Transmission sous contrainte de sécurité avec information adjacente aux récepteurs

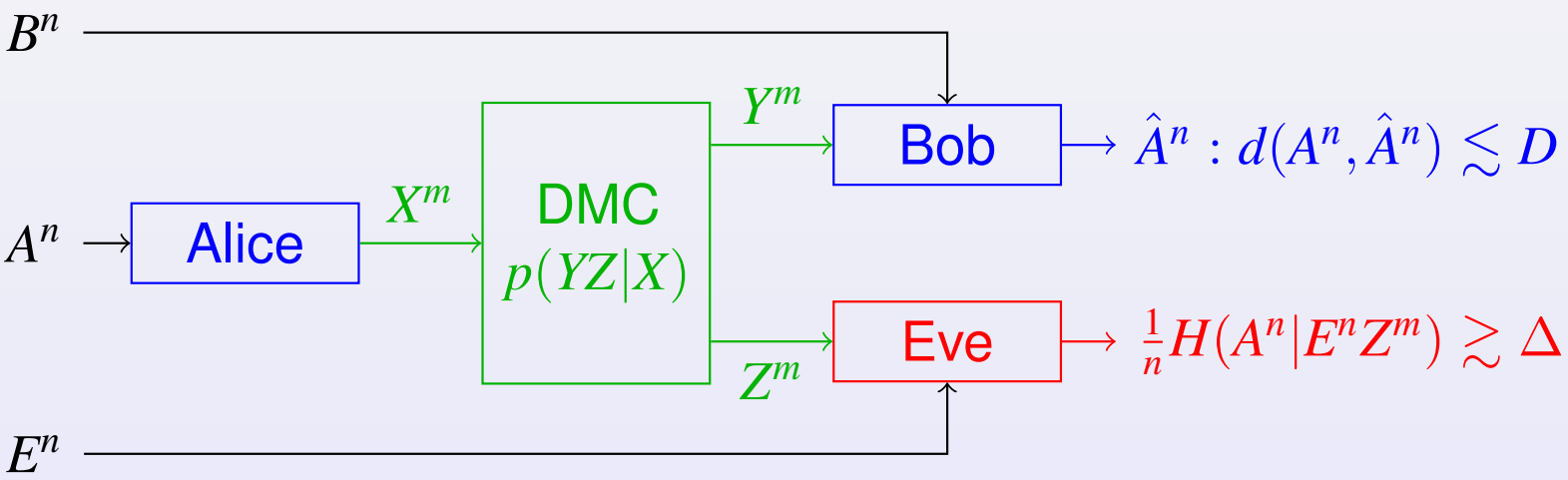
Joffrey Villard Pablo Piantanida

Dpt. Télécommunications, SUPELEC, France

23ème colloque du GRETSI

5 septembre 2011

Contexte

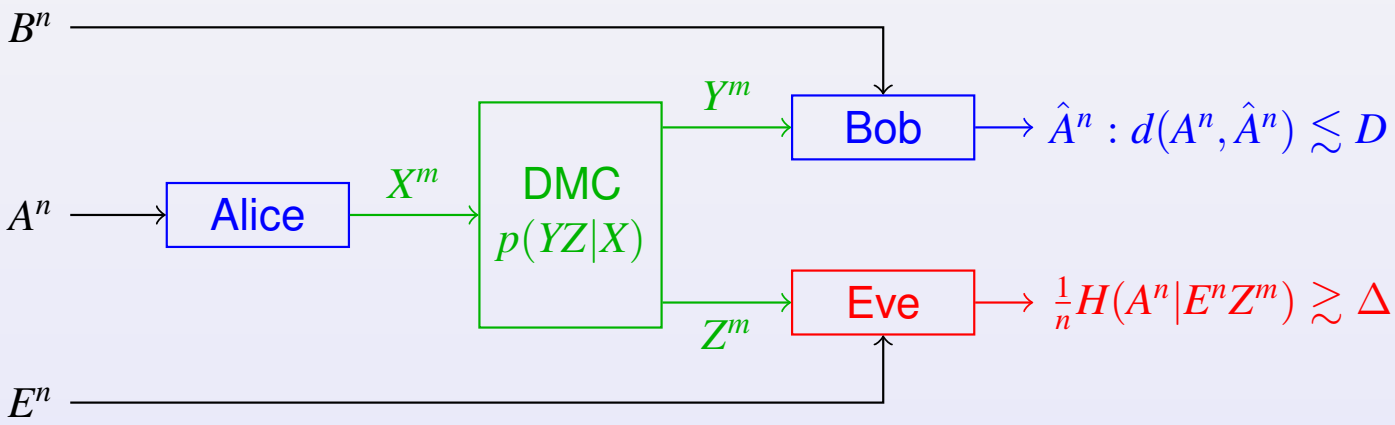


$k = \frac{m}{n}$ utilisations de canal par symbole de source.

