On the Duality Between State-Dependent Channels and Wiretap Channels

David Kibloff

Joint work with Samir M. Perlaza, Guillaume Villemaud and Leonardo S. Cardoso

Univ Lyon, Inria, INSA Lyon, CITI, F-69621 Villeurbanne, France

Oct. 11th 2016

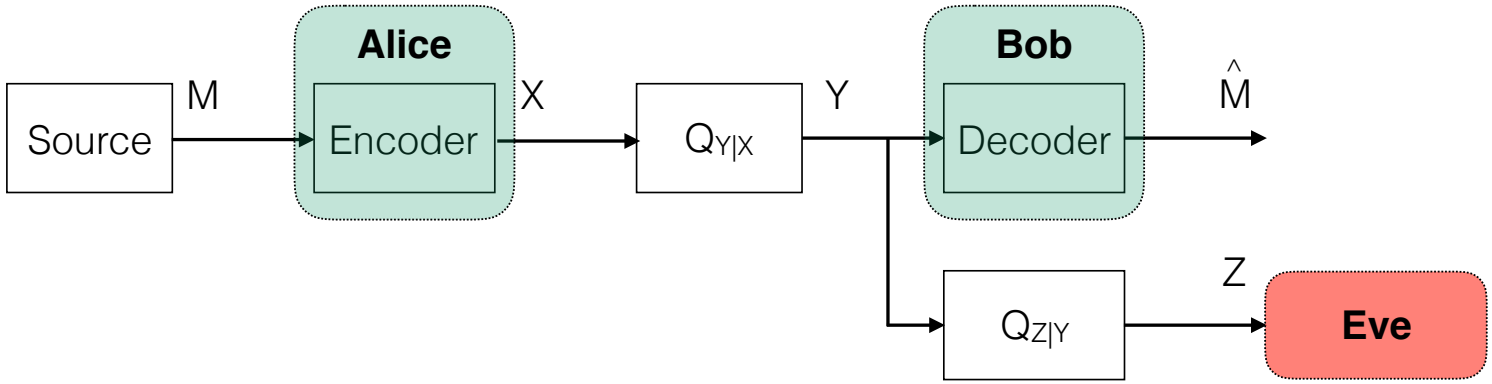
Introduction

Outline

Wiretap channel

Wiretap channel

Assumptions

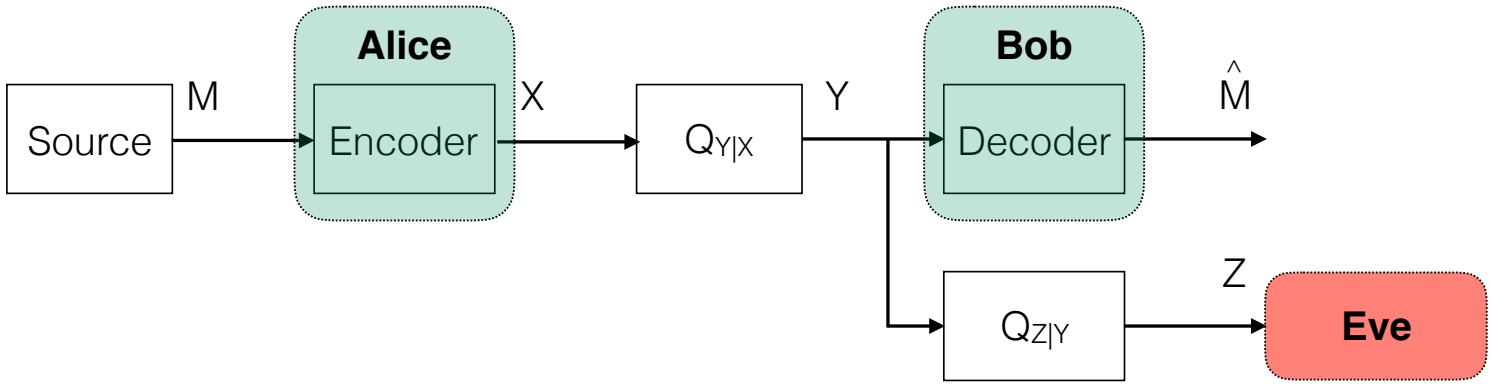


- Eve knows the coding scheme used by Alice and Bob.
- Eve has an infinite computation power.
- Eve observes a degraded version of the signal.
- The channel transition probabilities are known by Alice, Bob and Eve.

