CNT 4406, Spring 2024

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

3. Application: DNSSEC

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

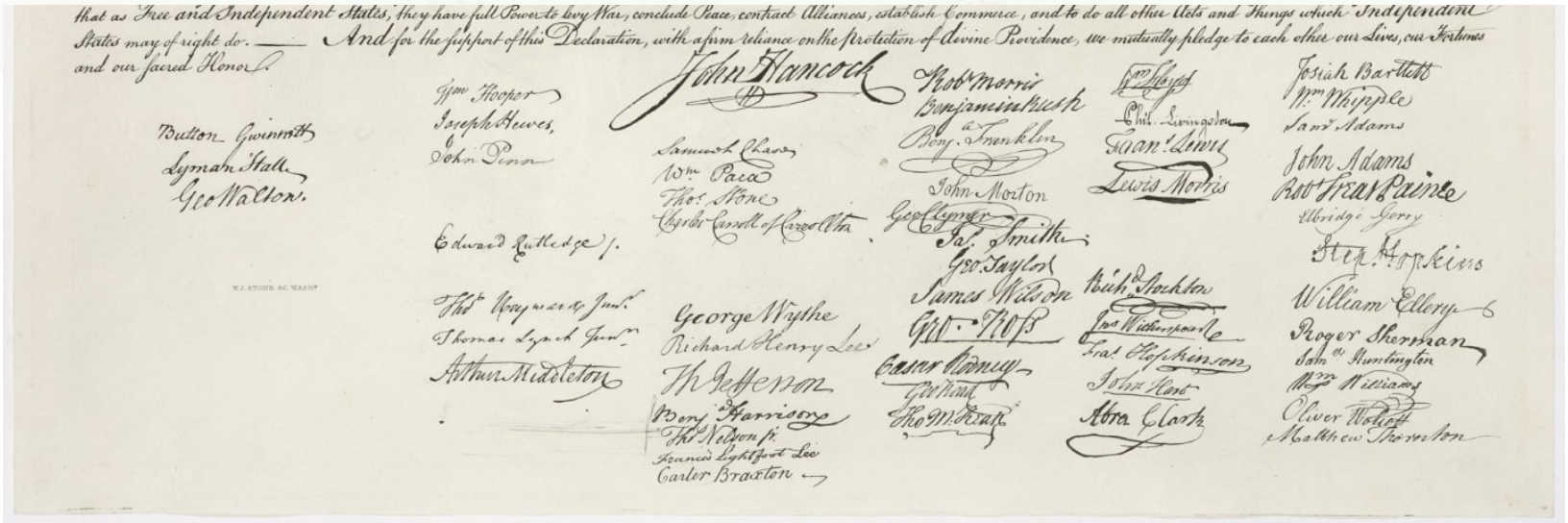
PAY TO THE ORDER OF: Mary Johnson $ 715,39
Seven hundred fifteen and 39/100 DOLLARS

PAYABLE AT
ALL LOREM BANK BRANCHES IN USA
ACCOUNT № 001234567

MEMO Monthly rent

J. Smith
AUTHORIZED SIGNATURE

Adobe Stock | #363410963



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

Button Gwinnett
Lyman Hall
Geo Walton

Wm Hooper
Joseph Hewes
John Penn

Edward Rutledge

Thos Heyward Junr
Thomas Lynch Junr
Arthur Middleton

Samuel Chase
Wm Paca
Thos Stone
Charles Carroll of Carrollton

George Wythe
Richard Henry Lee
Th Jefferson
Benj Harrison
Thos Nelson Jr.
Francis Lightfoot Lee
Carter Braxton

Robt Morris
Benjamin Rush
Benj Franklin
John Morton
Geo Clymer
Jas Smith
Geo Taylor
James Wilson
Geo Ross

