$\Rightarrow$
Hashing!
$\Rightarrow$
Syntax:
(Gen, H)
$Gen(1^\lambda)$
1^λ
S
$H^S(x)$
S
$x \in$
$\{o,1\}^*$
$h \in$
$\{0,1\}^l$
Remarks:
$l =$
$l(\lambda)$
λ
H^S
$l' >$
l
H
Gen
$s \xleftarrow{\$}$
$\{0,1\}^\lambda$
$H :$
$\{0,1\}^{l'} \rightarrow$
$\{0,1\}^l$
$l' >$
l
(Gen, H)
$\mathcal{A}$
$\forall$
$\lambda \in$
N

$Pr[Hash{-}Col_{\mathcal{A}}(\lambda) = 1] < v(\lambda)$

H
H'
$H'^S(x) =$
$H^S(x||0^\lambda)$
x, x'
H'
$x||o^\lambda$
$x'||0^\lambda$
H
H''
$H''^S(x_1...x_n) =$
$H^S(x_1...x_{n-1})$
$0...00$
$0...01$
f
x
$H^S(x) =$
$f(x)$
$\mathcal{H} :$
$\{0,1\}^l \rightarrow$
$\{0,1\}^\lambda$
$\mathcal{H}$
$\mathcal{H}$
$H^S(x) =$
$\mathcal{H}(s||x)$
$\mathcal{A}$
$q =$
$poly(\lambda)$
$x_1, ..., x_q$
$\mathcal{H}$
$\mathcal{H}$
$Pr[\mathcal{H}(s||x_i) = \mathcal{H}(s||x_j)] = 2^{-\lambda}$

$Pr[\exists i, j : \mathcal{H}(s||x_i) = \mathcal{H}(s||x_j)] \leq q^2 2^{-\lambda} = negl(\lambda)(unionbound)$

com-
pu-
ta-
tion-
ally