A. D. Wyner. "The Wire-Tap Channel". In: *Bell System Technical Journal* 54.8 (1975), pp. 1355–1387

Wiretap channel

Measures

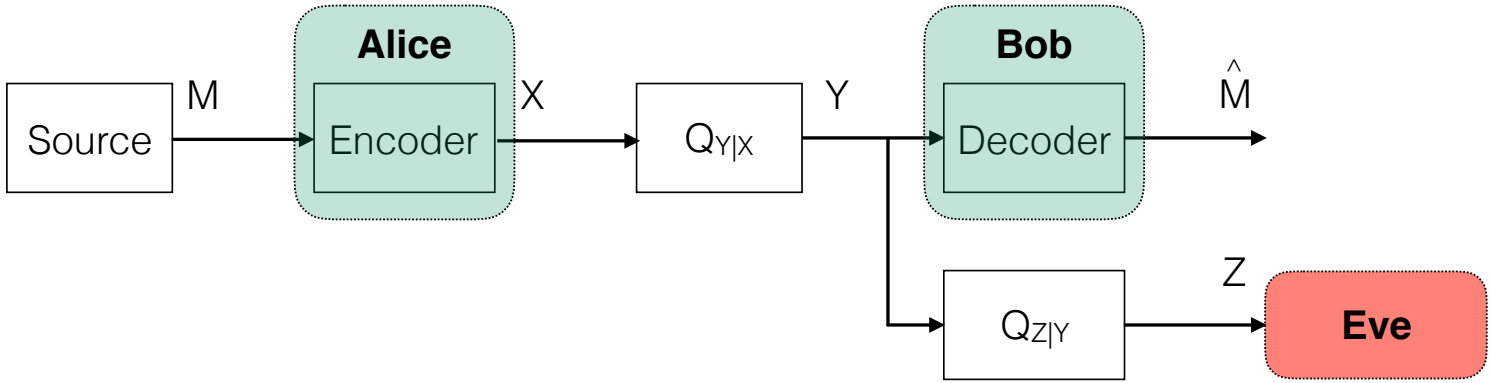


- Probability of error : $P_e = \Pr[\hat{M} \neq M]$.
- Normalized leakage : $L = \frac{1}{n} I(M; \boldsymbol{Z})$.

A. D. Wyner. "The Wire-Tap Channel". In: *Bell System Technical Journal* 54.8 (1975), pp. 1355–1387

Wiretap channel

Secrecy Capacity



Theorem (*)

The secrecy capacity C_s *of the wiretap channel* $K_W = \{\mathcal{X}, \mathcal{Y}, \mathcal{Z}, Q_{Y|X} Q_{Z|Y}\}$ *is*

$$C_s = \max_{Q_X} \left[I(X;Y) - I(X;Z) \right]. \tag{1}$$

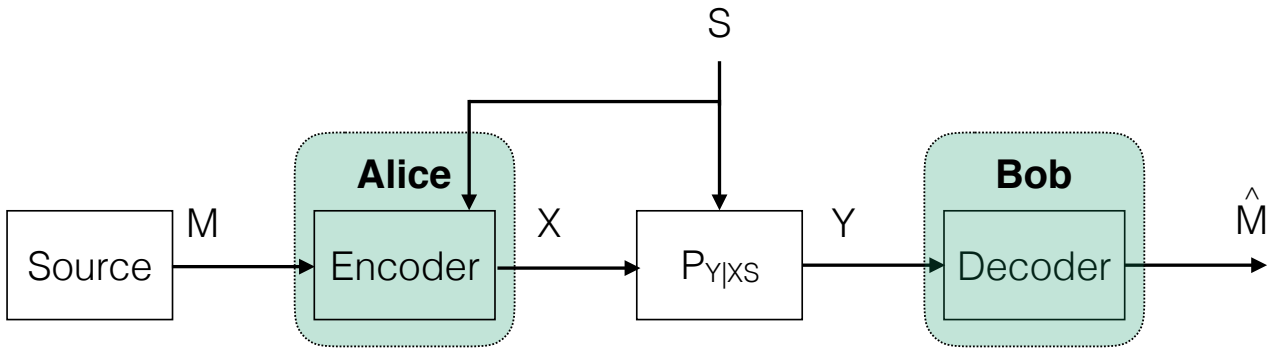
*A. D. Wyner. "The Wire-Tap Channel". In: *Bell System Technical Journal* 54.8 (1975), pp. 1355–1387

