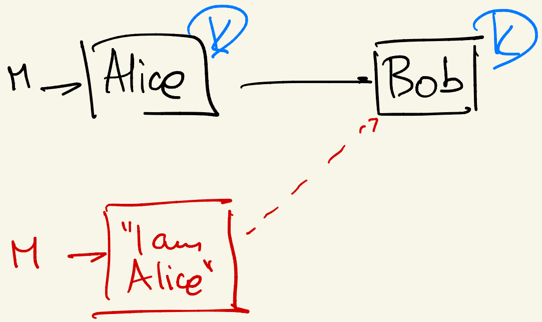
AUTHENTICATION

MESSAGE INTEGRITY



- AUTHENTICITY: Alice SENT M
- INTEGRITY: M IS THE MESSAGE Alice MEANT TO SEND

SECRET-KEY AUTH: MAC (MSG AUTH CODE)

Alice WILL ATTACH A Tag TO M

Bob WILL Verify TAG.

$$\mathrm{Tag}(K, M) = T$$

$$\mathrm{Ver}(K, M, T) = \begin{cases} 1 & \text{IF } T \text{ IS A LEGIT TAG FOR } M \\ 0 & \text{IF NOT} \end{cases}$$

FUNCTIONALITY $\mathrm{Ver}(K, M, \mathrm{Tag}(K, M)) = 1$

$\forall M \; \forall K.$

Eve TRIES TO FORGE: OUTPUTS M, T SO THAT $\mathrm{Ver}(K, M, T) = 1.$

ATTEMPT 1. $\mathrm{Tag}(k,M) = k$

$$\mathrm{Ver}(k,M,T) = \begin{cases} 1 & \text{IF } T = k \\ 0 & \text{IF NOT} \end{cases}$$

CAN Eve TRICK Ver INTO ACCEPTING?

ONLY W/P 2^{-k} IF SHE HASN'T SEEN ANY (M,T) PAIRS.

ADVERSARY MODEL

LEARNING PHASE: Eve SUBMITS MESSAGES M_i AND OBTAINS TAGS $T_i = \mathrm{Tag}(k, M_i)$.

FORGING PHASE: Eve TRIES TO PRODUCE $\boxed{M^*, T^*}$ S.T. $\mathrm{Ver}(k, M^*, T^*) = 1$. FORGERY

REQUIRE $M^* \neq M_i$ FOR ALL i.

CONSTRUCTION OF MAC

$\mathrm{Tag}(k,M) = F_k(M)$ $\quad$ $\mathrm{Ver}(k,M,T) = 1$ IFF $T = F_k(M)$.

Claim. IF F IS (s,q,ε)-HARD TO LEARN THEN $(\mathrm{Tag}, \mathrm{Ver})$ IS $(s,q,2^{-n}+\varepsilon)$-UNFORGEABLE.

$F_k : \{0,1\}^m \longrightarrow \{0,1\}^n$ $\quad m$ = MSG LENGTH

n = TAG LENGTH

m COULD BE VERY LARGE

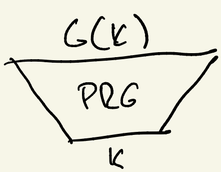
IN GGM COMPUTING F_k REQUIRES INVOKING PRG m TIMES.

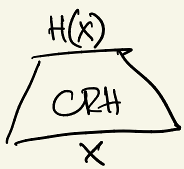
CAN WE AUTHENTICATE VERY LARGE MESSAGES "CHEAPLY"?

1. DESIGN A MORE EFFICIENT PRF OR
2. MSG LENGTH EXTENSION

MAC FOR SHORT MSGs $\longrightarrow$ MAC FOR LONG MSGs

COLLISION-RESISTANT HASH FUNCTIONS





COLLISION: $\exists\, x \neq x'$ s.t. $H(x) = H(x')$

WANT: HARD TO FIND A COLLISION.

SHA-256 AND SHA-3 CLAIM TO BE CRH.