Notre but : Trouver tous les triplets (k, D, Δ) atteignables

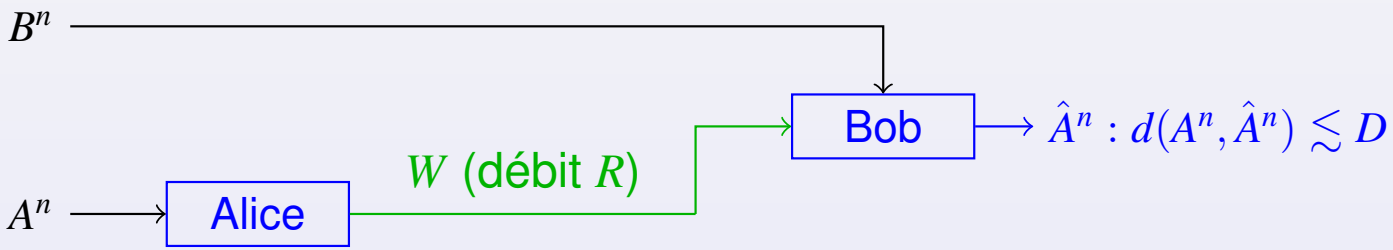
Compromis : min. k + min. D + Max. Δ

Questions



1. Comment utiliser l'information adjacente?

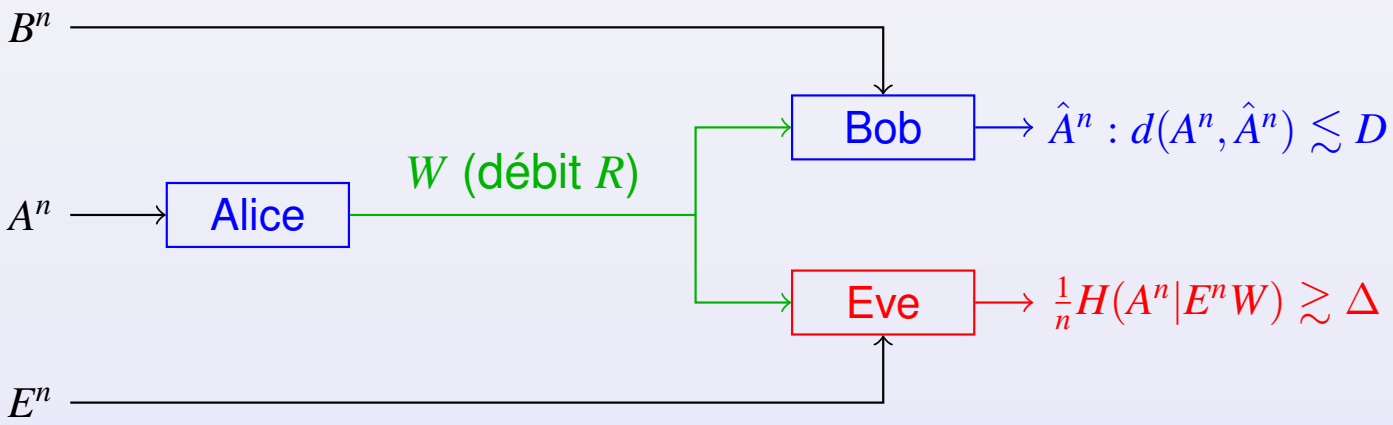
Questions



1 Comment utiliser l'information adjacente?

- [WynerZiv76]: diminuer le débit $R \geq I(V; A|B)$

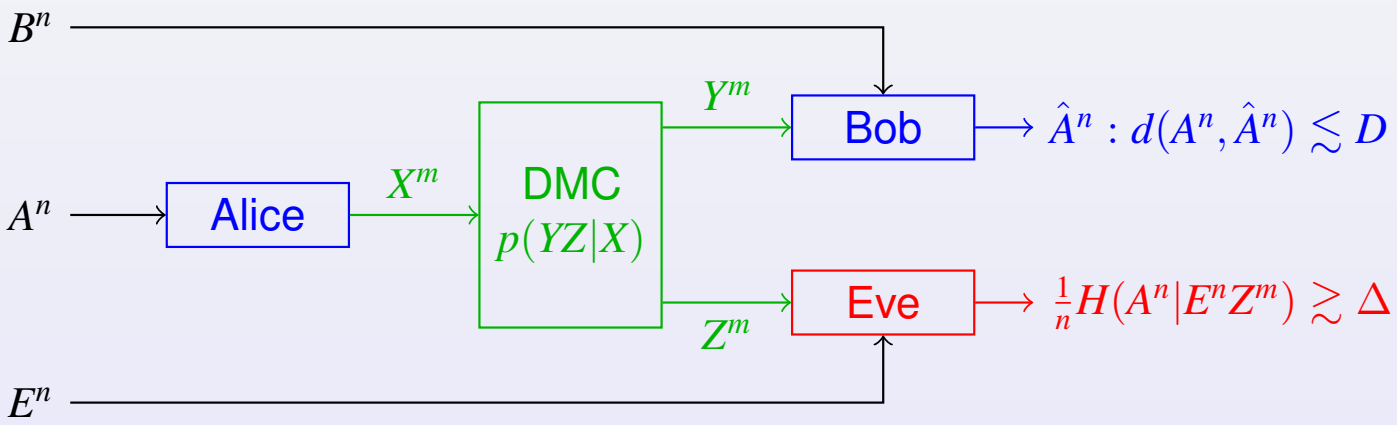
Questions



1 Comment utiliser l'information adjacente?

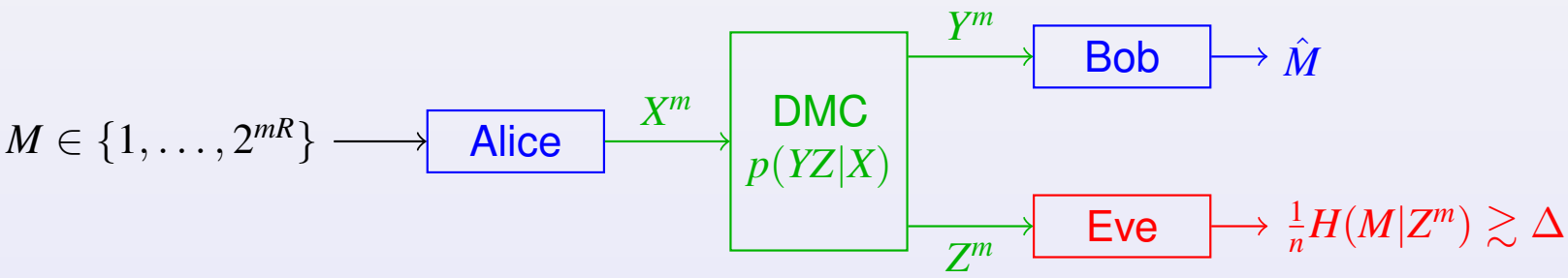
- [WynerZiv76]: diminuer le débit $R \geq I(V; A|B)$
- augmenter la sécurité ?