State-dependent channel

1. Wiretap Channel
2. State-Dependent Channel
3. Duality
4. Example
5. Conclusion

State-dependent channel

Assumptions

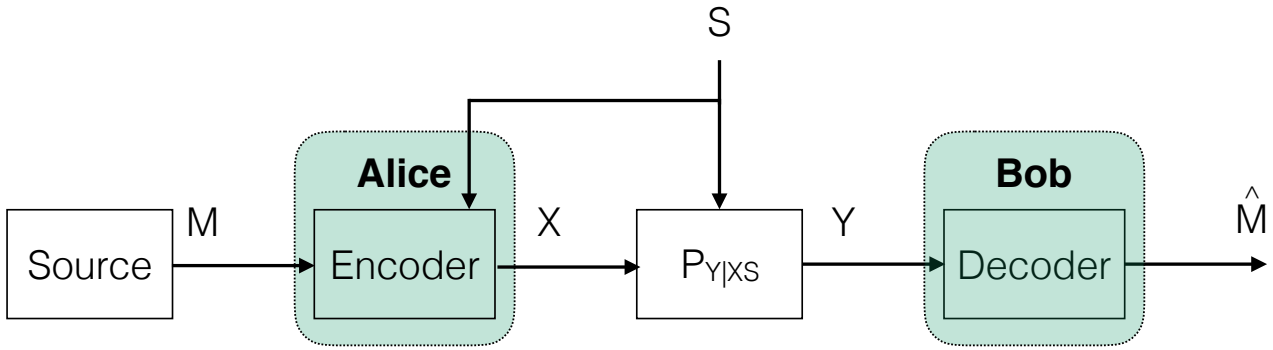


- The states are independent and identically distributed.
- The state S changes at each channel use according to P_S.
- The state information is non-causally available at the transmitter.
- The receiver doesn't know the state information.

S. I. Gelfand and M. S. Pinsker. "Coding for channel with random parameters". In: *Problems of Control and Information Theory* 9.1 (1980), pp. 19–31

State-dependent channel

Capacity



Theorem (*)

The capacity C of the state-dependent channel $K_S = \{\mathcal{S}, \mathcal{X}, \mathcal{Y}, P_S, P_{Y|XS}\}$ with non-causal state information at the transmitter is

$$C = \max_{P_{U|S}, \theta(U,S)} \left[I(U;Y) - I(U;S) \right], \tag{2}$$

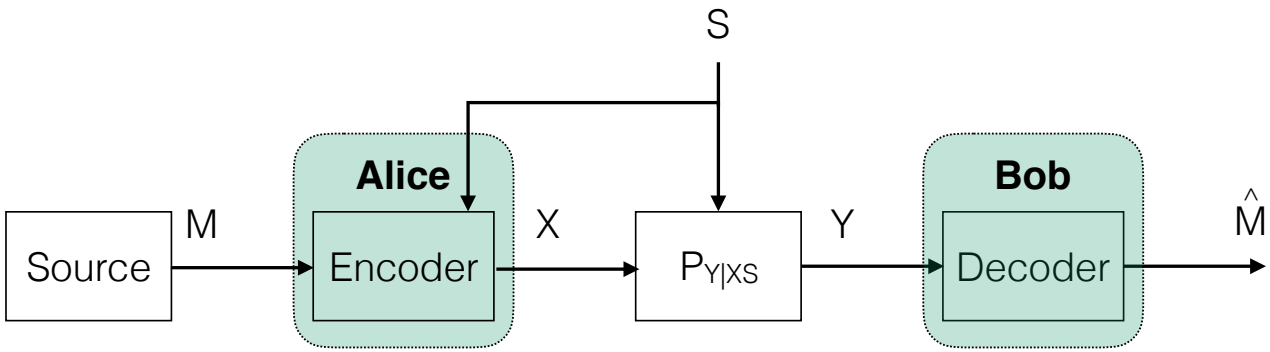
where U is an auxiliary random variable such that $|\mathcal{U}| \leq \min(|\mathcal{S}||\mathcal{X}|, |\mathcal{S}| + |\mathcal{Y}| - 1)$.