<u>ATTEMPTED Def.</u> $H : \{0,1\}^m \to \{0,1\}^n$ $(m > n)$ IS A (s,ε)-CRH IF $\forall A$ OF SIZE $\le s$,
$\Pr[A$ OUTPUTS $x \neq x'$ S.T. $H(x) \neq H(x')] \le \varepsilon$.

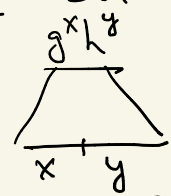
A "OUTPUTS A COLLISION x, x'"
size $= 2m$ $\quad \varepsilon = 1$.

$H_k : \{0,1\}^m \to \{0,1\}$ FAMILY INDEXED BY A KEY.

H_k IS A (s,ε)-<u>CRH</u> IF FOR EVERY CKT C OF SIZE $\le s$, $\Pr[C(k)$ OUTPUTS A COLLISION$] \le \varepsilon$

<u>Example</u> DLOG-BASED BASE g KEY $h \in G$

$$H_h(x,y) = g^x h^y$$



<u>Claim.</u> FIND COLLISION $\to$ SOLVE DLOG

$$g^x h^y = g^{x'} h^{y'} \to g^{x-x'} = h^{y'-y}$$

$$h = g^{\underbrace{(x-x')/(y-y')}_{\text{DLOG.}}}$$

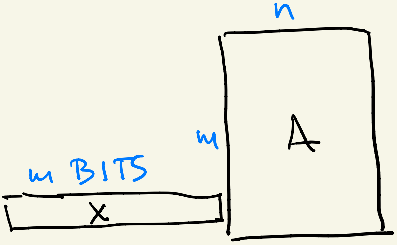
($y \neq y'$ BECAUSE $y = y' \to x = x' \to$ $(x,y), (x',y')$ IS NOT A COLLISION)

NOT AN EXAMPLE: $H_{a,b}(x,y) = ax+by \bmod q$

CAN FIND COLLISIONS BY SOLVING EQNS.

LWE-BASED: KEY A = RANDOM $m \times n$ $\mathbb{Z}_q$-MATRIX

$m > n \log q$



INPUT: $x \in \{0,1\}^m$

OUTPUT: $H_A(x) = xA \bmod q.$

CRH PROPERTY: HARD TO FIND $x \neq x'$ S.T

$$xA = x'A \longleftrightarrow \underbrace{(x-x')}_{\text{NONZERO}}A = 0 \bmod q.$$

Claim. x, x' COLLIDE $\longrightarrow$ CAN BREAK LWE

(DISTINGUISH $A, As+e$ FROM A, r)

HIT A WITH $(x-x')$ ON LEFT:

$$|(x-x')(As+e)| = |\underbrace{\cancel{(x-x')A}}_{0}\cdot s + \underbrace{(x-x')}_{\in\{0,-1,1\}^m}\cdot \underbrace{e}_{b\text{-BDD}}| \le \underbrace{bm}_{\text{SHORT}}$$

$(x-x')\cdot r$ = RANDOM IN $\mathbb{Z}_q$ (TYPICALLY LONG).

CRH: HARD TO FIND x, x' S.T. $H_k(x) = H_k(x')$

$$H_k : \{0,1\}^m \to \{0,1\}^n \qquad n < m$$

TRY DIFFERENT x'S UNTIL TWO COLLIDE.

PHP $\longrightarrow$ 2^n ATTEMPTS ARE ENOUGH.

BIRTHDAY ATTACK: $2^{n/2}$ TIME, $\approx \frac{1}{2}$ SUCC PROB

SAMPLE RANDOM $x_1, \dots, x_\ell$ (DISTINCT)

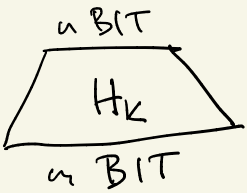
LOOK FOR i, j S.T. $x_i \neq x_j$ $H_k(x_i) = H_k(x_j)$.

