2014102004

DATE: / /

PAGE NO.:

Ameya Prabhu, UG2

Strong v/s Weak One-way functions.

a)

Defⁿ → A strong one-way function if it is easy to compute & $\forall$ PPTM A, $\exists \epsilon$, s.t. $\forall n \in \mathbb{N}$

$$Pr\left[x \leftarrow \{0,1\}^n, A(1^n, f(x)) \in f^{-1}(f(x))\right] \leq \epsilon(n).$$

For $\epsilon \rightarrow$ a negligible function.

Defⁿ → A weak one-way function if it is easy to compute & $\forall$ PPTM A, $\exists \epsilon$, s.t $\forall n \in \mathbb{N}$

$$Pr\left[x \leftarrow \{0,1\}^n, A(1^n, f(x)) \in f^{-1}(f(x))\right] \leq 1 - \frac{1}{q(n)}$$

where $q(n)$ is *any polynomial function.

b) We can basically turn our weak one-way functions into strong one-way functions by requiring the adversary to find the inverse of all outputs of inputs given in parallel by running f on many of them.

Lemma: Let $f: \{0,1\}^* \rightarrow \{0,1\}^*$ be a weak one-way function. $f(x_1, x_2, \ldots, x_m) = y_1, \ldots, y_i = f(x_i)$. There exists a polynomial $m(x)$ such that f is a strong one-way function.

Informal proof → Probability of each input being inverted $= 1 - \frac{1}{q(n)}$.

$$\left(\left(1 - \frac{1}{q(n)}\right)^{q(n)}\right)^n \approx \left(\frac{1}{e}\right)^n \rightarrow \text{neg.}$$

Hence, we obtained a negligible function!

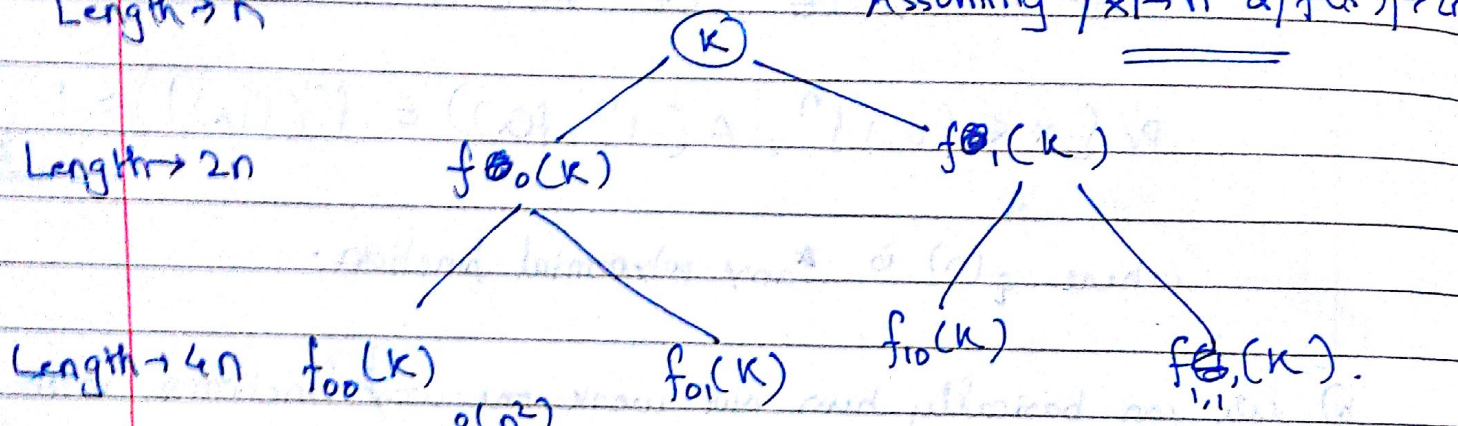
P.S. (Assuming all multiplications are independent).

(c) If one way functions don't exist, then collection of one way functions cannot exist. Hence, collection will exist if one-way exist.