Caesar Rodney
Geo Read
Tho M:Kean

Wm Floyd
Phil. Livingston
Fras. Lewis
Lewis Morris

Richd Stockton
Jno Witherspoon
Fras Hopkinson
John Hart
Abra Clark

Josiah Bartlett
Wm Whipple
Saml Adams

John Adams
Robt Treat Paine
Elbridge Gerry

Step Hopkins
William Ellery

Roger Sherman
Sam'el Huntington
Wm Williams
Oliver Wolcott

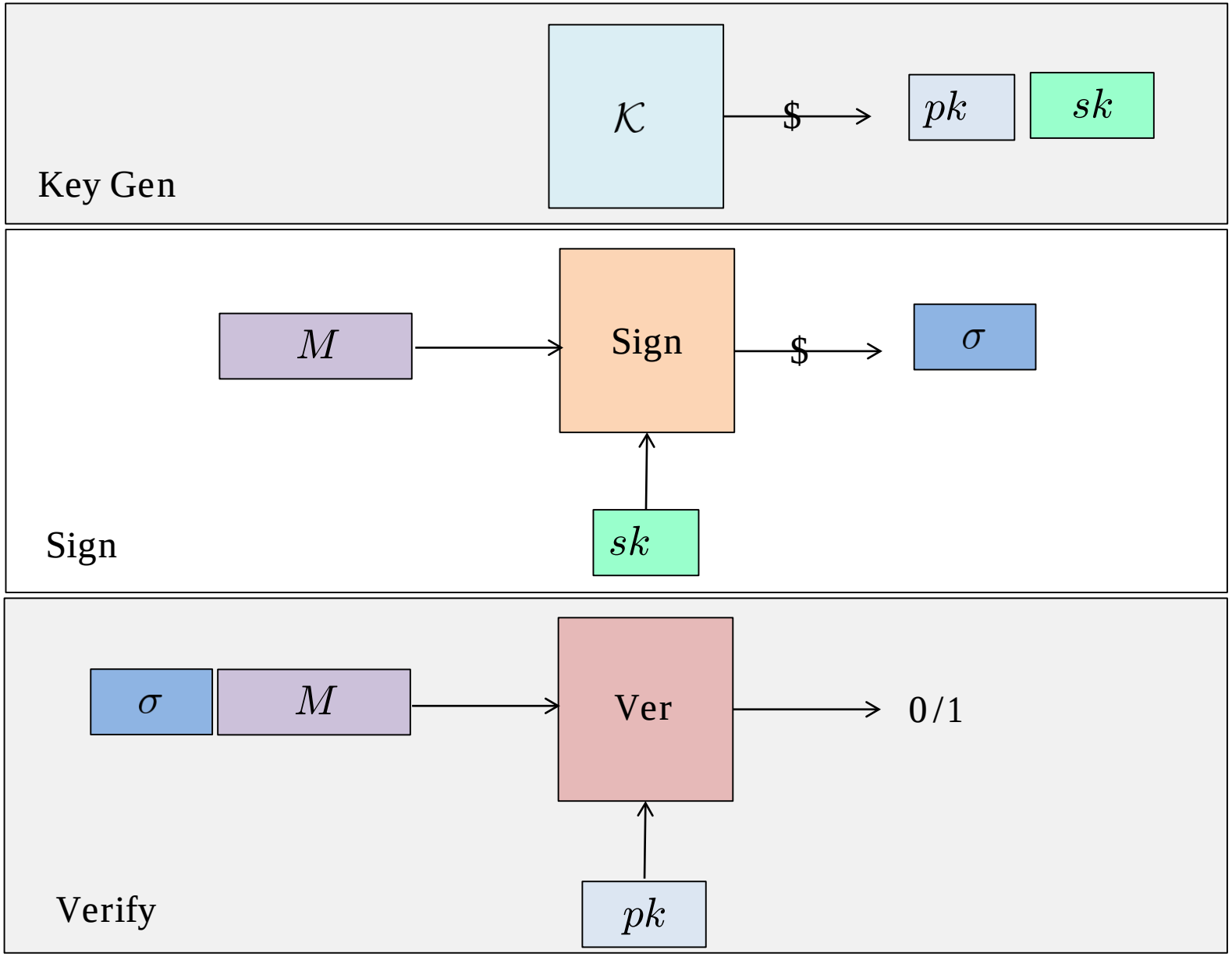
Matthew Thornton

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

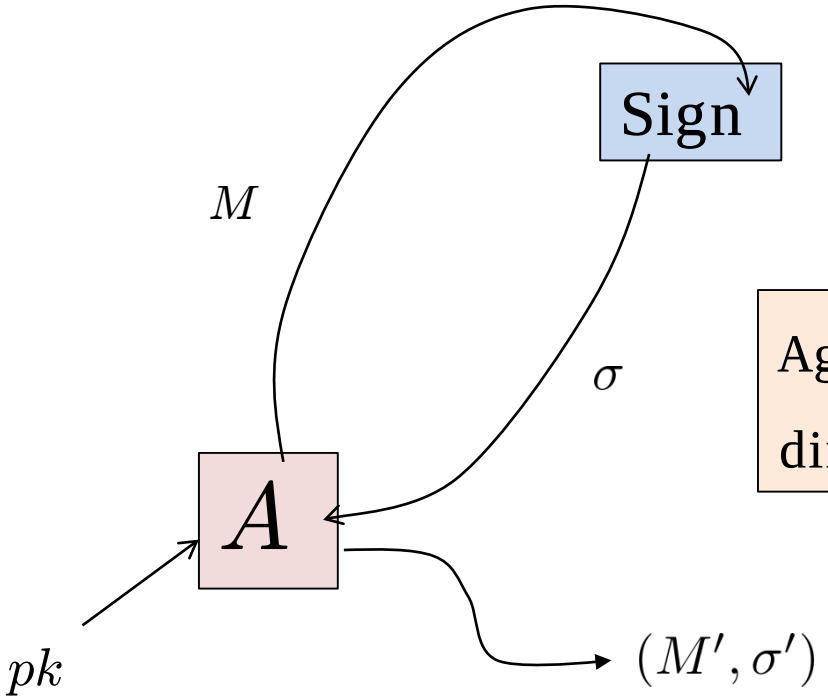
Digital Signature

- 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

3. Application: DNSSEC

A Bad Scheme: Plain RSA Signature

Key generation: Like RSA encryption

Sign:

