Secure Lossy Source Channel Wiretapping with Side Info. at the Receiving Terminals

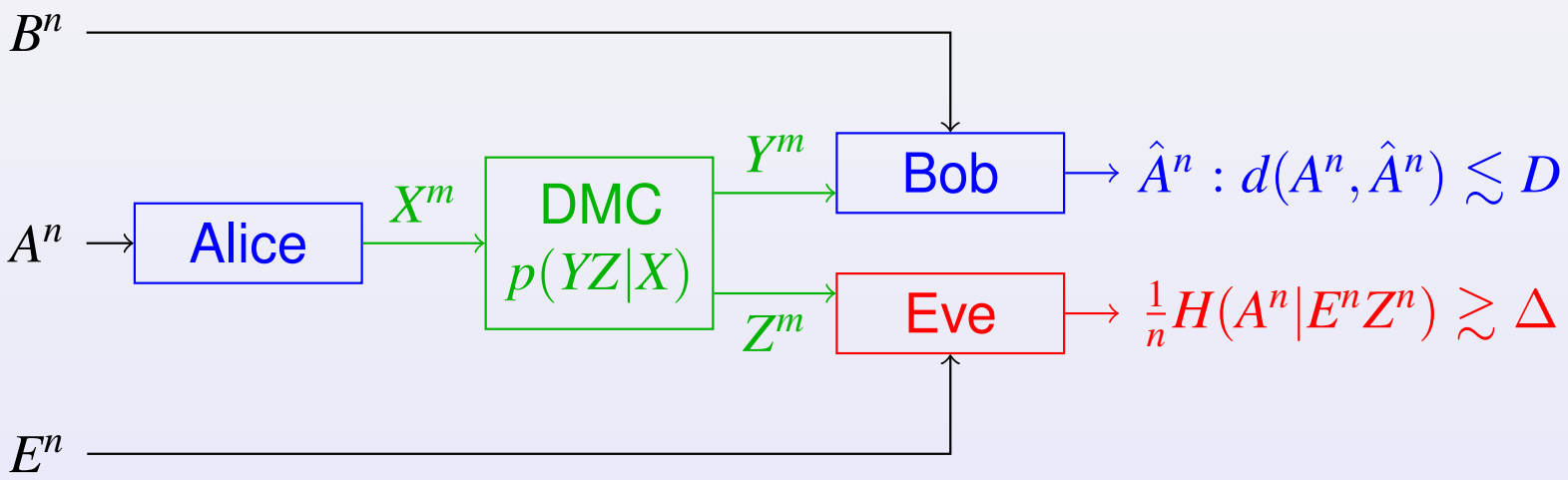
Joffrey Villard[1] Pablo Piantanida[1] Shlomo Shamai (Shitz)[2]

[1]Dpt. of Telecommunications, SUPELEC, France

[2]Dpt. of Electrical Engineering, Technion - Israel Institute of Technology, Israel

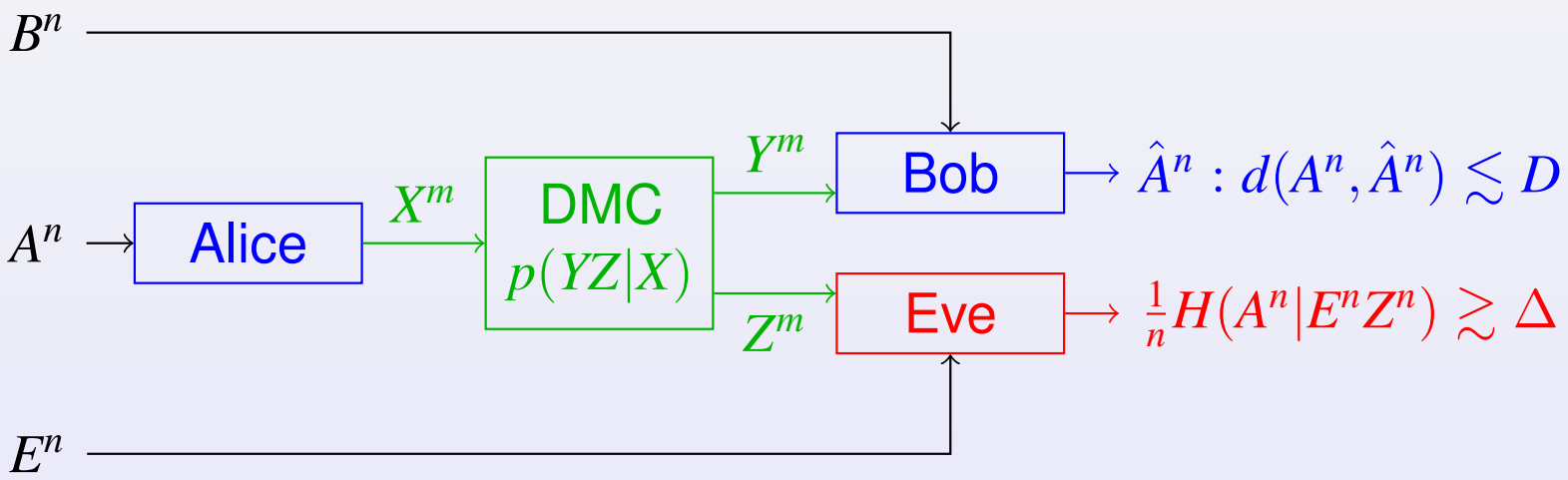
2011 IEEE International Symposium on Information Theory