Also, if one way function $f(x)$ exists, then we can find large functions too, without the exp computation!

Given an input K, $G(K)$ can be formed by a binary indexing, rather than a linear one, reducing the time complexity

Assuming $|x| \to n$ & $|f(x)| \to 2n$



$o(n^2)$ in time!

Hence, a collection exists & it is efficiently computable!

2) $F_K(x)$ is not pseudo-random as it is efficiently invertible.

$$F^{-1}_K(x) = K \oplus F_K(x)$$

, if given K & the output we know the inverse too!

Also, it is not pseudo-random as we can easily identify the output string from random!

(Needs some more proof I guess 😊)

3) $F(K, x) = y$. $x \in \{0,1\}^n$ $x \in \{0,1\}^n$
$y \in \{0,1\}^n$.

$F(K, x) \,||\, F(K, F(K, x))$ - is a PRF which is $\{0,1\}^k, \{0,1\}^n \to \{0,1\}^{2n}$ which is secure if $F(K, x)$ is secure, as both are random functions, and random functions if concatenated give bigger random functions.

4) (a) It is always zero. Always colliding! hence, not resistant obviously!

(b) Yes. To apply this ~~$\forall$~~ $m \in M$ & $\forall t \in T$, $|m| = |t|$ otherwise we'll have to pad with zeros. If so, then the hash function would be collision resistant as the hash would be similarly applied to any input, giving an indistinguishable output anyways.

(c) No. It is easily crackable by a birthday attack of 2^{16}, which is non-negligible.

(d) No. All messages of the same length will have the same ~~length~~ hash.

(e) No. $H(m)$ & $H(m \| 1^{|m|})$ have the same hash! Collision! Not collision resistant.

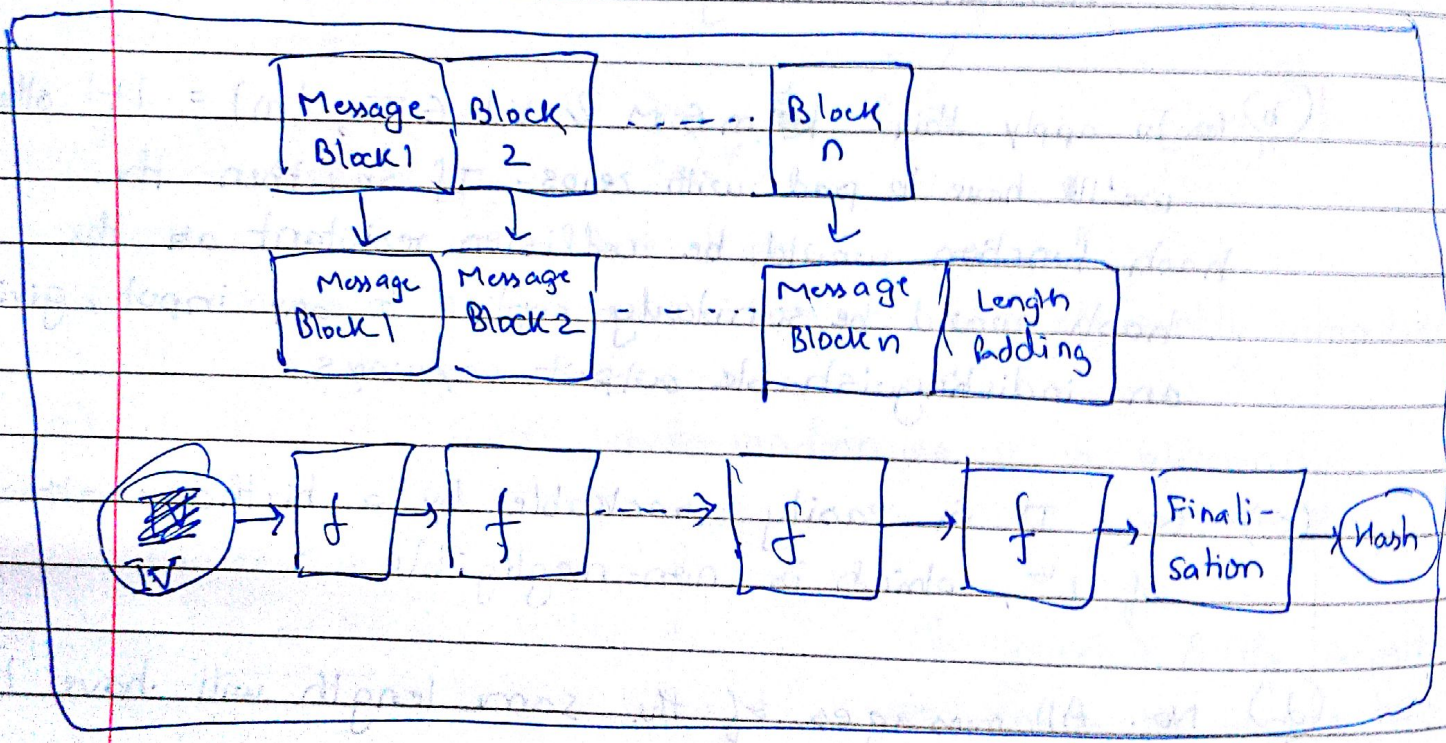
(f) Yes. As if $H'(m) = H'(m')$, then trivially $H(m) = H(m')$. Hence, this is collision resistant if the other is.

