[YAO] X_n PASSES NEXT BIT TEST

$\Leftrightarrow$

X_n PSEUDORANDOM

PROOF:

$\Rightarrow$ SINCE NEXT-BIT TEST IS A STATISTICAL TEST, THIS IS TRIVIAL.

X_n PSEUDORANDOM $\Rightarrow$ X_n PASSES ALL STATISTICAL TESTS

$\Rightarrow$ X_n PASSES NBT

PROOF BY CONTRADICTION: WANT TO SHOW,

IF X_n NOT PSEUDORANDOM,

THEN X_n FAILS NEXT-BIT TEST.

THAT IS,

IF $\exists D$ WHICH DISTINGUISHES X_n FROM U_n,

THEN $\exists A$ WHICH PREDICTS NEXT BIT OF X_n

ASSUME D DISTINGUISHES X_n FROM U_n WITH PROBABILITY $\varepsilon(n)$. BY PREVIOUS HYBRID ARGUMENT APPLIED TO X_n, U_n, $\exists i$ SUCH THAT

$$P_{i+1} - P_i > \frac{\varepsilon}{l}$$

WHERE l IS TOTAL # OF SAMPLES.

NOTE: $P_i = P_R\left[D\left(x_1 x_2 \ldots x_i u_{i+1} \ldots u_l\right) = 1\right]$

IDEA: $x_1, \ldots, x_i \leftarrow x_n$, $\$ b \in \{0,1\}$,
$u_{i+2}, \ldots, u_2 \leftarrow u_n$

IF $D(\ldots) = 1$, A PREDICTS $x_{i+1} = b$

IF $D(\ldots) = 0$, A PREDICTS $x_{i+1} = \bar{b}$

INTUITION: D OUTPUTS 1 MORE OFTEN WHEN $b = x_{i+1}$

CALCULATION:

$$\Pr[A(x_1,\dots,x_i) = x_{i+1}]$$

$$= \Pr[x_{i+1}=b] \cdot \Pr[D(x_1,\dots,x_i,x_{i+1},u_{i+2},\dots,u_2)=1]$$

$$+ \Pr[x_{i+1}=\bar{b}] \cdot \underbrace{\Pr[D(x_1,\dots,x_i,\bar{x_{i+1}},u_{i+2},\dots,u_2)=0]}_{\text{CALL THIS } q}$$

$$= \frac{1}{2}\cdot P_{i+1} + \frac{1}{2}\cdot q$$

WHAT IS q? LET'S EXPAND P_i

$$P_i = \Pr[D(x_1,\dots,x_i,u_{i+1},\dots,u_2)=1]$$

$$= \Pr[D(x_1,\dots,x_i,x_{i+1},u_{i+2},\dots,u_2)=1]\cdot \Pr[u_{i+1}=x_{i+1}]$$

$$+ \Pr[D(x_1,\dots,x_i,\bar{x_{i+1}},u_{i+2},\dots,u_2)=1]\cdot \Pr[u_{i+1}=\bar{x_{i+1}}]$$

$$= P_{i+1}\cdot\frac{1}{2} + (1-q)\cdot\frac{1}{2}$$

THUS,

$$q = 1 + P_{i+1} - 2 \cdot P_i$$

FINALLY, SUBSTITUTING THIS q VALUE YIELDS:

$$\Pr\left[A(x_1, \ldots, x_i) = x_{i+1}\right]$$

$$= \frac{1}{2} \cdot P_{i+1} + \frac{1}{2} \cdot q$$

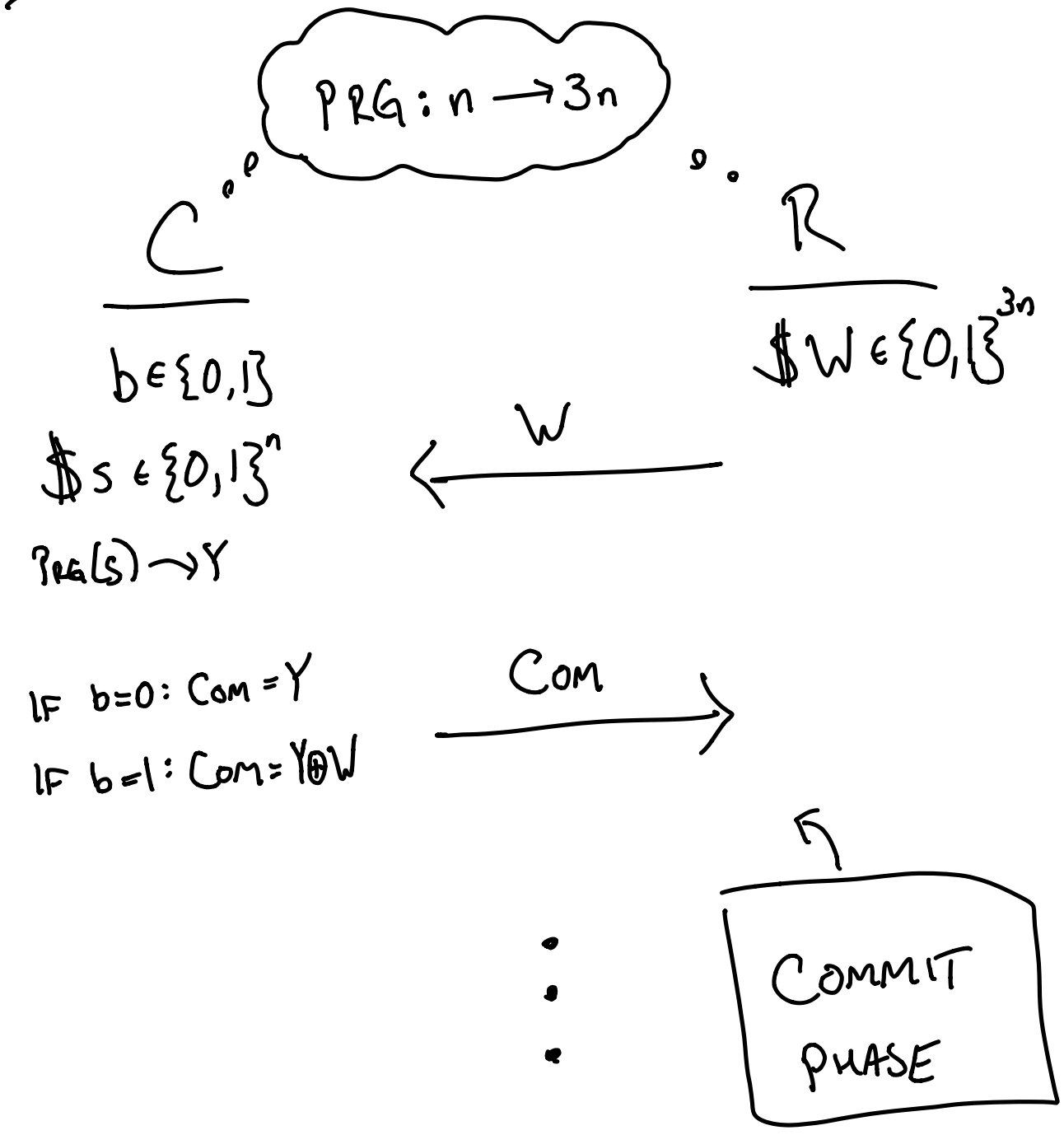
$$= \frac{1}{2} \cdot P_{i+1} + \frac{1}{2} \cdot \left(1 + P_{i+1} - 2 \cdot P_i\right)$$

