m

X → | Embed $y = x + f(k,m)$ | $\xrightarrow{y}$ public channel $v = y + z$ $\xrightarrow{v}$ | Extract | → $\hat{m}$

K

$m = \hat{m} \rightsquigarrow$ no errors

X → | Embed $y = x + f(k)$ | $\xrightarrow{y}$ public channel $v = y + z$ $\xrightarrow{v}$ | Extract | → Yes/No

k

H_0 γ? H_1

0 A

probability of miss   overlap   probability false acceptance

H_0

0   no overlap   A larger A

$f(\rho | H_0)$ γ? $f(\rho | H_1)$

0 ρ

Pmiss   Pfa