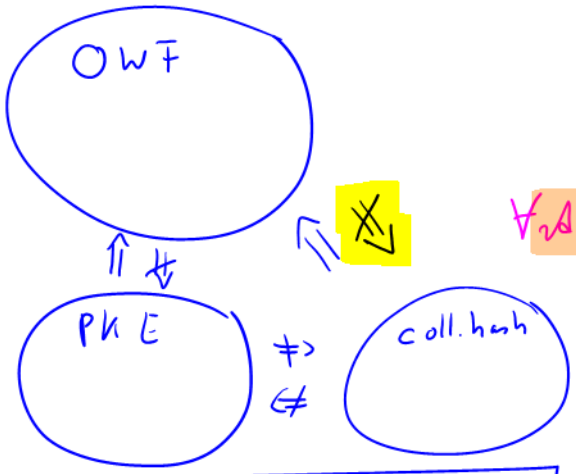
Lecture 2

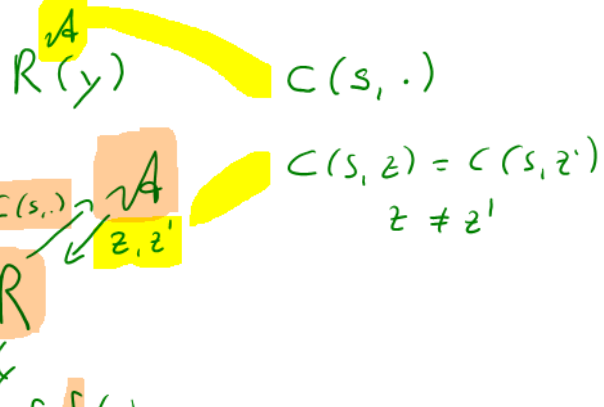
- OWF ⇒ coll. hash-function (theory)
- passwords: How to use passwords for authentication



candidate coll. hash-function construction → for this Claim: if f is OWF then h is CRH

Black-box reduction:

∃ PPT R
∃ construction h
∀ A, f Whenever A breaks CR of h
⇒ R^{A} breaks OWF of f



- Very strong A that breaks all h
- a random function F.

$f(1^\lambda, \cdot) : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}$

EVAL $(1^\lambda, x)$
assert $|x| = 2\lambda$
if $T[x] = \perp$
  $T[x] \leftarrow \$ \{0,1\}^{2\lambda}$
ret. $T[x]$

lazy sampling, Sample function step by step

$\forall$ poly-query R of poly size

$$\Pr\left[1 = \boxed{\text{OW game}_\lambda \xrightarrow{CH} R \xrightarrow{SAM} \text{Ideal Algos}_\lambda \xrightarrow{EVAL} \text{Ideal Algos}_\lambda}\right]$$

is negligible.

Theorem

OW game$_\lambda$
$x \leftarrow \$ \{0,1\}^{2\lambda}$
$y \leftarrow EVAL(x)$
$x^* \leftarrow CH(y, 1^\lambda)$
$y^* \leftarrow EVAL(x^*)$
if $y = y^*$ ret. 1
return 0.

Ideal Algos

SAM $(C(s,\cdot))$
assert $|s| = \lambda \wedge |\ | = 2\lambda$
$x \leftarrow \$ \{0,1\}^{2\lambda}$
$y \leftarrow C^T(s,x)$
update T
$y' \leftarrow y \oplus 1^\lambda$
While $y' \neq y$:
  $x' \leftarrow \$ \{0,1\}^{2\lambda}$
  $T' \leftarrow \$$ continuation of T
  $y' \leftarrow C^{T'}(s,x')$
  Update T on path of $C^{T'}(s,x')$ according to T'
ret. (x', x)

if no y-hit, y will not appear in T

(if T is already complete)

Ideal Algos

SAM $(C(s,\cdot))$
assert $|s| = \lambda \wedge |\ | = 2\lambda$
$z \leftarrow \$ \{0,1\}^{2\lambda}$
$y \leftarrow C^T(s,z)$
$z' \leftarrow \$ \{\omega : C^T(s,z) = y\}$
ret. (z, z')

EVAL $(1^\lambda, x)$
assert $|x| = \lambda$
if T_λ undefined:
  $T_\lambda \leftarrow \$ \{f : \{0,1\}^{2\lambda} \to \{0,1\}^{\lambda}\}$
ret. $T[x]$

sample entire function once & for all

evaluate the circuit step by step:
- evaluate normal gates until reaching a T-gate with value y
- run the same code as EVAL(x)
- continue until reaching the next T-gate.
...