g) $H'(m) = H(H(m))$. Yes!

for messages of a fixed length m == tag space t, and then it would be collision resistant!

5) a) MD construction is a method of building collision-resistant cryptographic hash functions from collision resistant one-way compression functions f.

Construction



b) Yes. It is necessary.

Say our input blocks are $h^s : \{0,1\}^{2n} \to \{0,1\}^n$

We want to make an MD construction $H^s : \{0,1\}^* \to \{0,1\}^n$

We are given that h^s is collision resistant.

Assuming collision in x & y where $|x| = |y|$

$H_s = m_1 m_2 \dots m_n$.

If $H_s(x) = H_s(y)$

then in the process there must have been equal blocks. Hence, the collision must have happened at some block i,

$\therefore h_i(x_1) = h_i(y_1)$ where $x_1 \neq y_1$

but $h_i(x_1) = h_i(y_1)$

Hence, contradiction to the fact that his was collision resistant.

If $|x| \neq |y|$, then we just append the length of the message to the end of the message. Hence, the messages itself are different, now!

6) a) True. 2nd preimage resistance is there $\nexists$ y, s.t given x, $h(x) = h(y)$. and collision resistance means $\nexists x, y$, s.t $h(x) = h(y)$.

b) False. We can derive pre-image resistance. Say, it was not pre-image resistant. Then, we can have an oracle given $H(m_1)$ returns m_1. We can have an m_1, compute $H(m_1)$ and consult the oracle, if it returns m_2, then $H(m_1) = H(m_2)$, a collision is found! But, since our hash is collision-resistant, we get a contradiction.

But, this assumes we would get an m_2, which is intuitive given that f maps infinitely-many inputs to a fixed no of outputs, so there is a high probability that $m_1 \neq m_2$.

However, it is possible to define 'pathological' hash functions that have perfect, provable second-preimage resistance, but not pre-image resistance.

Ex:- $f(x) = \begin{cases} 0 \,||\, x & \text{if } x \text{ is } n \text{ bits long} \\ 1 \,||\, g(x) & \text{otherwise} \end{cases}$

Pre-image is just the identity function, but it is provably second-preimage resistant.

i.e. it is bijective.

(c) (i) True. It is a MAC algorithm, hence resistant by definition.

(ii) True. It is difficult to trace the output back to input in the absence of the key, even if the attacker has similar other plaintexts.

(d) True. Even if one-part always differs, then $h(x)$ is always unique. Hence, collision-resistant

7) a) False. Given an x_1 & $y_1 \to h(x_1, y_1)$ and say x_2 & $y_2 \to h(x_2, y_2)$. We can solve for a & b. Then we can predict easily for a new x_3, y_3 the value of $h(x_3, y_3)$!