$$= \frac{1}{2} + \left[P_{i+1} - P_i\right]$$

$$> \frac{1}{2} + \frac{\varepsilon}{l}.$$

THUS, A PREDICTS THE $i+1^{ST}$ BIT OF X_n WITH SIGNIFICANT ADVANTAGE, WHICH COMPLETES THE PROOF. ■

[NAOR]: PRG $\Rightarrow$ COMMITMENT SCHEME



WHY IS THIS A GOOD COMMITMENT?

(1) HIDING: IF D DISTINGUISHES Y FROM $Y \oplus W$ FOR PSEUDORANDOM Y, D CANNOT DO THE SAME FOR TRULY RANDOM Y' BECAUSE Y' & $Y' \oplus W$ ARE BOTH RANDOM. SO D DISTINGUISHES Y FROM Y', MEANING PRG IS BROKEN.

② BINDING:

$PRG(s_1) =$ y_1

$\oplus$

$PRG(s_2) =$ y_2

w'

SUPPOSE R GETS UNLUCKY & CHOOSES

w' AS w IN COMMITMENT.

THEN C CAN CHEAT!

DECOM $= s_1$:

$COM = PRG(s_1) = y' \Rightarrow b = 0$

DECOM $= s_2$:

$COM = PRG(s_2) \oplus w' \Rightarrow b = 1$

$\underbrace{\qquad\qquad}_{PRG(S_1)}$

WITH SAME COMMITMENT,

$$COM = PRG(S_1).$$

$\therefore$ FOR EVERY PAIR OF SEEDS

$S_1, S_2, \exists W^*$ SUCH THAT

C CAN CHEAT ON W^*.

How MANY SUCH PAIRS?

$|S_1| + |S_2| = 2n$, SO

AT MOST 2^{2n}

BUT: 2^{3n} TOTAL W TO CHOOSE FROM.

THUS: IF $W \in \{0,1\}^{3n}$ IS RANDOM,

$$\Pr_R[C \text{ CAN CHEAT ON } W] < \frac{2^{2n}}{2^{3n}} = \frac{1}{2^n}$$

SO COMMITMENT IS BINDING WITH PROBABILITY $1 - \frac{1}{2^n}$. ∎

HIDING:	POLY-TIME ADV CAN'T TELL
BINDING:	∞-POWERFUL ADV CAN'T CHANGE MIND (EXCEPT W/ PROBABILITY $\frac{1}{2^n}$)

WHAT IF WE WANTED THIS:

HIDING:	∞-POWERFUL ADV
BINDING:	POLY-TIME ADV

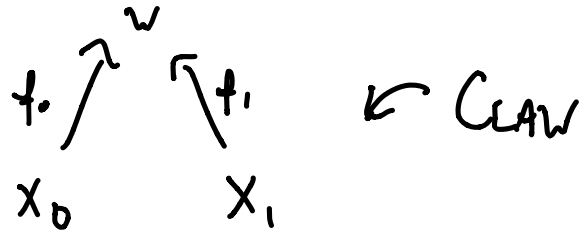
NECESSARY ASSUMPTION: CLAW-FREE PAIR

LET f_0, f_1 BE 1-WAY PERMUTATIONS

S.T. NO POLY-TIME ADV CAN FIND

X_0, X_1 S.T. $f_0(X_0) = f_1(X_1)$

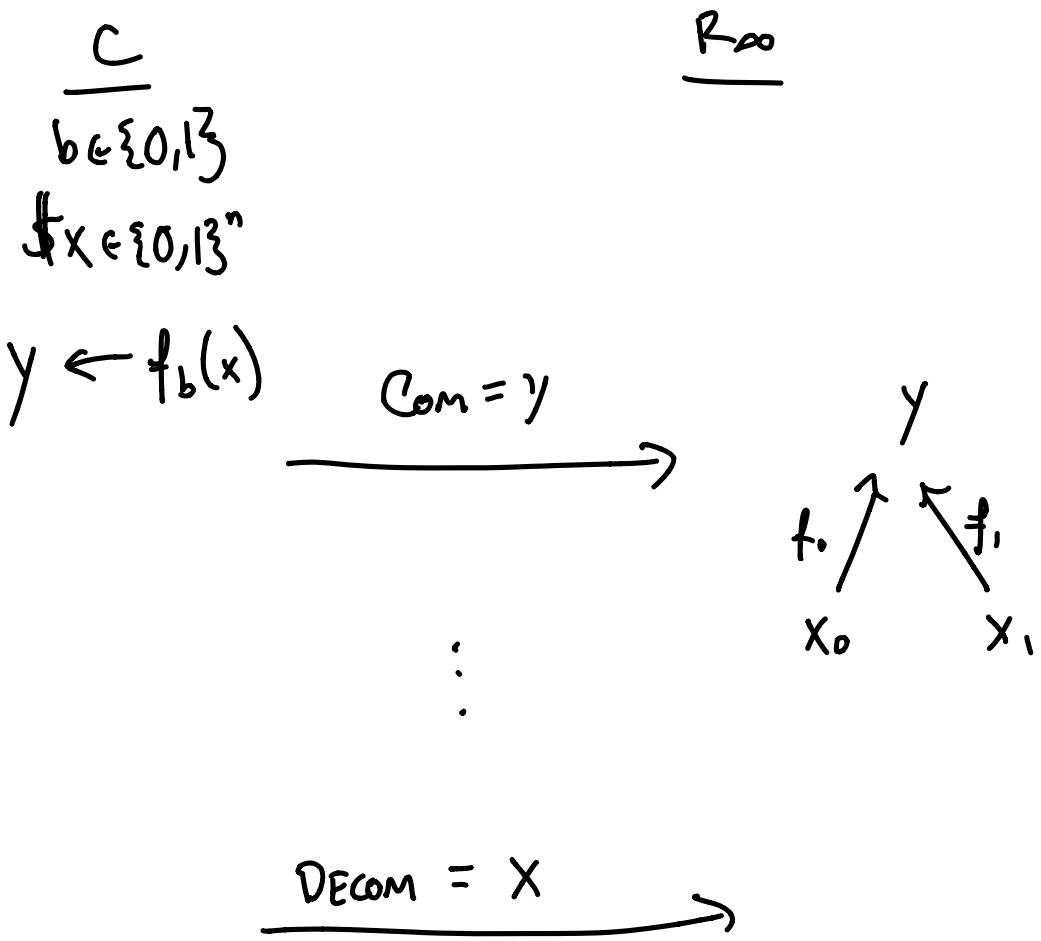
PICTURE:



← CLAW

THEN THE FOLLOWING SCHEME IS

PERFECTLY HIDING, COMPUTATIONALLY BINDING:



HIDING: $y = f_0(x_0)$ AND $f_1(x_1)$, SO COULD BE $b=0$ OR 1

BINDING: TO CHANGE MIND, C MUST FIND A CLAW.

Intro to Random Functions

Goldreich, Goldwasser, Micali [GGM]

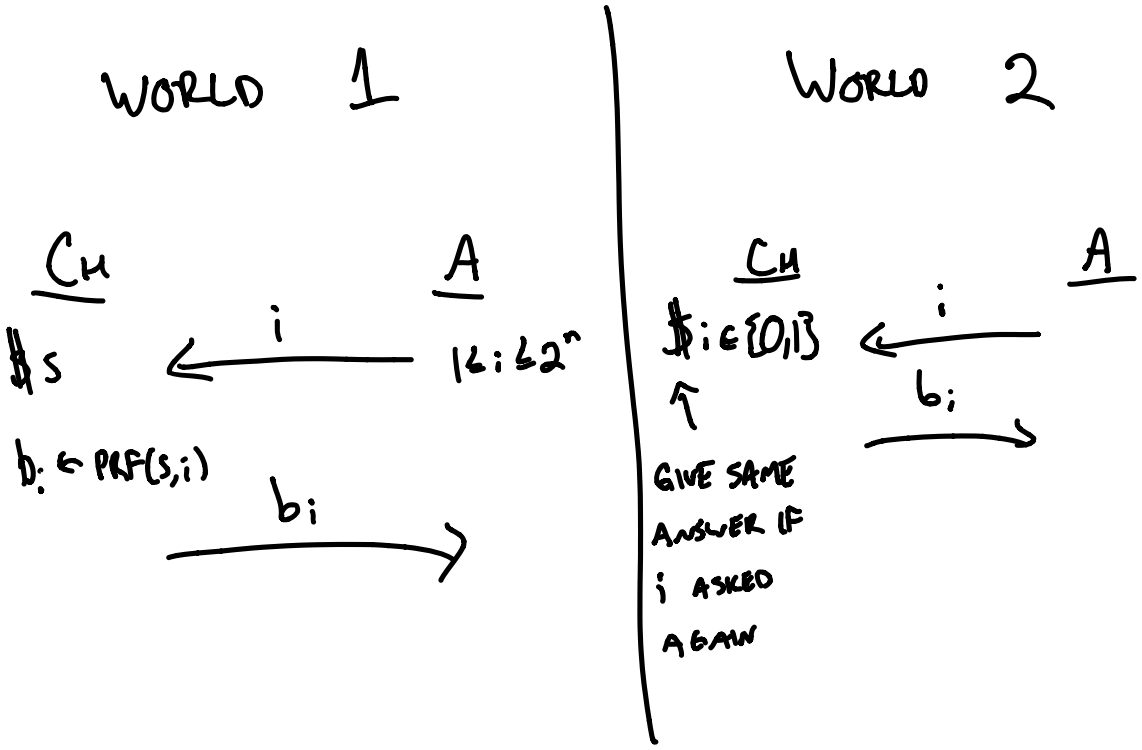
Pseudo-Random Functions (PRF)

Idea: $PRF(SEED, i) =$

Any poly-size subset of bits appears truly random.

Intuition: Models random function f w/ n bit output

GAME-BASED SECURITY DEFINITION:



NO PPT A CAN DISTINGUISH WORLDS.

IMPORTANT: PRF IS MEMORYLESS. CAN'T HAVE MEMORY GROW W/ # OF QUERIES.