- To sign a message, “decrypt” it:

Verify:

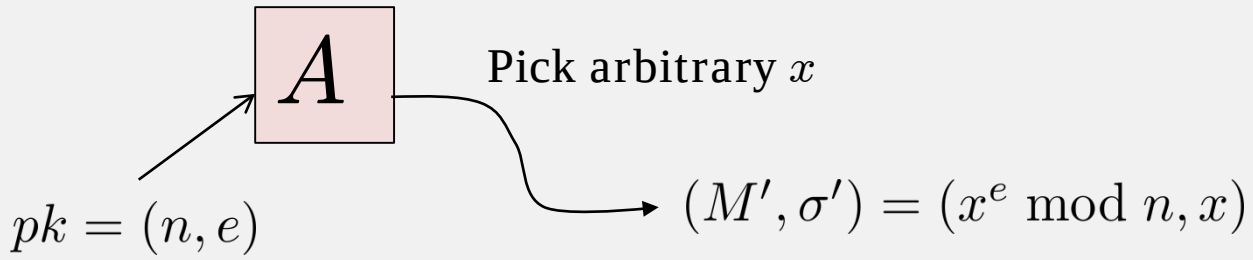
- To verify a signature, “encrypt” it and compare with the message

Issues with Plain RSA Signature

- **Feasibility**: Can sign only short messages

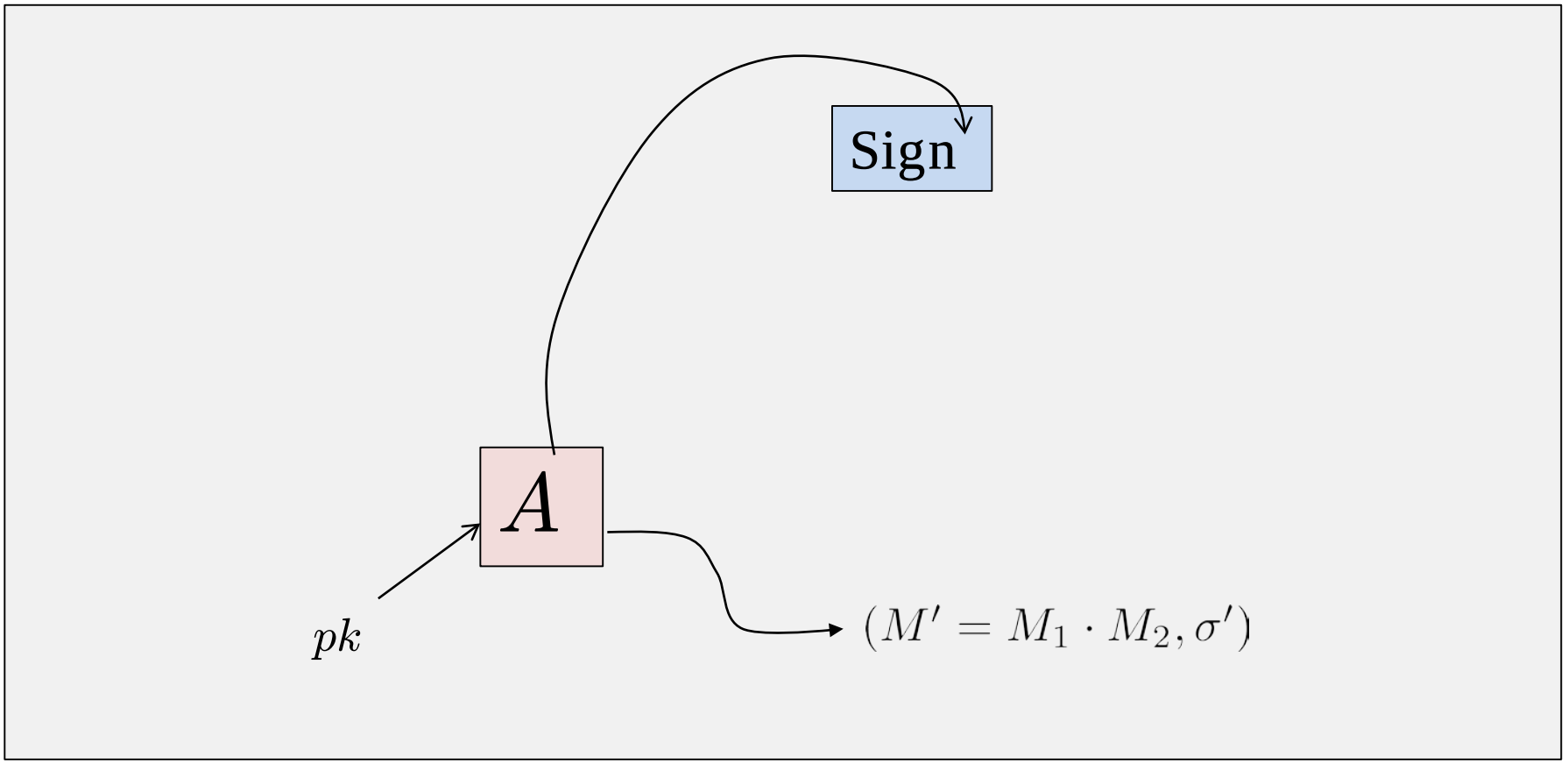
- **Security**: Can easily break unforgeability security

