CRHF

$H \leftarrow \mathcal{H}$

$Pr[A(H) \to x,y : x \neq y \wedge H(x)=H(y)] \leq \varepsilon$

if it's compressing make it more compressing

PKE $(pk, sk) \leftarrow Gen$

$Enc_{pk}(m)$

$Dec_{sk}(c)$

[IND CPA]

is OWF

$f(pk \| m) = (pk, Enc_{pk}(m))$.

Alek: [illegible]

EUFCMA:

negligible Pr of accepting forgery

IND CPA

negligible advantage at distinguishing btwn a encryption of 0, 1.

OWP

bijective OWF

OWF

$x \leftarrow \Sigma^n$

$y = f(x)$

$f(A(1^n, y)) = y$ w/ negligible Pr

$f_k(x) = G_{x_1}(G_{x_2}(\dots G_{x_n}(k)\dots))$

UOWHF

Fix x, $H \leftarrow \mathcal{H}$

Choose $y \neq x$ and get $H(x)=H(y)$ negligible Pr

$f(x) = \pi(x) \| h(x)$

hard core bit

$G(x) \neq$ OWF

$f \leftarrow \mathcal{Z}$ vs $f \leftarrow$ All indistinguishing.

Lamport 1 time Signatures

$\begin{bmatrix} f(x_{00}) & f(x_{01}) & f(x_{02}) \\ f(x_{10}) & f(x_{11}) & f(x_{12}) \cdots \end{bmatrix}$

PRG $\longleftrightarrow$ PRF

$G(U_n) \approx U_{2n}$

$f(k,0) \| f(k,1) \| \dots$ until enough digits

Longer messages: $\to$ hashing

Many messages: $\to$ Tree thing, make and sign new vk's.

Signatures

(vk, sk)

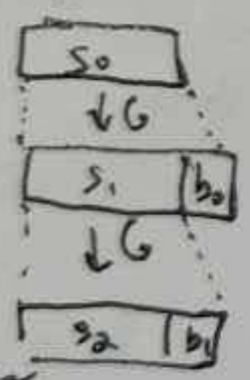
$Sign(sk, m)$

$Ver(vk, \sigma)$

[EUFCMA]

y_{OWF}

Length Extension:



Thm: For Every OWF $f(x)$, $\langle r, x \rangle$ for random r is a hard core pred.

i.e., given $f(x)$, can't guess $h(x)$ w/ non negl advantage.

Next bit test: given any prefix can't guess the next bit

let $f_k \leftarrow \mathcal{Z}$

$Sign(sk=k, m) = f_k(m)$

MAC $\to$ OWF

$f(k) = Mac(k,0) \| Mac(k,1) \| Mac(k,2) \| \dots \| Mac(k,\ell)$

$Sk \leftarrow Gen$

$Mac(sk, m)$

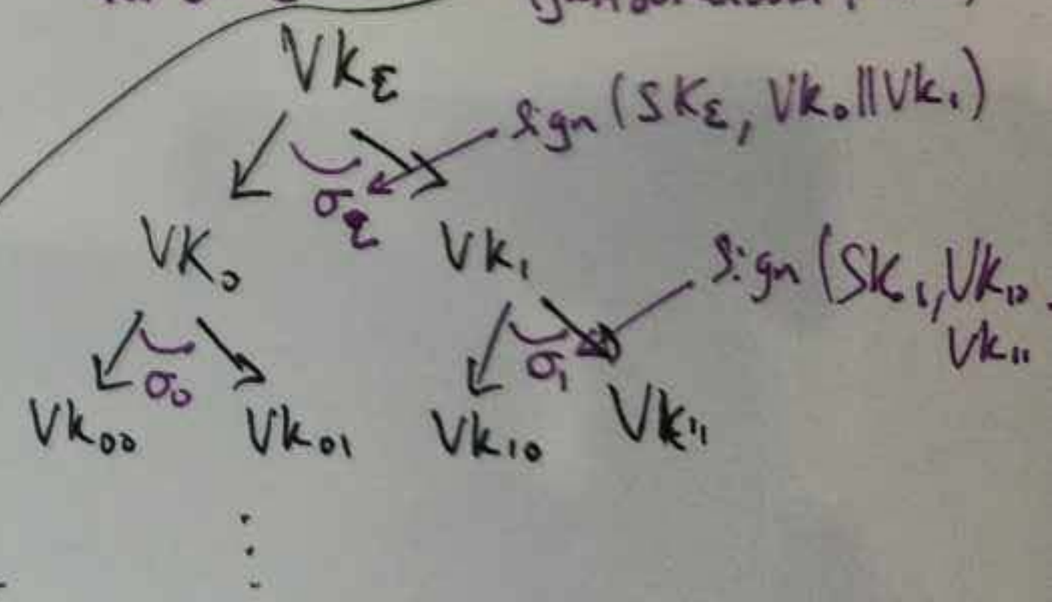
$Ver(sk, \sigma)$

[EUFCMA]

Decrease mem. Req. w/ PRF

$r_x = PRF(k,x)$ r_x random bits for Gen@ node x

make it stateless w/ a PRF (just for random paths)



Can even make it deterministic

$Sign(Sk_{\dots}, m)$