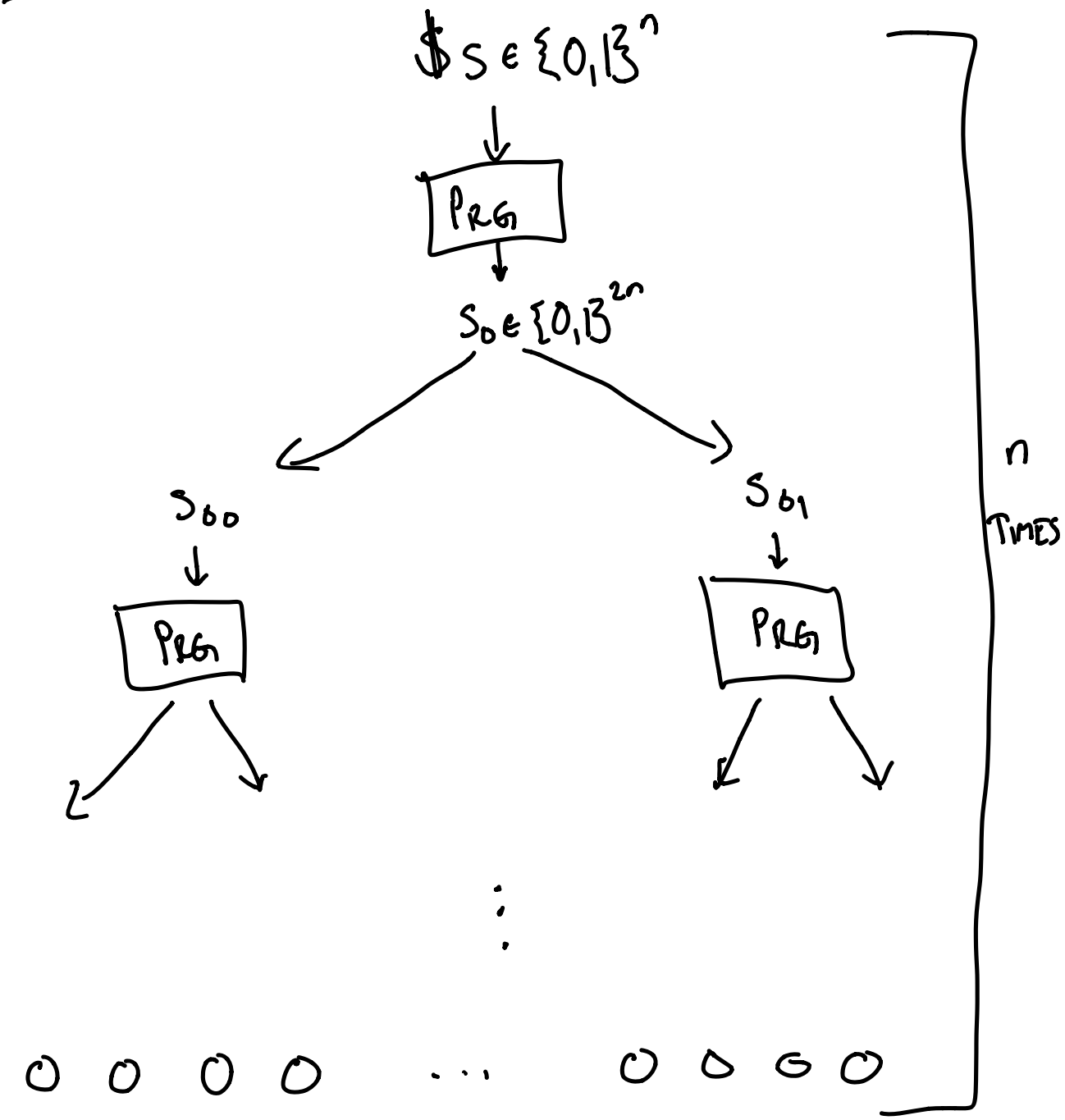
Application of PRF: Identity Authentication

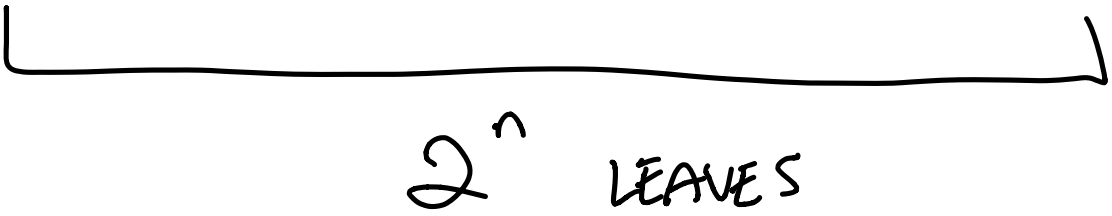
Give s to members of "secret society"

To authenticate, ask for $PRF(s, i)$ for never-before-used $i \in [1, 2^n]$.

Even if imposter overheard $PRF(s, j)$, $j \neq i$, doesn't help.

[GGM] GIVEN ANY PRG: $n \to 2n$, CAN CONSTRUCT PRF.