Questions



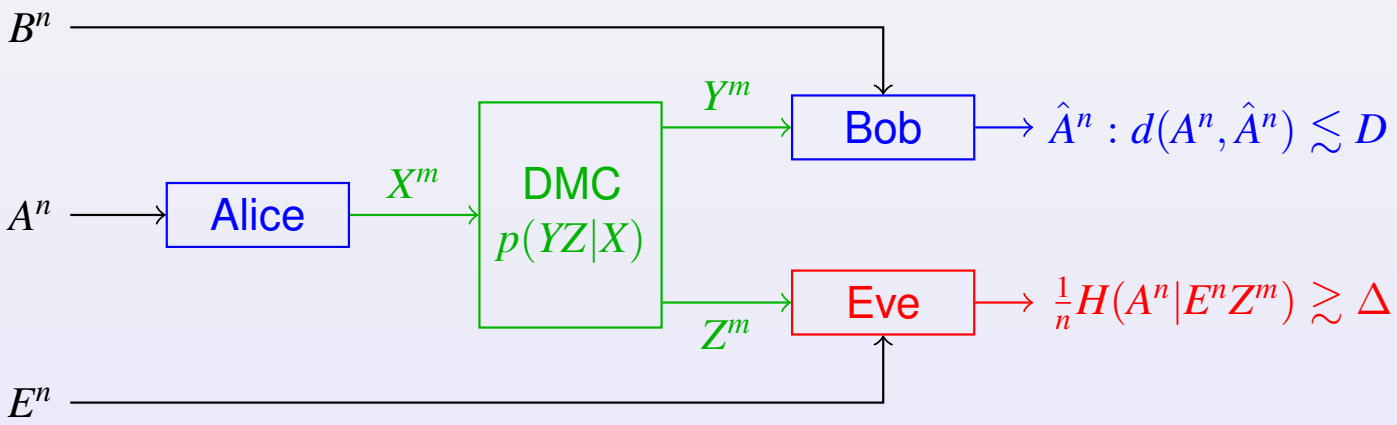
1. Comment utiliser l'information adjacente?
2. Comment tirer avantage du canal ?

Questions



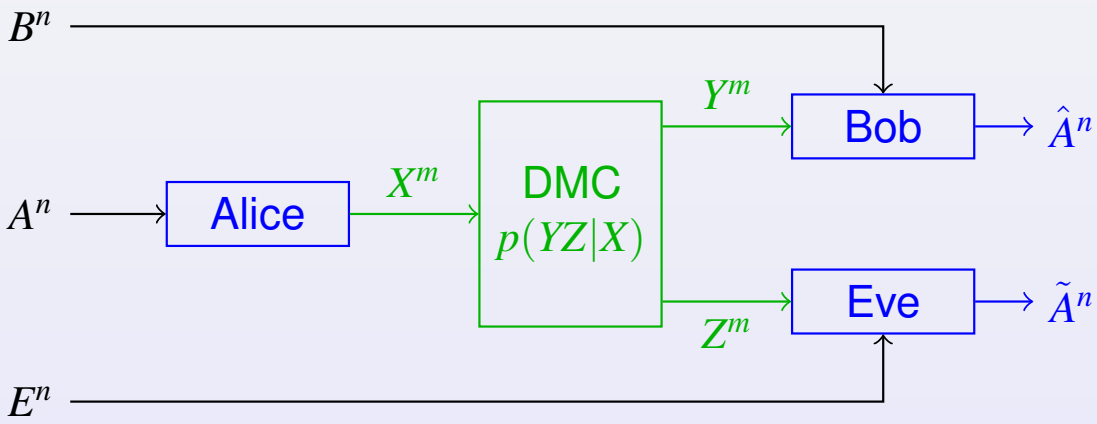
1. Comment utiliser l'information adjacente?
2. Comment tirer avantage du canal ?
   - [Wyner75][CsiszàrKörner78]: augmenter la sécurité

Questions



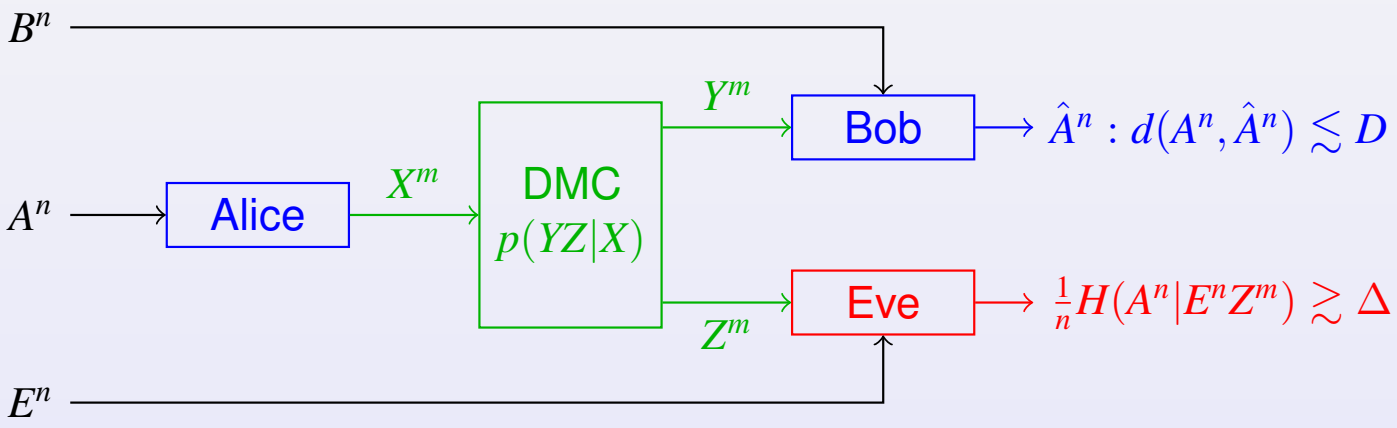
1. Comment utiliser l'information adjacente?
2. Comment tirer avantage du canal ?
3. Le problème est-il séparable ?

