INFORMED SECURE WATERMARKING USING OPTIMAL TRANSPORT

Patrick Bas

CNRS - LAGIS, Lille, France

25 may 2011

Outline

Outline

Security in Watermarking

Adversary

- Limited or unlimited power

Materials

- Watermark detector/decoder
- Contents watermarked with the same key/messages
- Knowledge about the embedding and decoding algorithm (Kerckhoffs' principle)

Objectives

- Estimate the secret key
- Alter/copy the message

Security in Watermarking

Adversary

- Limited or unlimited power

Materials

- Watermark detector/decoder
- Contents watermarked with the same key/messages
- Knowledge about the embedding and decoding algorithm (Kerckhoffs' principle)

Objectives

- Estimate the secret key
- Alter/copy the message

Security in Watermarking

Adversary

- Limited or unlimited power

Materials

- Watermark detector/decoder
- Contents watermarked with the same key/messages
- Knowledge about the embedding and decoding algorithm (Kerckhoffs' principle)

Objectives

- Estimate the secret key
- Alter/copy the message

Security framework

Materials

- Gaussian host
- i.i.d. host
- Same secret key
- Watermarked contents only: WOA

Goals

- Design a secure scheme
- Minimise the embedding distortion
- Maximise the robustness

Security framework

Materials

- Gaussian host
- i.i.d. host
- Same secret key
- Watermarked contents only: WOA

Goals

- Design a secure scheme
- Minimise the embedding distortion
- **Maximise the robustness**

How to maximise robustness?

- Use informed coding and side information from the Host (Costa's idea)
- Generate different coding regions for the same message
- Embedding: go toward the closest one

How to maximise robustness?

- Use informed coding and side information from the Host (Costa's idea)
- Generate different coding regions for the same message
- Embedding: go toward the closest one

How to maximise robustness?

- Use informed coding and side information from the Host (Costa's idea)
- Generate different coding regions for the same message
- Embedding: go toward the closest one

Outline

1 :Distribution Splitting (I/II)

Stego-security a.k.a. Perfect Secrecy

- $p(x) = p(y|k)$

Binary Embedding

- $p_{Y|K} = (p_{Y|K,m=0} + p_{Y|K,m=1})/2$

Partitionning function $g(.)$

- $p_{Y|K,m=0}(\mathbf{x}) = 2g(\mathbf{x})p_X(\mathbf{x})$
- $p_{Y|K,m=1}(\mathbf{x}) = 2(1-g(\mathbf{x}))p_X(\mathbf{x})$

1 :Distribution Splitting (I/II)

Stego-security a.k.a. Perfect Secrecy

- $p(x) = p(y|k)$

Binary Embedding

- $p_{Y|K} = (p_{Y|K,m=0} + p_{Y|K,m=1})/2$

Partitionning function $g(.)$

- $p_{Y|K,m=0}(x) = 2g(x)p_X(x)$
- $p_{Y|K,m=1}(x) = 2(1-g(x))p_X(x)$

1 :Distribution Splitting (I/II)

Stego-security a.k.a. Perfect Secrecy

- $p(x) = p(y|k)$

Binary Embedding

- $p_{Y|K} = (p_{Y|K,m=0} + p_{Y|K,m=1})/2$

Partitionning function $g(.)$

- $p_{Y|K,m=0}(x) = 2g(x)p_X(x)$
- $p_{Y|K,m=1}(x) = 2(1-g(x))p_X(x)$

1 :Distribution Splitting (I/II)