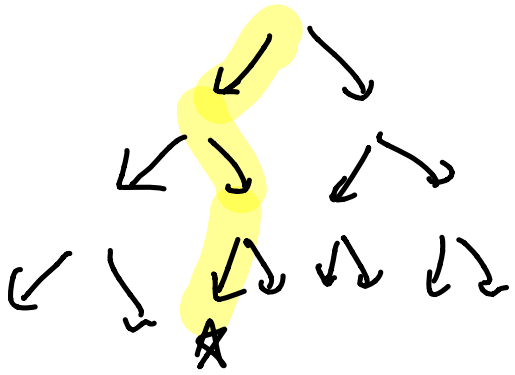




$PRF(S, i)$

↑ ROOT ↑ PATH

$i = 010 \Rightarrow$

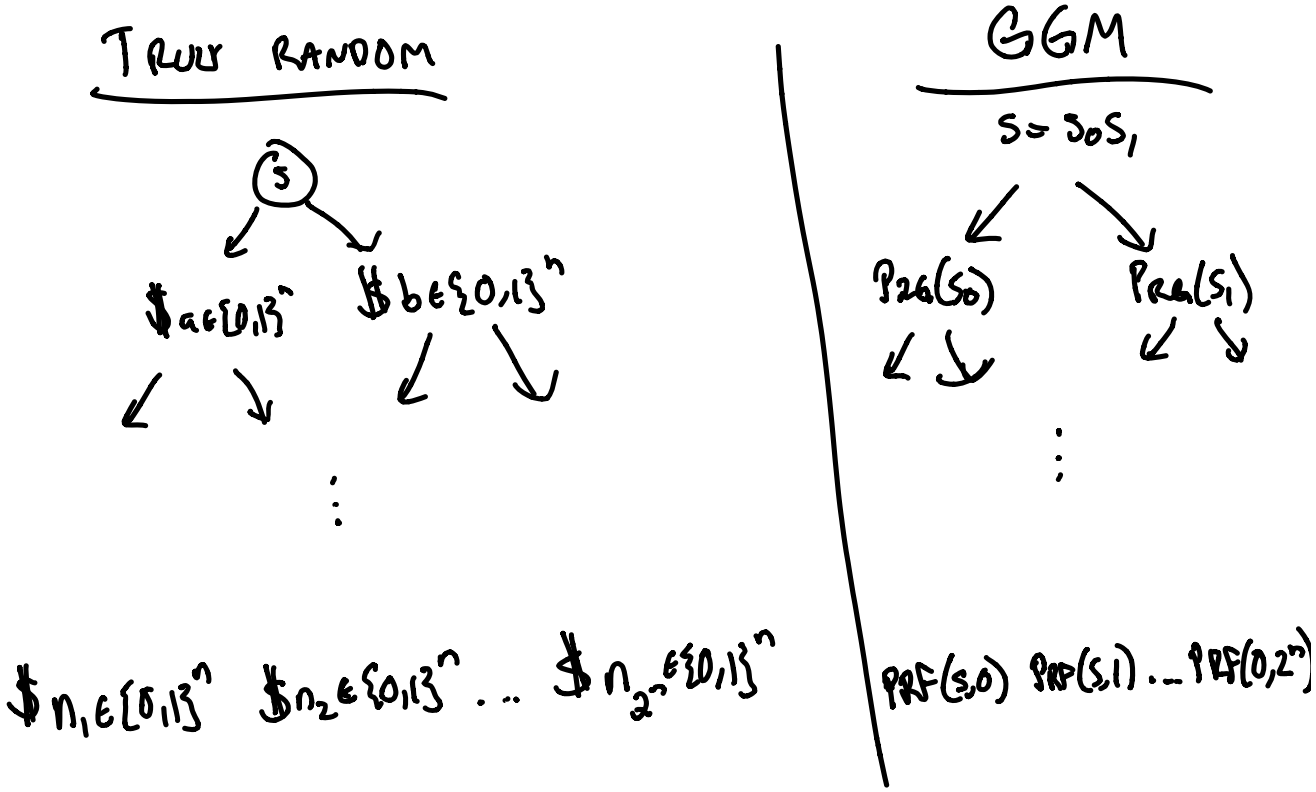


PRF OUTPUTS FIRST BIT OF PRG OUTPUT AT LEAF LEVEL.

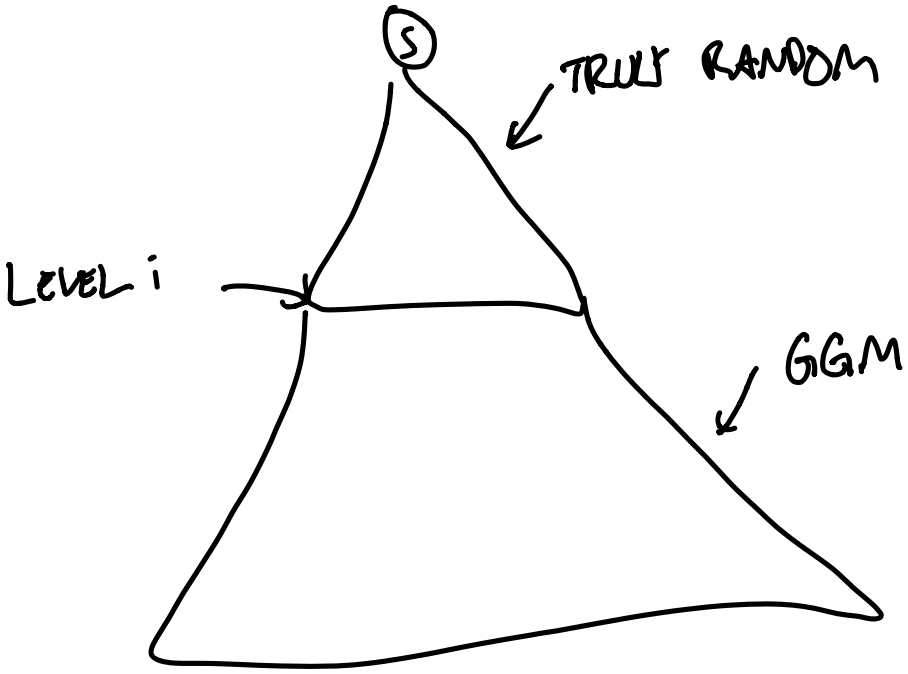
PROOF IDEA:

IF ADV DISTINGUISHES PRF OUTPUTS FROM RANDOM, WE CAN USE ADV TO BREAK THE UNDERLYING PRG.

TO PROVE: WE USE A HYBRID ARGUMENT



HYBRID P_i



ON LEVEL i, WE PLACE INPUTS WHICH WE WANT TO DISTINGUISH AS EITHER RANDOM OR PSEUDORANDOM, AT THE LOCATIONS WHERE THE PPT ADVERSARY'S QUERIES CROSS THROUGH LEVEL i.