Questions



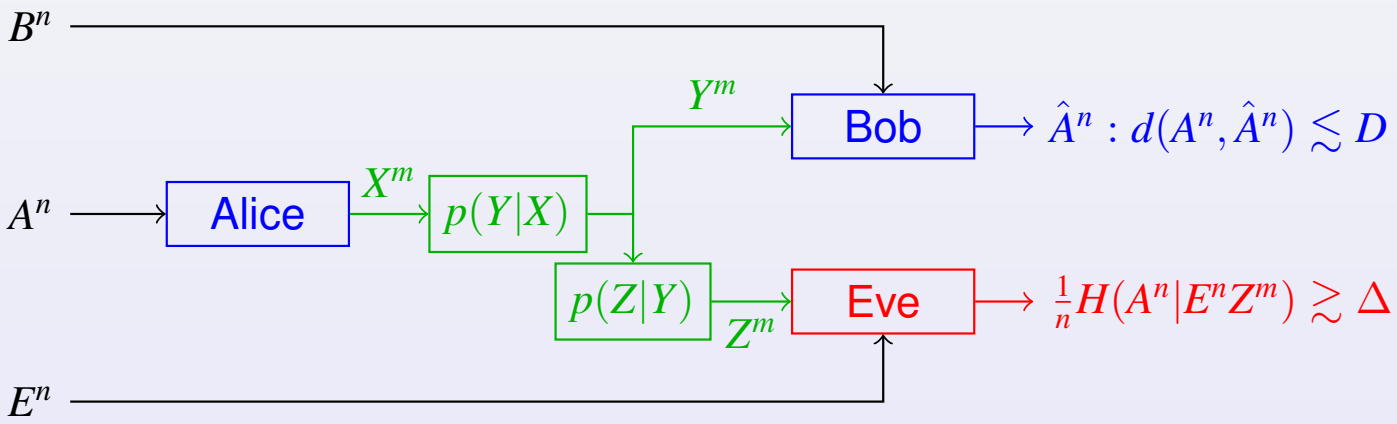
1. Comment utiliser l'information adjacente?
2. Comment tirer avantage du canal ?
3. Le problème est-il séparable ?
   - pour aider Bob et Ève, [Tuncel06] : schéma conjoint optimal

Questions



1. Comment utiliser l'information adjacente?
2. Comment tirer avantage du canal ?
3. Le problème est-il séparable ?
   - pour aider Bob et Ève, [Tuncel06] : schéma conjoint optimal

Questions



1. Comment utiliser l'information adjacente?
2. Comment tirer avantage du canal ?
3. Le problème est-il séparable ?
   - pour aider Bob et Ève, [Tuncel06] : schéma conjoint optimal
   - si $A \multimap B \multimap E$, $X \multimap Y \multimap Z$, [Merhav08]:

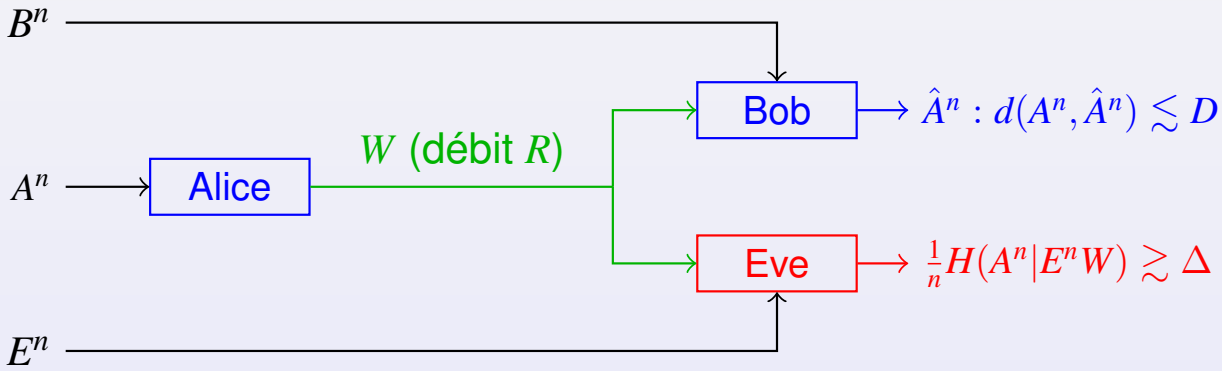
codage source de Wyner-Ziv $+$ codage canal de Wyner (*wiretap channel*)

Plan

1. Sous-problèmes
   - Codage source sous contrainte de sécurité
   - Codage canal sous contrainte de sécurité
2. Schéma numérique
   - Atteignabilité
   - Conditions d'optimalité
3. Schéma hybride

Plan

Codage source sous contrainte de sécurité



Caractérisation des triplets (R, D, Δ) atteignables

$$R \geq I(V;A|B)$$

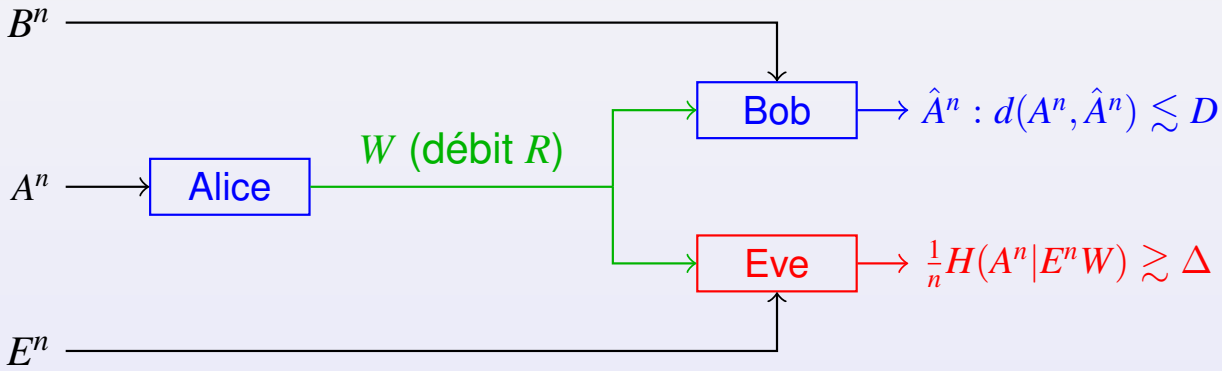
$$D \geq \mathbb{E}\left[d(A, \hat{A}(V,B))\right]$$

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

pour $U \multimap V \multimap A \multimap (B,E)$, et $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$.

