Cryptographic hash functions

Hyoungshick Kim
Department of Software
College of Software
Sungkyunkwan University

What is cryptographic hash function?

$$h = H(M)$$

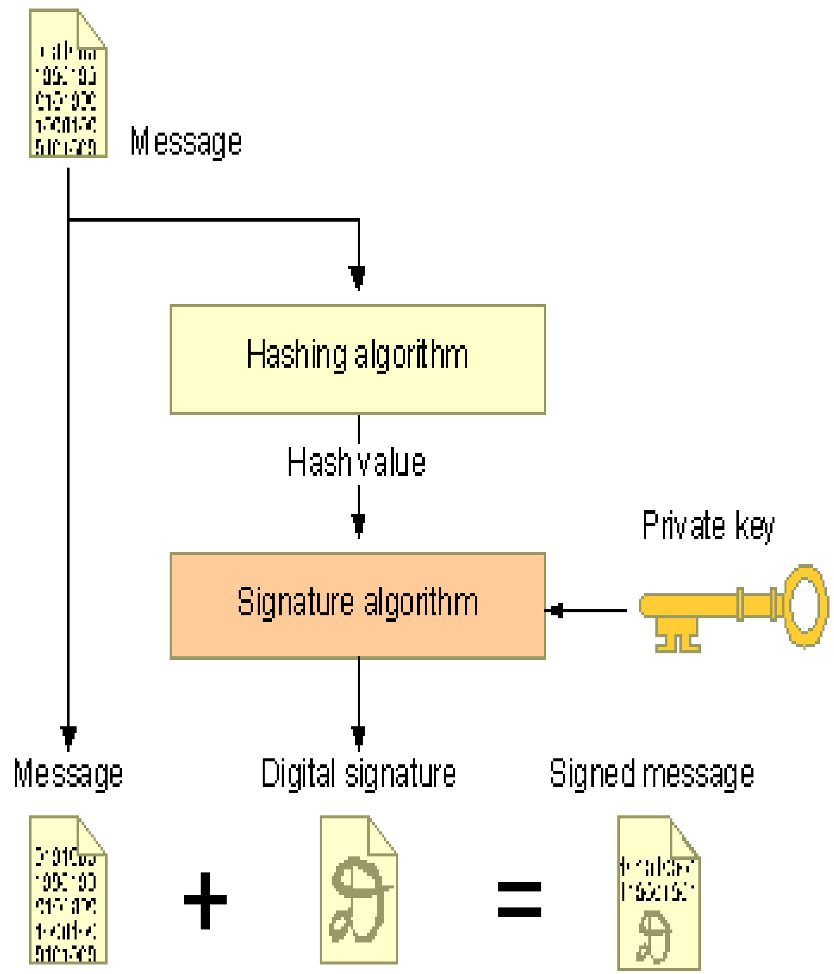
- Regular hash function (used for hash table)
  - Large input domain → small fixed output
  - Well distributed: $P(H(x)=i) \approx 1/N$

This is not enough for cryptographic hash functions!

Hash function motivation

- Suppose Alice signs M
  - Alice sends M and $S = [M]_{Alice}$ to Bob
  - Bob verifies that $M = \{S\}_{Alice}$
- If M is big, $[M]_{Alice}$ costly to ***compute*** & ***send***
- Suppose instead, Alice signs $h(M)$ where $h(M)$ is much smaller than M
  - Alice sends M and $S = [h(M)]_{Alice}$ to Bob
  - Bob verifies that $h(M) = \{S\}_{Alice}$

- First, create a message digest using a cryptographic hash
- Then, sign the message digest with your private key



Cryptographic hash functions

- A cryptographic hash function distills a message M down to a hash H(M)
- Additional properties

1. Pre-image resistance:

   - Given h = H(x), hard to find x

2. Weak collision resistance:

   - Given h = H(x), hard to find any x’ such that H(x’) = h

3. Strong collision resistance:

   - Hard to find any pair x and y such that H(x) = H(y)