No sign query needed!



Exercise: Forging Plain RSA For Targeted Msg

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

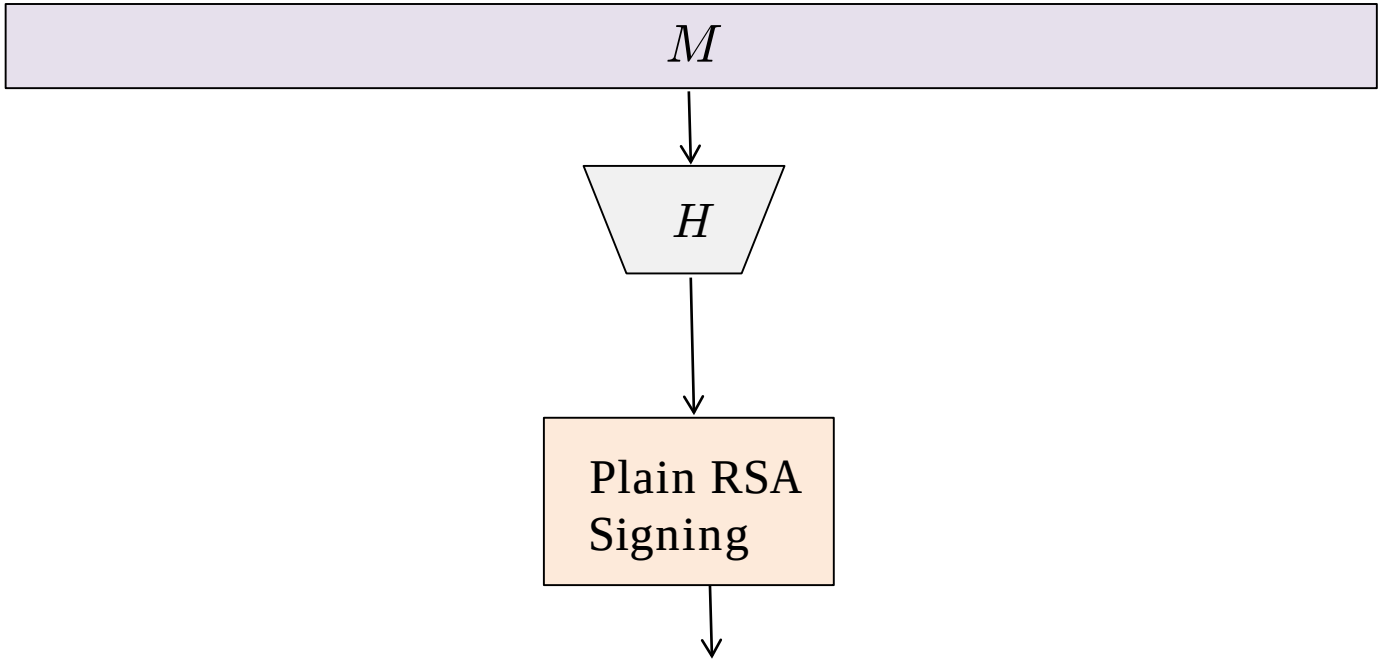


Hash-then-Sign Paradigm

Plain RSA Signature → Full Domain Hash (FDH)

Key generation: Like Plain RSA

Sign: To sign message M



Question: How to verify?