J. Villard & P. Piantanida, *Secure Multiterminal Source Coding with Side Information at the Eavesdropper*, soumis à IEEE Trans IT, arXiv:1105.1658

Codage source sous contrainte de sécurité



Caractérisation des triplets (R, D, Δ) atteignables

$$R \geq I(V;A|B)$$

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

$$\Delta \leq H(A|VB) + I(A;B|U) - I(A;E|U)$$

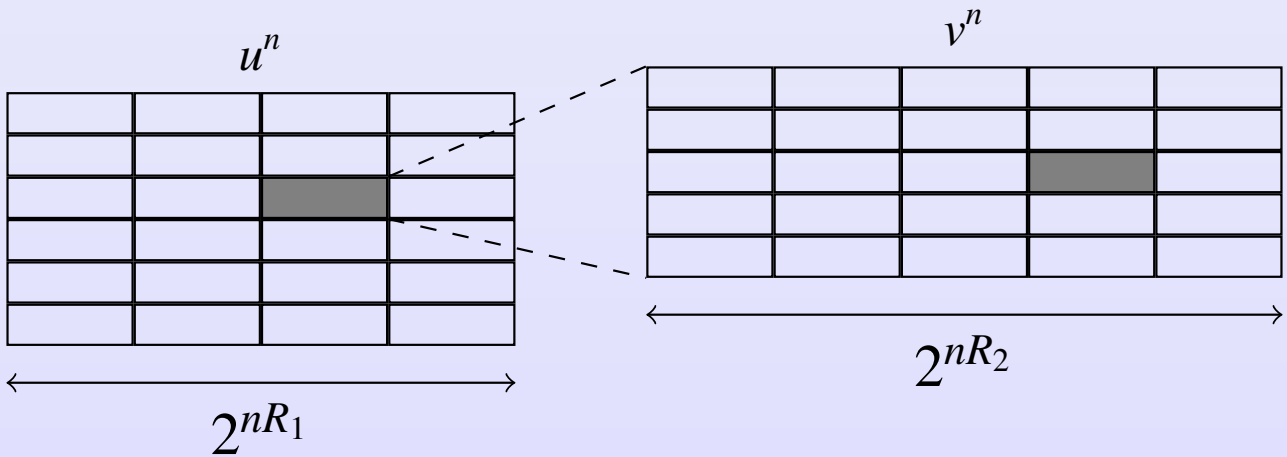
pour $U \multimap V \multimap A \multimap (B,E)$, et $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$.

J. Villard & P. Piantanida, *Secure Multiterminal Source Coding with Side Information at the Eavesdropper*, soumis à IEEE Trans IT, arXiv:1105.1658

Atteignabilité

- description de A en 2 couches U, V
- messages r_1, r_2 de débits resp. R_1, R_2
- superposition ($U \multimap V \multimap A$)
- binning *à la* Wyner-Ziv

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



Atteignabilité (suite)

- Distorsion à Bob

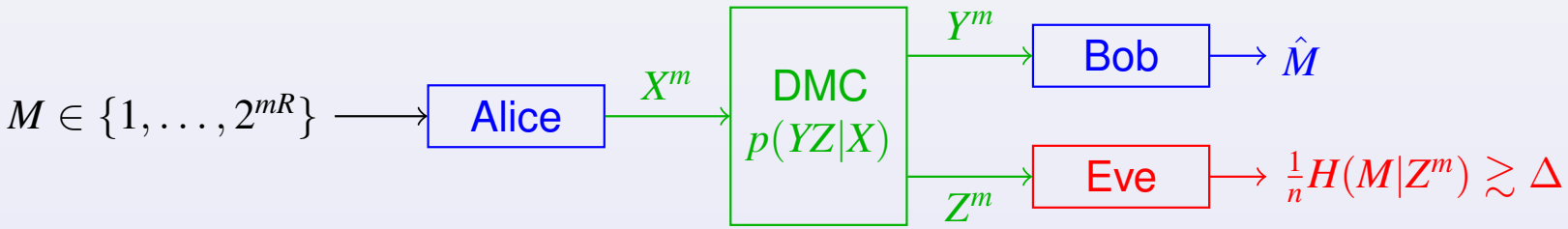
$$\mathbb{E}\left[d(A^n, g(f(A^n), B^n))\right] \approx \mathbb{E}\left[d(A, \hat{A}(V, B))\right]$$

- Incertitude à Eve

$$\begin{aligned} H(A^n|f(A^n)\,E^n) &= H(A^n|r_1 r_2 E^n) \\ &= H(A^n|r_1 E^n) - I(A^n; r_2|r_1 E^n) \\ &\geq H(A^n|r_1 E^n) - H(r_2) \\ &\geq n\left[H(A|UE) - R_2\right] \end{aligned}$$

Plan

Codage canal sous contrainte de sécurité



wiretap channel [Wyner75][CsiszàrKörner78]