Quiz

Q. Which of these is almost a good cryptographic hash function?

1. Use CBC to encrypt x, take last output block
2. Use CTR to encrypt x, take last output block

   Previous blocks can be changed.
3. Use ECB to encrypt x, hash is XOR of all output blocks

   Same output if m_0 switches to m_1
4. Use CTR to encrypt x, hash is XOR of all output blocks

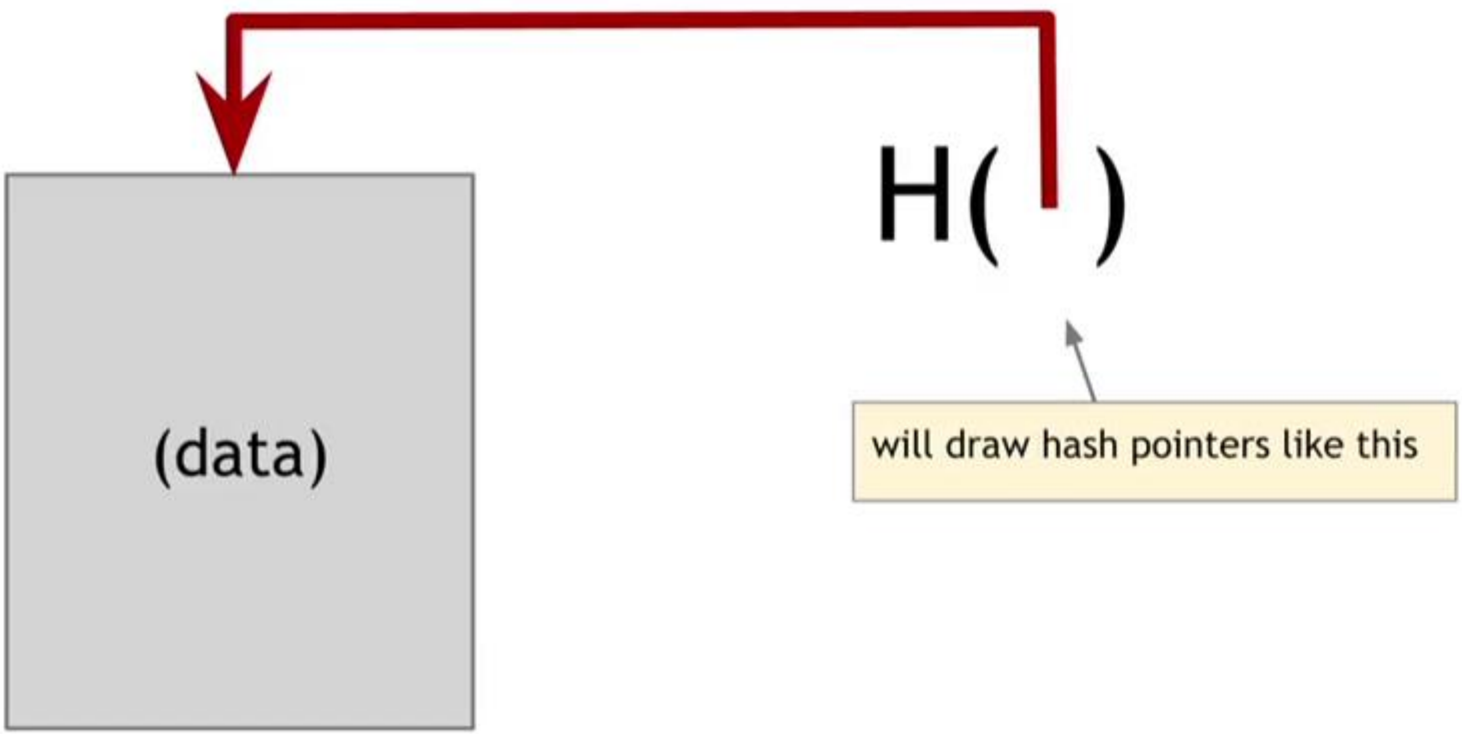
   No order!

