

Funct: We use The lemme to prove theorem.

PROOF (of THH). Set
$$Y = (S, h(S, X))$$
 $V = V_{d+l} = (S, V_{e}), Y = 10,15d+l$
 $Col(Y) = P_{T} E Y = Y' J$
 $= P_{T} E S = S' \wedge h(S, X) = h(S', X') J$
 $= P_{T} E S = S' \wedge h(S, X) = h(S, X') J$
 $= P_{T} E S = S' \wedge h(S, X) = h(S, X') J$
 $= P_{T} E S = S' \wedge h(S, X) = h(S, X') J$
 $= 2^{-d} \cdot P_{T} E h(S, X) = h(S, X') J$
 $= 2^{-d} \cdot P_{T} E X = X' J \cdot P_{T} E h(S, X) = h(S, X')$
 $= 2^{-d} \cdot (P_{T} E X = X' J \cdot P_{T} E h(S, X) = h(S, X')$

PrIh(S, X) = h(S, X') |
$$X \neq X'J$$
)

(This because

PrIAJ = PrIANBJ + PrIANBJ

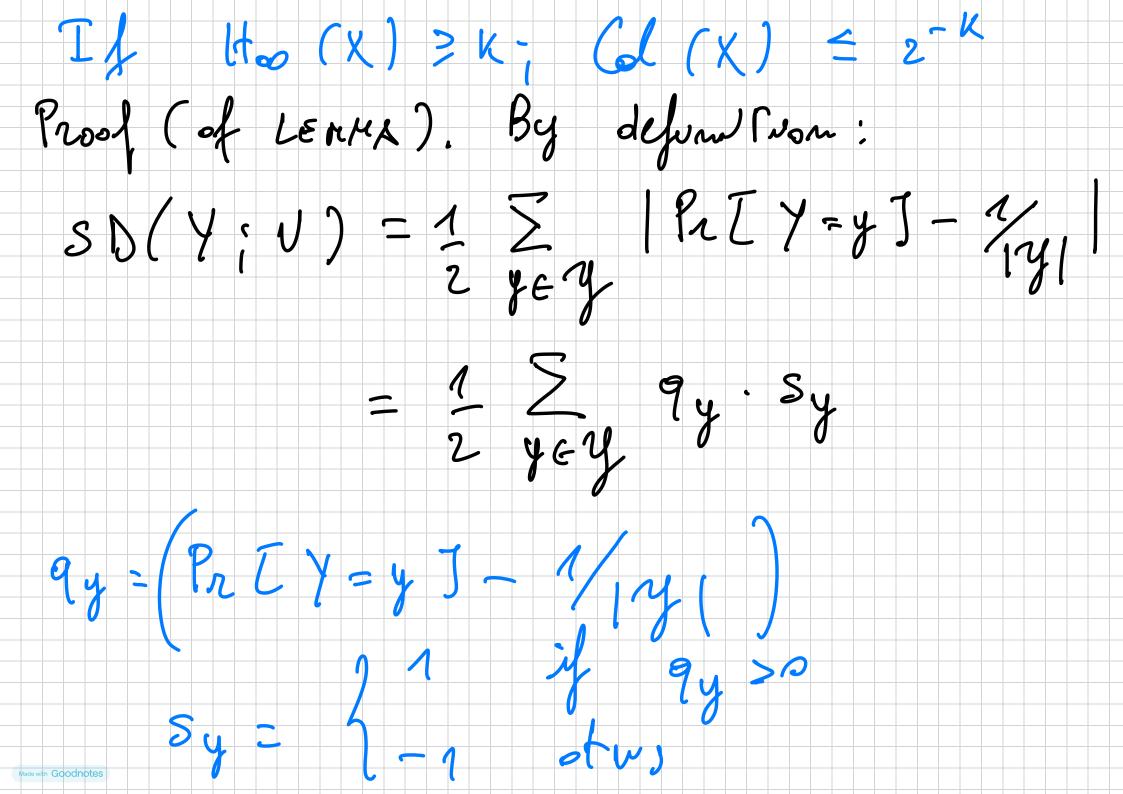
= PrIBJ · PrIA | BJ +

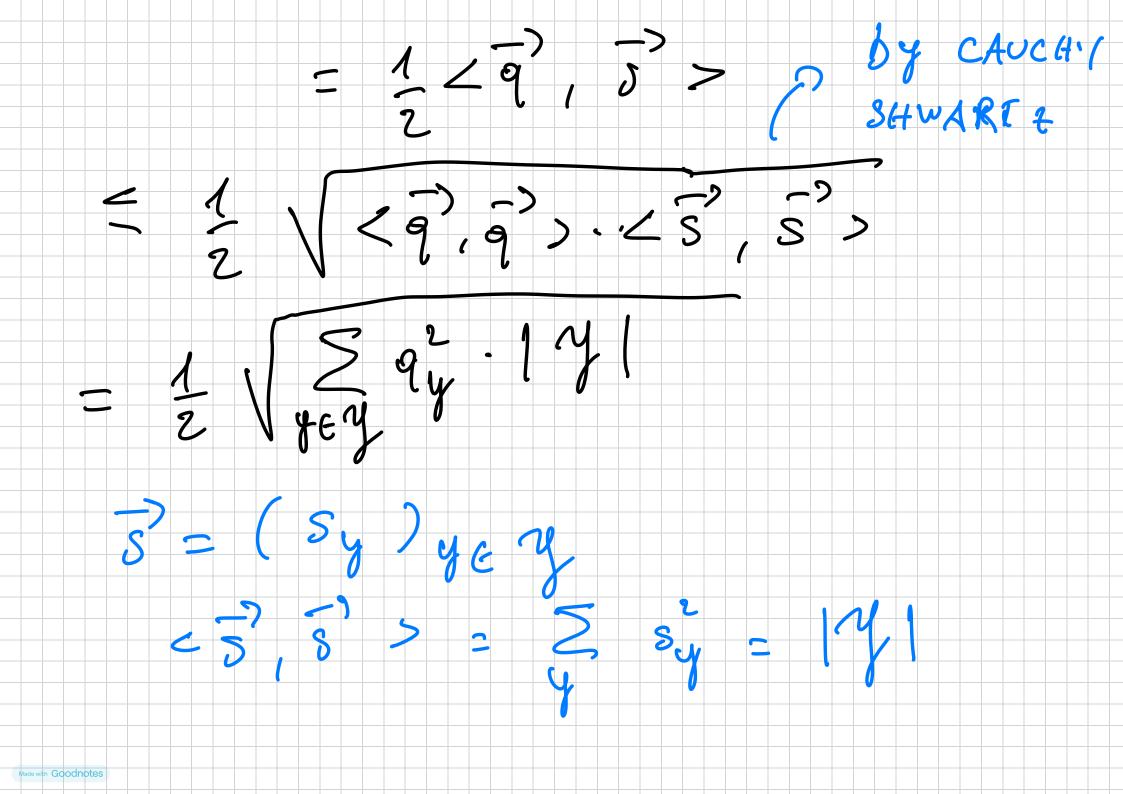
+ PrIBJ · PrIA | BJ)

= 2^{-d} (Col(X) + PrIh(S, X) = h(S, X')

 $\wedge X \neq X'J$)

$$\begin{cases}
2^{-6} \left(2^{-K} + 2^{-\ell} \right) \\
= \frac{1}{2^{1+\ell}} \left(2^{\ell-K} + 1 \right) \\
\left(\ell-K = 2 - 2 \log (1/\epsilon) \right) \\
= \frac{1}{2^{1+\ell}} \left(2^{\ell-K} + 1 \right) \\
= \frac{1}{2^{1+\ell}} \left(2^{\ell-K} + 2^{\ell-k} \right) \\
= \frac{1}{2^{\ell-k}} \left(2^{\ell-K} + 2^{\ell-k} \right) \\
= \frac{1}{2^{\ell-k}} \left(2^{\ell-K} + 2^{\ell-k} \right$$