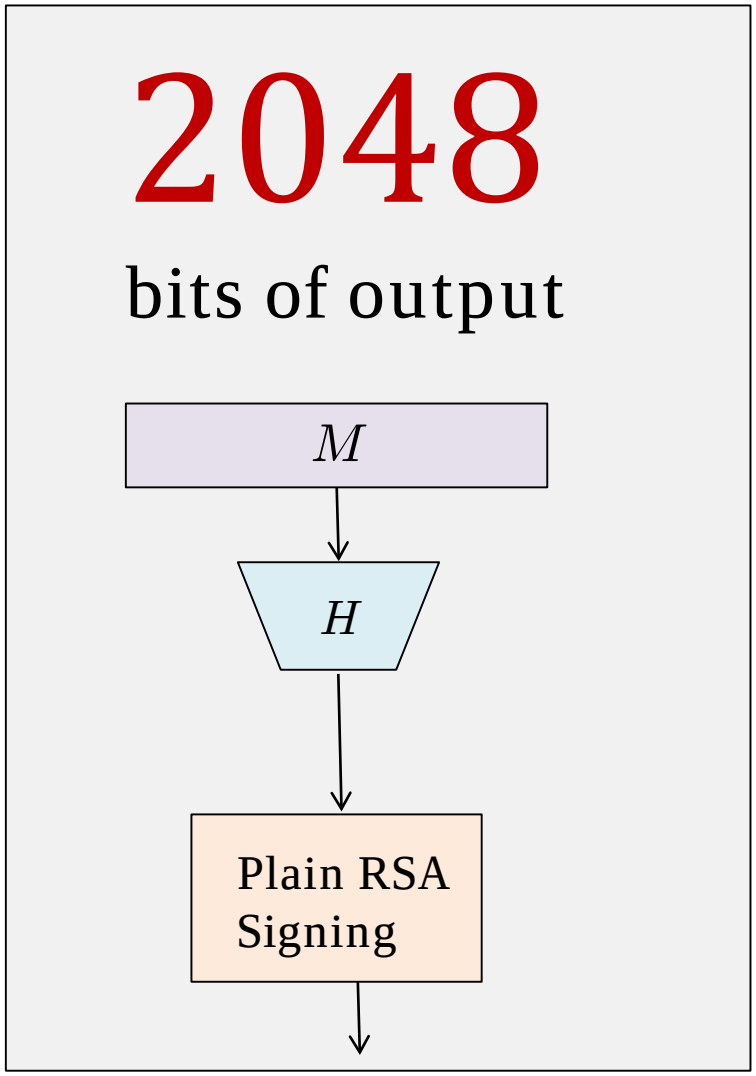
Security Requirement for Hash Function

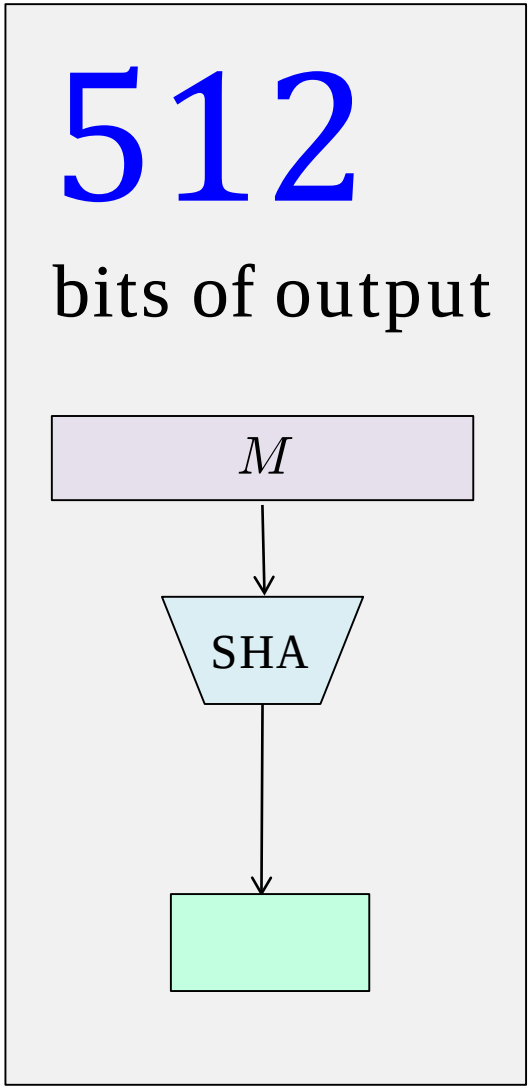
What intuition suggests: Hash must be collision-resistant

