

CIS 5371, FALL 2025

DIGITAL SIGNATURE

VIET TUNG HOANG

The slides are loosely based on those of
Prof. Mihir Bellare, UC San Diego.

Agenda

1. High-level Overview

2. Building Signature Scheme

The Need For Signing Is Ubiquitous

THE CHEQUE PAPER CONTAINS COLORED MICROPRINTING AND WATERMARK, PROTECTED BY THE LAW OF THE UNITED STATES.

John Smith

765 Dolor sit Amet APT B5
Brooklyn, NY, 12345

CHECK № 0007

DATE: Aug. 11, 2019

PAY TO THE ORDER OF: Mary Johnson \$ 715,39
Seven hundred fifteen and $\frac{39}{100}$ DOLLARS

PAYABLE AT
ALL LOREM BANK BRANCHES IN USA
ACCOUNT Nº 001234567

MEMO Monthly rent

J. Smith
AUTHORIZED SIGNATURE

that as Free and Independent States, they have full Power to levy War, conclude Peace, contract Alliances, establish Commerce, and to do all other Acts and Things which Independent States may of right do. — And for the support of this Declaration, with a firm reliance on the protection of Divine Providence, we mutually pledge to each other our Lives, our Fortunes and our sacred Honor.

John Hancock Samuel Adams Josiah Bartlett

Button Gwinnett
Lyman Hall
Geo Walton.

Y^{rs} Hooper
Joseph Hewes,
John Penn

John Hancock

Samuel Chace
Wm. Paro
Thos. Stone
Chas. Canell of Hired Ma

Robt Morris
 Benjamin Rush
 Benj. Franklin

John Morton
Geo. Lymer
J. P. Smith

Phil. Livingston
 Isaac Lewis
 Lewis Morris

Josiah Bartlett
 Wm Whipple
 Sam Adams
 John Adams
 Rufus Paine
 Elbridge Gerry

Edward Rutledge).

The Wynne & Junr
 Thomas Lynch Junr
 Arthur Middleton

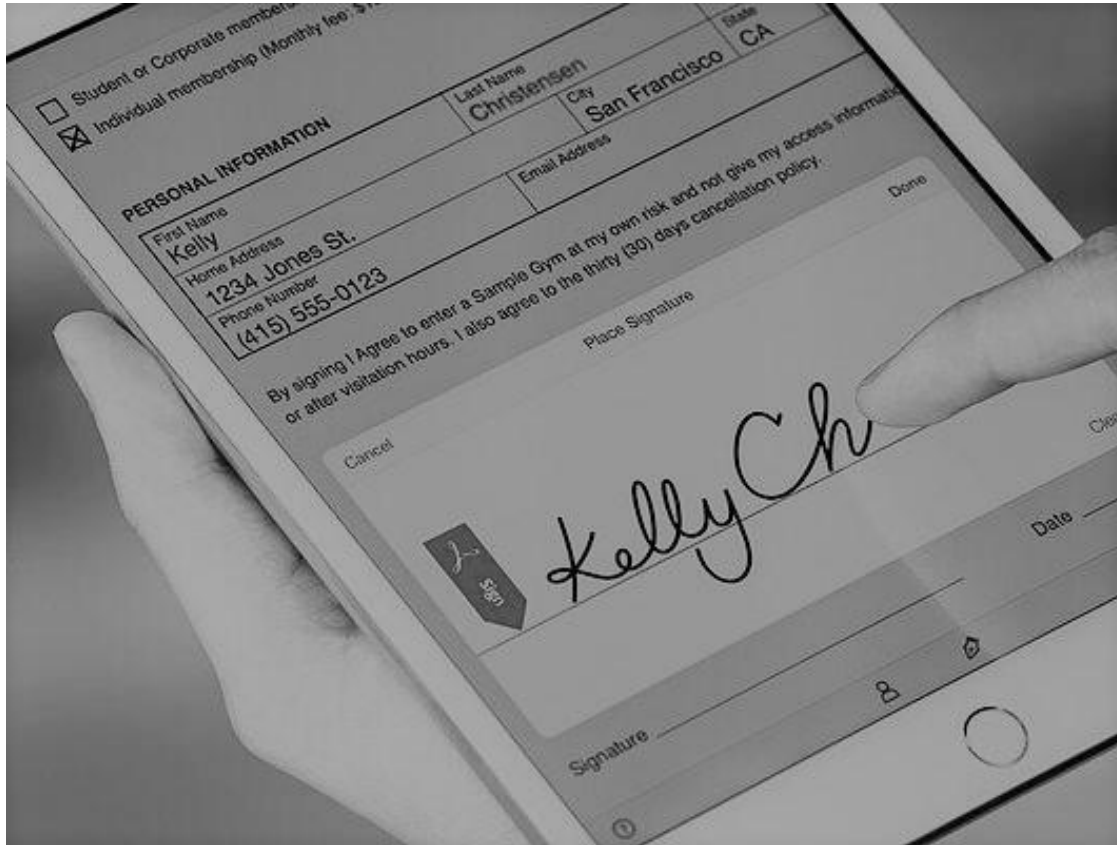
George Wythe
Richard Henry Lee
Th Jefferson
Wm Harrison
Th Nelson Jr.
Francis Lightfoot Lee
Carler Braxton

