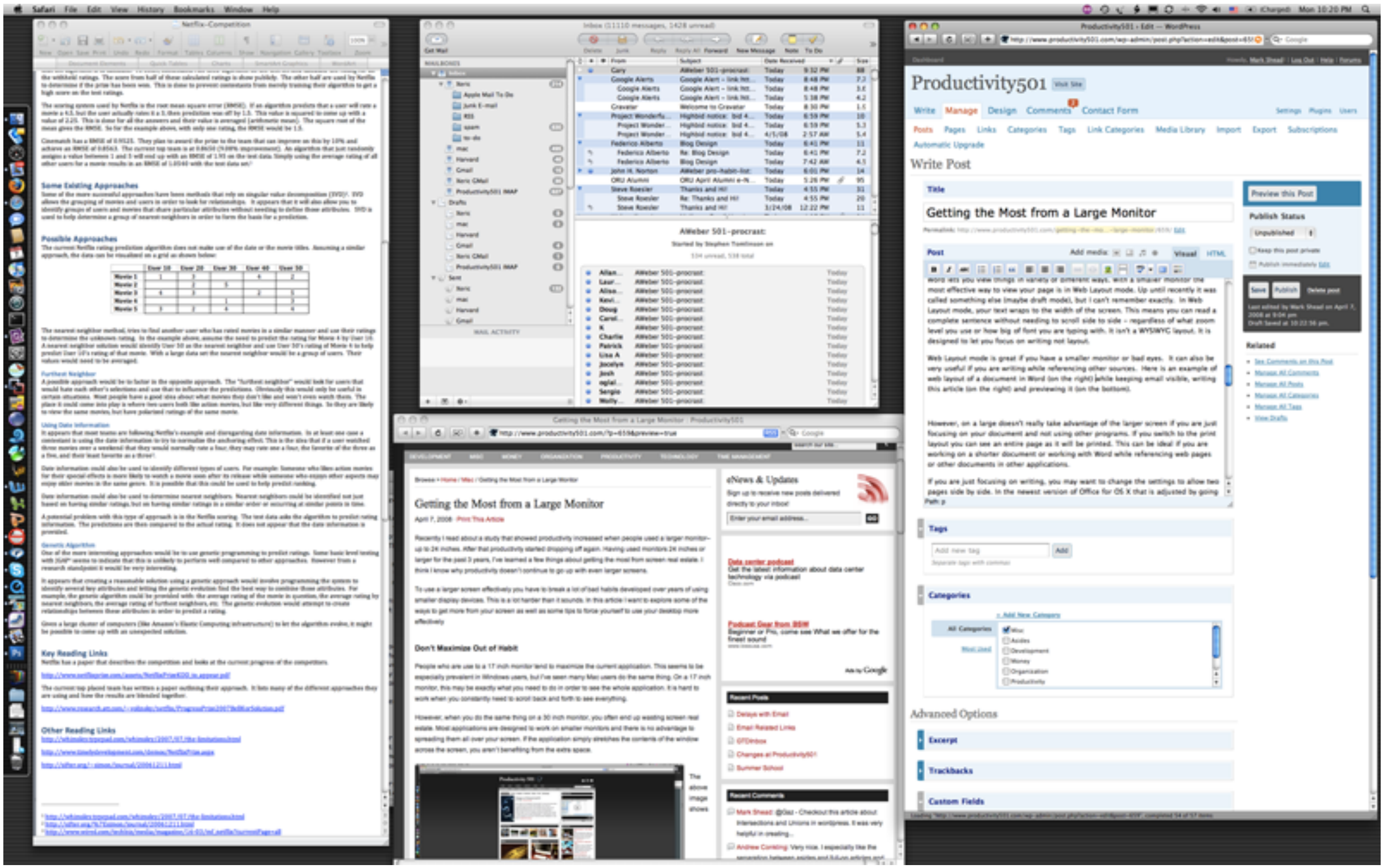
Midterm Review & Memory Efficient General Attacks to Hashes

Yan Huang

1. Economy of mechanism
2. Fail-safe defaults
3. Complete mediation
4. Open design
5. Separation of privilege
6. Least privilege
7. Least common mechanism
8. Psychological acceptability

