	$H(A\|UE)-I(V;A\|U)$

Time-Sharing

Segment (I)–(II)

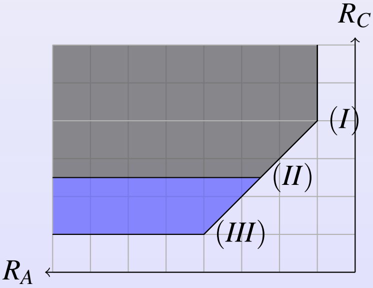
$$\begin{aligned} D &= \mathbb{E}\left[d(A, \hat{A}(V, W))\right] \\ \Delta &= H(A|UE) - I(V; A|UW) \\ R_A + R_C &= I(VW; AC) \end{aligned}$$



Time-Sharing

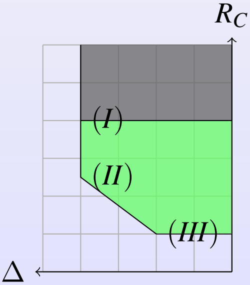
Segment (I)–(II)

$$D = \mathbb{E}\left[d(A, \hat{A}(V, W))\right]$$
$$\Delta = H(A|UE) - I(V; A|UW)$$
$$R_A + R_C = I(VW; AC)$$

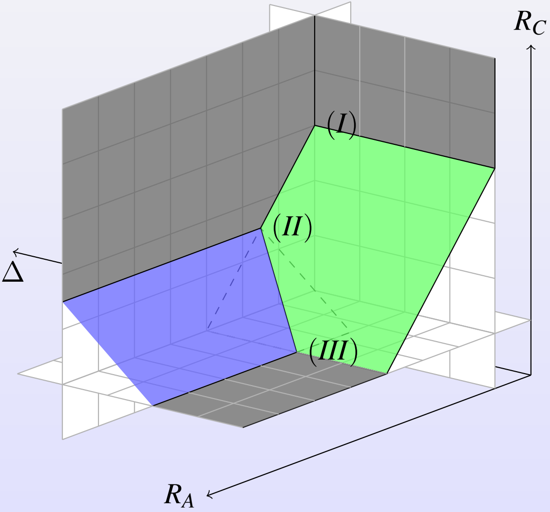


Segment (II)–(III)

$$D = \mathbb{E}\left[d(A, \hat{A}(V, W))\right]$$
$$\Delta - R_C = H(A|UE) - I(V; A|U) - I(W; C|V)$$
$$R_A + R_C = I(VW; AC)$$

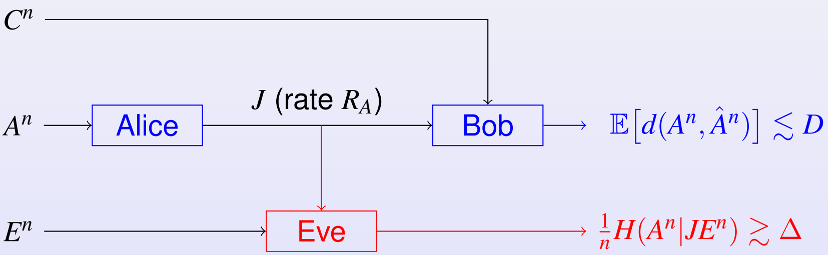


Achievable Region for Some Fixed D



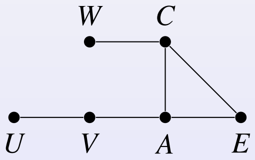
Outline

Context

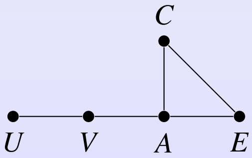

C^n
A^n
Alice
J (rate R_A)
Bob
$\mathbb{E}\left[d(A^n, \hat{A}^n)\right] \lesssim D$
E^n
Eve
$\frac{1}{n}H(A^n|JE^n) \gtrsim \Delta$

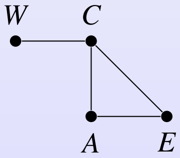
Auxiliary Variables

Inner Bound



Outer Bound





Uncoded Side Information

Theorem (Rate-Distortion-Equivocation Region)

$(R_A, \quad D, \Delta) \in \mathbb{R}_+^3$ is achievable i.f.f. there exist

- r.v. U, V on some finite sets $\mathcal{U}, \mathcal{V}$, resp., s.t.

$$p(uvace) = p(u|v)p(v|a)p(ace) \; ,$$

- a function $\hat{A} : \mathcal{V} \times \mathcal{C} \to \mathcal{A}$, s.t.