Pat. Smith
 Geo. Taylor
 James Wilson
 Geo. Tross
 Caesar Ramsey
 Garbark
 Tho. M. Deane

Rich^d Stockton
Jas Wickersham
Genl. Hopkins
John Hart
Abra Clark

Stephen Hopkins
 William Ellery
 Roger Sherman
 Johnth Huntington
 M^{rs} Williams
 Oliver Wolcott
 Matthew Thornton

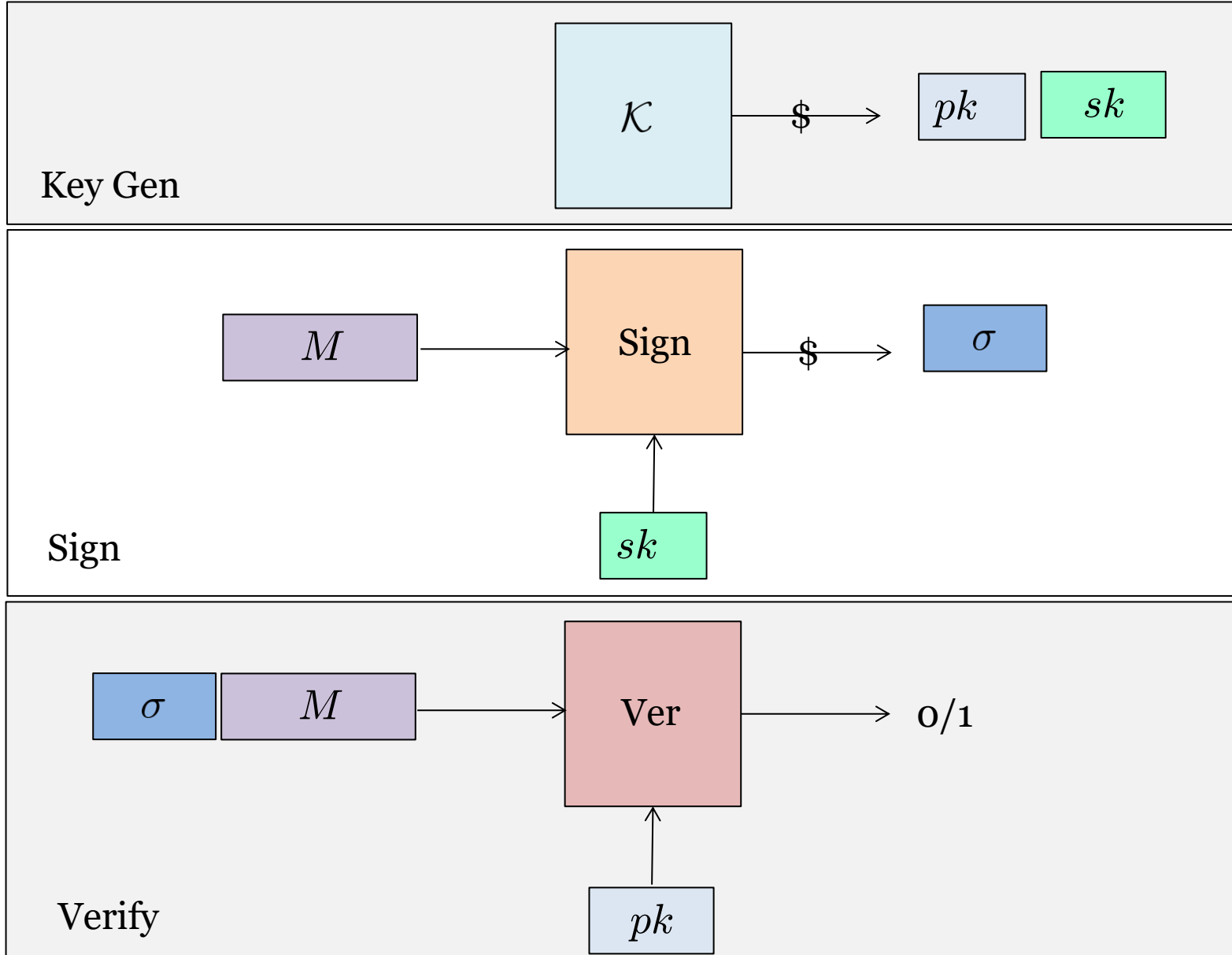
How To Sign Electronically?