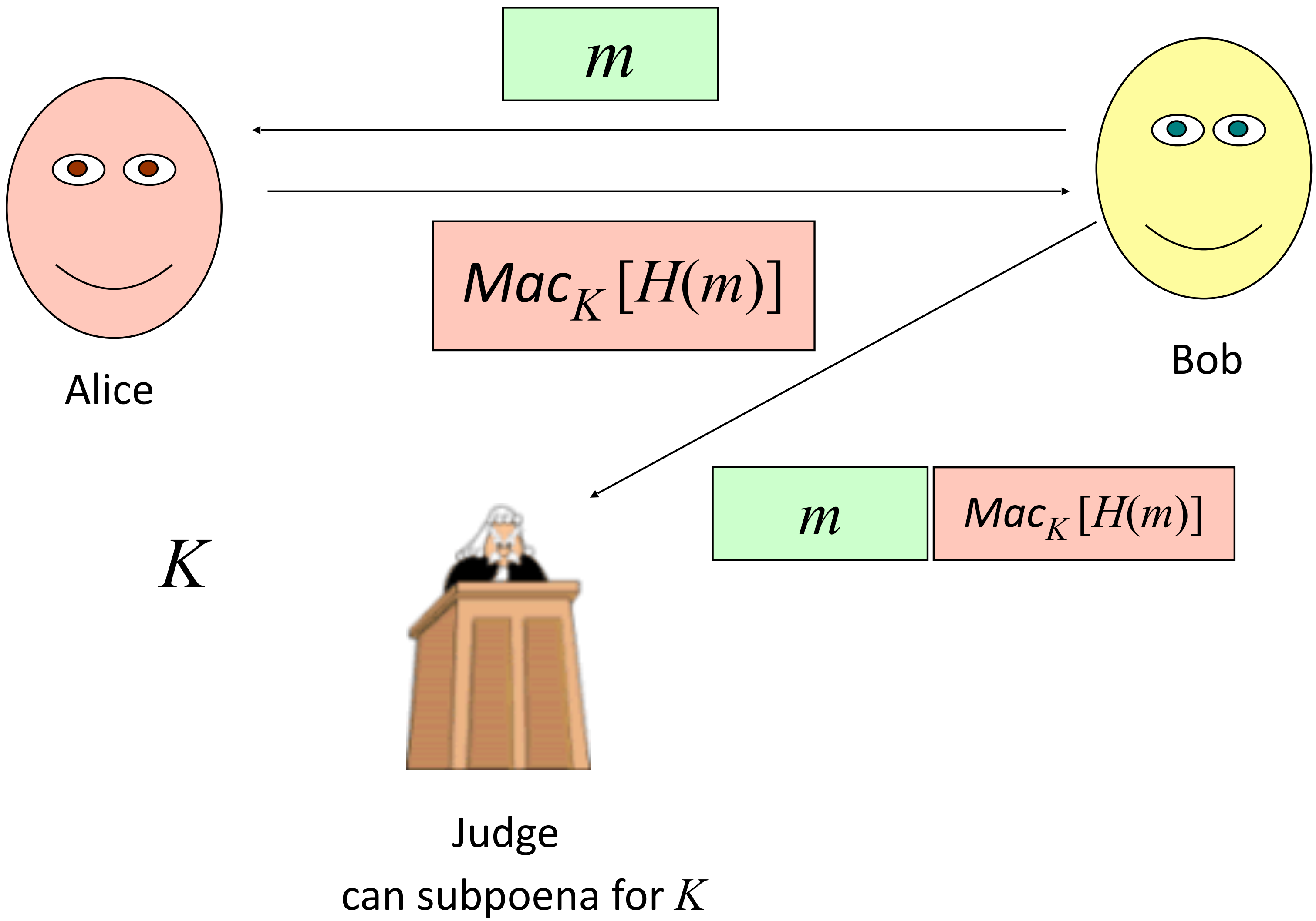
Least Common Mechanism



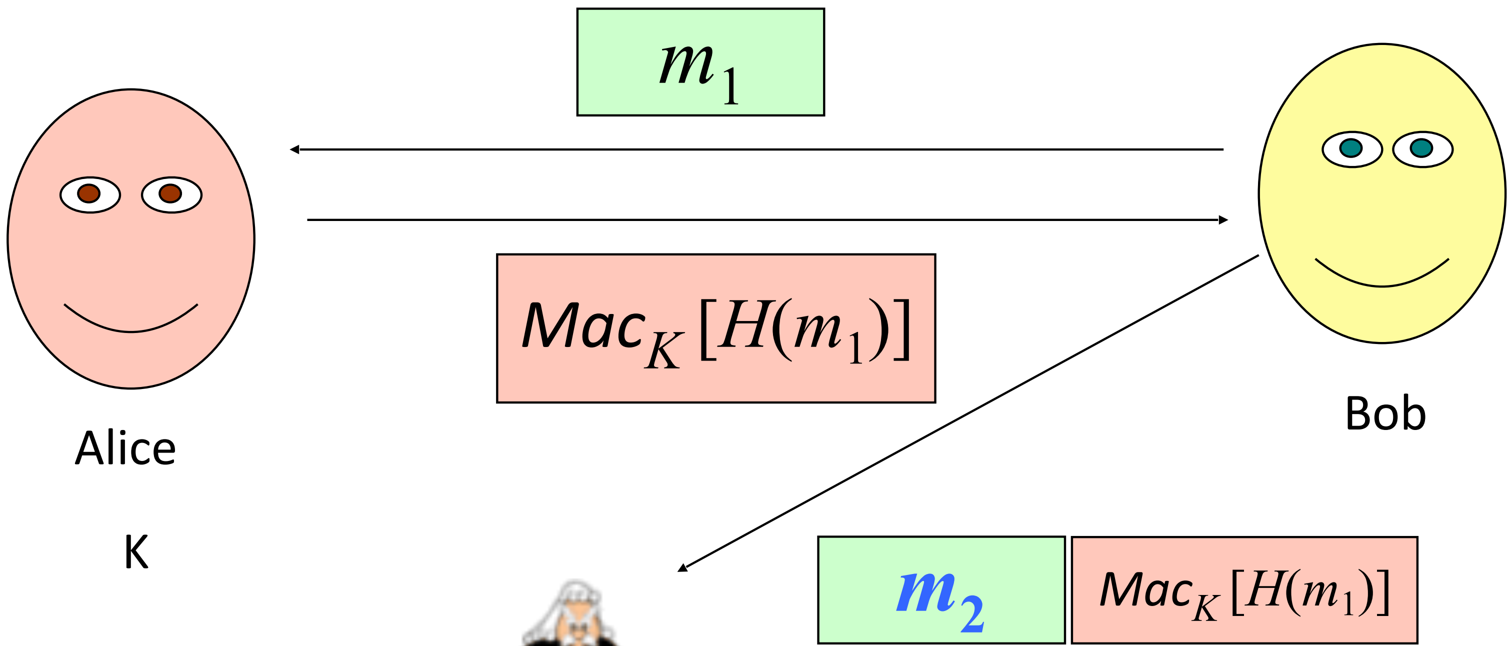
Basic Crypto

Memory Attacks

IOU Request Protocol



Attacking IOU Request Protocol



Bob picks m_1 and m_2 such that $H(m_1) = H(m_2)$.

Finding m_1 and m_2

Bob generates different agreeable m_1 messages:

```
I, {Alice | Alice Hacker | Alice P. Hacker | Ms. A. Hacker},{owe | agree to pay} Bob{the sum of | the amount of}{$2 | $2.00 | 2 dollars | two dollars}{by | before}{January 1st | 1 Jan | 1/1 | 1-1}{2016 | 2016 AD}.
```

How many different-text messages are there?

Finding m_1 and m_2

Bob generates 2^{10} different agreeable m_2 messages:

`I,{Alice | Alice Hacker | Alice P. Hacker | Ms. A. Hacker},{owe | agree to pay}Bob{the sum of | the amount of}{`**`$2 quadrillion | $2000000000000000 | 2 quadrillion dollars | two quadrillion dollars`**`}{by | before}{January 1`st` | 1 Jan | 1/1 | 1-1}{2016 | 2016 AD}.`

Bob's Quadrillionaire Plan

- For each message $m_{1,i}$ and $m_{2,i}$, Bob computes $H(m_{1,i})$ and $H(m_{2,i})$.
- If $H(m_{1,i}) = H(m_{2,j})$ for some i and j, Bob sends Alice $m_{1,i}$, gets $\text{Mac}_K[H(m_{1,i})]$ back.
- Bob sends the judge $m_{2,j}$ and $\text{Mac}_K[H(m_{1,i})]$.

Chances of Success

- Assume the Hash function H is good (uniform randomly distributed outcome)

What is the probability that $H(m_{1,i}) = H(m_{2,j})$ for some i and j ?

Birthday "Paradox"

Assuming real birthdays assigned randomly:

N/D = probability there are no duplicates

1 - N/D = probability there is a duplicate

$$= 1 - 365! \,/\, ((365 - k)!(365)^k)$$

Applying to Birthdays

- For $n = 365$, $k = 20$:

  P(365, 20) ≈ .4114

- For $n = 365$, $k = 40$:

  P (365, 40) ≈ .8912

Chances of Success

- Assume the Hash function H is good (uniform randomly distributed outcome) but has only 128-bit outputs

What is the probability that $H(m_{1,i}) = H(m_{2,j})$ for some i and j ?