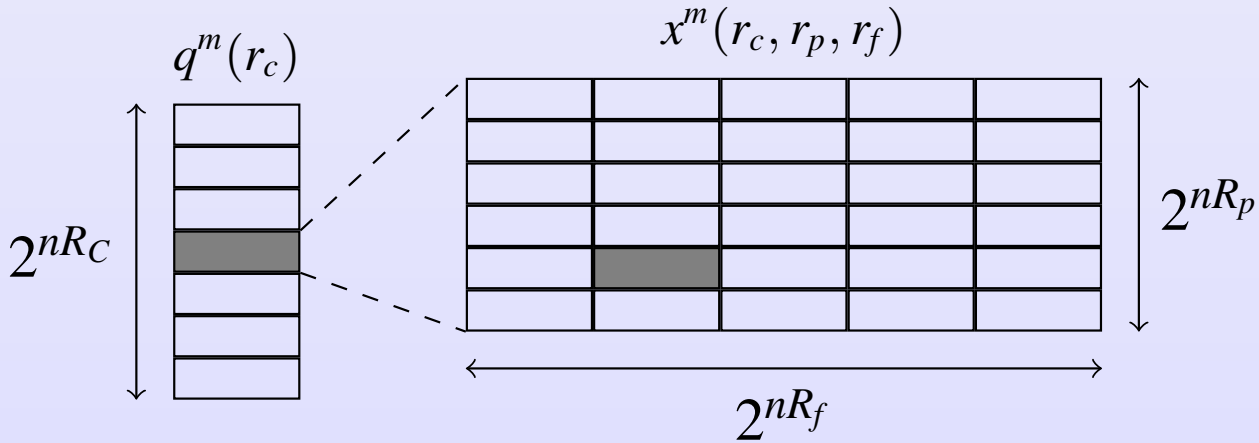
$$0 \leq \Delta \leq R$$
$$R \leq I(T;Y)$$
$$\Delta \leq I(T;Y|Q) - I(T;Z|Q)$$

pour $Q \multimap T \multimap X \multimap (Y,Z)$.

Atteignabilité [CsiszàrKörner78]

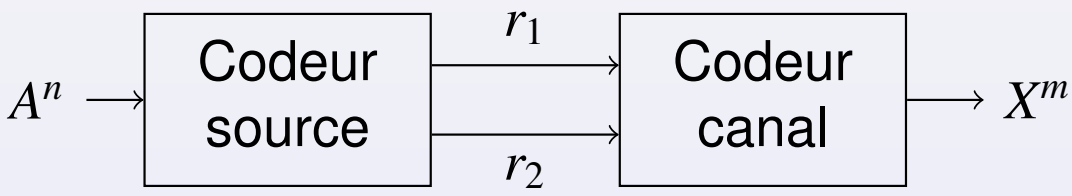
- 2 couches Q, X
- messages r_c, r_p de débits resp. R_c, R_p
- bruit numérique r_f de débit R_f ajouté sur X

$$R_c < I(Q;Y)$$
$$R_p + R_f < I(X;Y|Q)$$
$$R_f < I(X;Z|Q)$$



Plan

Structure “séparée”



Séparation opérationnelle

- 2 parties séparées
- étude conjointe

Caractérisation

- variables de source indépendantes des variables de canal
- optimisation conjointe

J. Villard, P. Piantanida and S. Shamai, *Secure Lossy Source-Channel Wiretapping with SI at the Receiving Terminals*, ISIT 2011, arXiv:1105.4555

Atteignabilité

Encodage

- description de A en U, V
- combinaison des bits : $M : (r_1, r_2) \mapsto (r_c, r_p)$
- deux couches Q, X pour transporter r_c, r_p
- $+$ bruit r_f pour protéger r_p

$$\begin{aligned} R_1 &> I(U;A|B) \\ R_2 &> I(V;A|UB) \\ R_1 + R_2 &= R_c + R_p \end{aligned} \qquad \begin{aligned} R_c &< kI(Q;Y) \\ R_p + R_f &< kI(X;Y|Q) \\ R_f &< kI(X;Z|Q) \end{aligned}$$

Atteignabilité

Encodage

- description de A en U, V
- combinaison des bits : $M : (r_1, r_2) \mapsto (r_c, r_p)$
- deux couches Q, X pour transporter r_c, r_p
- $+$ bruit r_f pour protéger r_p

$$\begin{aligned} R_1 &> I(U;A|B) \\ R_2 &> I(V;A|UB) \\ R_1 + R_2 &= R_c + R_p \end{aligned} \qquad \begin{aligned} R_c &< kI(Q;Y) \\ R_p + R_f &< kI(X;Y|Q) \\ R_f &< kI(X;Z|Q) \end{aligned}$$

Incertitude à Eve

- Eve peut utiliser conjointement E^n et Z^m

$\rightarrow$ résultats source et canal ne s'appliquent pas directement

- pour traites les termes conjoints : $R_1 \leq R_c$

Région intérieure correspondante

$(k, D, \Delta) \in \mathbb{R}_+^3$ est atteignable s'il existe

- des v.a. U, V, Q, T, X t.q.

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

- une fonction $\hat{A} : \mathcal{V} \times \mathcal{B} \to \mathcal{A}$,

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

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

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

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

Plan

Conditions d'optimalité et schémas optimaux

La variable aléatoire B est moins bruitée que E p/r A, si

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

pour tout U t.q. $U \multimap A \multimap (B,E)$. On note $B \succeq_A E$.