Lots of apps to digitize
signatures

Problem: A digitized signature is easily copied → forgery

Digital Signature Scheme: Syntax



Digital Signature versus MAC

MAC

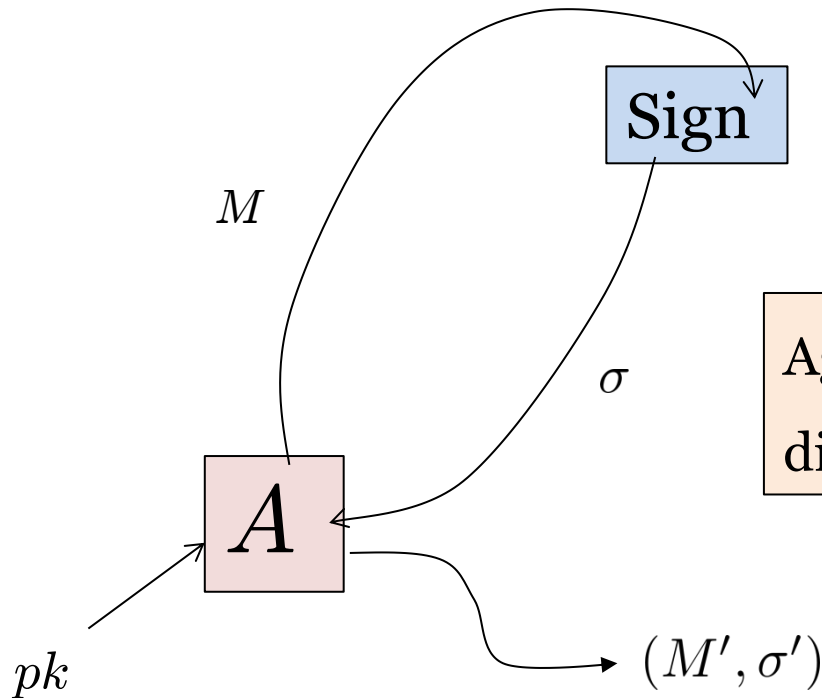
- Verifier needs to share a secret key with signer
- Verifier can impersonate signer

Digital Signature

- Verifier needs no secret
- Verifier cannot impersonate signer

Digital Signature: Unforgeability Security

- Similar to MAC security
- **Difference:** The adversary is given the public key



Again, digital signature doesn't directly thwart replay attack.