Context



$k = \frac{m}{n}$ channel uses per source symbol.

Context



$k = \frac{m}{n}$ channel uses per source symbol.

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

Tradeoff: min. ch. uses + min. distortion + Max. equivocation

First Questions

How to use the side information?

- decrease the rate [SlepianWolf73][WynerZiv76]
- increase security [VillardPiantanida10]

First Questions

How to use the side information?

- decrease the rate [SlepianWolf73][WynerZiv76]
- increase security [VillardPiantanida10]

How to take advantage of the channel?

- increase security [Wyner75][CsiszàrKörner78]

First Questions

How to use the side information?

- decrease the rate [SlepianWolf73][WynerZiv76]
- increase security [VillardPiantanida10]

How to take advantage of the channel?

- increase security [Wyner75][CsiszàrKörner78]

Does separation hold?

- to help both Bob and Eve, a joint scheme is optimal [Tuncel06]
- to help Bob and blur Eve?

First Questions

How to use the side information?

- decrease the rate [SlepianWolf73][WynerZiv76]
- increase security [VillardPiantanida10]

How to take advantage of the channel?

- increase security [Wyner75][CsiszàrKörner78]

Does separation hold?

- to help both Bob and Eve, a joint scheme is optimal [Tuncel06]
- to help Bob and blur Eve?

$\rightarrow$ If $A \multimap B \multimap E$, $X \multimap Y \multimap Z$, [Merhav08]:

Wyner-Ziv source encoder $+$ wiretap channel encoder

References

Information-theoretic security.

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

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

Source coding with side-information.

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

Secure channel coding.

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.

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*, pp.442–447, 2007.

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

J. Villard and P. Piantanida. Secure lossy source coding with SI at the decoders. In *Proc. Allerton*, pp.733–739 , 2010.

Secure joint source/channel coding.

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

- $(A_i, B_i, E_i)_{i\geq 1}$: i.i.d. random variables on $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$ with joint distribution $p(a, b, e)$
- $X \mapsto (Y, Z)$: a memoryless broadcast channel with transition probability $p(y, z|x)$
- $d : \mathcal{A} \times \mathcal{A} \to [0\,; d_{max}]$: a finite distortion measure