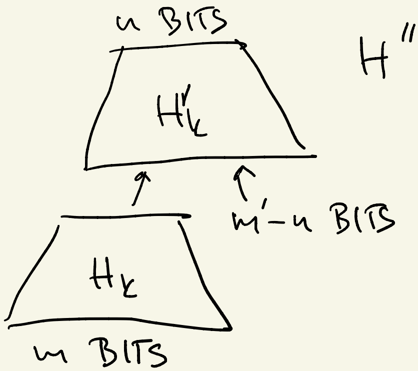
$$\mathbb{E}[\#(x_i, x_j) \text{ S.T. } H_k(x_i) = H_k(x_j)]$$
$$= \binom{\ell}{2} \Pr[H_k(x_i) = H_k(x_j)]$$
$$\geq \binom{\ell}{2} \cdot 2^{-n}$$

IF $\boxed{\ell = 2^{n/2}}$, $\mathbb{E}[\#\text{COLLISIONS}] \geq \frac{1}{2}$.

IN FACT $\Pr[\exists \text{ COLLISION}]$ IS CONSTANT

COMPRESSION USING CRH

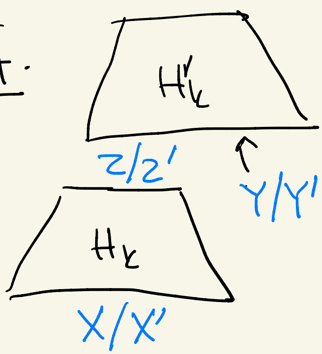




COMPOSITION

Claim IF H_k IS A (s,ε)-CRH AND H'_k IS A $(s+t,\varepsilon')$-CRH $(t = \text{size } H_k)$ THEN H''_k IS $(s, \varepsilon+\varepsilon')$-CRH.

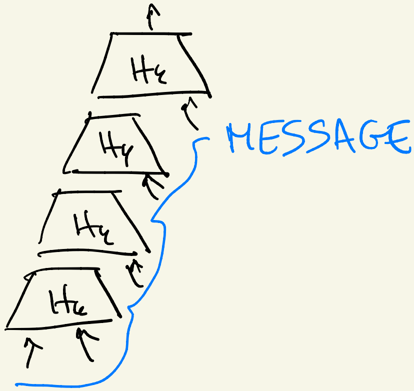
Proof.



SUPPOSE $H''_k(X,Y) = H''_k(X',Y')$

IF $ZY \neq Z'Y'$
THEN ZY, $Z'Y'$ COLLIDE IN H'_k
ELSE $Z \neq Z'$ AND $X \neq X'$
SO X, X' COLLIDE IN H_k.

MERKLE - DAMGÅRD



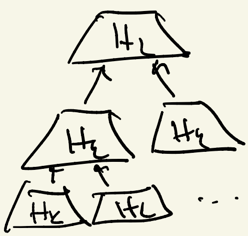
CAN HASH IT IN STREAMING MANNER

ℓ COPIES $(t = \text{size } H_k)$

H_k IS (s, ε)-CRH

$\rightarrow$ MD IS $(s - t\ell, \ell\varepsilon)$-CRH.

MERKLE TREE



$H_k : \{0,1\}^{2n} \rightarrow \{0,1\}^n$

$\rightarrow$ MT IS $(s - t \cdot \log\ell, \ell\varepsilon)$-CRH

WILL BE USEFUL LATER

MAC FOR SHORT MSGS $\longrightarrow$ MAC FOR LONG MSGS

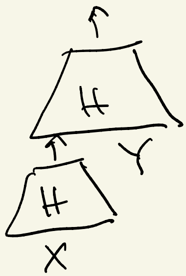
(Tag, Ver) IS FOR LENGTH n

$$\text{Tag}'(k, M) = \text{Tag}(k, H_k(M))$$

$$\text{Ver}'(k, M, T) = \text{Ver}(k, H_k(M), T).$$

Claim H_k IS CRH AND (Tag, Ver) IS SECURE THEN (Tag', Ver') IS.