Agenda

1.High-level Overview

2.Building Signature Scheme

A Bad Scheme: Plain RSA Signature

Key generation: Like RSA encryption

Sign:

- To sign a message, “decrypt” it:

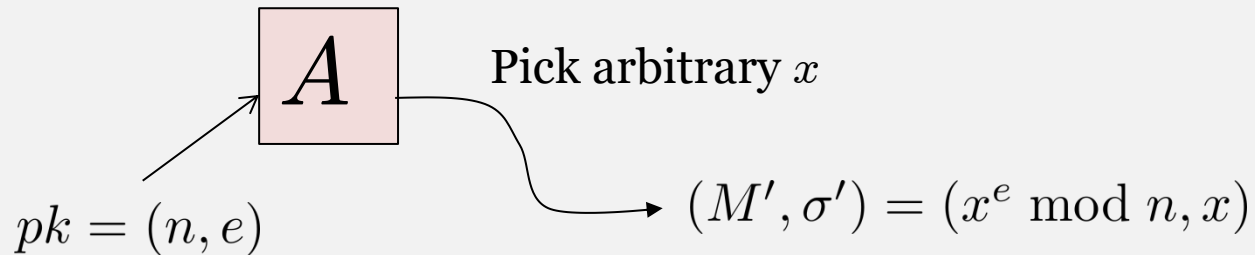
Verify:

- To verify a signature, “encrypt” it and compare with the message

Issues with Plain RSA Signature

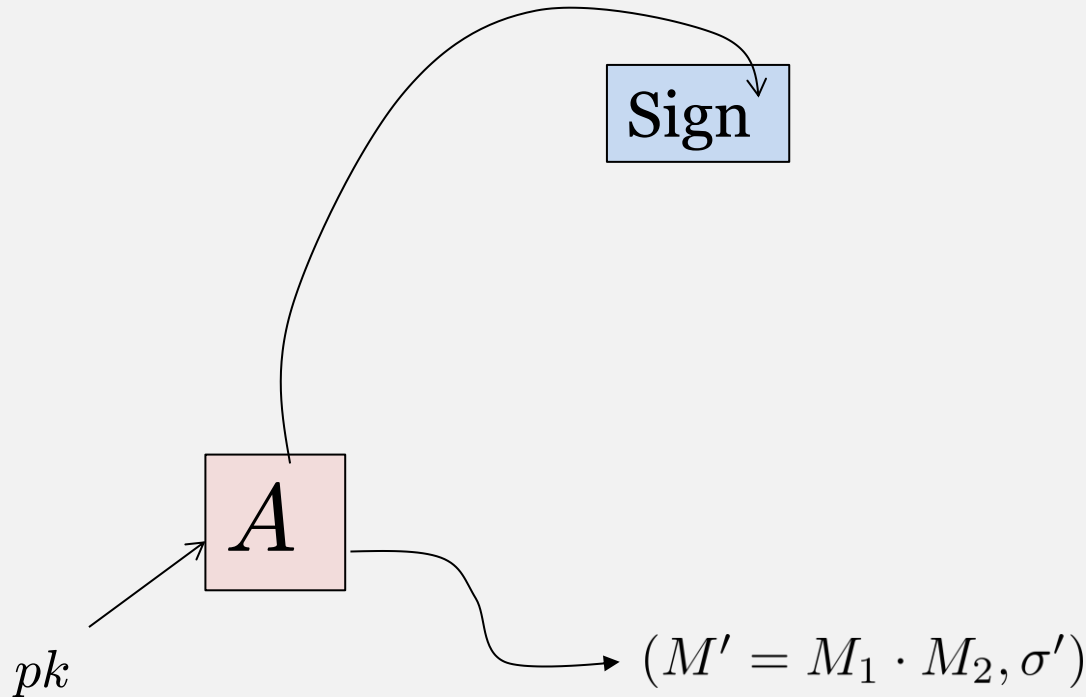
- **Feasibility:** Can sign only short messages
- **Security:** Can easily break unforgeability security

No sign query needed!