*S. I. Gelfand and M. S. Pinsker. "Coding for channel with random parameters". In: *Problems of Control and Information Theory* 9.1 (1980), pp. 19–31

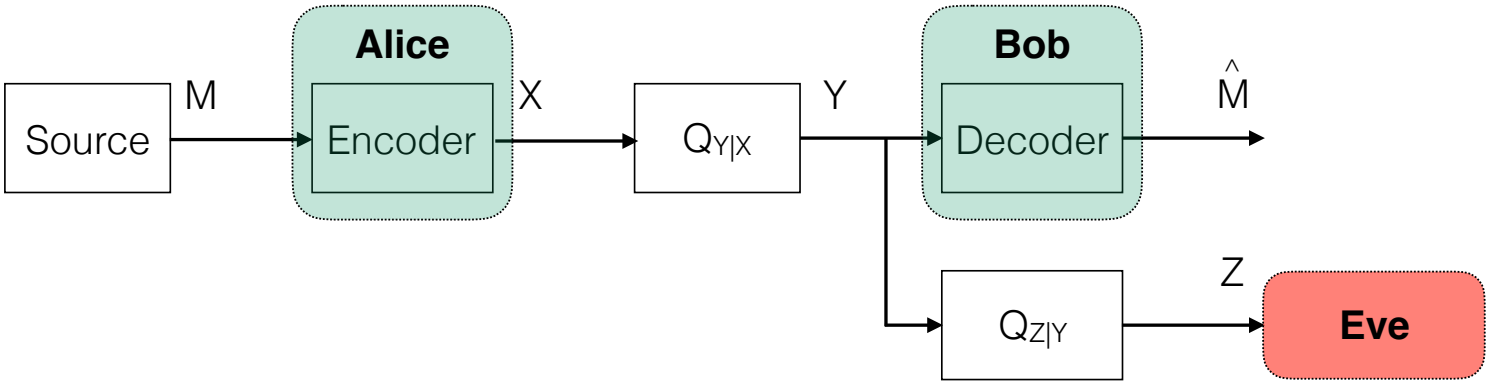
Duality

Duality

Main Result



State-dependent channel



Wiretap channel

Duality

Main Result

Theorem (*)

Let $K_W = (\mathcal{X}, \mathcal{Y}, \mathcal{Z}, Q_{Y|X} Q_{Z|Y})$ *be a WTC, and* $K_S = (\mathcal{S}, \mathcal{X}, \mathcal{Y}, P_S, P_{Y|X\,S})$ *be an SDC satisfying*

$$P^*_{UX|S}(ux|s) = Q^*_{UX|V}(ux|v) = P^*_{U|S}(u|s)\mathbb{1}_{\{x=\theta^*(u,s)\}}, \tag{3}$$

$$I(X;Z) = I(U;S), \quad \text{and} \quad I(X;Y) = I(U;Y), \tag{4}$$

where U *is an auxiliary random variable such that* $|\mathcal{U}| \leq \min\left(|\mathcal{X}||\mathcal{S}|, |\mathcal{Y}| + |\mathcal{S}| - 1\right)$, *and* $\theta : \mathcal{U} \times \mathcal{S} \to \mathcal{X}$ *is a deterministic bijective mapping. Then,*

$$\bar{\mathcal{R}}_{WTC} = \bar{\mathcal{R}}_{SDC}, \tag{5}$$

with $\bar{\mathcal{R}} = \{R : R \text{ is achievable}\}$.