Conditions d'optimalité et schémas optimaux

La variable aléatoire B est moins bruitée que E p/r A, si

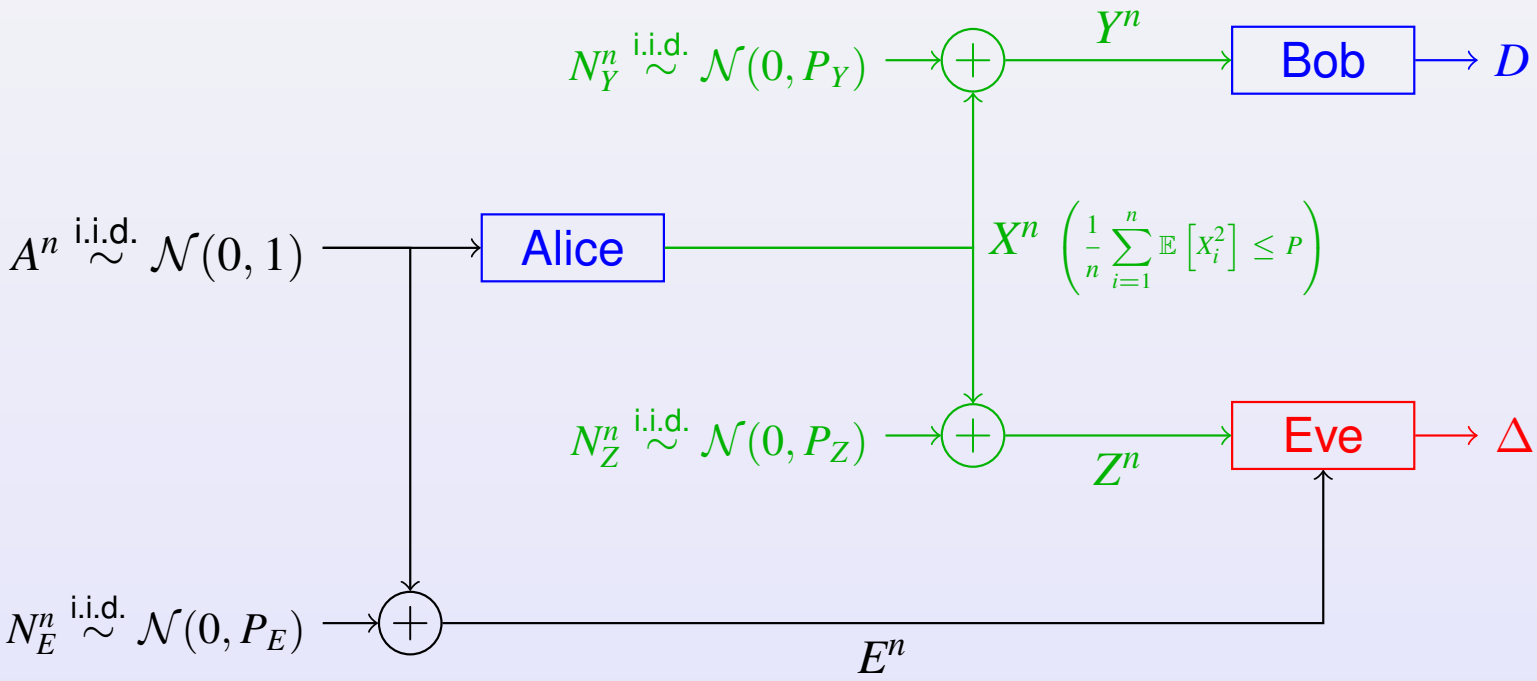
$$I(U;B) \geq I(U;E)$$

pour tout U t.q. $U \multimap A \multimap (B,E)$. On note $B \succeq_A E$.

	$B \succeq_A E$	$E \succeq_A B$
$Y \succeq_X Z$	Wyner-Ziv + codage pour wiretap	?
$Z \succeq_X Y$	Wyner-Ziv + codage canal classique	codage source sécurisé + codage canal classique