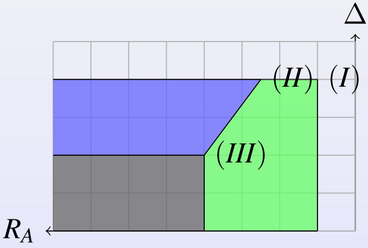
$$R_A \geq I(V;A|C)$$

$$D \geq \mathbb{E}\left[d(A, \hat{A}(V,C))\right]$$

$$\Delta \leq H(A|UE) - I(V;A|UC)$$

Uncoded Side Information (cont.)

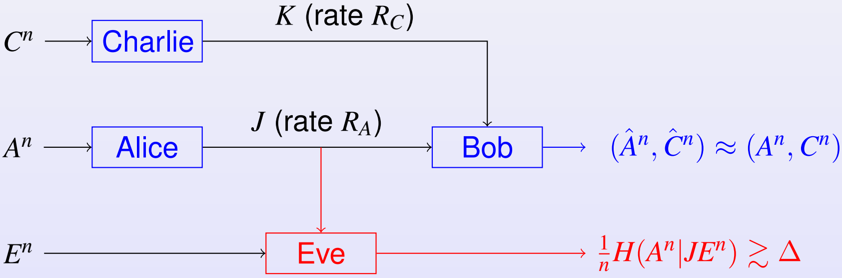
- Achievability: point (I) with $W = C$



- Converse: new proof
- Wyner-Ziv coding achieves the optimal performance if one side information is less noisy than the other (optimal choice: $U^* = \emptyset$ or $U^* = V$)

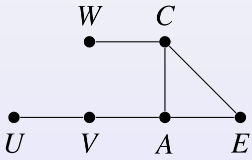
Outline

Context

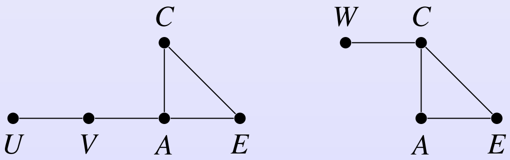

C^n
Charlie
K (rate R_C)
A^n
Alice
J (rate R_A)
Bob
$(\hat{A}^n, \hat{C}^n) \approx (A^n, C^n)$
E^n
Eve
$\frac{1}{n} H(A^n | J E^n) \gtrsim \Delta$

Auxiliary Variables

Inner Bound



Outer Bound



Lossless Compression of Both Sources

Theorem (Compression-Equivocation Rates Region)

$(R_A, R_C, \quad \Delta) \in \mathbb{R}^3_+$ is achievable i.f.f. there exists

- r.v. U on some finite set $\mathcal{U}$ s.t.

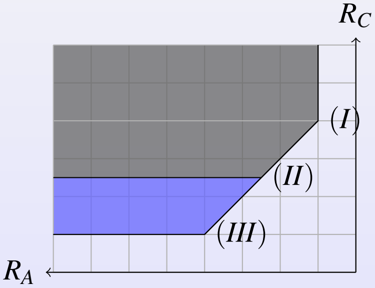
$$p(uace) = p(u|a)p(ace),$$

$$\begin{aligned} R_A &\geq H(A|C) \\ R_C &\geq H(C|U) \\ R_A + R_C &\geq H(AC) \end{aligned}$$

$$\Delta \leq H(A|UE) - H(A|UC)$$

Lossless Compression of Both Sources (cont.)

- Achievability: points (I) and (II) with $V = A$ and $W = C$



- Converse: new proof

- Slepian-Wolf coding is sufficient
  if E is less noisy than C ($U^* = A$, and $\Delta = 0$)

Outline

Giving U to Eve is also optimal

- Alice can enable Eve to decode the common message U:

$$R_A \geq (\cdot) + [I(U;C) - I(U;E)]_+ \ ,$$

  with no loss on secrecy

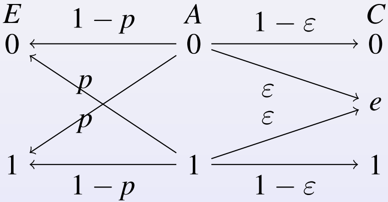
- Achievability: OK
- Converse: new proof