Stego-security a.k.a. Perfect Secrecy

- $p(x) = p(y|k)$

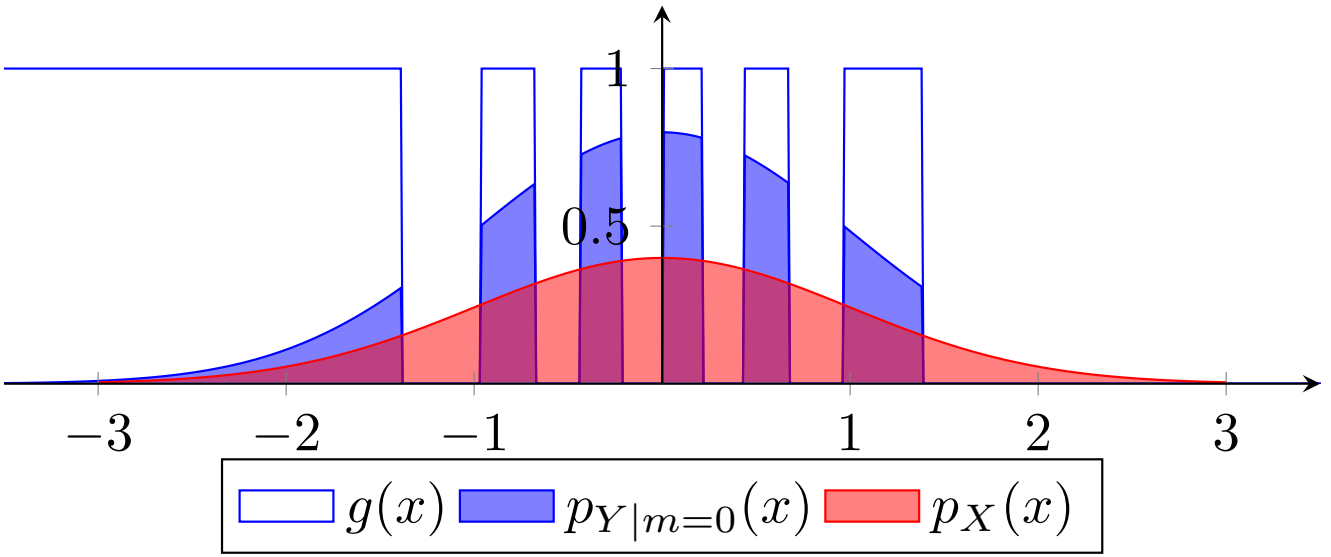
Binary Embedding

- $p_{Y|K} = (p_{Y|K,m=0} + p_{Y|K,m=1})/2$

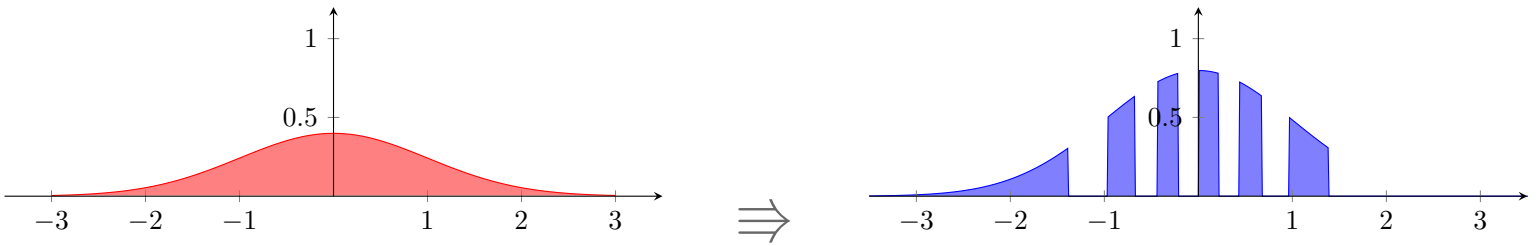
Partitionning function $g(.)$

- $p_{Y|K,m=0}(\mathbf{x}) = 2g(\mathbf{x})p_X(\mathbf{x})$
- $p_{Y|K,m=1}(\mathbf{x}) = 2(1-g(\mathbf{x}))p_X(\mathbf{x})$

1: Distribution Splitting (II/II)



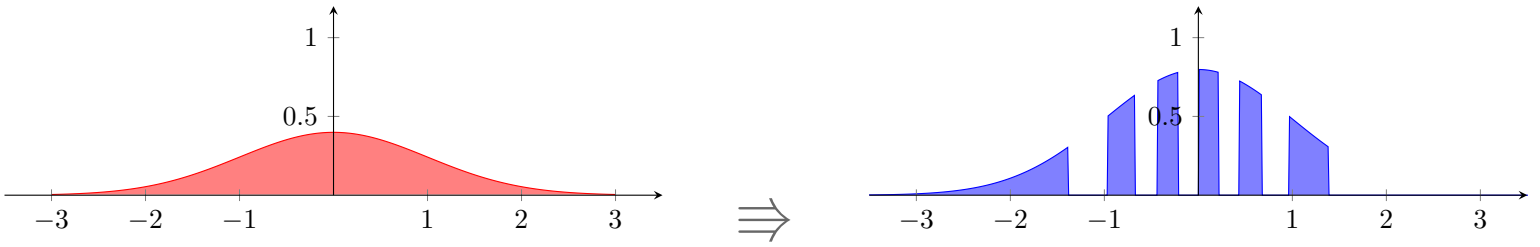
2: Distribution Matching



Requirement for Distribution Matching

- Find a mapping $y = T(x)$ such that $x \sim p_X$ and $y \sim p_{Y|m=0,1}$

2: Distribution Matching



Requirement for Distribution Matching

- Find a mapping $y = T(x)$ such that $x \sim p_X$ and $y \sim p_{Y|m=0,1}$

3: Distortion Minimisation

- Minimise the average L^2 distortion

Solution for distortion matching and distortion minimisation:

1. Optimal Transportation
2. $T(x) = F^{-1}_{Y|d} \circ F_X(x)$,
3. $\sigma_w^2 = \int_0^1 (F_Y^{-1}(x|d) - F_X^{-1}(x))^2 dx$