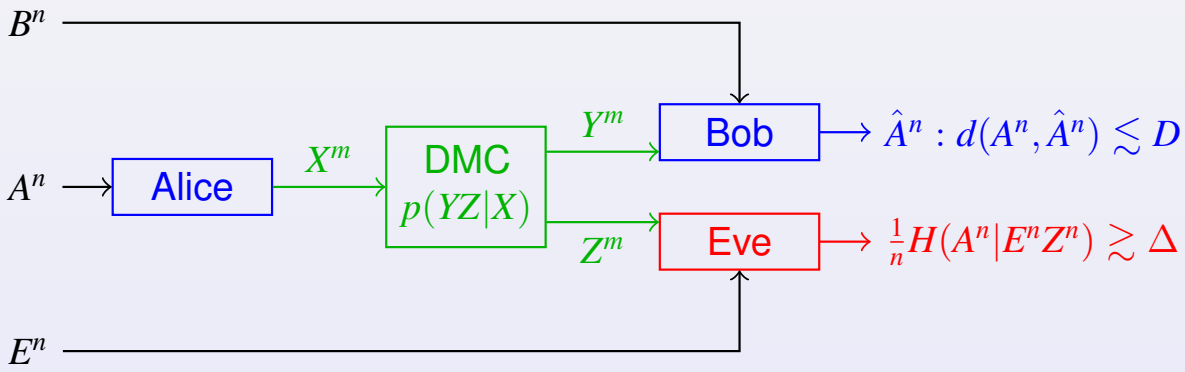
Definitions

- $(A_i, B_i, E_i)_{i\geq 1}$: i.i.d. random variables on $\mathcal{A} \times \mathcal{B} \times \mathcal{E}$ with joint distribution $p(a, b, e)$
- $X \mapsto (Y, Z)$: a memoryless broadcast channel with transition probability $p(y, z|x)$
- $d : \mathcal{A} \times \mathcal{A} \to [0\,; d_{max}]$: a finite distortion measure

An (n, m)-code for source-channel coding is defined by

- A (stochastic) encoding function at Alice $F : \mathcal{A}^n \to \mathcal{X}^m$
- A decoding function at Bob $g : \mathcal{Y}^m \times \mathcal{B}^n \to \mathcal{A}^n$

Definitions (cont.)



A tuple $(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if, for any $\varepsilon > 0$, there exists an (n, m)-code (F, g) such that:

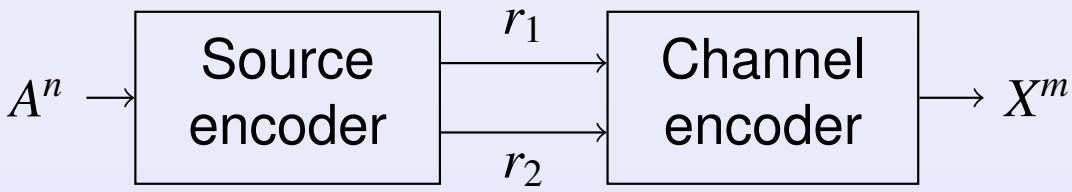
$$\begin{aligned} \frac{m}{n} &\leq k + \varepsilon \\ \mathbb{E}\left[d(A^n, g(Y^m, B^n))\right] &\leq D + \varepsilon \\ \frac{1}{n} H(A^n|E^n, Z^m) &\geq \Delta - \varepsilon \end{aligned}$$

Outline

Coding Scheme

Operational separation

- two independent components
- not stand-alone



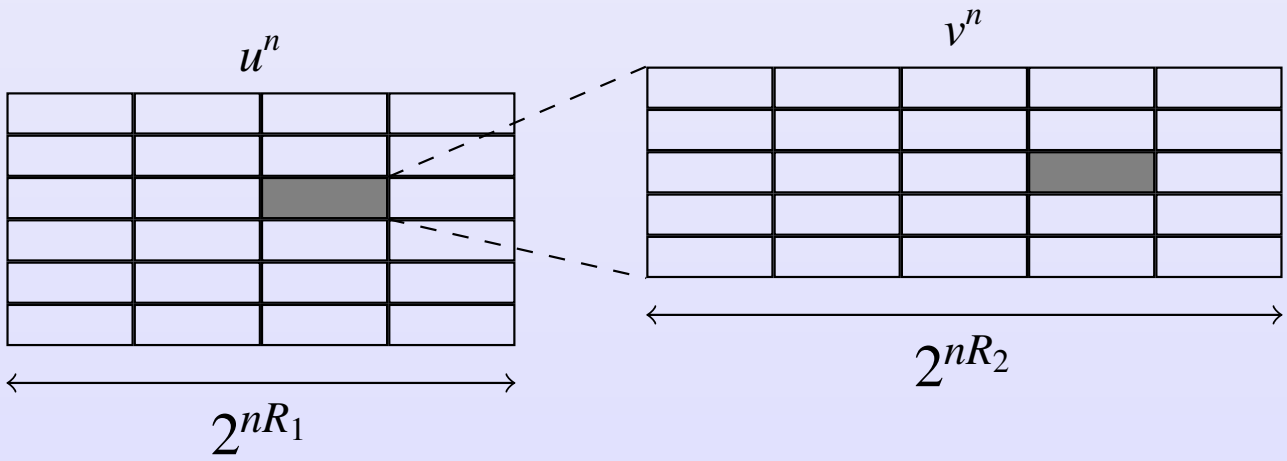
Single letter

- independent source and channel variables
- joint optimization

Source encoder

- description of A in 2 layers U, V with rates R_1, R_2
- superposition coding ($U \multimap V \multimap A$)
- random binning *a la* Wyner-Ziv