- *cf.* broadcast channel with confidential messages [Csiszàr & Körner–1978]

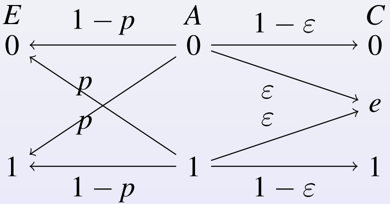
- optimal choice U^*:
  part of V which conveys "more information" about E than C

Outline

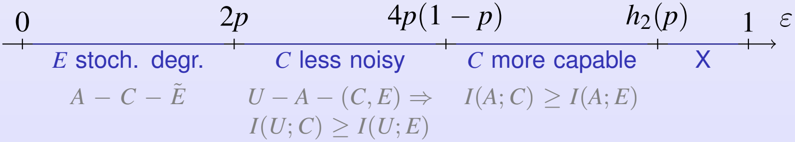
Binary Source with BEC and BSC Side Informations



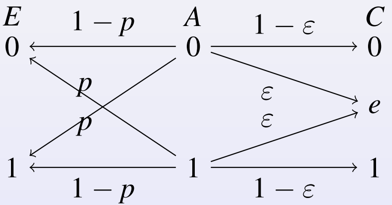
Binary Source with BEC and BSC Side Informations



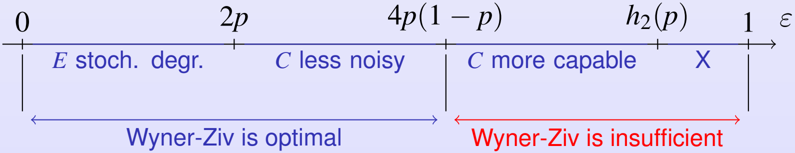
Neither Bob nor Eve is a lessnoisy decoder for all values of (p, ε):



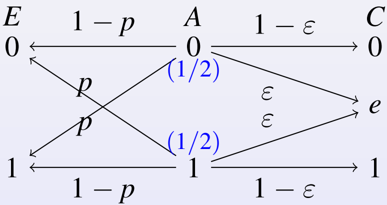
Binary Source with BEC and BSC Side Informations



Neither Bob nor Eve is a lessnoisy decoder for all values of (p, ε):

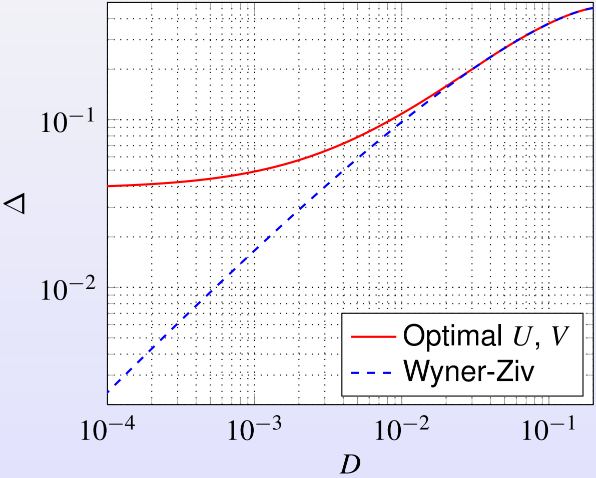


Binary Source with BEC and BSC Side Informations



- distortion d: Hamming distance
- source A: uniformly distributed

Illustration ($p = 0.1$, $\epsilon = h_2(p) \approx 0.469$)



Equivocation rate at Eve as a function of the distortion level at Bob

Summary and Discussion

- Single-letter inner and outer bounds on the general rates-distortion-equivocation region
- Results of optimality
  - uncoded side information
  - distributed lossless compression

Ongoing work:

- Source-channel coding with security constraints

with P. Piantanida
Secure Multiterminal Source Coding with Side Information at the Eavesdropper
submitted to *IEEE Trans. on Inf. Theory*, available on arXiv:1105.1658.

with P. Piantanida and S. Shamai
Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals
to be presented at *ISIT 2011*.

with P. Piantanida
Secure Multiterminal Source Coding with Side Information at the Eavesdropper
submitted to *IEEE Trans. on Inf. Theory*, available on arXiv:1105.1658.

with P. Piantanida and S. Shamai
Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals
to be presented at *ISIT 2011*.

Thank you for your attention.