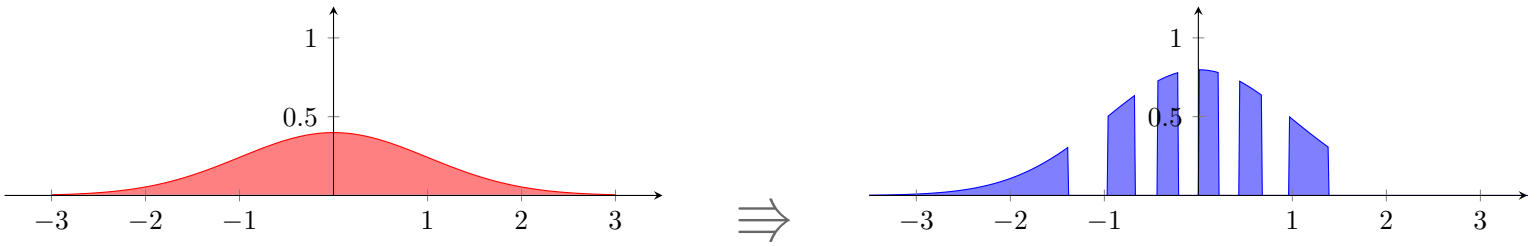
3: Distortion Minimisation

- Minimise the average L^2 distortion

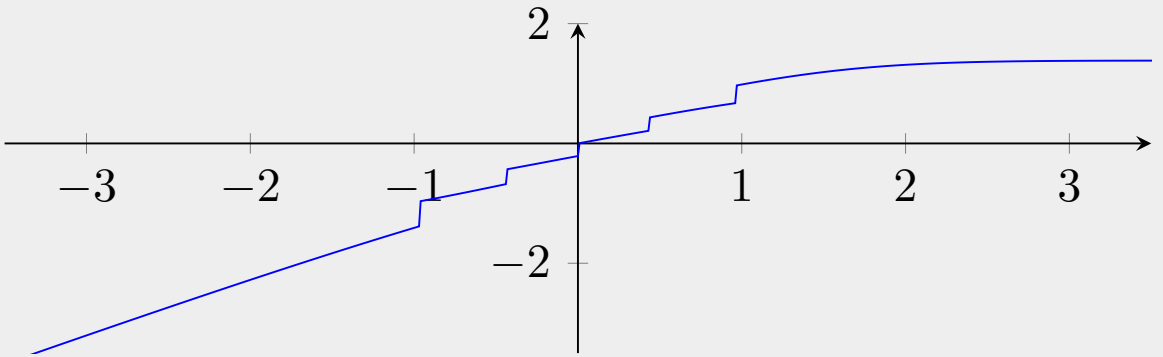
Solution for distortion matching and distortion minimisation:

1. Optimal Transportation
2. $T(x) = F^{-1}_{Y|d} \circ F_X(x)$,
3. $\sigma_w^2 = \int_0^1 (F_Y^{-1}(x|d) - F_X^{-1}(x))^2 dx$