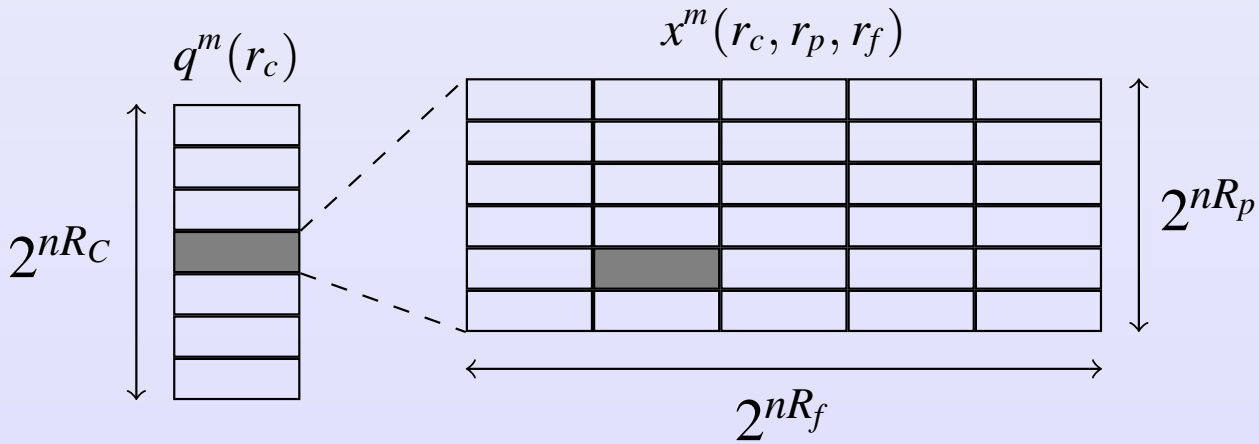
$$R_1 > I(U;A|B)$$
$$R_2 > I(V;A|UB)$$



Channel encoder

- 2 layers Q, X with rates R_c, R_p
- bits recombination: $M : (r_1, r_2) \mapsto (r_c, r_p)$
- random noise with rate R_f on X *a la* Csiszàr-Körner

$$\begin{aligned} R_1 + R_2 &= R_c + R_p \\ R_1 &\leq R_c \end{aligned} \qquad \begin{aligned} R_c &< kI(Q;Y) \\ R_p + R_f &< kI(X;Y|Q) \end{aligned}$$



Performance

Distortion at Bob:

- Bob can decode (r_c, r_p) from Y^m
- Bob can decode (u^n, v^n) from $(r_1, r_2) = M^{-1}(r_c, r_p)$

$$\mathbb{E}\left[d(A^n, g(Y^m, B^n))\right] \approx \mathbb{E}\left[d(A, \hat{A}(V, B))\right]$$

Performance

Distortion at Bob:

- Bob can decode (r_c, r_p) from Y^m
- Bob can decode (u^n, v^n) from $(r_1, r_2) = M^{-1}(r_c, r_p)$

$$\mathbb{E}\left[d(A^n, g(Y^m, B^n))\right] \approx \mathbb{E}\left[d(A, \hat{A}(V, B))\right]$$

Equivocation at Eve:

- source terms: [VillardPiantanida10]
- channel terms: $R_f < kI(X;Z|Q)$ [CsiszàrKörner78]
- remaining joint terms: $R_1 \leq R_c$

$$\frac{1}{n}H(A^n|E^nZ^n) \gtrsim H(A|UE) - R_2 + R_p + R_f - kI(X;Z|Q)$$

Outline

Inner and Outer Bounds

Theorem (Inner bound)

$(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if there exist

- r.v. U, V, Q, T, X s.t.