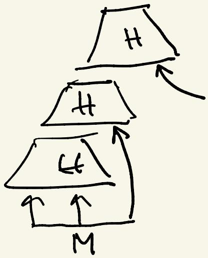
IF $M^* \neq M_i$ THEN $H_k(M^*)$ SHOULD BE $\neq H_k(M_i)$



(X, Y) AND $(H(X), Y)$ COLLIDE IN M-D

COLLISION AMONG DIFFERENT LENGTH MESSAGES

SOLUTION: HASH $(M, \ell(M))$.



$\ell(M) \neq \ell(M')$

DIGITAL SIGNATURES

Alice^{SK} $\xrightarrow{M, \mathrm{Sign}(SK, M) = T}$ Bob^{PK} $\quad \mathrm{Ver}(PK, M, T)$

Eve^{PK} $\xrightarrow{M^*, T^*}$ Bob

Eve WANTS TO MAKE Bob ACCEPT

(ξ, ε) : $\Pr[\text{Bob ACCEPTS Eve's } (M^*, T^*)] \leq \varepsilon$

Eve HAS ACCESS TO A SIGNING ORACLE

$\xrightarrow{M_i}$
$\xleftarrow[\mathrm{Sign}(SK, M_i)]{}$

$M^* \neq M_i$ FOR ALL i.

HOW TO SIGN A 1-BIT MESSAGE

$M \in \{0,1\}$

Eve OBSERVES $\mathrm{Sign}(sk, 0)$ E.G.
SHOULD FORGE SIGNATURE OF 1.

$Y_0 = G(X_0)$ $Y_1 = G(X_1)$ X_0, X_1 SECRET KEY
Y_0, Y_1 PUBLIC KEY

$\mathrm{Sign}(sk, M) = X_M$
$\mathrm{Ver}(PK, M, T)$ accepts if $G(X_M) = Y_M$.

Eve OBSERVES $\underline{X_0}$ ALSO KNOWS $\underline{Y_0}, \underline{Y_1}$
CAN SHE COME UP WITH $\underline{X_1}$?

NO IF PRG IS SECURE.

DIGITAL SIGNATURES		ID PROTOCOLS
WROTE M	← PROOF →	KNOWS SK
	← ATTACK →	
USE SIGN ORACLE FORGE	• LEARNING • BREAK	EAVESDROP IMPERSONATE P^*
NONINTERACTIVE $M^* \neq M_i$	DIFFERENCE	INTERACTIVE

$^{x}P \xrightarrow{h = g^R} V \quad g^x = PK$

$\xleftarrow{c \text{ RANDOM}}$ LIMITED INTERACTION

$\xrightarrow{R + cx} \quad h \cdot PK^c \overset{?}{=} g^r$

① $P \xrightarrow{c} V$? C HAS TO BE CHOSEN AFTER h

IDEA: SET $C = R(h)$ WHERE R IS A RANDOM ORACLE

RANDOM ORACLE MODEL

USED PRF, BUT IN ANALYSIS WE PRETENDED PRF IS TRULY RANDOM.

ASSUME Alice, Bob, Eve HAVE ACCESS TO A TRULY RANDOM FUNCTION R

$\text{Alice}^R \xrightarrow{M, R(M)} \text{Bob}^R$

$\text{Eve}^R \xrightarrow{M^*, R(M^*)} \text{Bob}^R$

Alice : $R(001) = 111$

$R(110) = 100$ INDEP.

Bob : $R(111) = 011$ INDEP.

$R(110)$

MAC IN ROM

ATTEMPT: $Tag^R(M) = R(M)$

$Ver^R(M,T) \longleftrightarrow T \overset{?}{=} R(M)$

EASY TO FORGE

PROPER ROM MAC

Alice^R (K) $\longrightarrow$ Bob^R (K)