Claim 0:

$$\Pr\left[1 \leftarrow \boxed{\text{OV game}_\lambda \xrightarrow{CH} R \xrightarrow{SAM} \xrightarrow{EVAL} \text{Ideal Alg}_\lambda \xleftarrow{EVAL}}\right] \approx \Pr\left[1 \leftarrow \boxed{\text{OV game}_\lambda \xrightarrow{CH} R \xrightarrow{SAM} \xrightarrow{EVAL} \text{Ideal Alg}_\lambda \xleftarrow{EVAL}}\right] = (*)$$

Claim 1:

$$\left|\Pr\left[1 \leftarrow \boxed{\text{OV game}_\lambda \xrightarrow{CH} R \xrightarrow{SAM} \xrightarrow{EVAL} \text{Ideal Alg}_\lambda \xleftarrow{EVAL}}\right] - \Pr\left[1 \leftarrow \boxed{\text{Random OV game}_\lambda \xrightarrow{CH} R \xrightarrow{SAM} \xrightarrow{EVAL} \text{Ideal Alg}_\lambda \xleftarrow{EVAL}}\right]\right| \leq \text{negl}(\lambda)$$

OV game$_\lambda$
$x \leftarrow \$ \{0,1\}^{2\lambda}$
$y \leftarrow EVAL(x)$
$x^* \leftarrow CH(y, 1^\lambda)$
$y^* \leftarrow EVAL(x^*)$
if $y = y^*$ ret. 1
return 0.

Random OV game$_\lambda$
$y \leftarrow \$ \{0,1\}^{2\lambda}$
$x^* \leftarrow CH(y, 1^\lambda)$
$y^* \leftarrow EVAL(x^*)$
if $y = y^*$ ret. 1
return 0.

Proof sketch:
In OV game, each y has prob. $\frac{|T^{-1}(y)|}{2^{2\lambda}}$
In Random OV game$_\lambda$, each y has prob. $2^{-2\lambda} = \frac{2^\lambda}{2^{3\lambda}}$
Using Chernoff bound (later in course), we can show that
$\Pr_{y,T}\left[|T^{-1}(y)| > 10 \cdot 2^\lambda\right] \leq \text{negl}(\lambda)$
Overall loss $\underbrace{\frac{1 \cdot 2^\lambda}{2^{2\lambda}} + \text{negl}(\lambda)}_{\text{negl}(\lambda)}$

Claim 2:

If R does not make a SAM-hit, then (*) is negligible

SAM returns (z, z') on query $C(s,\cdot)$
$\rightarrow y \in \text{path}^{T,r}(z)$ or $y \in \text{path}^{T,r}(z')$

Proof sketch:
Let's use Random OV game$_\lambda$ and Ideal Algos (lazy sampling), then T does not have a pre-image for y after each Sam-query. Moreover, the probability of a y-hit on EVAL is $2^{-\lambda}$ (due to lazy sampling). As R only makes poly many queries, R only gets a pre-image of y with prob. $(\text{poly} + 1) \cdot 2^{-\lambda}$.

Main Lemma

The probability of a Sam-hit is negligible.

Proof: Union bound over all Sam queries and z & z'
(poly; factor 2)

Claim A: Sam returns (z, z') such that each of them individually is uniform over $\{0,1\}^{2\lambda}$ (even though they are not independent!)

Claim B: For a uniform z, $\Pr_{z,T}[C^T(s,z) \text{ making a } y\text{-hit}] \leq \text{negl}$.

Proof: Use lazy sampling perspective.
T does not contain y before the call to Sam. Now, $C^T(s,z)$ is evaluated on uniformly random z leading to two types of queries:
(i) queries already in T $\rightarrow$ answer by y ✓
(ii) queries not in T $\rightarrow$ random answer
$\Pr[\text{answer} = y] = 2^{-\lambda}$ ✓

$2^{-\lambda} \cdot t$ (#queries)

Claim 2 (restated)
Sam returns (z, z') such that each of them individually is uniform over $\{0,1\}^{2\lambda}$ (even though they are not independent!)

Proof:
(use T-pre-sampling perspective)
- first z is uniformly random (clearly)
- 2nd z':

$$\Pr[z'] = \Pr_z\left[\underbrace{C^T(s,z) = C^T(s,z')}_{y}\right] \cdot \frac{1}{|\{\omega : C^T(s,\omega) = y\}|}$$

$$= \frac{|\{z : C^T(s,z) = y\}|}{2^{2\lambda}} \cdot \frac{1}{|\{\omega : C^T(s,\omega) = y\}|} = 2^{-2\lambda}$$

which is correct for the uniform distribution over $\{0,1\}^{2\lambda}$.

Recap:

- equivalence lazy sampling & pre-sampling T
- random y instead of random x and $y := T[x]$
  → ok because no y is very likely by itself anyway, thus difference is small.
- EVAL-hits on y have prob. $2^{-\lambda}$ (use lazy sampling perspective)
- SAM-hits on y are unlikely
  - z, z' are uniform
  → no y-hit via lazy sampling perspective
  - union bound over all queries and z and z'

Wish: (1) OWF $\not\Rightarrow$ coll.-res. hash $\Leftrightarrow$ $\exists$ OWF $\wedge$ $\neg \exists$ coll. res hash

(2) $\forall$ OWF f $\forall$ candidate constructions h^f

$\exists$ inefficient $\mathcal{A}$ s.t. "no reduction works for $\mathcal{A}$"

against h^f

Good statement

inefficient & provided as an oracle

(= heuristic)

- most proofs also work when f is a OWF implemented a a random oracle

$$g(x) := f(x) \| 0$$

- excludes class of techniques