Practice: Forging Plain RSA For Targeted Msg

Goal: The forged message must be a **specific** one

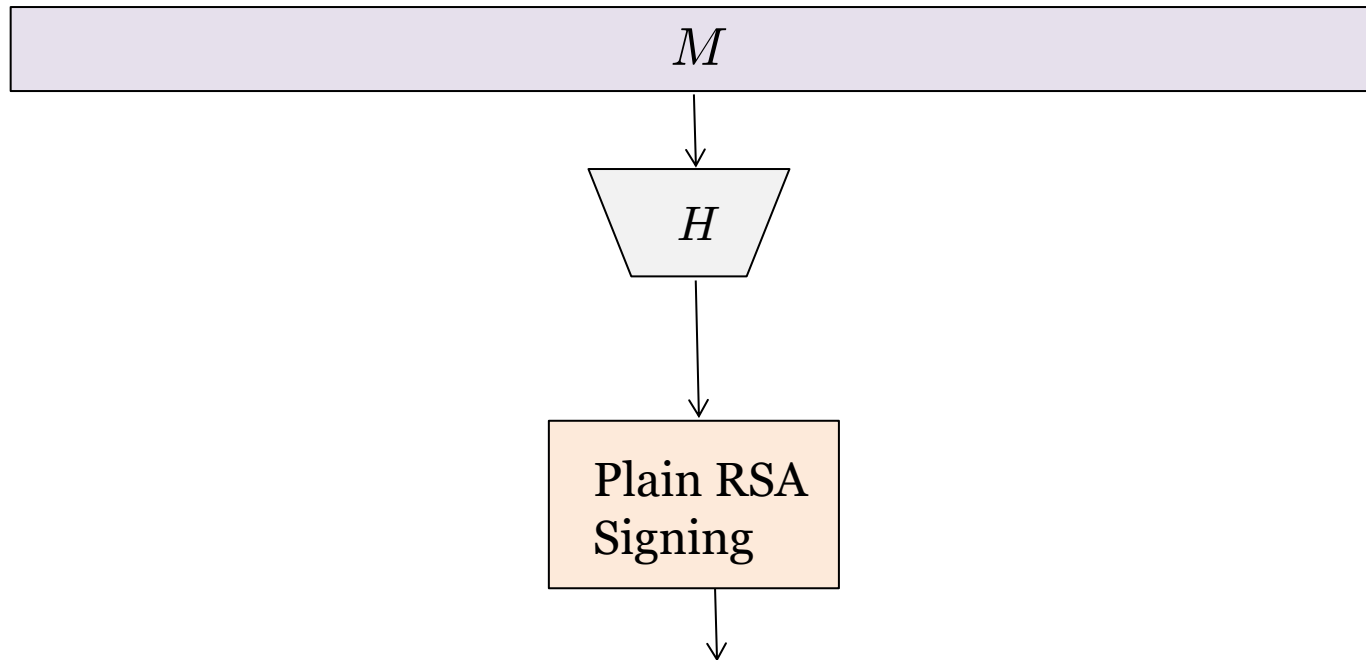


Hash-then-Sign Paradigm

Plain RSA Signature → Full Domain Hash (FDH)

Key generation: Like Plain RSA

Sign: To sign message M



Question: How to verify?

Security Requirement for Hash Function

What intuition suggests: Hash must be collision-resistant

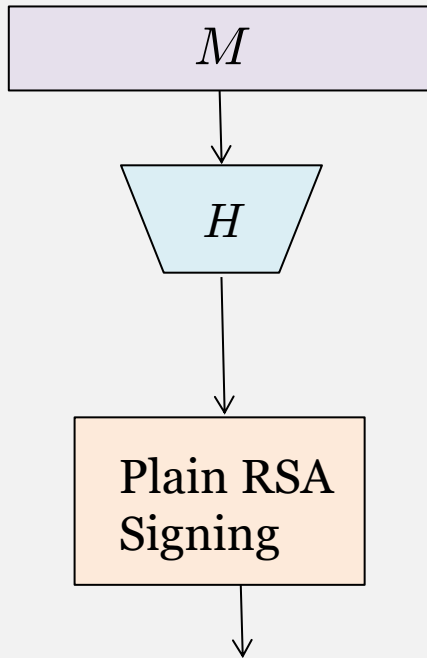
If $H(M) = H(M')$ then M and M' have the same signature