   Same output if m_0 switches to m_1

Hash pointer

- Hash pointer is
  - pointer to where some information is stored, and
  - (cryptographic) hash of the information

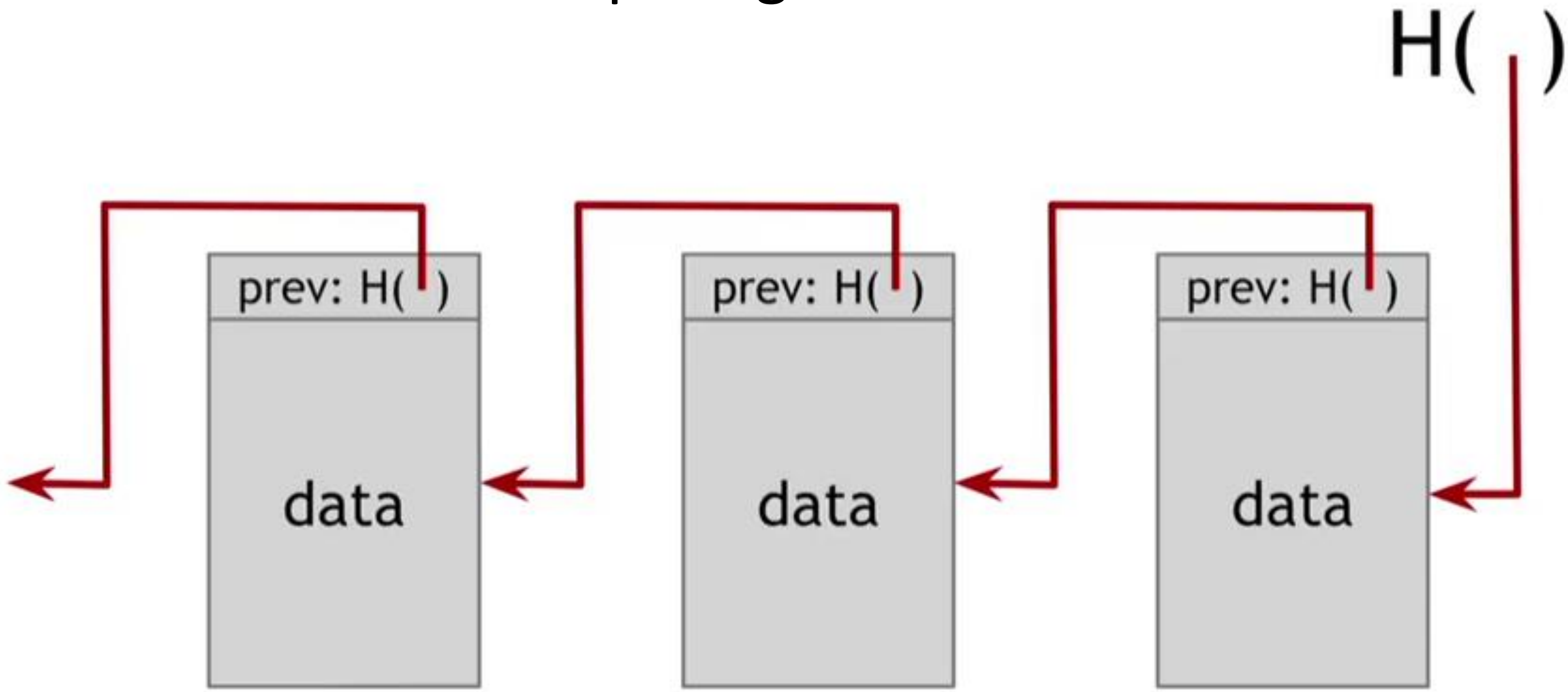
- If we have a hash pointer, we can
  - ask to get the information back, and
  - verify that it hasn’t changed



We can build data structures with hash pointers.