*D. Kibloff et al. "On the duality between state-dependent channels and wiretap channels". In: *Proc. of IEEE Global Conference on Signal and Information Processing, Washington, DC.* Dec. 2016

Duality

Proof sketch

- **Coding Scheme:** Gelfand-Pinsker coding scheme*.
  - Fix a distribution $P_{U|S}$.
  - Generate K sequences $\boldsymbol{U}$ according to $\prod_{t=1}^{n} P_U(U_t)$.
  - Define a bijective function $\theta : \mathcal{U} \times \mathcal{S} \to \mathcal{X}$.
  - $\boldsymbol{X} = \theta(\boldsymbol{U}, \boldsymbol{S})$, where $\boldsymbol{U}$ is chosen to be jointly typical with $\boldsymbol{S}$.
  - Joint typical decoding is used at the decoder.

*S. I. Gelfand and M. S. Pinsker. "Coding for channel with random parameters". In: *Problems of Control and Information Theory* 9.1 (1980), pp. 19–31

Duality

Proof sketch

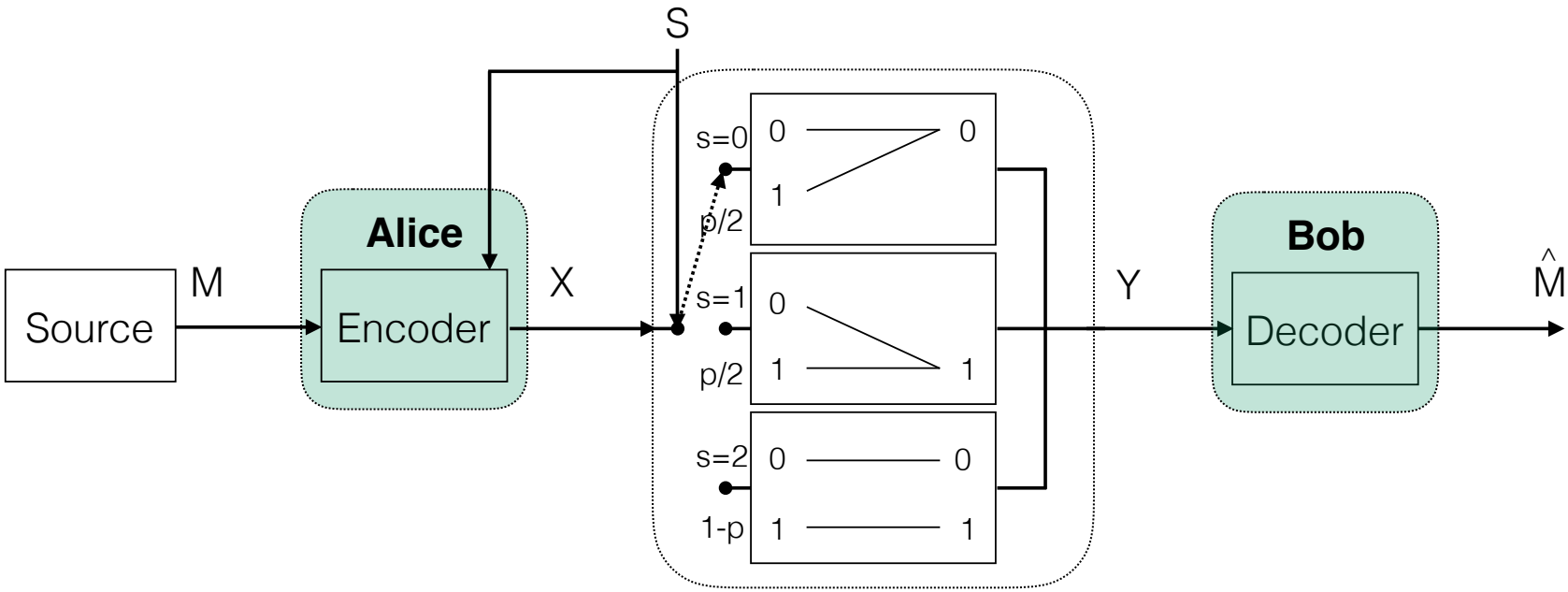
- **Coding Scheme:** Gelfand-Pinsker coding scheme*.
- If $I(X;Y) \geq I(U;Y)$, then $\bar{\mathcal{R}}_{SDC} \subseteq \bar{\mathcal{R}}_{WTC}$:
  - This scheme achieves the capacity of the SDC;
  - When plugged into the WTC, the scheme achieves a fraction of the secrecy capacity;
  - The probability of error is bounded with typicality arguments;
  - The leakage is bounded due to the assumption $I(U;S) = I(X;Z)$.
- If $I(X;Y) \leq I(U;Y)$, then $\bar{\mathcal{R}}_{WTC} \subseteq \bar{\mathcal{R}}_{SDC}$.
- Finally, $I(X;Y) = I(U;Y)$ yields $\bar{\mathcal{R}}_{SDC} = \bar{\mathcal{R}}_{WTC}$.