$$U \multimap V \multimap A \multimap (B, E) \quad \perp\!\!\!\perp \quad Q \multimap T \multimap X \multimap (Y, Z)$$

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

$$I(U;A|B) \leq kI(Q;Y)$$

$$I(V;A|B) \leq kI(T;Y)$$

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

$$\Delta \leq H(A|UE) - \Big[I(V;A|UB) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+$$

Inner and Outer Bounds

Theorem (Inner bound)

$(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if there exist

- r.v. U, V, Q, T, X s.t.

$$U \multimap V \multimap A \multimap (B, E) \quad \perp\!\!\!\perp \quad Q \multimap T \multimap X \multimap (Y, Z)$$

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

$$I(U;A|B) \leq kI(Q;Y)$$

$$I(V;A|B) \leq kI(T;Y)$$

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

$$\Delta \leq H(A|UE) - \Big[I(V;A|UB) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+$$

Inner and Outer Bounds

Theorem (Inner bound)

$(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if there exist

- r.v. U, V, Q, T, X s.t.

$$U \multimap V \multimap A \multimap (B, E) \quad \perp\!\!\!\perp \quad Q \multimap T \multimap X \multimap (Y, Z)$$

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

$$I(U; A|B) \leq kI(Q; Y)$$

$$I(V; A|B) \leq kI(T; Y)$$

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

$$\Delta \leq H(A|UE) - \Big[I(V; A|UB) - k\Big(I(T; Y|Q) - I(T; Z|Q)\Big)\Big]_+$$

Inner and Outer Bounds

Theorem (Inner bound)

$(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if there exist

- r.v. U, V, Q, T, X s.t.

$$U \multimap V \multimap A \multimap (B, E) \quad \perp\!\!\!\perp \quad Q \multimap T \multimap X \multimap (Y, Z)$$

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

$$I(U;A|B) \leq kI(Q;Y)$$

$$I(V;A|B) \leq kI(T;Y)$$

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

$$\Delta \leq H(A|UE) - \Big[I(V;A|UB) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+$$

Inner and Outer Bounds

Theorem (Inner bound)

$(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable if there exist

- r.v. U, V, Q, T, X s.t.

$$U \multimap V \multimap A \multimap (B, E) \quad \perp\!\!\!\perp \quad Q \multimap T \multimap X \multimap (Y, Z)$$

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

$$I(U;A|B) \leq kI(Q;Y)$$

$$I(V;A|B) \leq kI(T;Y)$$

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

$$\Delta \leq H(A|UE) - \Big[I(V;A|UB) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+$$

Inner and Outer Bounds

Theorem (Outer bound)

If $(k, D, \Delta) \in \mathbb{R}_+^3$ is achievable, then there exist

- r.v. U, V, Q, T, X s.t.

$$(U,V) \multimap A \multimap (B,E) \quad \perp\!\!\!\perp \quad Q \multimap T \multimap X \multimap (Y,Z)$$

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

$$I(V;A|B) \leq kI(T;Y)$$

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

$$\Delta \leq H(A|UE) - \Big[I(V;A|B) - I(U;A|B) - k\Big(I(T;Y|Q) - I(T;Z|Q)\Big)\Big]_+$$