For $n = 2^{128}$, $k = 2^{65}$: P $(2^{128}, 2^{60}) > 0.86$

Only Half of the chance will the

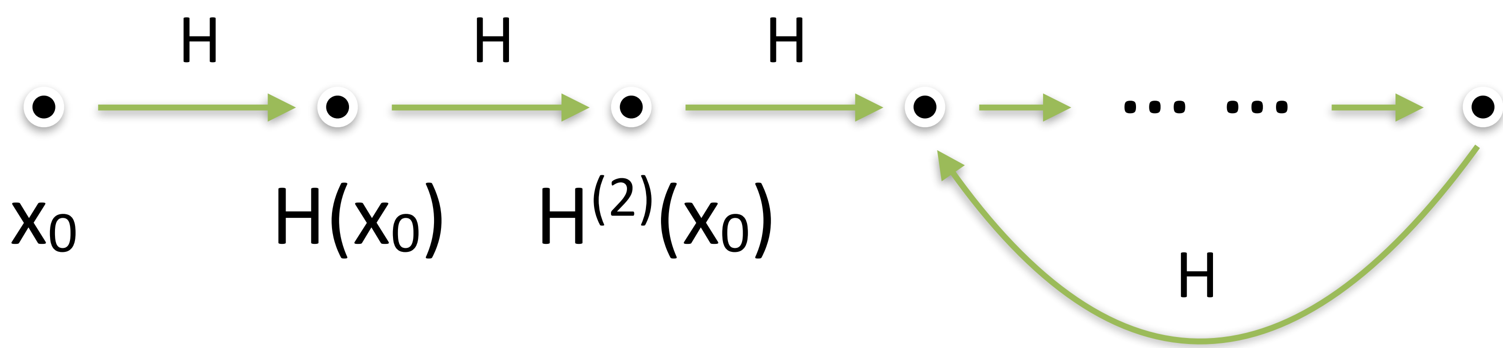
two pre-images of the collision come from two different message groups.

How much memory does birthday attack require?

$>16 \times 2^{60}$ bytes!

Realistic?

Constant Memory Hash Attacks (1)



Hash *meaningful* messages

Set 0 = Bob is {*good, hardworking*} and {*honest, trustworthy*} {*worker, employee*}.

Set 1 = Bob is a {difficult, problematic} and {taxing, irritating} {worker, employee}.

Define function *g*:

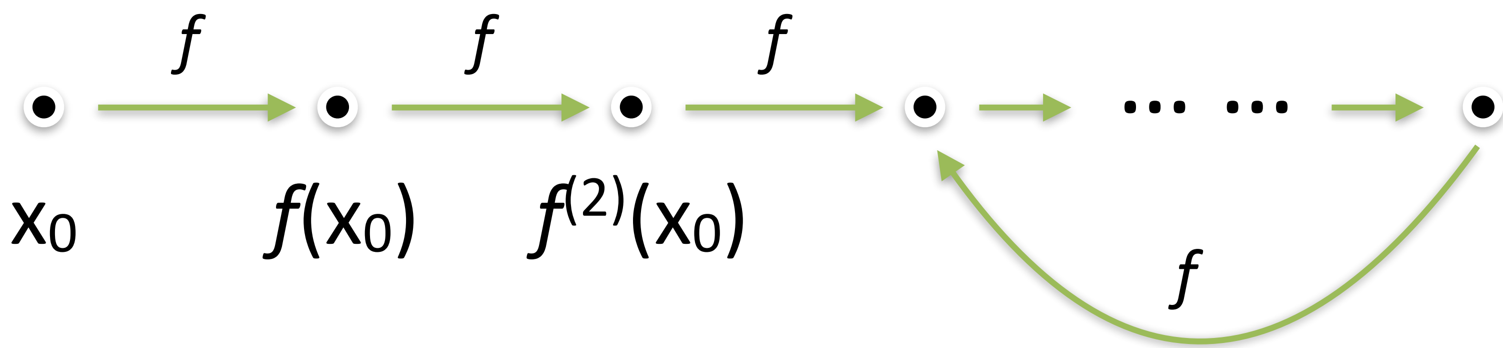
g(0000) = Bob is a good and honest worker.

g(0001) = Bob is a difficult and taxing worker.

g(1010) = Bob is a hardworking and honest worker.

g(1011) = Bob is a problematic and taxing employee.

Constant Memory Hash Attacks (2)



Define f: $\{0,1\}^l \longrightarrow \{0,1\}^l$

$f(x) = H(g(x))$