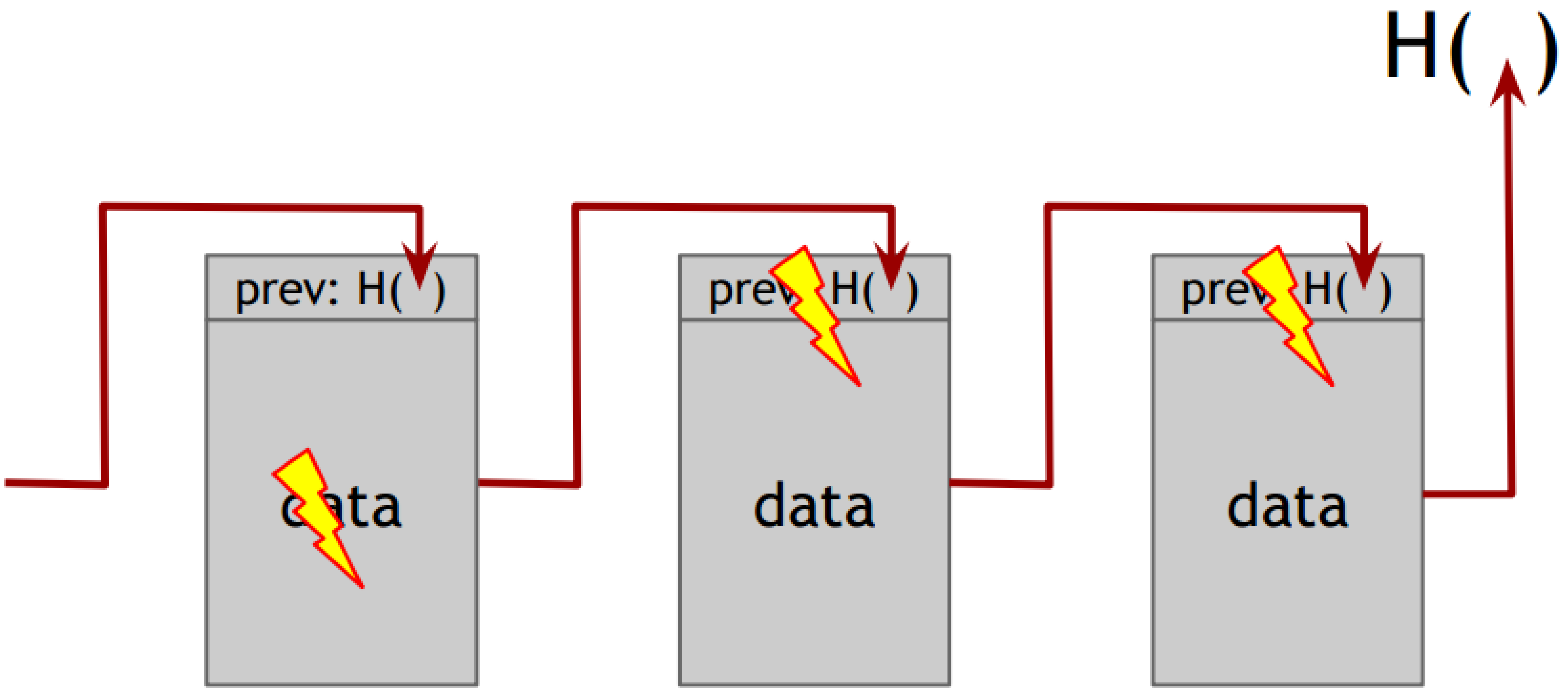
Hash chain

We can detect tampering.