Outline

Less noisy conditions

Less noisy condition $B \succeq_A E$

Random variable B is less noisy than E w.r.t. A, if

$$I(U;B) \geq I(U;E)$$

for each r.v. U s.t. $U \multimap A \multimap (B,E)$ form a Markov chain

Less noisy conditions

Less noisy condition $B \succeq_A E$

Random variable B is less noisy than E w.r.t. A, if

$$I(U;B) \geq I(U;E)$$

for each r.v. U s.t. $U \multimap A \multimap (B,E)$ form a Markov chain

- $B \succeq_A E \quad \Rightarrow \quad U = \emptyset$

  Wyner-Ziv source encoder $+$ wiretap channel encoder

Less noisy conditions

Less noisy condition $B \succeq_A E$

Random variable B is less noisy than E w.r.t. A, if

$$I(U;B) \geq I(U;E)$$

for each r.v. U s.t. $U \multimap A \multimap (B,E)$ form a Markov chain

- $B \succeq_A E \quad \Rightarrow \quad U = \emptyset$

  Wyner-Ziv source encoder $+$ wiretap channel encoder

- $Z \succeq_X Y \quad \Rightarrow \quad Q = T = X$

  secure source encoder $+$ classical channel encoder

Outline

Optimal Schemes

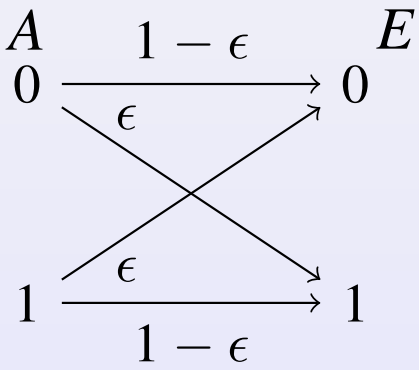
	$B \succeq_A E$	$E \succeq_A B$
$Y \succeq_X Z$	Wyner-Ziv source enc. + wiretap channel enc.	?
$Z \succeq_X Y$	Wyner-Ziv source enc. + classical channel enc.	secure source enc. + classical channel enc.

Outline

Counterexample: Sources

Binary source with BSC side information at Eve

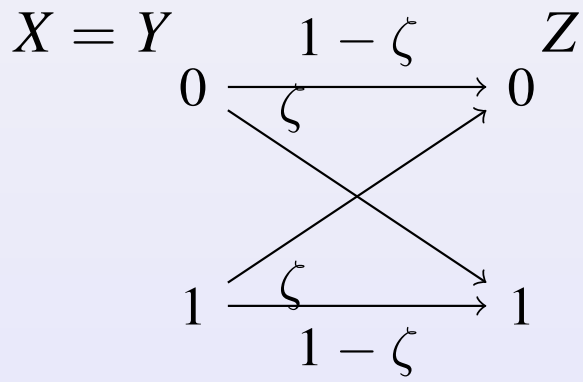
$$B = \emptyset$$



- source A: uniformly distributed
- lossless reconstruction at Bob: $D = 0$
- $A \multimap E \multimap B$

Counterexample: Channels

Type-II wiretap channel



- matched bandwidth: $k = 1$
- $X \multimap Y \multimap Z$

Counterexample: Numerical Evaluation

Parameters

- $\epsilon = 0.1, \zeta = 0.1$

Numerical results

- Operationnaly separated scheme: $\Delta_{\max} = 0.056$
- Naive analog scheme ($X = A$): $\Delta_{\max} = 0.258$
  $+$ matches the outer bound

Counterexample: Numerical Evaluation

Parameters

- $\epsilon = 0.1, \zeta = 0.1$

Numerical results

- Operationnaly separated scheme: $\Delta_{\max} = 0.056$
- Naive analog scheme ($X = A$): $\Delta_{\max} = 0.258$
  $+$ matches the outer bound

Consequences

- The proposed scheme is not optimal in this case.
- Analog schemes can be useful

Summary and Discussion

- Single-letter inner and outer bounds in the general case

Summary and Discussion

- Single-letter inner and outer bounds in the general case
- Proposed scheme:

  secure source coding $+$ wiretap channel coding

$\rightarrow$ Operational separation

Summary and Discussion

- Single-letter inner and outer bounds in the general case
- Proposed scheme:

  secure source coding $+$ wiretap channel coding

$\rightarrow$ Operational separation

- Results of optimality under some less noisy conditions

$+$ Separation

Summary and Discussion

- Single-letter inner and outer bounds in the general case
- Proposed scheme:

  secure source coding $+$ wiretap channel coding

$\rightarrow$ Operational separation

- Results of optimality under some less noisy conditions

$+$ Separation

- Simple counterexample with pure analog scheme

On-going work

- Hybrid digital/analog schemes for secure transmission

On-going work

- Hybrid digital/analog schemes for secure transmission
- Optimal in some cases for the transmission of a Gaussian source over a Gaussian channel
- Outperforms both digital and analog schemes

On-going work

- Hybrid digital/analog schemes for secure transmission
- Optimal in some cases for the transmission of a Gaussian source over a Gaussian channel
- Outperforms both digital and analog schemes

$\rightarrow$ to be presented at ITW 2011

On-going work

- Hybrid digital/analog schemes for secure transmission
- Optimal in some cases for the transmission of a Gaussian source over a Gaussian channel
- Outperforms both digital and analog schemes

$\rightarrow$ to be presented at ITW 2011

Thank you for your attention.