Plan

Exemple gaussien



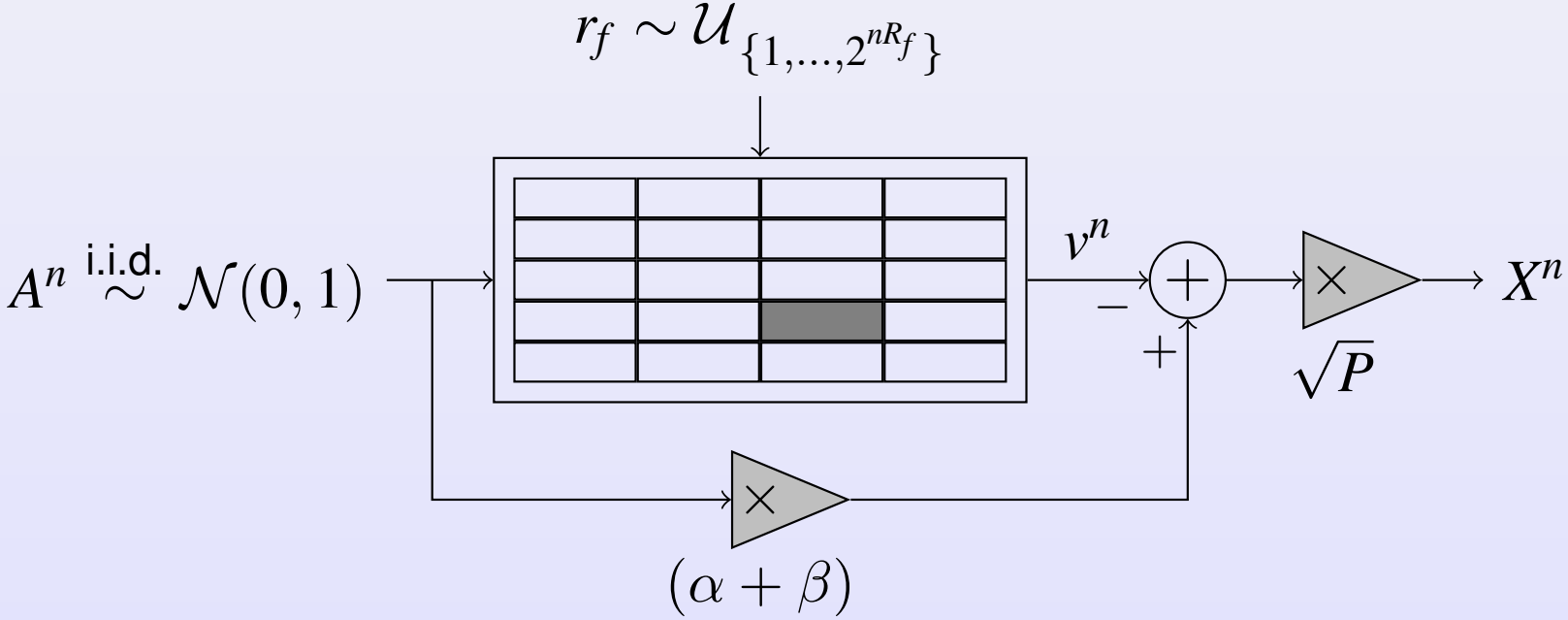
Hypothèse : $P_Y < P_Z$

On a bien : $E \succeq_A B$ et $Y \succeq_X Z$

Distorsion : erreur quadratique, $d(a,b) = (a-b)^2$

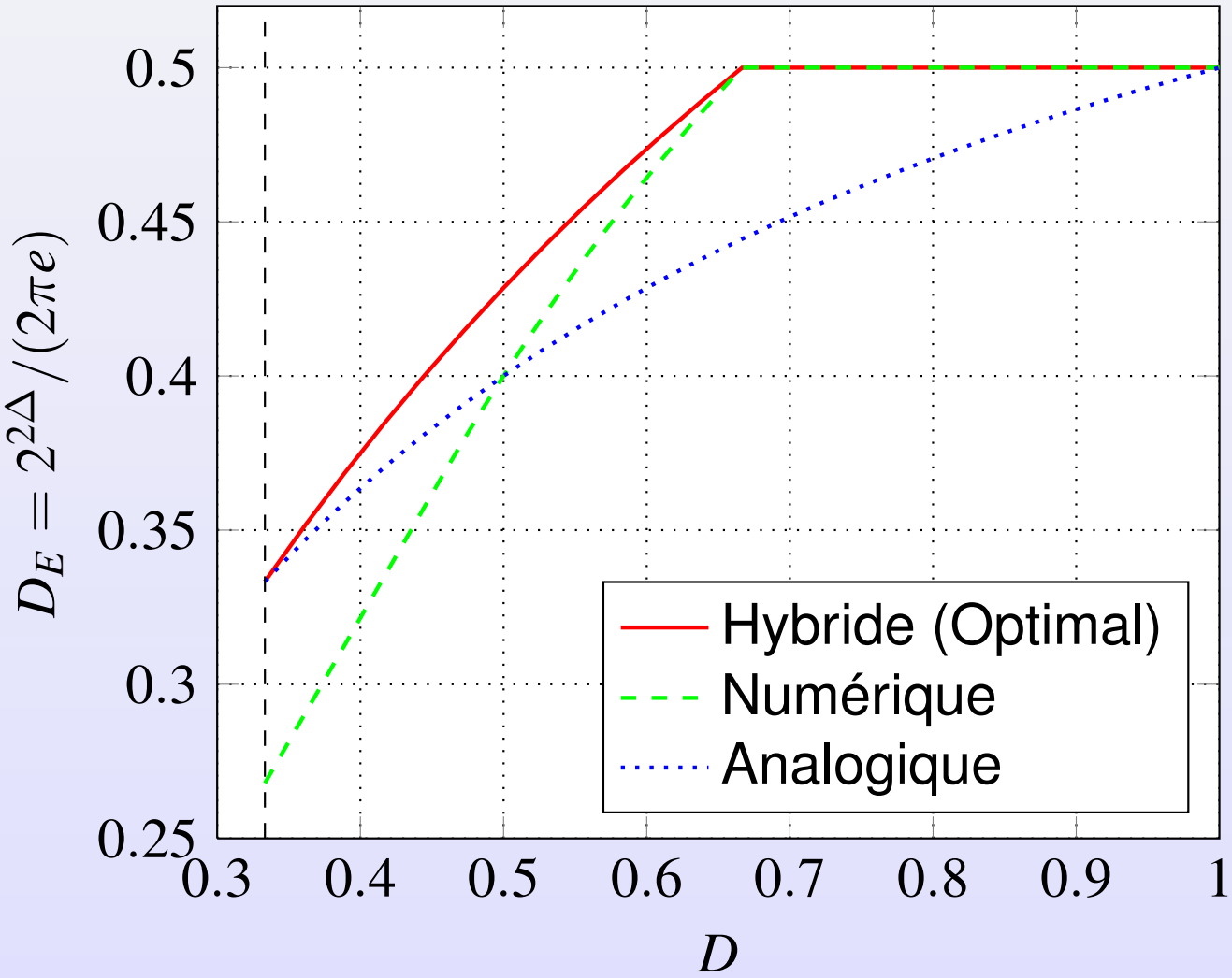
Codage hybride

Mots de code v^n : $V = \alpha A + \gamma N$
où $\alpha \in \mathbb{R}$, $\beta < 1$, $\gamma = \sqrt{1-\beta^2}$ et $N \overset{\perp\!\!\!\perp A}{\sim} \mathcal{N}(0,1)$.



J. Villard, P. Piantanida and S. Shamai, *Hybrid Digital/Analog Schemes for Secure Transmission with Side Information*, ITW 2011, arXiv:1109.0696

Résultats numériques



Conclusion

- Codage de source sous contrainte de sécurité : caractérisation de la région atteignable

Conclusion

- Codage de source sous contrainte de sécurité : caractérisation de la région atteignable
- Schéma numérique :

  codage de source sécurisé $+$ codage canal pour wiretap

$\rightarrow$ Séparation opérationnelle

Conclusion

- Codage de source sous contrainte de sécurité : caractérisation de la région atteignable

- Schéma numérique :

  codage de source sécurisé $+$ codage canal pour wiretap

$\rightarrow$ Séparation opérationnelle

- Optimal sous certaines conditions ($B \succeq_A E$ ou $Z \succeq_X Y$)

$+$ Séparation

Conclusion

- Codage de source sous contrainte de sécurité : caractérisation de la région atteignable
- Schéma numérique :

  codage de source sécurisé $+$ codage canal pour wiretap

$\rightarrow$ Séparation opérationnelle

- Optimal sous certaines conditions ($B \succeq_A E$ ou $Z \succeq_X Y$)

$+$ Séparation

- Schéma hybride optimal dans certains cas gaussiens, binaires, ...

Merci de votre attention.

J. Villard and P. Piantanida
Secure Multiterminal Source Coding with Side Information at the Eavesdropper
soumis à *IEEE Trans. Inf. Theory*, arXiv:1105.1658

J. Villard, P. Piantanida and S. Shamai
Secure Lossy Source-Channel Wiretapping with Side Information at the Receiving Terminals
ISIT 2011, arXiv:1105.4555

J. Villard, P. Piantanida and S. Shamai
Hybrid Digital/Analog Schemes for Secure Transmission with Side Information
ITW 2011, arXiv:1109.0696