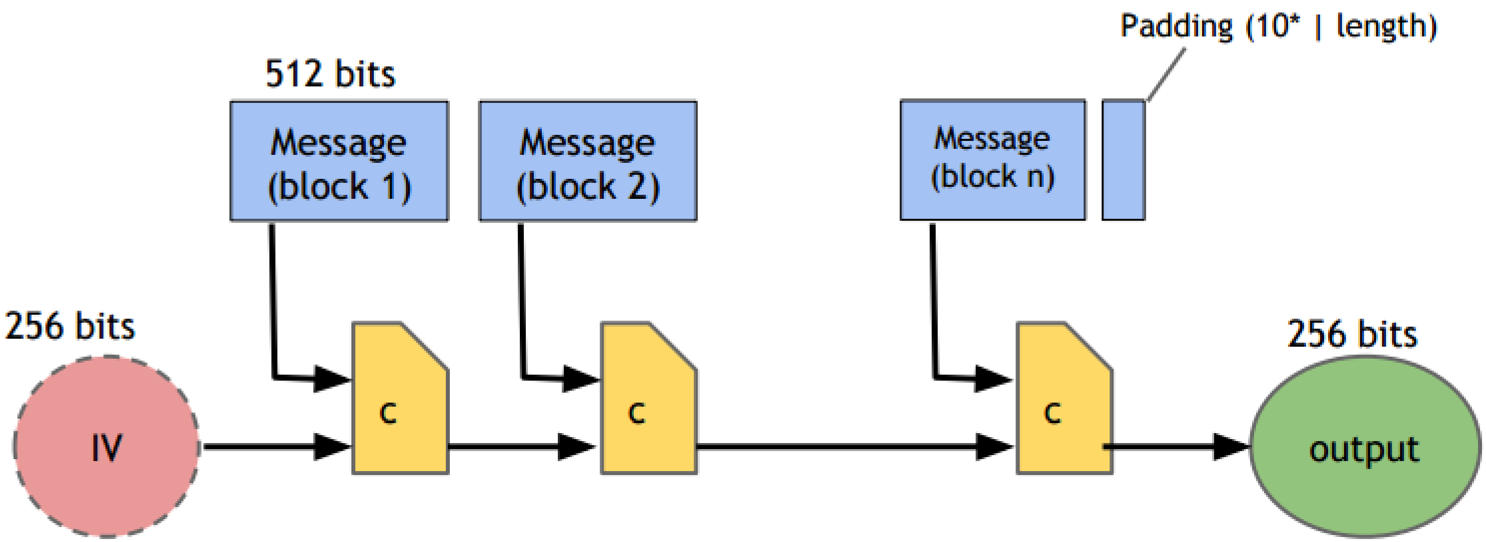
Use case: tamper-evident log

Propagation of modifications



Modifications to any data will propagate forever.