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

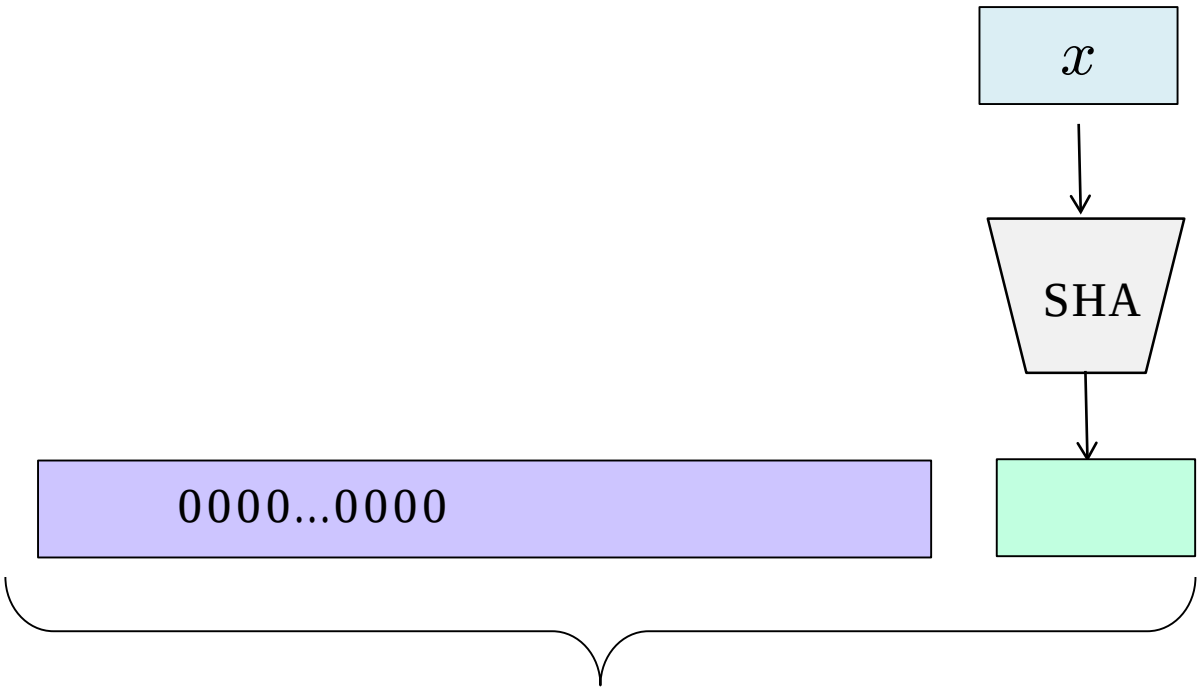
What proof requires: Hash is modeled as a random oracle