And even without computing anything: we know

b) $h(0,0) = 0$.

(b) True. The average case success probability is

1 − Average case failure probability

$= 1 -$ Failure at every timestep

$= 1 - \left(1 - \frac{1}{M}\right)^{q}$.

(c) True. Similarly here average case success probability is

$1 -$ Avg case failure prob

$\doteq 1 -$ (Failure at every step)$^{q-1}$

$= 1 - \left(1 - \frac{1}{M}\right)^{q-1}$

(d) True. Avg case success probab

$= 1 -$ Avg case failure.

$= 1 - \left(1 - \frac{1}{M}\right)\left(1 - \frac{2}{M}\right) \cdots \left(1 - \frac{(Q-1)}{M}\right)$

(1st resistant; 2 of them resistant; Q-1 of them resistant)

(1st it; 2nd it; $Q-1^{th}$ it.)

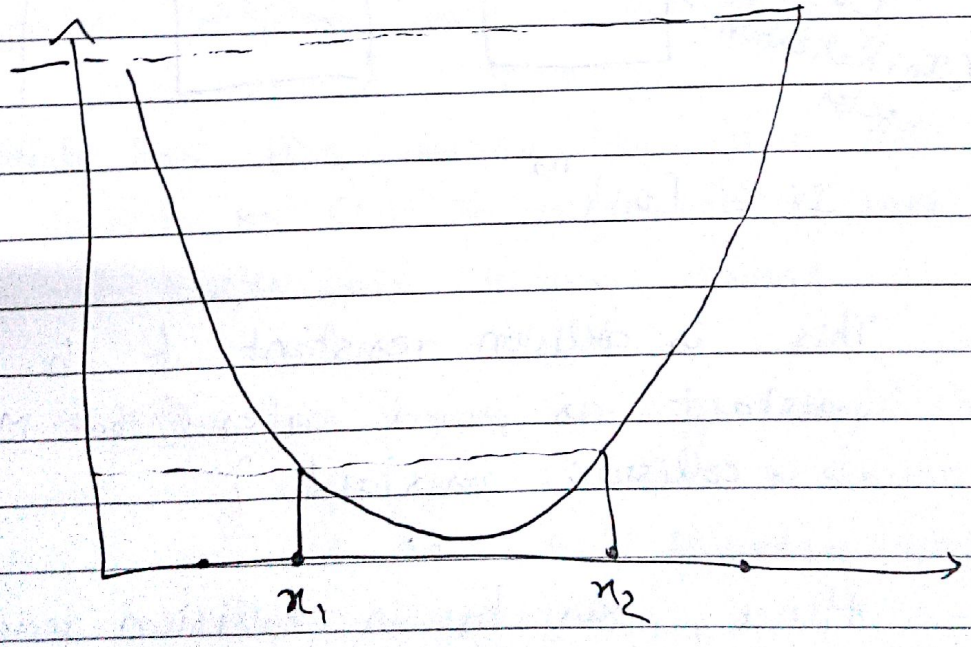
$= 1 - \left(\frac{M-1}{M}\right)\left(\frac{M-2}{M}\right) \cdots \left(\frac{M+1-Q}{M}\right)$

8) $H : \{0,1\}^n \to \{0,1\}^m$.

$h(x) = (x^2 + ax + b) \pmod{2^m}$.

~~For every x which is a multiple of 2^m the n bit string~~

The quadratic curve is bounded graphically somewhat like this



Since it is quadratic in nature, it is symmetric about the point $\left(\frac{-a}{2}\right)$. Hence, it is easy to find preimage for certain a's & b's.

for any $x \in Z_{2^m}$.

9)

$$h_1 = \begin{cases} 0 \,||\, x & \text{if } x \in \{0,1\}^n \\ 1 \,||\, h(x) & \text{otherwise.} \end{cases}$$

h_1 is a $(n+1)$ bit hash function.