IF ADV DISTINGUISHES TRULY RANDOM TREE FROM GGM TREE W/ ADVANTAGE ε, THEN THERE EXISTS HYBRIDS P_i, P_{i+1} SUCH THAT

$$P_i - P_{i+1} > \frac{\varepsilon}{n}$$

WHERE $P_i = P_R[\text{ADV OUTPUTS } 1 \text{ IN } i^{TH} \text{ HYBRID}]$

ONLY DIFFERENCE BETWEEN P_i & P_{i+1} IS THAT $(i+1)^{ST}$ LEVEL IS EITHER RANDOM (P_i) OR PSEUDORANDOM (P_{i+1}). THUS, BY PLACING SAMPLES AT $(i+1)^{ST}$ LEVEL,

WE GET A DISTINGUISHER D WHICH DISTINGUISHES RANDOM SAMPLES FROM PSEUDORANDOM SAMPLES W/ ADVANTAGE $\frac{\varepsilon}{n}$ (ASSUMING WE GUESS i CORRECTLY).

THUS: PRG $\Rightarrow$ PRF

PAUL STOP HERE FOR DISCUSSION

NEW TOPIC:

DIGITAL SIGNATURES

WANT: ELECTRONIC VERSION OF SIGNATURES S.T. I CAN SIGN THINGS BUT FORGERS CANNOT FORGE IT.

SINCE COMPUTERS CAN COPY BITS, SIGNATURE MUST DEPEND ON DOCUMENT BEING SIGNED. OTHERWISE FORGER CAN TAKE MY SIGNATURE ON D_1 & COPY IT TO ANY OTHER DOCUMENT D_2.

First Attempt at Public Key Signatures

[Diffie Hellman] (1976):

① $\text{KeyGen}(1^k, R) \rightarrow (pk, sk)$

- 1^k: security parameter
- pk: public key — publish publicly
- sk: secret key — keep private

② $\text{Sign}(D, pk, sk, R) \rightarrow \sigma(D)$

- D: document
- $\sigma(D)$: signature of D

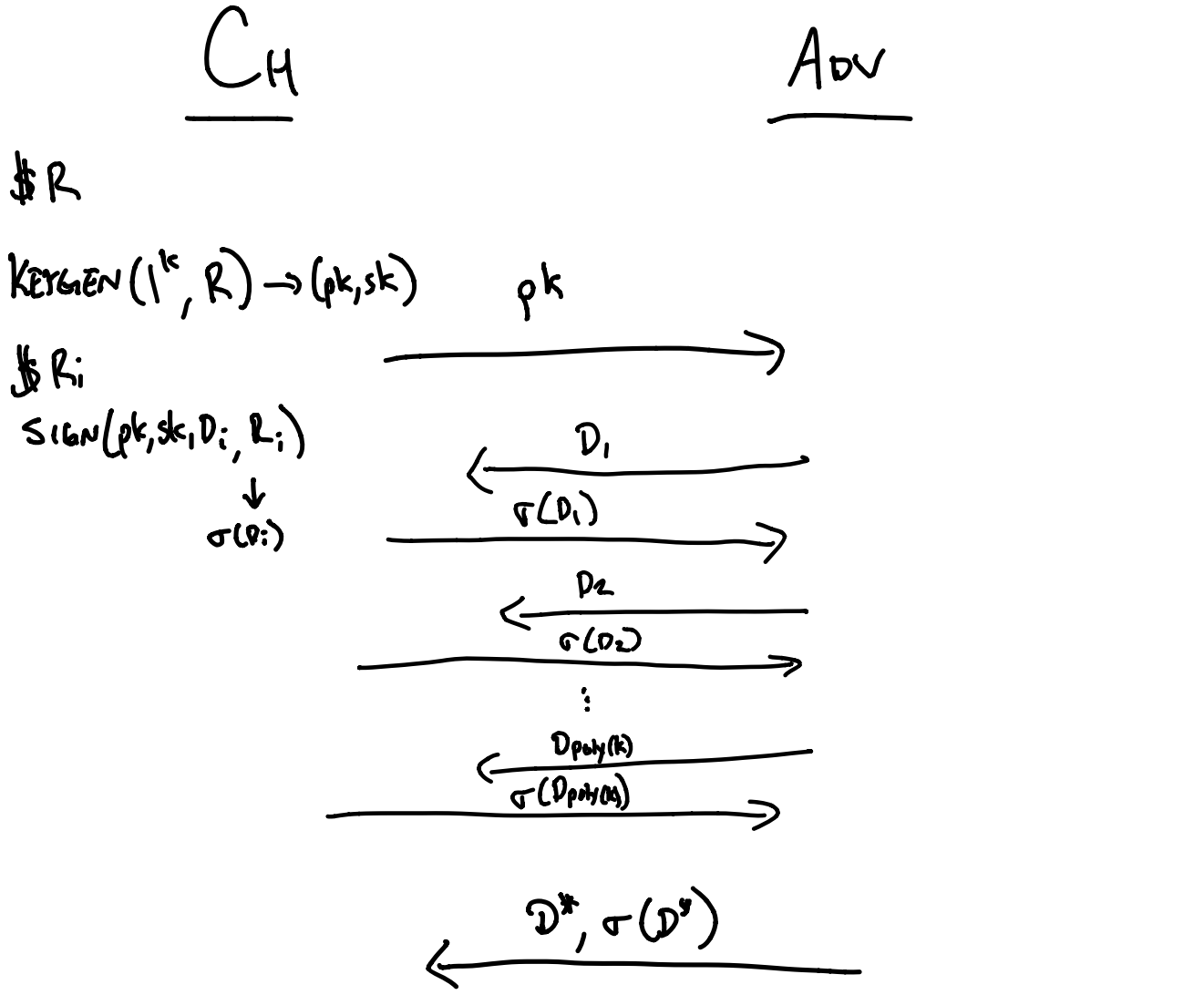
③ $\text{Verify}(pk, D, \sigma(D)) \rightarrow$ Accept or Reject

SIGNATURE DEFINITION:

A SIGNATURE SCHEME CONSISTS OF ①, ②, ③, (PPT ALGORITHMS) SUCH THAT:

(CORRECTNESS): IF ①, ②, ③ ARE RUN PROPERLY, THEN ③ WILL ACCEPT ALL SIGNED DOCUMENTS.