A Gap of Demand and Supply





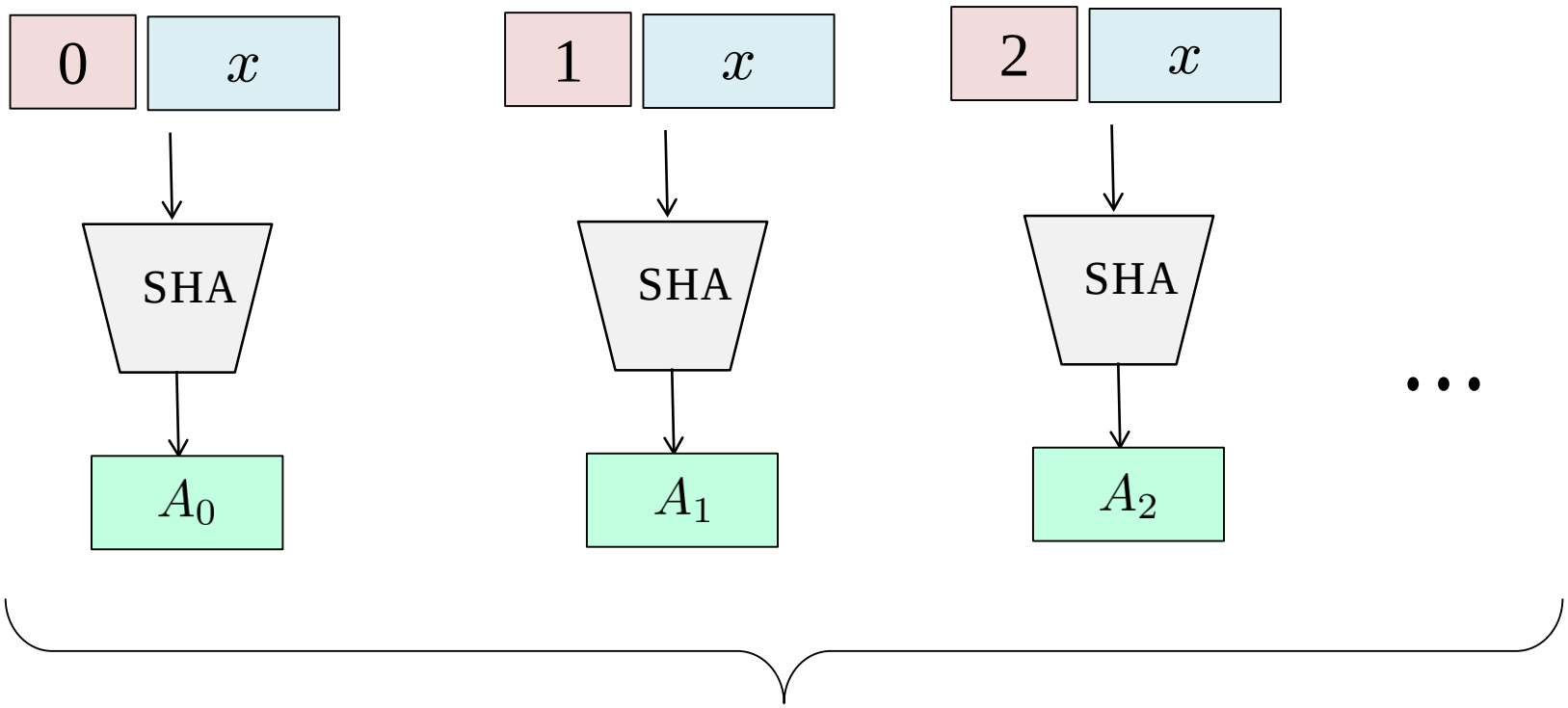
A Common Wrong Way to Hash



2048-bit string Y, viewed as a number in $\mathbb{Z}_N$

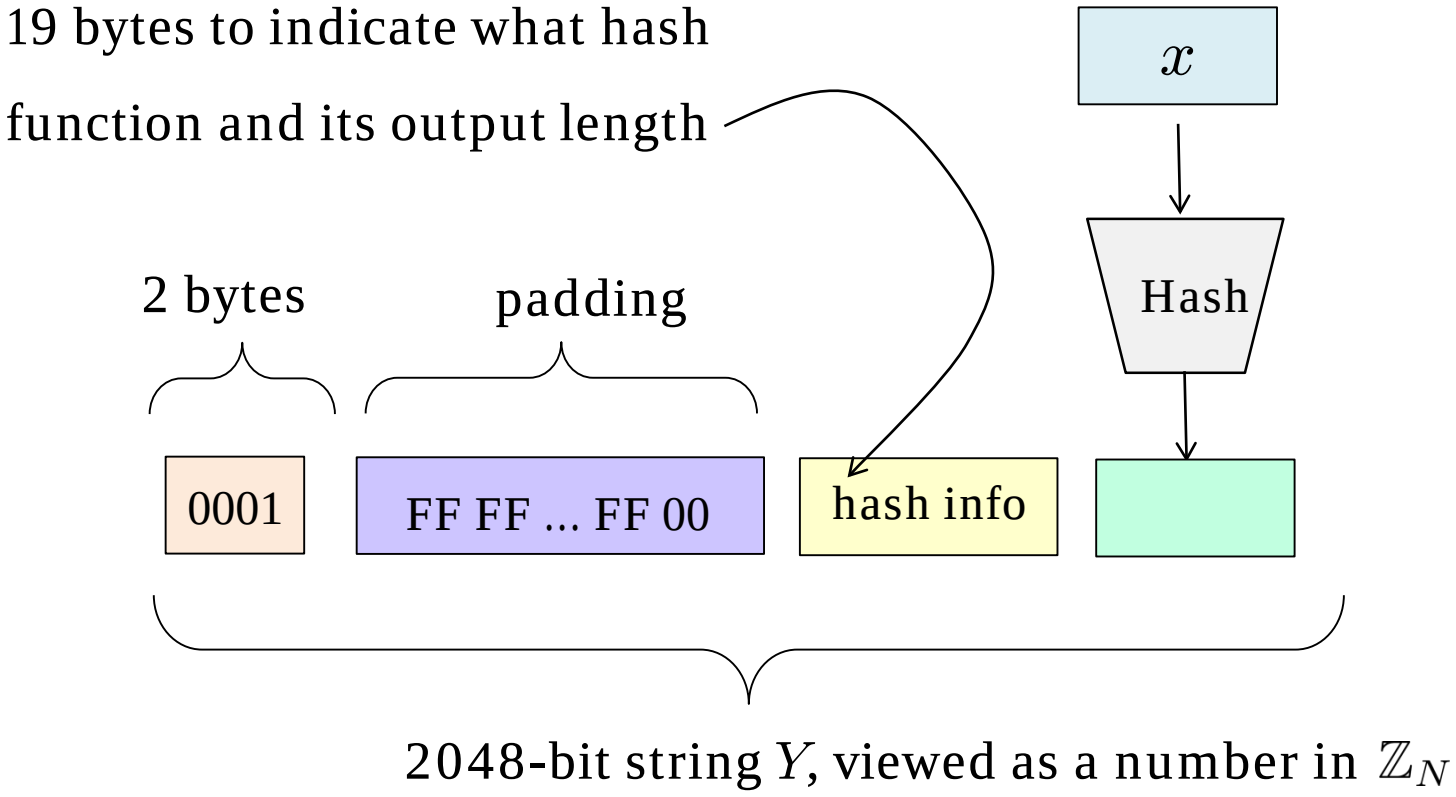
Broken by Desmedt and Odlyzko in 1985

How to Hash Properly



