Hash Functions

Review of desirable properties
Applications (contd.)
Construction (MD5)

Desirable Properties

① OW "one-way" (pre-image resistance)
② CR Collision resistance (strong)
③ TCR Target collision resistance (weak)
④ PRF Pseudo-randomness
⑤ NM Non-malleability

Given $h(x)$, should not be able to find $h(x+1)$.

NM $\Rightarrow$ OW

Applications (contd.)

(4) Commitments

Alice has value x (e.g., auction bid)
Alice then computes C(x) and submits it as her bid
"commitment to x"

C(x) is her "sealed bid"

When bidding is over, Alice "opens" C(x) to reveal x

Binding : Alice should not be able to open C(x) in multiple ways.

Secrecy : Auctioneer seeing C(x) should not learn anything about x

NM : Given C(x) shouldn't be possible to produce C(x-1)

Need: NM, CR, OW (really need more for secrecy!)
$h'(x) = h(x) \,||\, msb(x)$

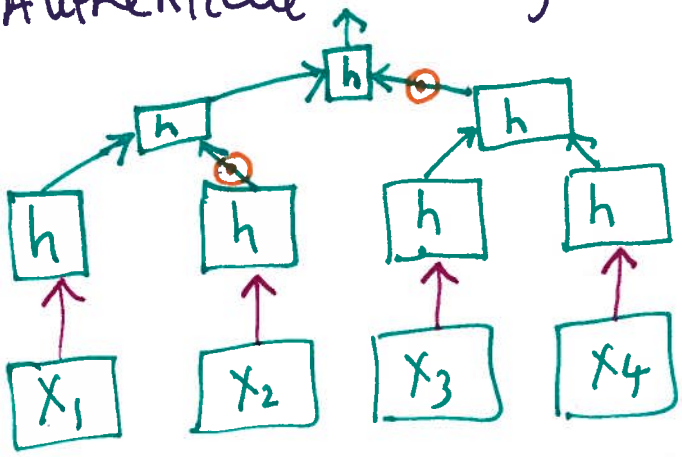
How: $C(x) = h(r \,||\, x)$ $r \in_R \{0,1\}^{256}$

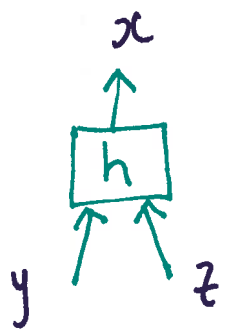
to open reveal r & x

randomized

(5) Merkle tree

Authenticate n objects (e.g., time-stamping)





$$x = h(y \,||\, z)$$

root is authenticator for all n values
(put in New York Times)

Show leaf & ancestors & their siblings
to prove leaf is in tree

One branch of the hash tree can be verified without having the entire tree unlike in a hash list

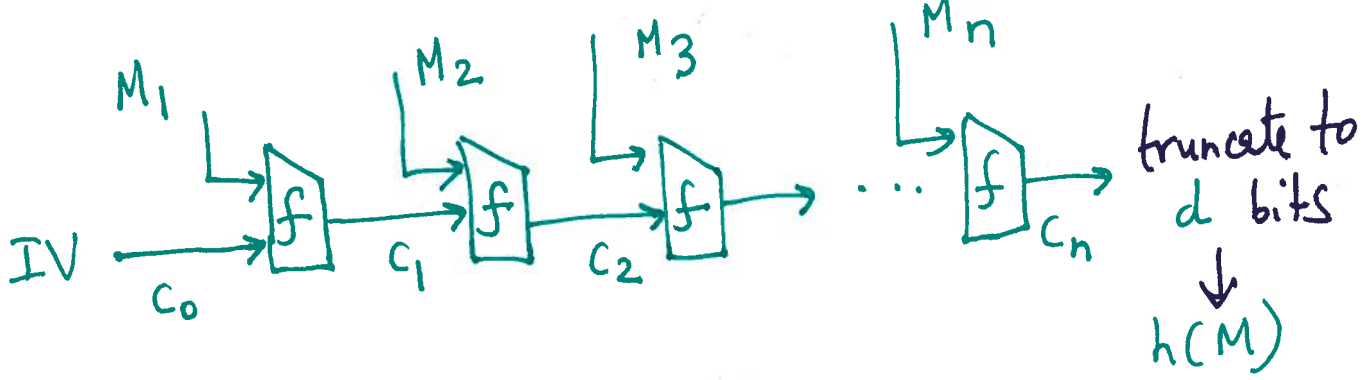
Need: CR

Construction ("Merkle-Damgard" style)

- Choose output size d (e.g., $d=160$)
- Choose chaining variable c (e.g., $c=160$)
  better if $c \geq 2d$
- Choose block size b for message
- Design "compression fn" f

$$f: \{0,1\}^c \times \{0,1\}^b \rightarrow \{0,1\}^c$$

- Choose c-bit (initialization vector)
- Pad message so m's new length is multiple of b bits



Padding: hashinput 0000 pad with 0000
hashinput 0000 pad with 00

Collision on two (or more) inputs.
Solution: Include length of original M in pad

OBSERVATIONS

IV is arbitrary, but fixed

Thm: If f is CR, so is h.