*S. I. Gelfand and M. S. Pinsker. "Coding for channel with random parameters". In: *Problems of Control and Information Theory* 9.1 (1980), pp. 19–31

Example

Example

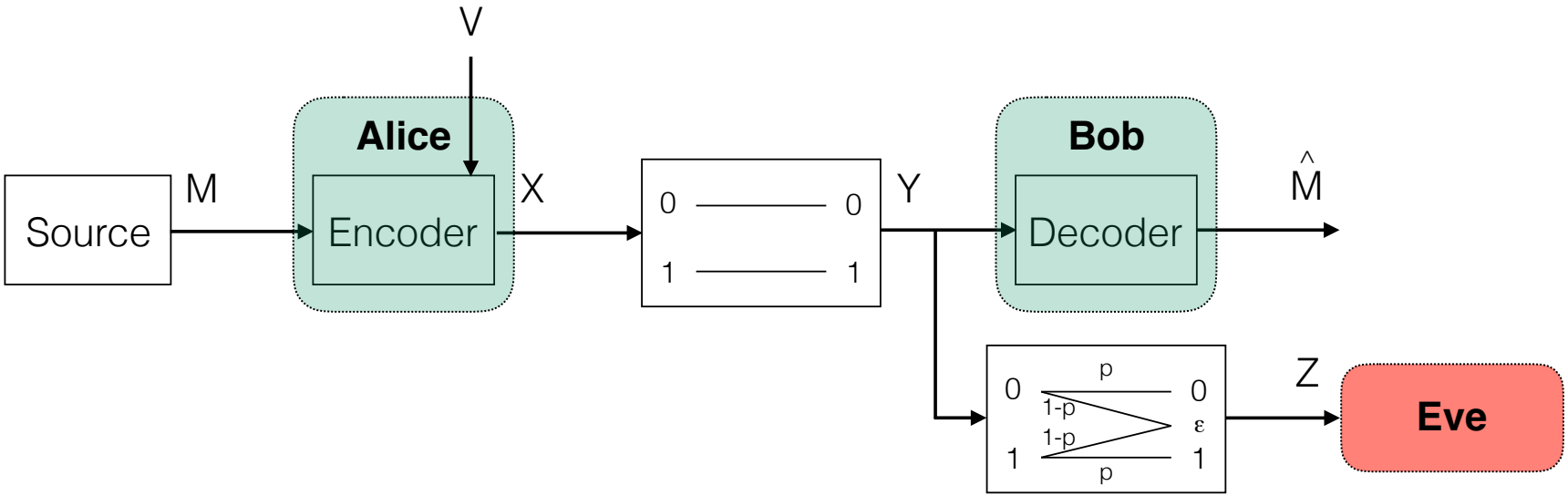
State-dependent Channel



- $\theta(u,0)=0; \quad \theta(u,1)=1;$
  $\theta(0,2)=0; \quad \theta(1,2)=1.$
- $P_{U|S}(0|0)=P_{U|S}(1|1)=1;$
  $P_{U|S}(0|2)=P_{U|S}(1|2)=\frac{1}{2}.$
- $I(U;Y)=1; \quad I(U;S)=p;$
- $\mathbf{C}=\mathbf{1}-\mathbf{p}.$