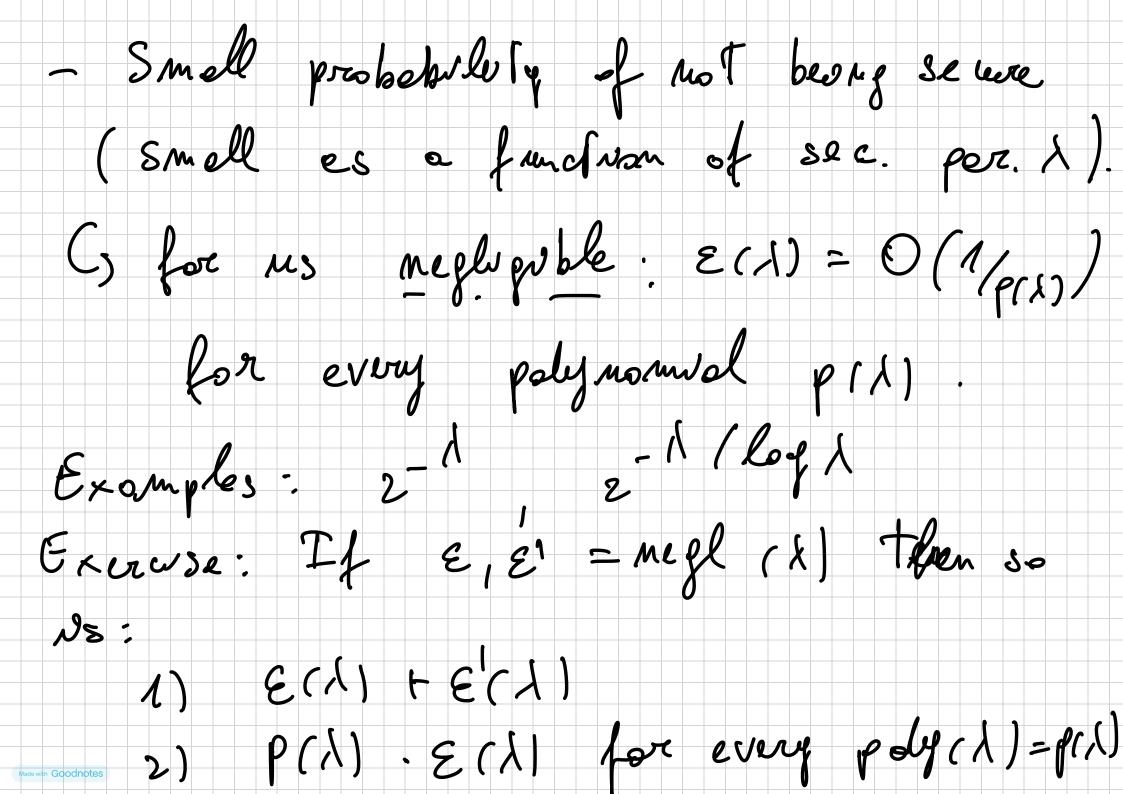


let's expend Zingy S (Palysylland) Pril/=41

3 D

COMPUTATIONAL SECURITY More sevog forom infortation theory. GOAL: Overcome ell the lum Te Troms ve hore en countered. TRADS-OFF: Weeker Security. - Adv vs resonnce - bounded PROBABICISTIC POLYNOMIAL-TIMES TURING MACHINE It can use coirs (konslommes)?

Intrustructly: For every surpret or, every rouslow tape re A (2; rc) termine les un sour polynomiel number of steps Nm 121,110 = 1 POLYNOHAL: P(X) = poly (X) P(N) = O(X^c) for some constant



- Introduce compute (Nomally lieral

problems and prove security vs

equivalent to breeting those problems.