The preimage is just the identity function for digests which begin with 0! ~~collision~~

It ~~was~~ is bijective across the space of n-bit inputs, hence doesn't have a second-preimage attack but it is given $h(x)$ starting with 0, removing the zero gives x as the remaining string!

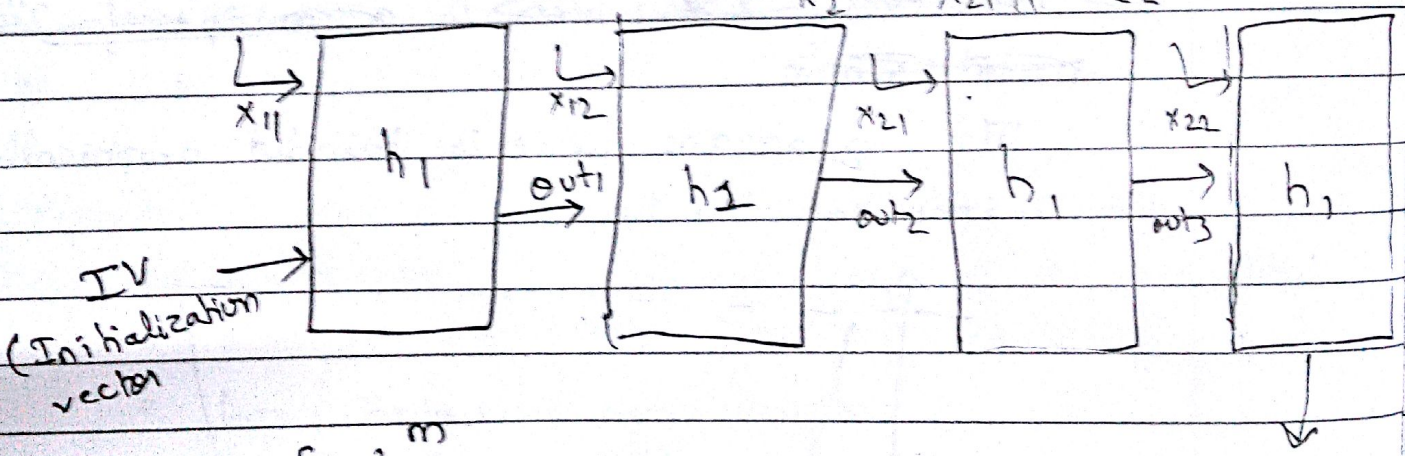
10) We use MD-construction for this

$x_{11}, x_{12}, x_{21}, x_{22} = \{0,1\}^n$.

$x = x_1 \,||\, x_2$.

$x_1 = x_{11} \,||\, x_{12}$

$x_2 = x_{21} \,||\, x_{22}$



$IV \in \{0,1\}^m$

This is collision resistant if h_1 is collision resistant as proved earlier (that MD construction is collision resistant).

Hence, our h_2 is collision resistant!

b) (M3)

This is the generalized version. It is capable of defined in this way due to the MD construction. We break it into blocks recursively in a tree structure, until each block is of size $\{0,1\}^m$ & then

$$x = x_1 \| x_2$$
$$x = (x_{11} \| x_{12}) \| (x_{21} \| x_{22})$$
$$\vdots$$
$$\boxed{x = x_1 x_2 \ldots\ldots\ldots x_m}$$

Given a function $h : \{0,1\}^{2m} \to \{0,1\}^m$, we can construct an MD-construction of 2m blocks in the similar manner as on the left (2m blocks will be there).

hi would be collision resistant given h is collision resistant as ~~by definition of~~ MD construction generates collision resistant functions.

11) CBC Mode has this disadvantage that the C_i depends on C_{i-1} to be correct, hence all Ciphertext blocks are linearly chained.

Hence, $C_1, C_2, \ldots, C_{\ell/2-1}$ would be decrypted perfectly, but $C_{\ell/2}$ would be incorrectly decrypted and all the other following blocks would be incorrectly decrypted.

$\therefore (\ell/2+1)$ plaintext blocks would be corrupted inespective of whether the further blocks after $C_{\ell/2}$ were correctly recieved.