(EXISTENTIAL)
(2) UNFORGEABILITY): NO PPT ADVERSARY CAN WIN THE FOLLOWING GAME, EXCEPT WITH NEGLIGIBLE PROBABILITY



ADV WINS IF: $D^* \neq D_i \ \forall i \in [1, \text{poly}(k)]$ AND $\text{VERIFY}(pk, D^*, \sigma(D^*)) = \text{ACCEPT}$

INTUITION: EVEN IF ADVERSARY SEES poly(k) VALID SIGNATURES ON ARBITRARY DOCUMENTS, ADV CANNOT FORGE SIGNATURE ON NEW DOC.

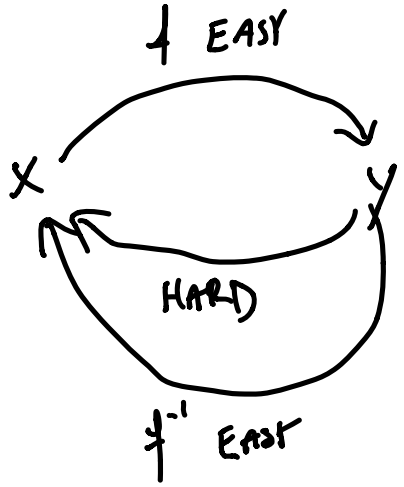
IMPORTANT CONCERN: ADV SHOULD NOT BE ABLE TO CONSTRUCT $\sigma(D_1 \| D_2)$ FROM $\sigma(D_1), \sigma(D_2)$.

OTHERWISE, CAN FORGE ON ANY DOCUMENT WITH $\sigma(0), \sigma(1)$.

CONSTRUCTING SIGNATURES

BUILDING BLOCK:

TRAPDOOR PERMUTATIONS: (f, f^{-1})



INVERTING f HARD UNLESS GIVEN f^{-1}

PROBLEM: FOR A PARTICULAR (f, f^{-1}),

ADV MIGHT HAVE f^{-1}

HARD-CODED INTO IT.

SOLUTION: USE EXPONENTIALLY LARGE

FAMILY. $\{(f, f^{-1})\} = F$.

RANDOMLY SAMPLE $(f, f^{-1}) \in F$

AT START OF PROTOCOL.

$\Pr[\text{ADV KNOWS } f^{-1}] = \text{NEGLIGIBLE}$.

FLAWED CONSTRUCTION IDEA

sk	pk
f^{-1}	f

$\$ x$

$\sigma(x) \triangleq f^{-1}(x)$

PROBLEM: f ONLY HARD TO INVERT ON RANDOM x. DOCUMENTS NOT NECESSARILY RANDOM.

ATTACK: COMPUTE $f(w) = m$ FOR $\$w$.

$D^* = m$, $\sigma(D^*) = w$

LAMPORT 1-TIME SIGNATURE

sk, pk ONLY GOOD FOR SIGNING m TOTAL BITS

SUPPOSE $m=5$ FOR EXAMPLE.

ASSUME f IS 1-WAY PERMUTATION

KEYGEN:

sk

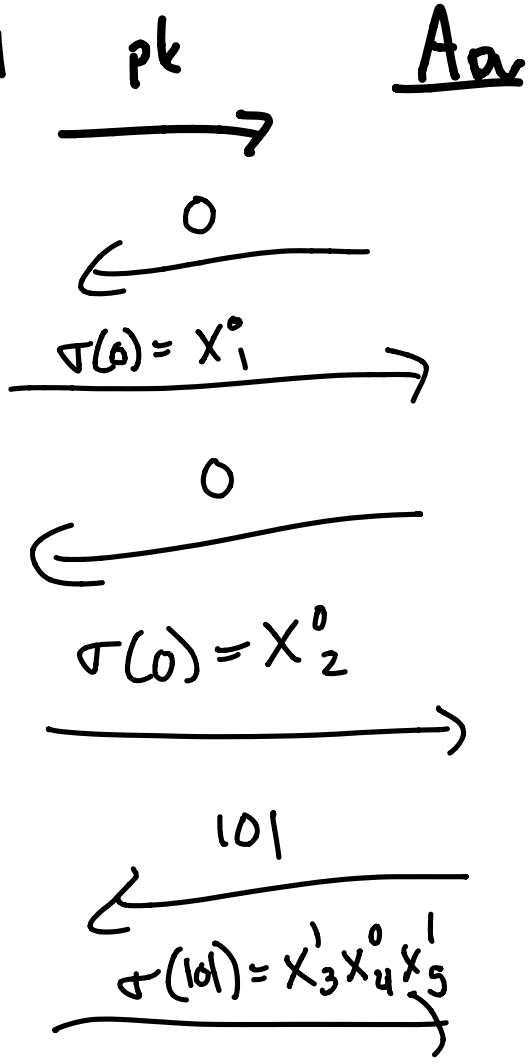
x_1^0	x_2^0	x_3^0	x_4^0	x_5^0
x_1^1	x_2^1	x_3^1	x_4^1	x_5^1

pk

$f(x_1^0)$	$f(x_2^0)$	$f(x_3^0)$	$f(x_4^0)$	$f(x_5^0)$
$f(x_1^1)$	$f(x_2^1)$	$f(x_3^1)$	$f(x_4^1)$	$f(x_5^1)$

ALL x_j^i ARE RANDOM

SIGNING:

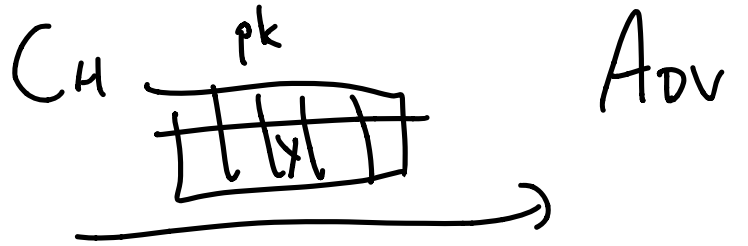


REVEAL ONE OF ENTRIES IN EACH COLUMN, BUT NEVER BOTH.

