lunedì 24 gennaio 2022 17:00

$P(b=1|\bar{b}=0) + P(b=0|\bar{b}=1) = 0,2$

$P(b=1|\bar{b}=1) + P(b=0|\bar{b}=0) = 0,8$

M SBAGLIATO GIUSTO M*

$P(b=1|\bar{b}=0) + P(b=0|\bar{b}=1) = 0,75$

$P(b=1|\bar{b}=1) + P(b=0|\bar{b}=0) = 0,25$

1,5 / 1 - 2·0,75 / 0,5

0,5 0,5 0,5

UPPER BOUND.

$d_b(x_0, x_1) = |1 - P_{b|b}(1|0) - P_{b|\bar{b}}(0|1)| \leq |1 - 2 \cdot 0,2| \leq 0,6.$

$< 0,2$ $< 0,2$

0,5 sim

$d(x_0, x_1) = 1 - P_{b|\bar{b}}(1|0) - P$

M → 0 0,8 — D →

$P(b=1|\bar{b}=0) + P(b=0|\bar{b}=1) = \text{fallisce} : 0,2$ ma fatto meglio.

$P(b=1|b=1) + P(b=0|\bar{b}=0) = 0,8$

Problem 1

1.1) Consider a security mechanism M which can be distinguished from its ideal counterpart M^* by a distinguisher D with the following probabilities

- D correctly identifies M with probability 0.8
- D correctly identifies M^* with probability 0.25

Can you find an *upper bound* to the unconditional security level of M in terms of distinguishability?

Can you find a *lower bound*?