$\text{Tag}(K,M) = R(K,M)$

$\text{Ver}(K,M,T) \leftrightarrow R(K,M)=T$

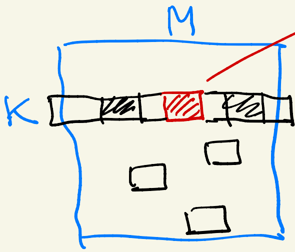
Eve^R

EVE'S SIGNING QUERY BUDGET

Eve OBSERVES $M_1, \underline{R(K,M_1)}, \ldots, M_q, \underline{R(K,M_q)}$

SHE NEEDS TO FIND $M^* \neq M_i$ WITH $R(K,M^*)$

INDEPENDENT OF K



TO FORGE Eve MUST QUERY $R(K,M^*)$ FOR SOME M^*

$$\Pr[\text{Eve QUERIES } R(K,?)] \leq q' \cdot 2^{-k}$$

EVE'S R-QUERY BUDGET

IMPAGLIAZZO-RUDICH: STAT. SECURE KEY EXCHANGE IS IMPOSSIBLE IN ROM.

$P \xrightarrow{h=g^{R'}} V$

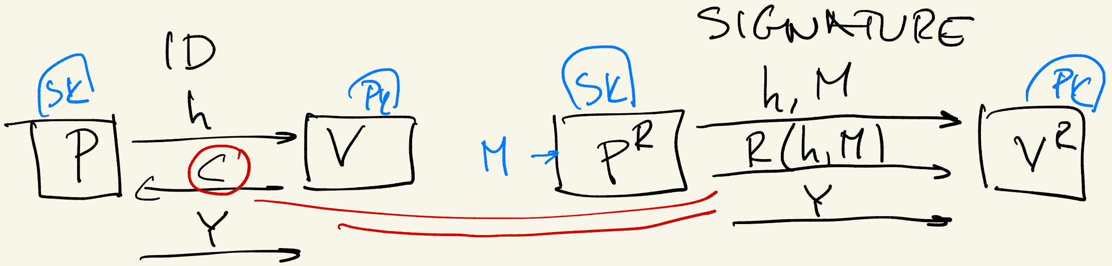
$\xleftarrow{C}$ REPLACE BY $R(h,M)$

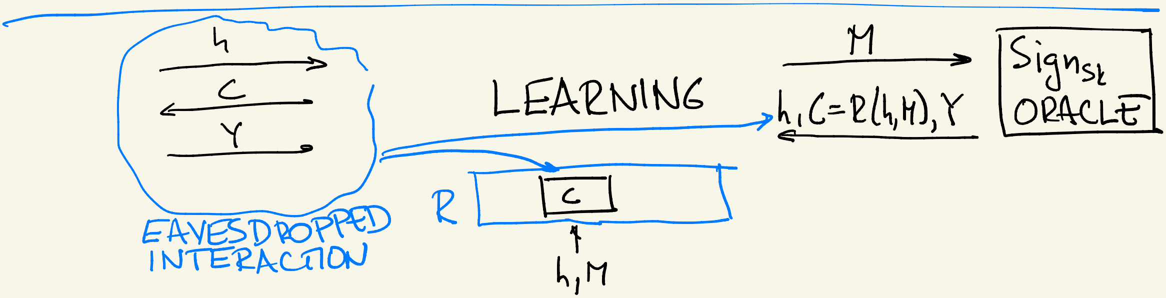
$\xrightarrow{R+CX}$ $h \cdot PK^C \stackrel{?}{=} g^r$

SCHNORR IDENTIFICATION

SCHNORR SIGNATURE

SCHNORR ID IS SECURE AGAINST EAVESDROPPING → SCHNORR SIGNATURES SECURE IN ROM.





IMPERSONATION

GUESS INDEX I OF QUERY h^*, M^*

INITIATE IMPERSONATION

$\xrightarrow{h^*}$

$\xleftarrow{C^*}$

SET $R(h^*, M^*) = C^*$

IF GUESS WAS CORRECT (WITH PROB $\geq 1/q$)

ANSWER C^* BY Y^*.

FORGERY

$\xrightarrow{h^*, M^*, C^*, Y^*}$

IF QUERY (h^*, M^*) WAS NEVER MADE FOR Pr(ACCEPT) VERY LOW