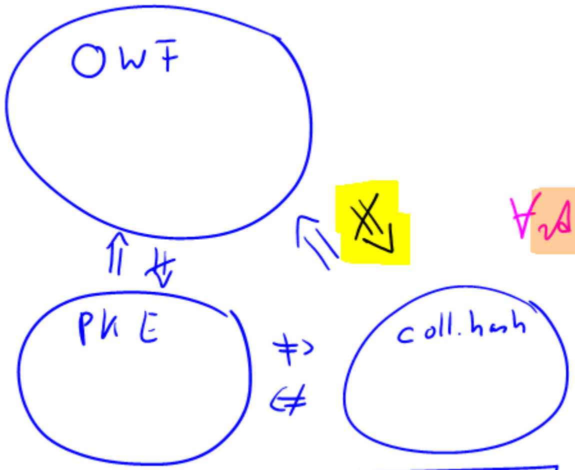
Lecture 2

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

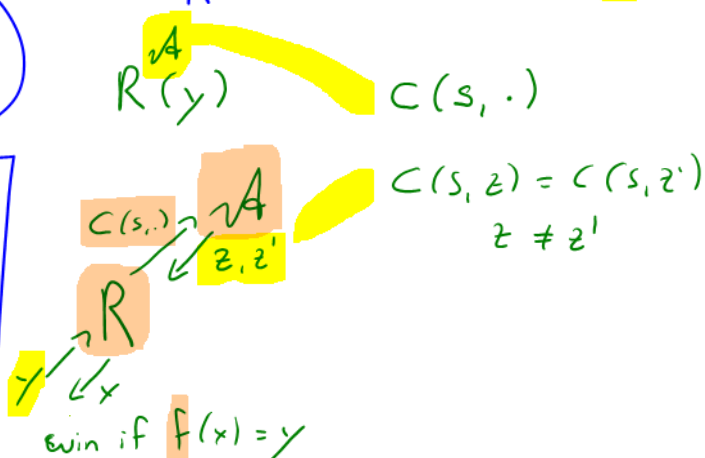


Candidate coll. hash-function construction

Black-box reduction: for this

Claim
if f is OWF
then h is CRH

$\exists$ PPT R
$\exists$ construction h
$\forall \lambda, \mathcal{A}, f$ whenever $\mathcal{A}$ breaks CR of h
$\Rightarrow R^{\mathcal{A}}$ breaks OWF of f



- very strong $\mathcal{A}$ that breaks all h
- a random function F.

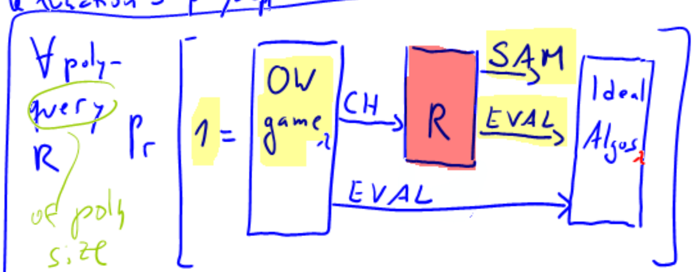
$f(1^\lambda, \cdot): \{0,1\}^{2\lambda} \longrightarrow \{0,1\}^\lambda$

EVAL$(1^\lambda, x)$

lazy sampling, sample function step by step

assert $|x| = 2\lambda$
if $T[x] = \bot$
  $T[x] \leftarrow_\$ \{0,1\}^\lambda$
ret. $T[x]$

Theorem



is negligible.

OW game$_\lambda$
$x \leftarrow_\$ \{0,1\}^{2\lambda}$
$y \leftarrow \text{EVAL}(x)$
$x^* \leftarrow \text{CH}(y, 1^\lambda)$
$y^* \leftarrow \text{EVAL}(x^*)$
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
  $y' \leftarrow C^{T'}(s, x')$
if no y-hit, y will not appear in T | Update T on path of $C^{T'}(s, x')$ according to T'
ret. (x', x)

(if T is already complete)

Ideal Algos

SAM$(C(s,\cdot))$
assert $|s| = \lambda \wedge |\;| = 2\lambda$
$z \leftarrow_\$ \{0,1\}^{2\lambda}$
$y \leftarrow C^T(s, z)$
$z' \leftarrow_\$ \{w : C^T(s, z) = y\}$
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. $T[x]$

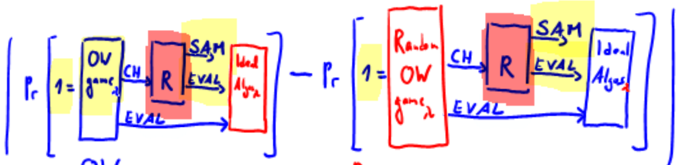
sample entire function once & for all

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

Claim 0:

$= (*)$

Claim 1:



$\leq negl(\lambda)$

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.

Random OW game$_\lambda$

$y \leftarrow \$ \{0,1\}^\lambda$

$x^* \leftarrow CH(y, 1^\lambda)$

$y^* \leftarrow EVAL(x^*)$

if $y = y^*$ ret. 1

return 0.

Proof sketch:

In OW game, each y has prob. $\frac{|T^{-1}(y)|}{2^{2\lambda}}$

In Random OW game$_\lambda$, each y has prob. $2^{-\lambda} = \frac{2^\lambda}{2^{2\lambda}}$

Using Chernoff bound (later in course), we can show that

$$\Pr_{y,T}\left[|T^{-1}(y)| > 10 \cdot 2^\lambda\right] \leq negl.(\lambda)$$

Overall loss $\underbrace{\frac{9 \cdot 2^\lambda}{2^{2\lambda}} + negl(\lambda)}_{negl(\lambda)}$

Claim 2:

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

SAM returns (z, z') on query $C(s,.)$

$y \in path^{T,C}(z)$ or $y \in path^{T,C}(z')$

Proof sketch:

Let's use Random OW 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. $(poly + 1) \cdot 2^{-\lambda}$.

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, $\Pr_{z,T}[C^T(s,z)$ making a y-hit$] \leq negl.$

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 → answer ≠ y ✓

(ii) queries not in T → random answer

$\Pr[answer = y] = 2^{-\lambda}$ ✓

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':

$$\Pr[z']$$

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

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

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 $\Leftarrow$ $\exists$ OWF $\wedge$ $\neg\exists$ coll. res hash

(2) $\forall$ OWF f $\forall$ candidate constructions h^f
$\exists$ inefficient $\mathcal{A}$ against h^f s.t. "no reduction works for $\mathcal{A}$"

Good statement

inefficient & provided as an oracle
(→ heuristic)
– most proofs also work when f is a OWF implemented a random oracle

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

– excludes class of techniques