Example

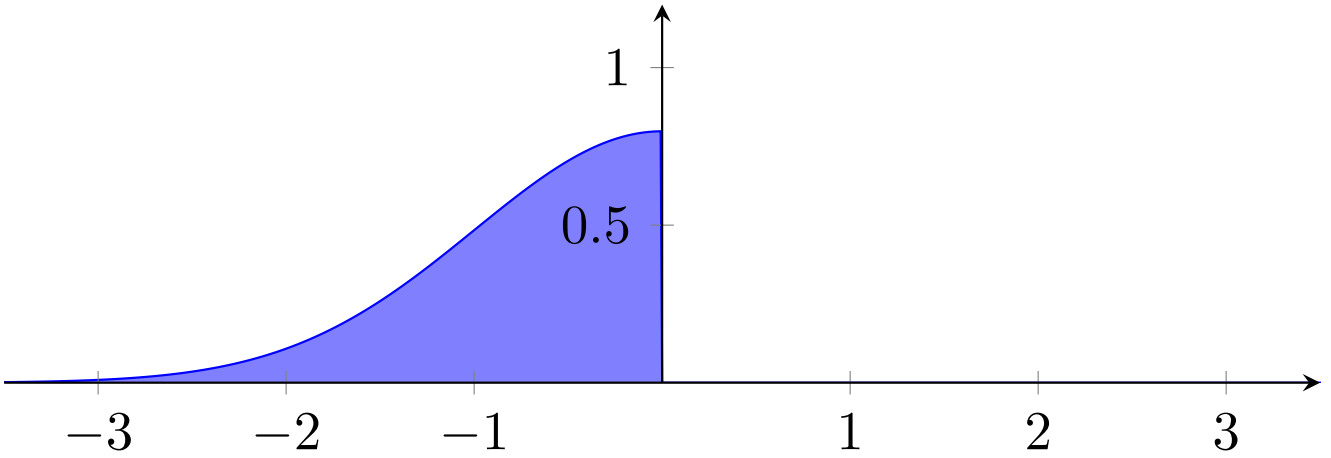


Example of $T(x)$



Different partitioning functions I/IV

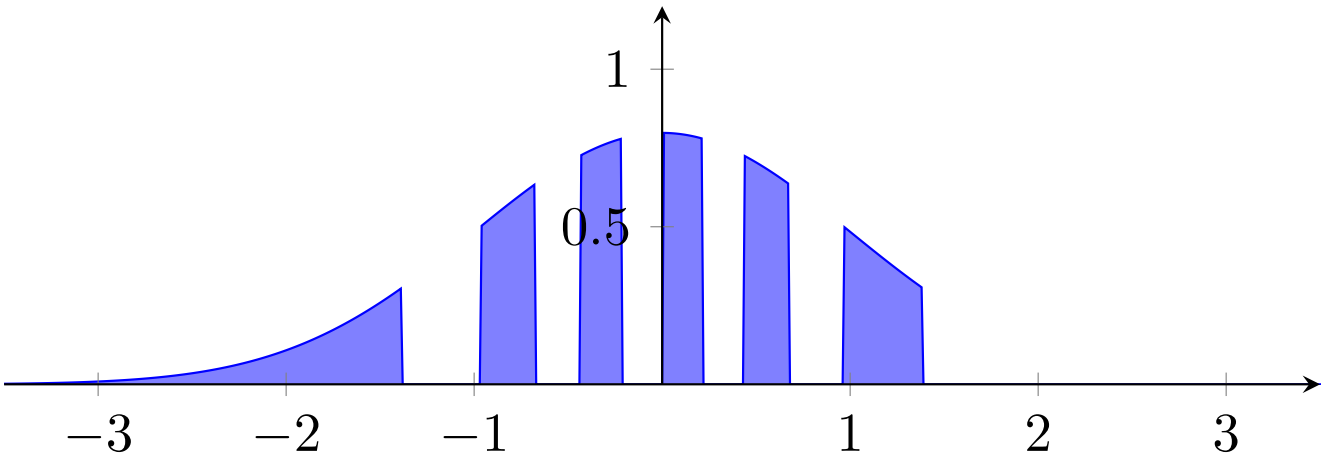
Transport Natural Watermarking (TWN) [1] (non informed):



[1] B. Mathon, P. Bas, F. Cayre, and B. Macq, ***"Optimization of Natural Watermarking Using Transportation Theory"*** in MM&Sec'09 : Proceedings of the 11th ACM workshop on Multimedia and security, New York, NY, USA, 2009, pp. 33–38, ACM.

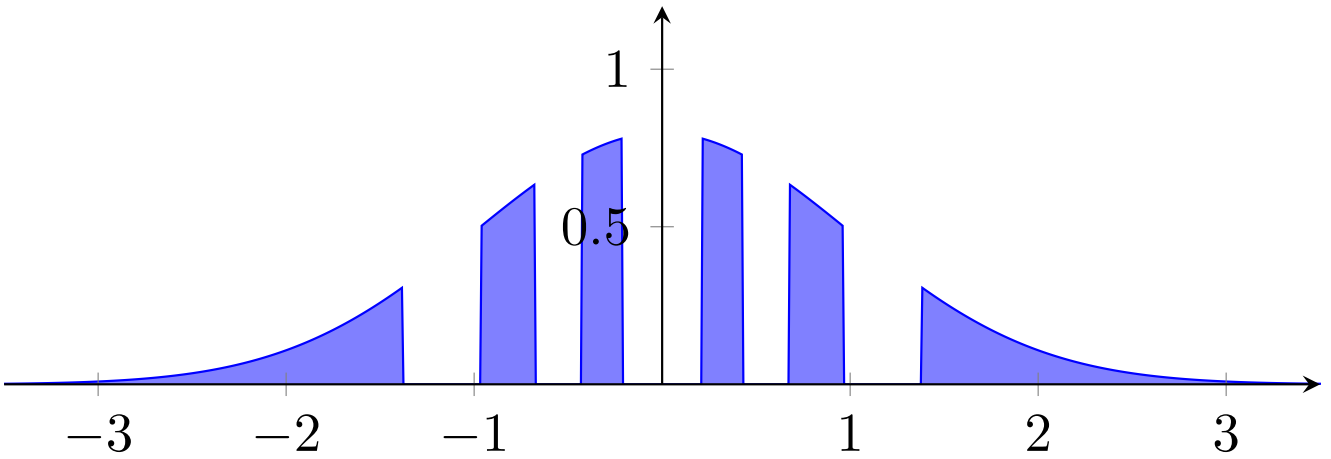
Different partitioning functions II/IV

p **Natural Watermarking** (p-NW): each coding region has the same probability p:



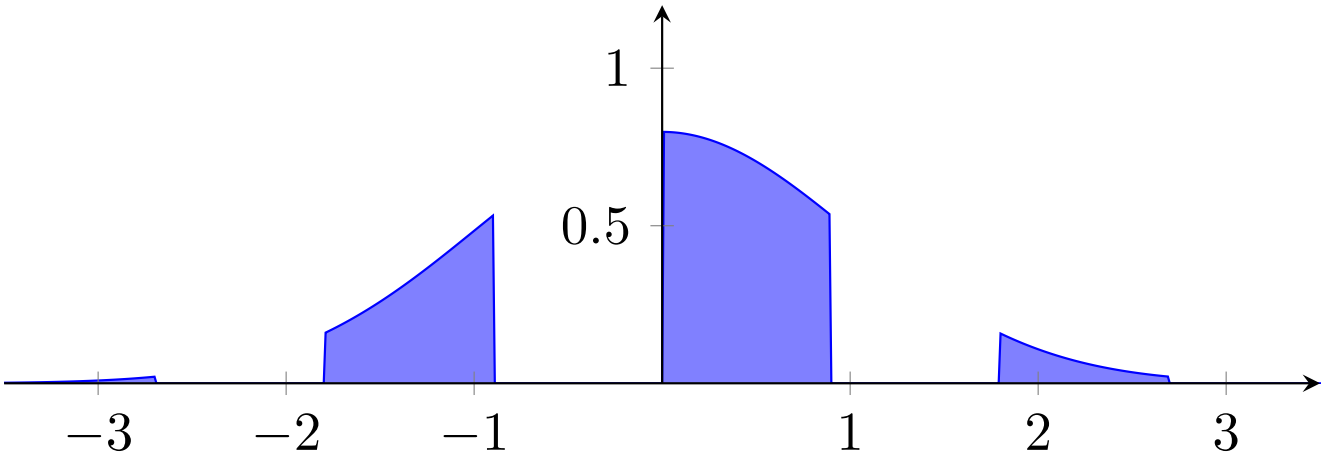
Different partitioning functions III/IV

$\bar{p}$ Natural Watermarking ($\bar{p}$-NW): **p Natural Watermarking** symmetrised on 0:



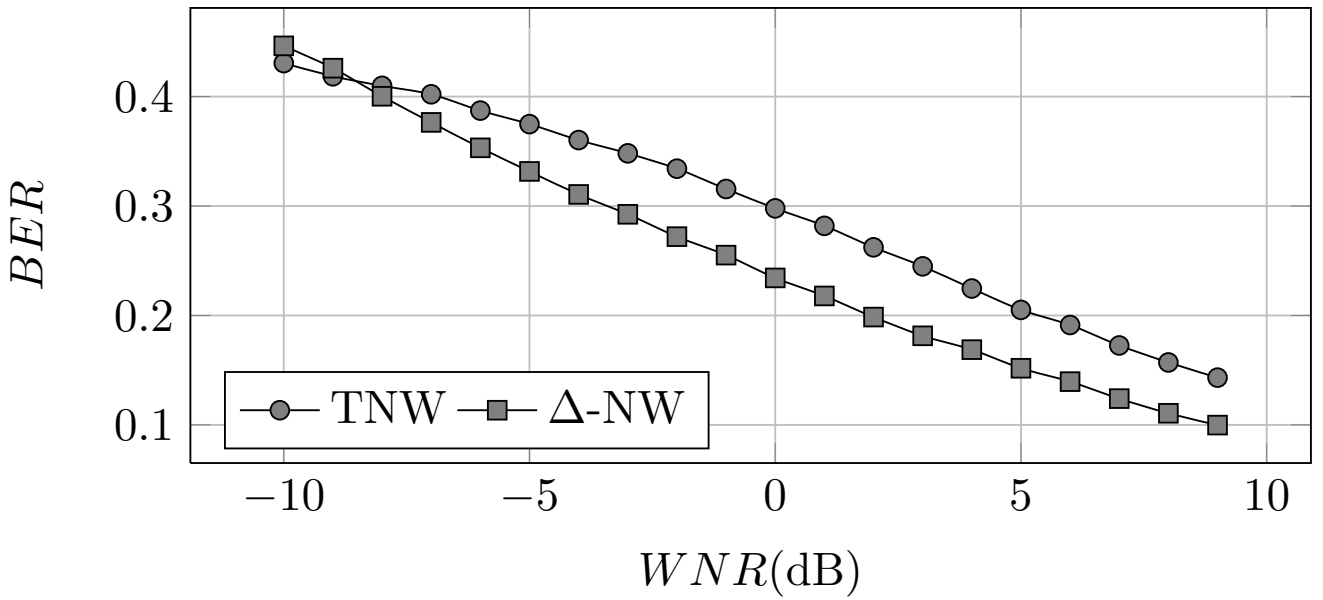
Different partitioning functions IV/IV

Δ **Natural Watermarking** (Δ-NW): each coding region has the same width:

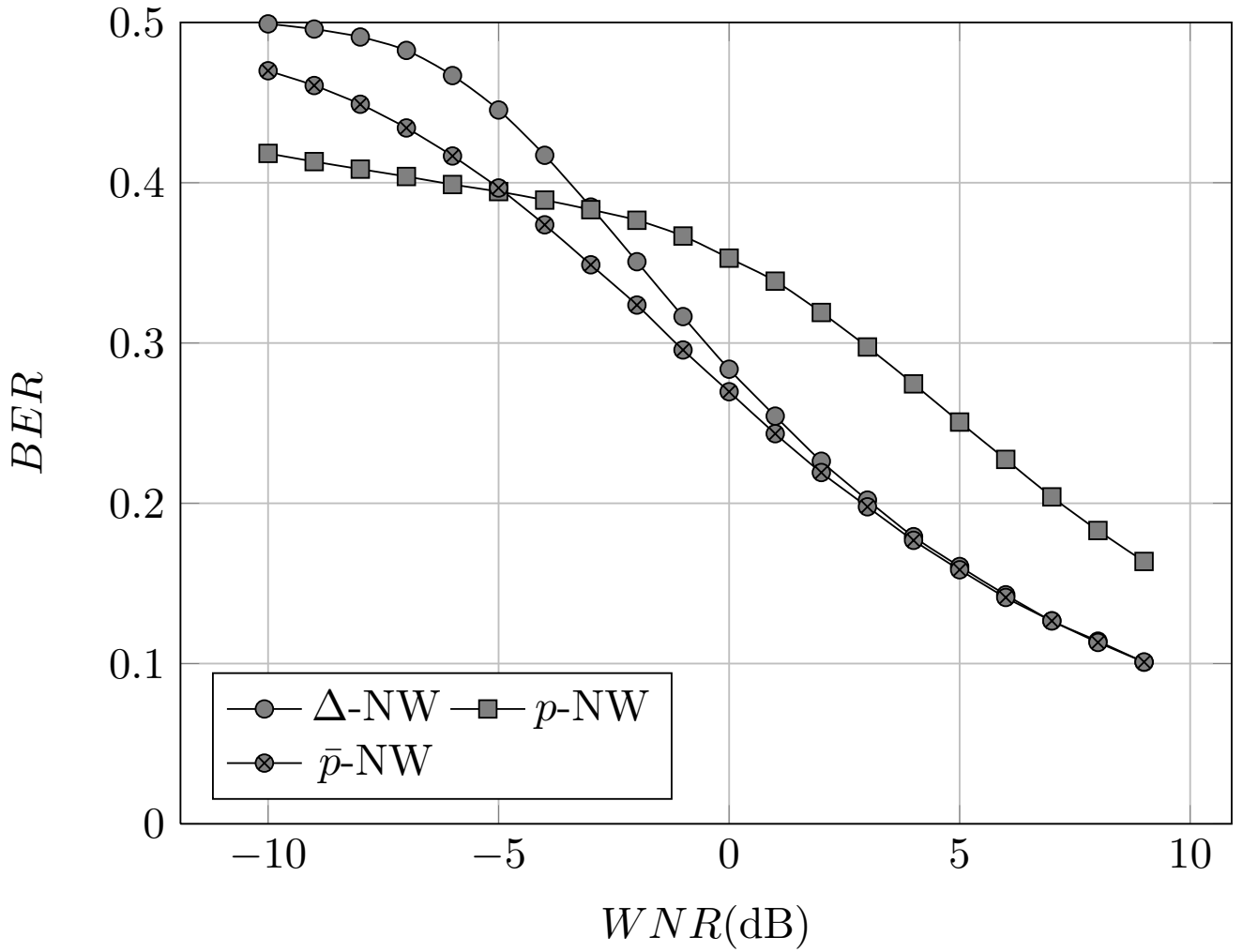


Outline

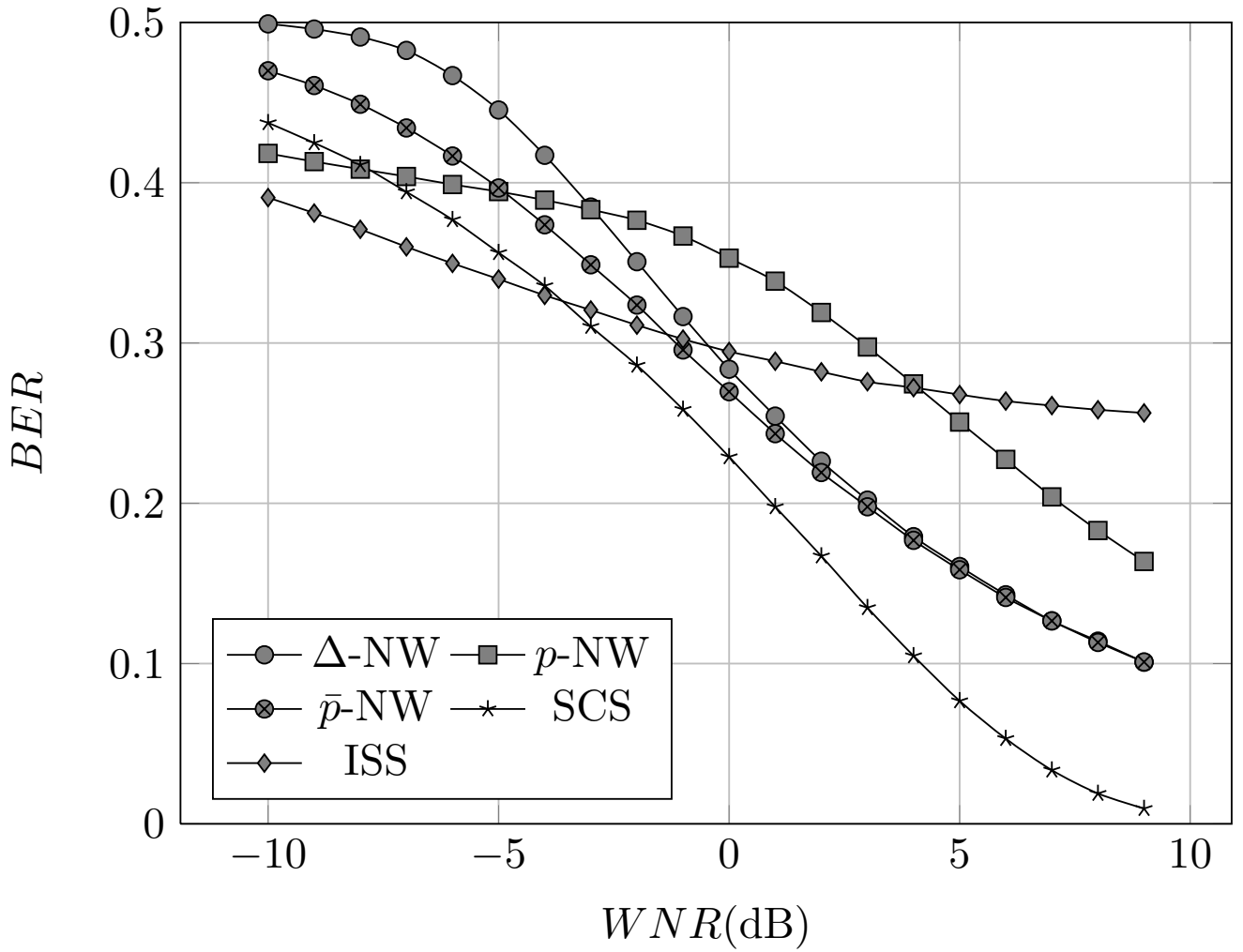
Non-informed Vs informed coding



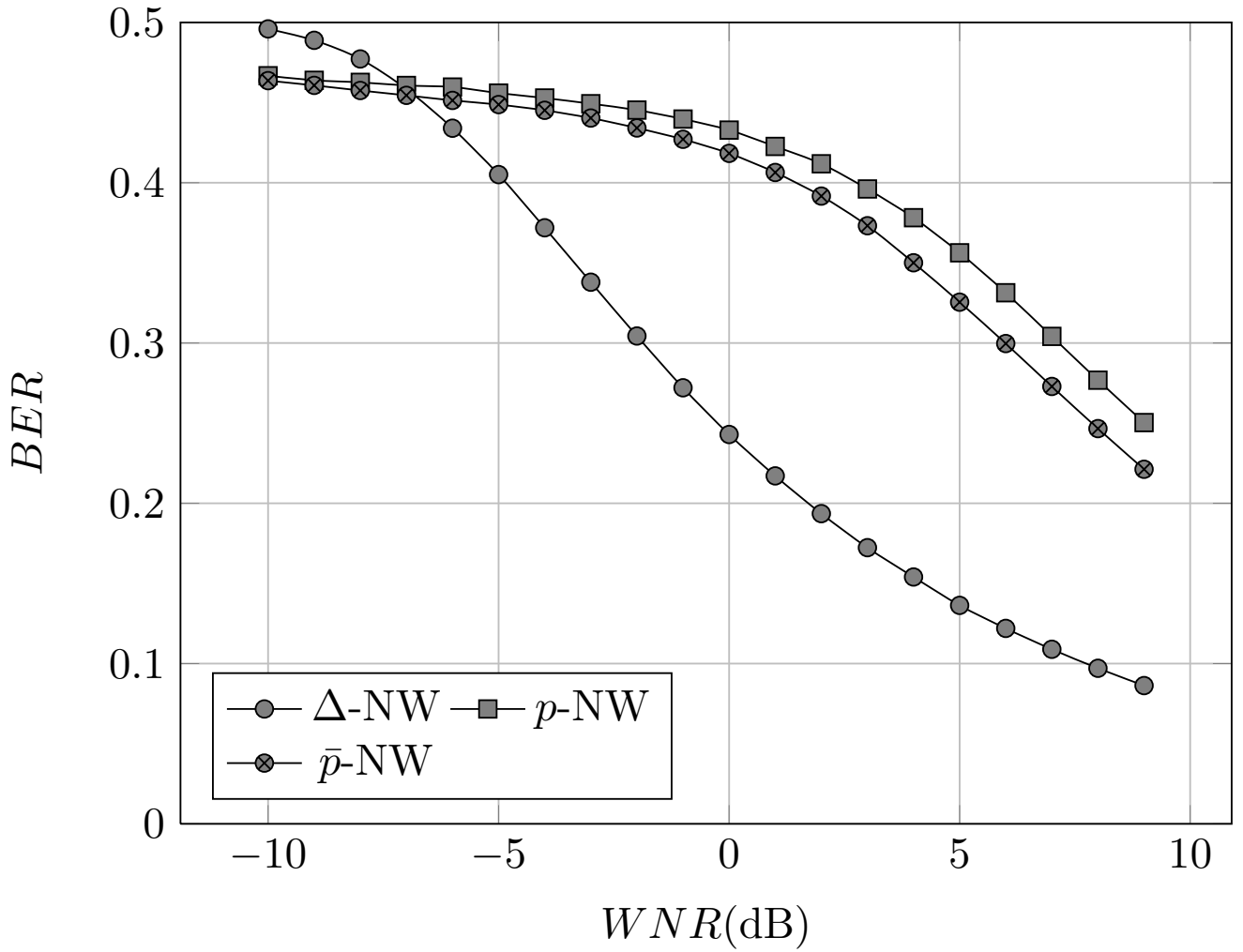
$WCR = -5dB$



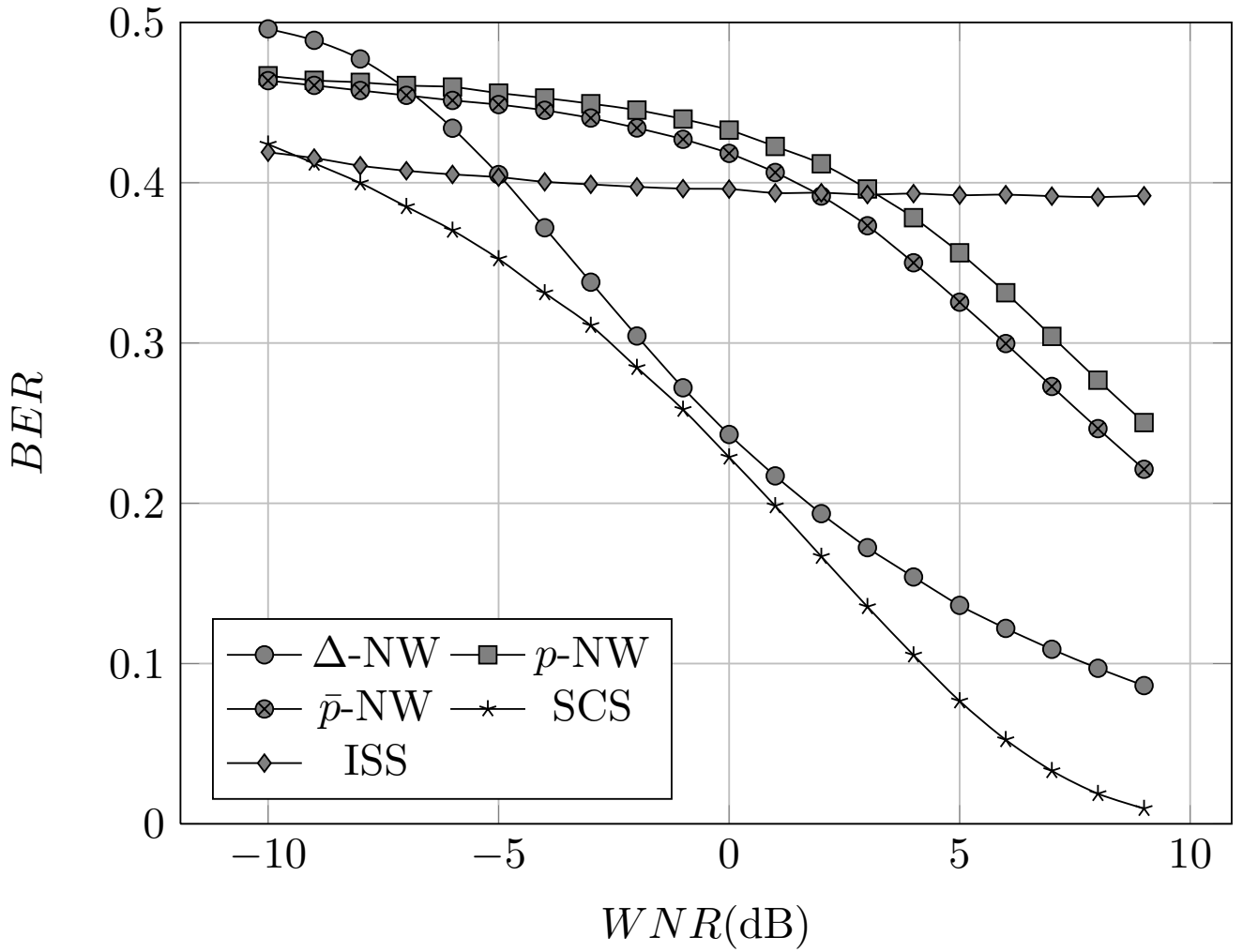
$WCR = -5dB$



$WCR = -11dB$



$WCR = -11dB$



Outline

Conclusions and perspectives

Conclusions

- Importance of distribution splitting and distribution matching to design secure scheme
- Optimal transport adapted in 1-D
- Gain of using Informed Coding
- The best partitioning depends of the *WCR* and the *WNR*

Perspectives

- Links with secure adaptations of SCS (IH11)
- What is the secure capacity?
- Can we find secure error correcting codes to increase the quality of service?

Conclusions and perspectives

Conclusions

- Importance of distribution splitting and distribution matching to design secure scheme
- Optimal transport adapted in 1-D
- Gain of using Informed Coding
- The best partitioning depends of the *WCR* and the *WNR*

Perspectives

- Links with secure adaptations of SCS (IH11)
- What is the secure capacity?
- Can we find secure error correcting codes to increase the quality of service?