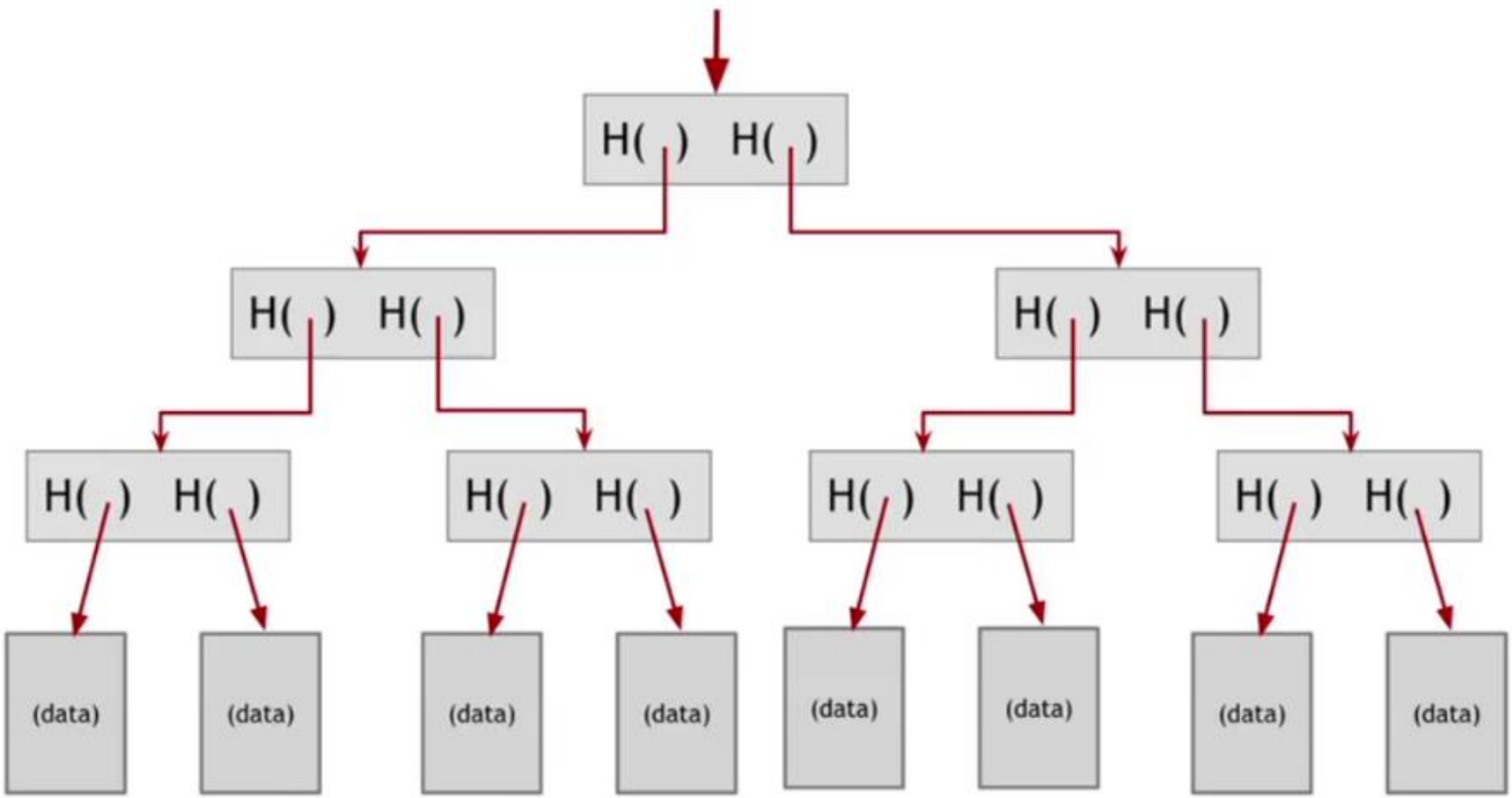
Merkle-Dåmgard construction (e.g., with SHA-256)



Theorem: If c is *collision-free*, then the hash is *collision-resistant*.

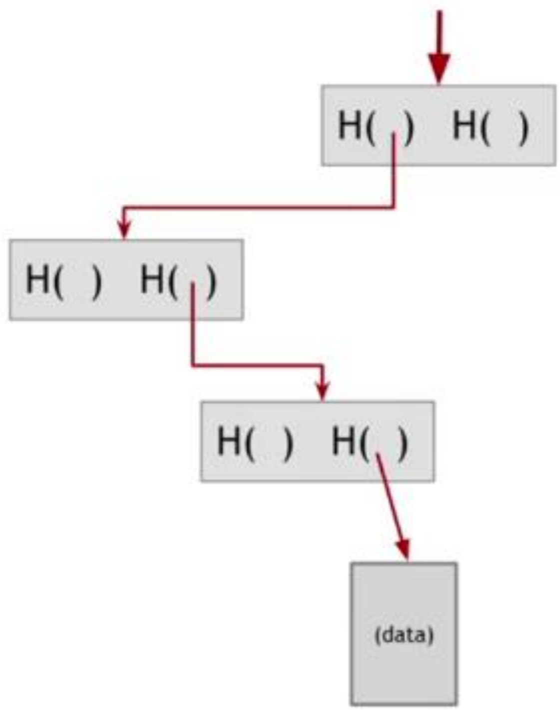
Binary tree with hash pointers

We call this “Merkle tree”.



Advantages of Merkle tree

- Tree holds many items but just need to remember the root hash.
- We can verify membership in O(log n) time/space.



Questions?

Sungkyunkwan
Campus
Sciences
established
University
university
campus
School
Suwon
Seoul
Natural
Korean
Graduate
English
Social
Global
edit
constructed
Professors
Confucian
Institute
Building
Humanities
lecturers
schools
Science
Administration
Academic
ASLE-Korea
Education
Engineering
located
Joseon
Anniversary
Advanced
campuses
Complex
Business
Zone
city
two
four
also
now