VERIFY: CHECK $f(sk) = pk$ ON THOSE VALUES

HOW DO WE SHOW FORGING THIS SCHEME BREAKS THE 1-WAY PERMUTATION f?

GIVEN $y = f(x)$, WANT TO INVERT y USING AN ADV THAT FORGES SIGNATURES. PUT y RANDOMLY INSIDE PUBLIC KEY pk.



ADV DOESN'T KNOW WHICH ONE IS y, THEY ALL LOOK RANDOM.

IF ADV ASKS US TO SIGN USING y, WE CAN'T. WE HAVE TO RESTART & TRY AGAIN.

BUT, WITH PROBABILITY $1/2$, HE ASKS FOR THE OTHER VALUE IN THE COLUMN.

THEN, WHEN HE FORGES, $\frac{1}{n}$

CHANCE THAT HE SHOWS US $f^{-1}(y)$.

PROBLEM: ONCE WE SIGN m BITS, OUR KEY IS DEAD.

HOW DO WE REFRESH OUR KEY?

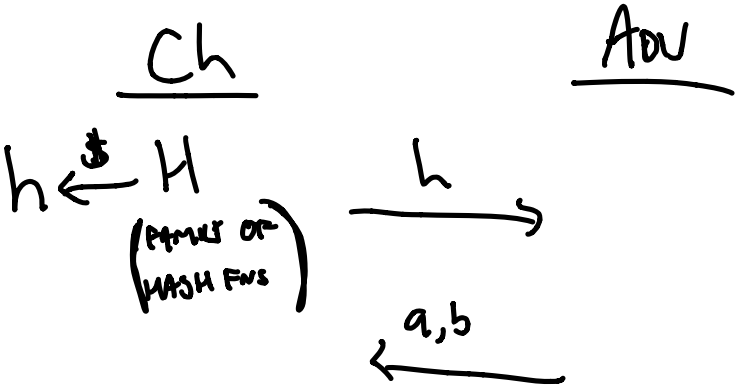
SOLUTION: USE HASH FUNCTIONS

Collision-Resistant Hash Functions

Hash function: Any length decreasing function

$$h: \{0,1\}^m \to \{0,1\}^n, \quad n < m$$

Collision-resistant hash function:



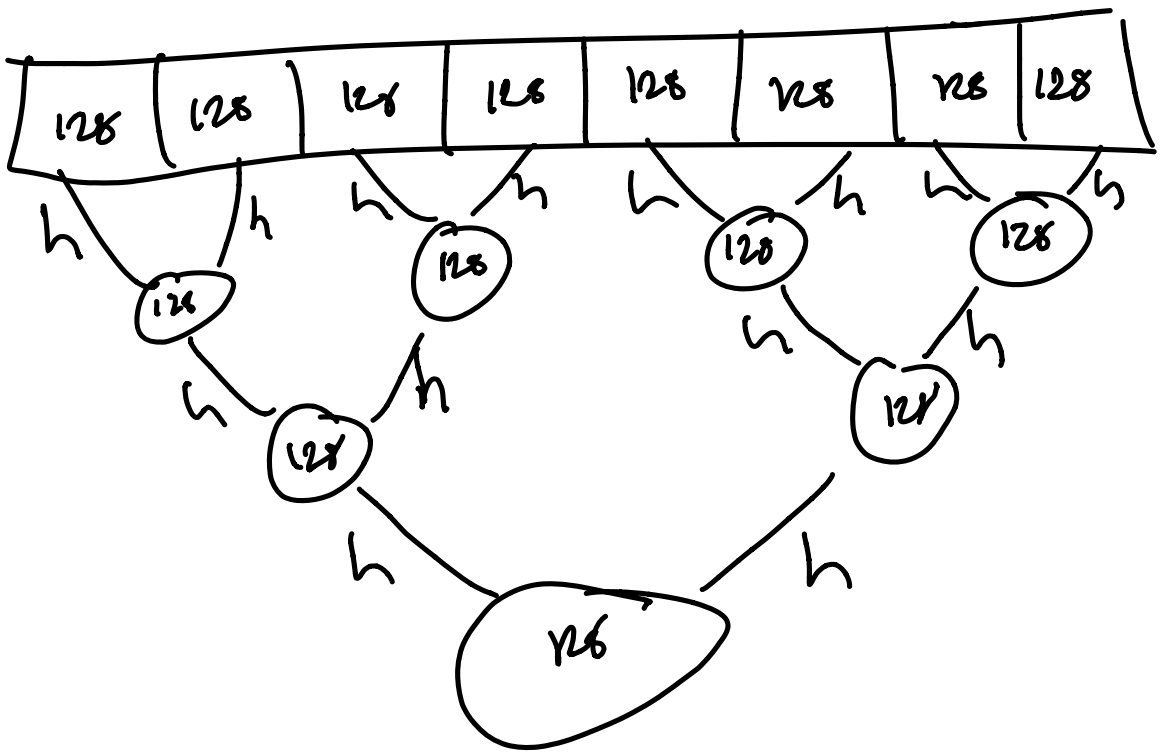
Adv wins if $h(a) = h(b)$

H is a collision resistant family of hash functions if no Adv PPT can win, except with negligible probability

IDEA: INSTEAD OF SIGNING D,
SIGN $h(D)$.

IF ADV FORGES THIS NEW SCHEME,
HE EITHER FOUND A NEW D' WHERE
$h(D) = h(D')$ (A COLLISION) OR
HE TRULY SIGNED A NEW DOCUMENT.

CAN USE HASH FUNCTION TO SHRINK
ARBITRARY-SIZE DOCUMENTS TO
CONSTANT SIZE USING MERKLE HASH
TREE.



IF FIND COLLISION IN WHOLE TREE, IMPLIES COLLISION FOR h SOMEWHERE IN THE TREE (GOOD EXERCISE).

BACK TO OUR PROBLEM:

PROBLEM: ONCE WE SIGN M BITS, OUR KEY IS DEAD.

How do we REFRESH OUR KEY?

IDEA: [NAOR YUNG]