What proof requires: Hash is modeled as a random oracle

A Gap of **Demand** and **Supply**

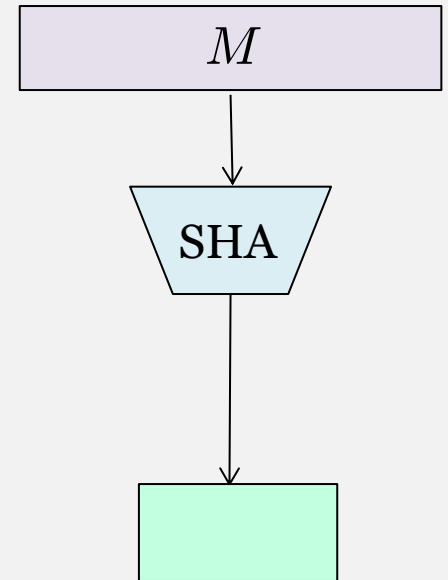
2048

bits of output

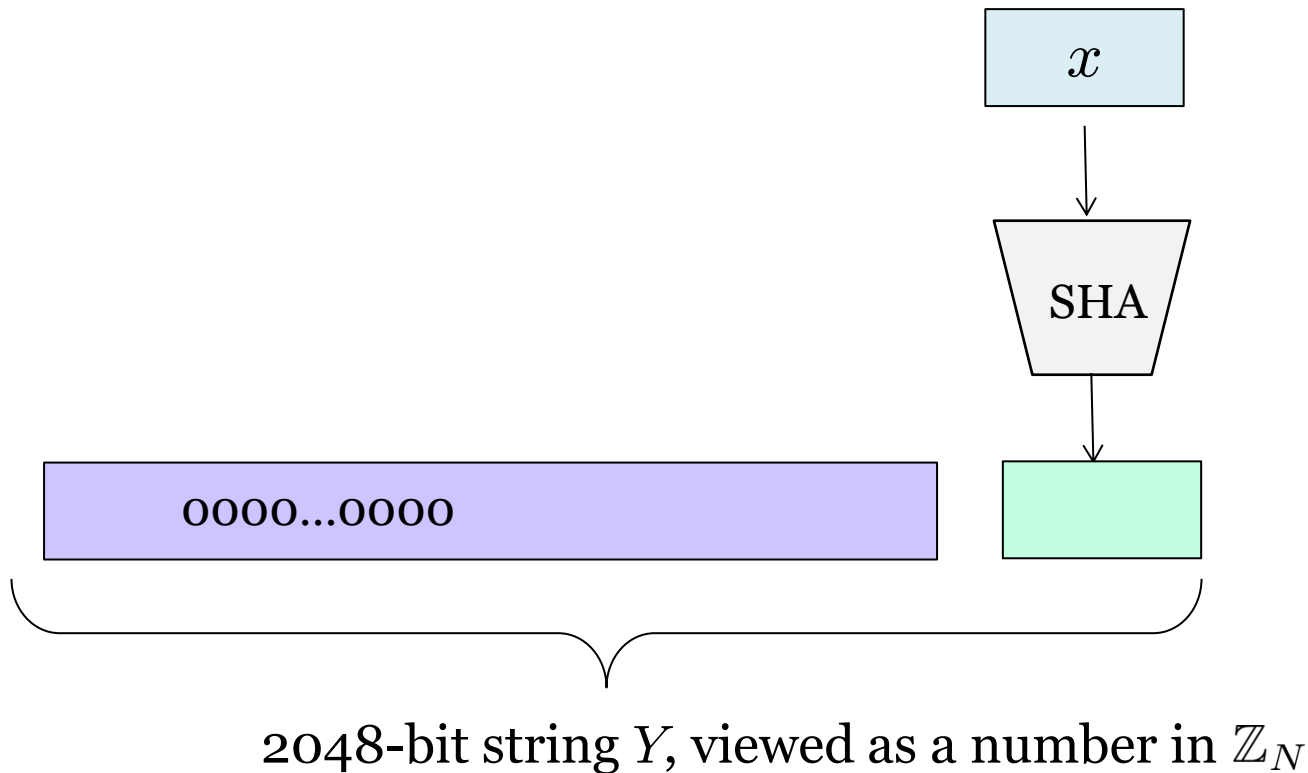


512

bits of output

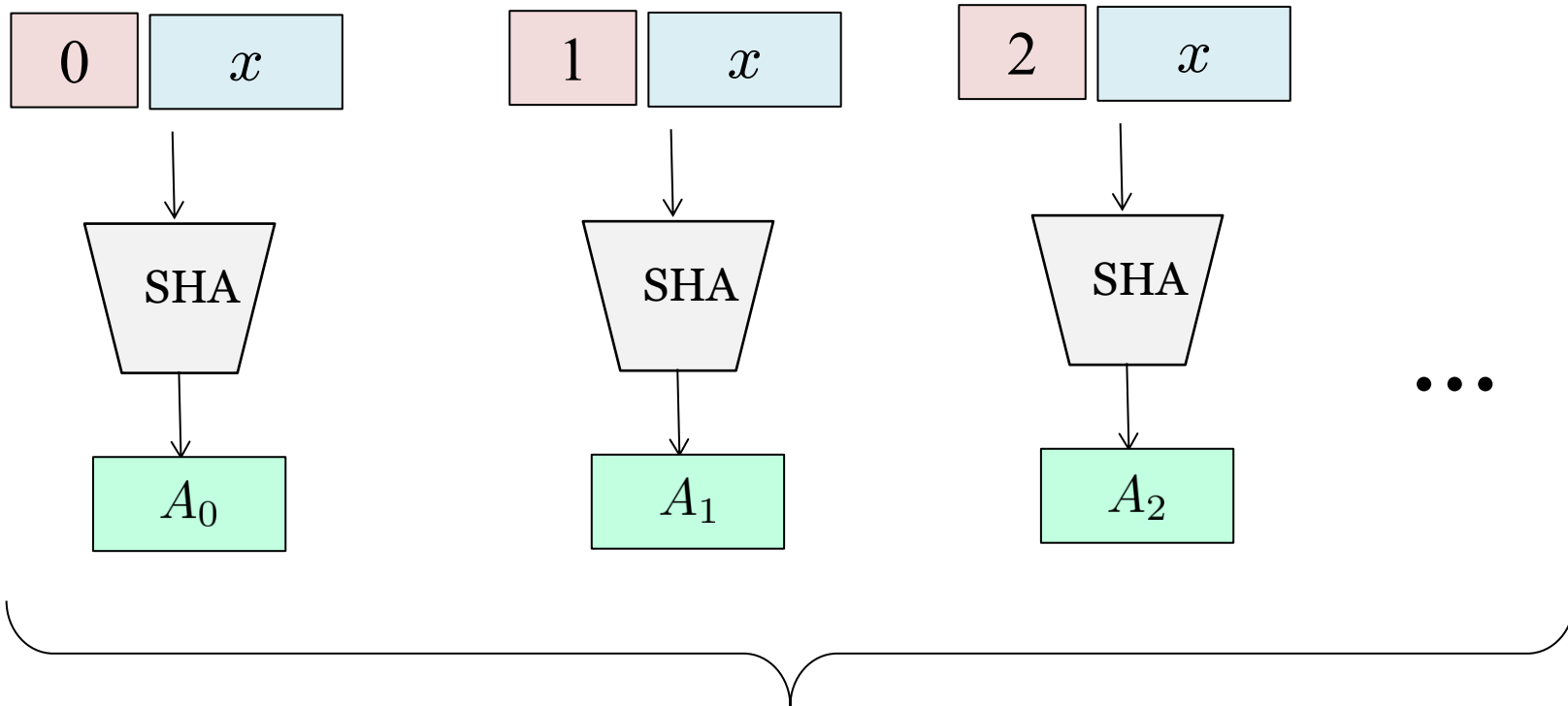


A Common Wrong Way to Hash



Broken by Desmedt and Odlyzko in 1985

How to Hash Properly



Use the first $m = \lceil \log_2(N) \rceil$ bits and take mod N

Hashing in PKCS#1

19 bytes to indicate what hash function and its output length