Pf: Work backwards through chain from h-collision to find f-collision.

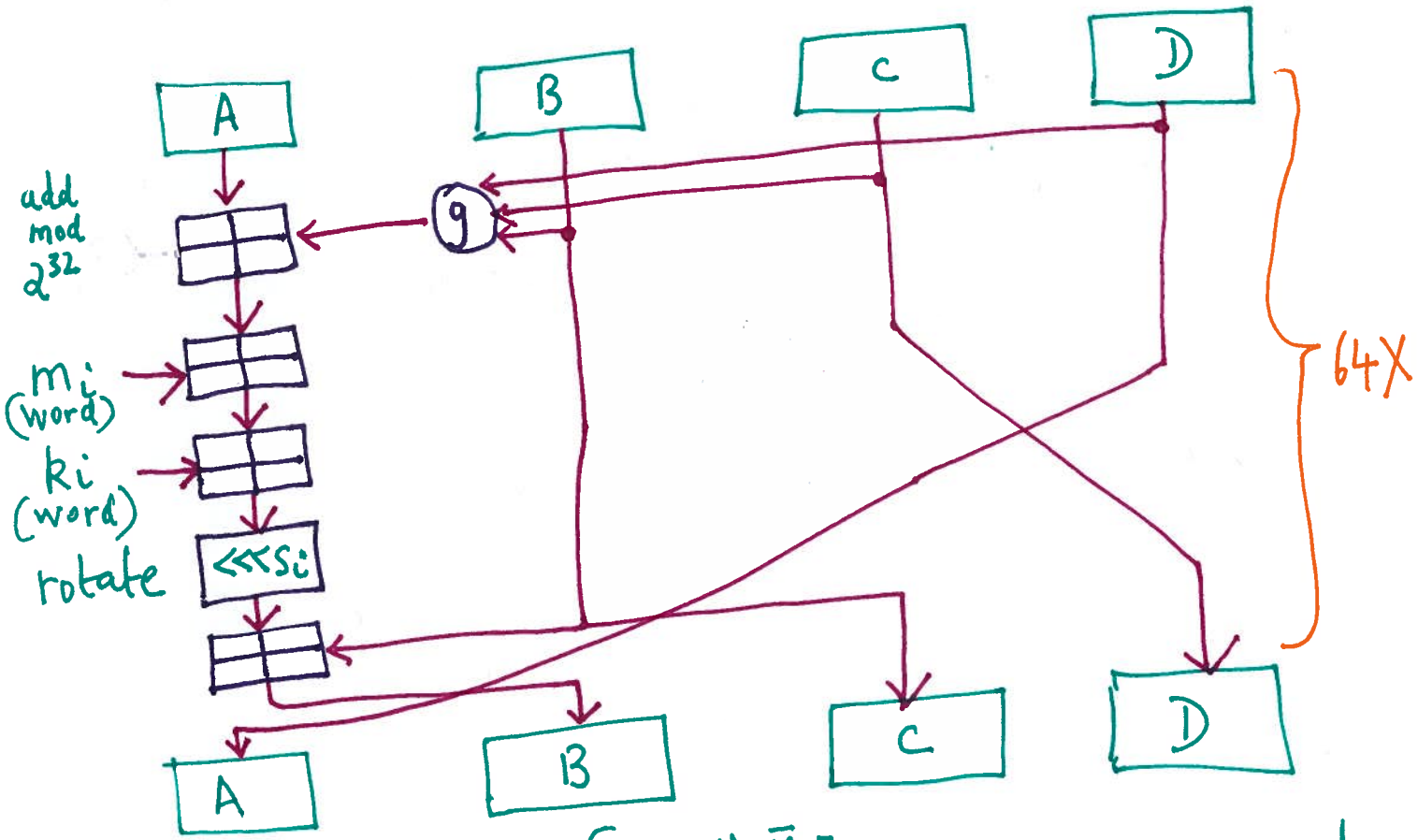
Thm: Same for OW.

AES etc, hard to change keysize

TYPICAL COMPRESSION FUNCTION (MD5)

- chaining vaneble & output are 128 = 4×32 bits
- IV = fixed value
- 64 rounds; each modifies state (in reversible way) based on selected message word
- message block b = 512 bits considered as 16 32-bit words
- Uses end-around XOR

SHA-3 contest underway



$$g(x,y,z) = \begin{cases} xy \vee \bar{x}z \\ xz \vee y\bar{z} \\ x \oplus y \oplus z \\ y \oplus x\bar{z} \end{cases}$$ depending on round