Example

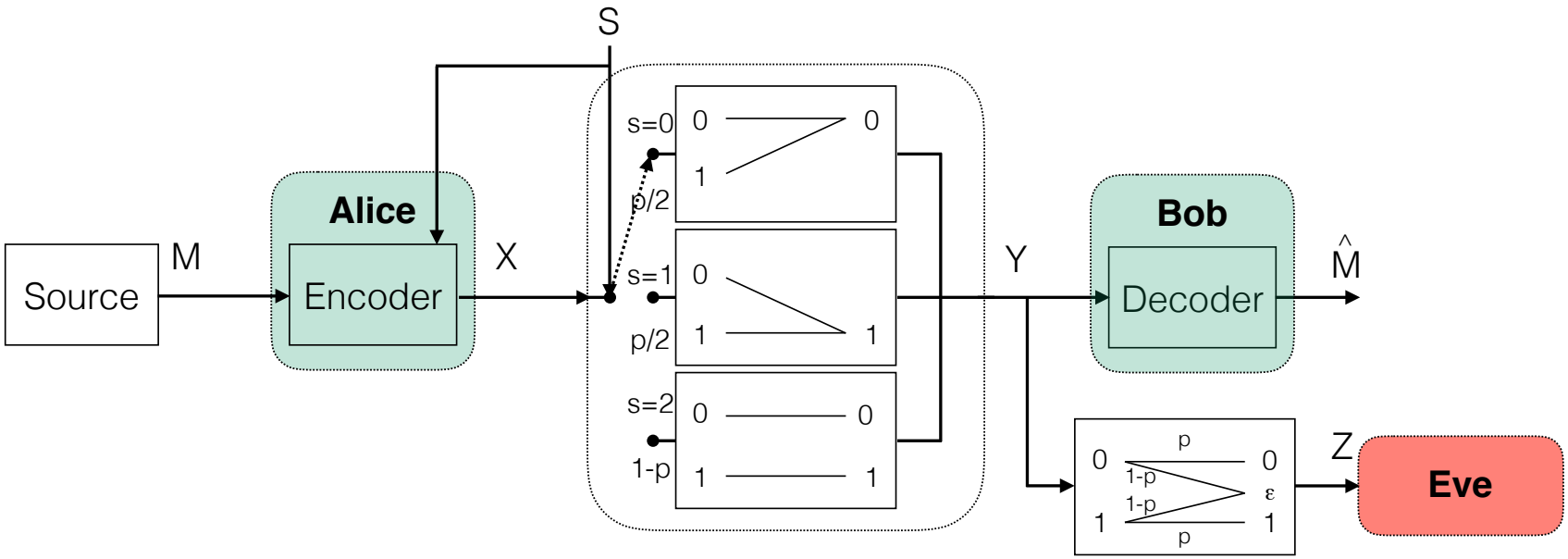
Wiretap Channel



- $\theta(u,0) = 0; \quad \theta(u,1) = 1;$
  $\theta(0,2) = 0; \quad \theta(1,2) = 1.$
- $P_{U|V}(0|0) = P_{U|V}(1|1) = 1;$
  $P_{U|V}(0|2) = P_{U|V}(1|2) = \frac{1}{2}.$
- $I(X;Y) = 1; \quad I(X;Z) = p;$
- $\mathbf{C_s = 1 - p}.$

Conclusion

Conclusion



$$\mathbf{C_s = C = 1 - p}.$$

- Combatting the eavesdropper and combatting the lack of channel state information at the receiver are two non-concurrent tasks.
- These tasks can be achieved with the same coding scheme.

Perspectives

- Gaussian example.
- Simplify the conditions required to obtain the duality to extract only the necessary and sufficient conditions.


A. D. Wyner. "The Wire-Tap Channel". In: *Bell System Technical Journal* 54.8 (1975), pp. 1355–1387.


S. I. Gelfand and M. S. Pinsker. "Coding for channel with random parameters". In: *Problems of Control and Information Theory* 9.1 (1980), pp. 19–31.


D. Kibloff et al. "On the duality between state-dependent channels and wiretap channels". In: *Proc. of IEEE Global Conference on Signal and Information Processing, Washington, DC*. Dec. 2016.

David Kibloff

david.kibloff@inria.fr

https://cybernets.inria.fr/collaborators/kibloff/