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

Hashing in PKCS#1



Agenda

1. High-level Overview

2. Building Signature Scheme

3. Application: DNSSEC

DNS Recap

Refer to ns1.google.com as

authoritative for google.com

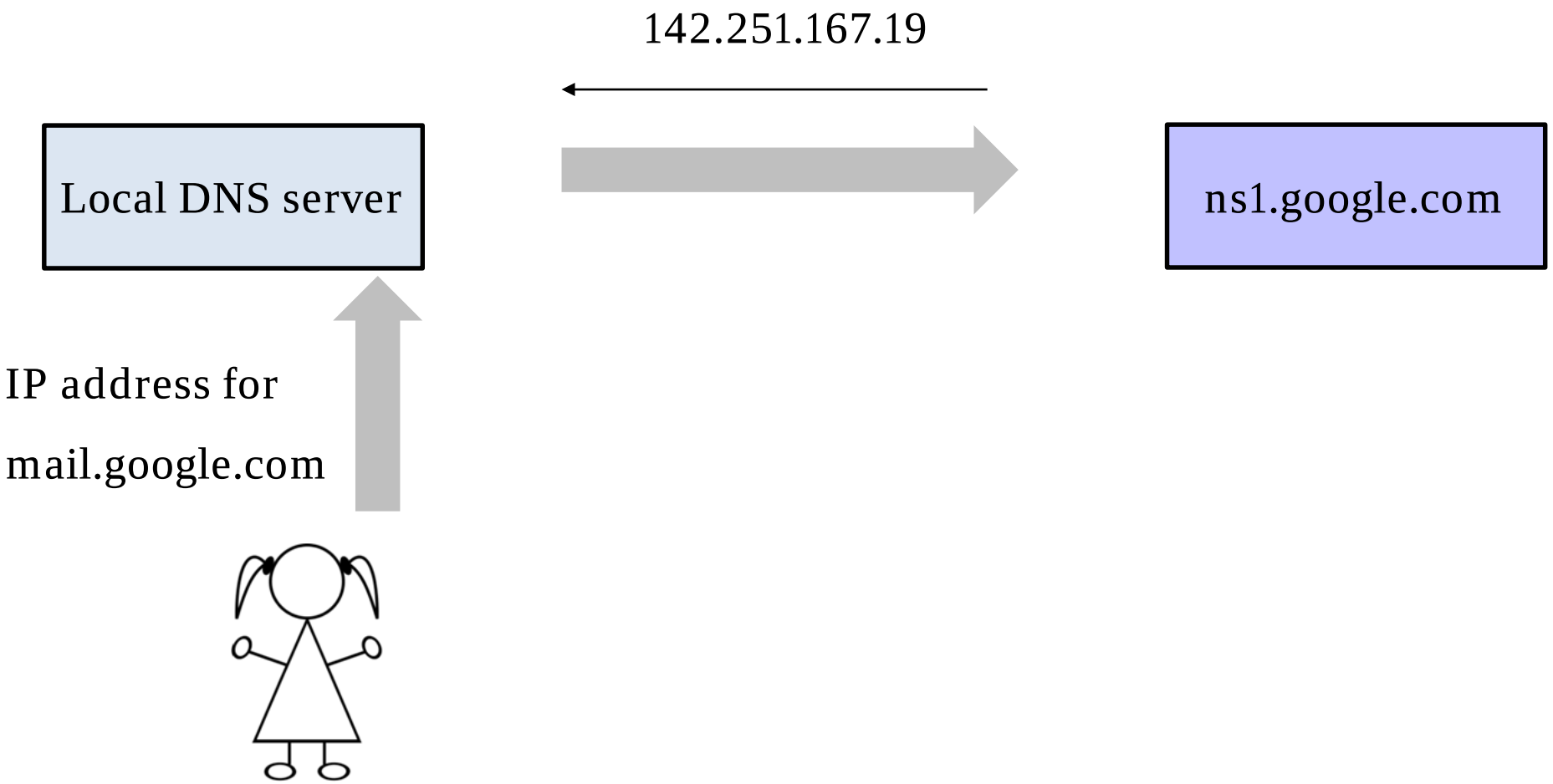
Local DNS server

Root DNS

IP address for

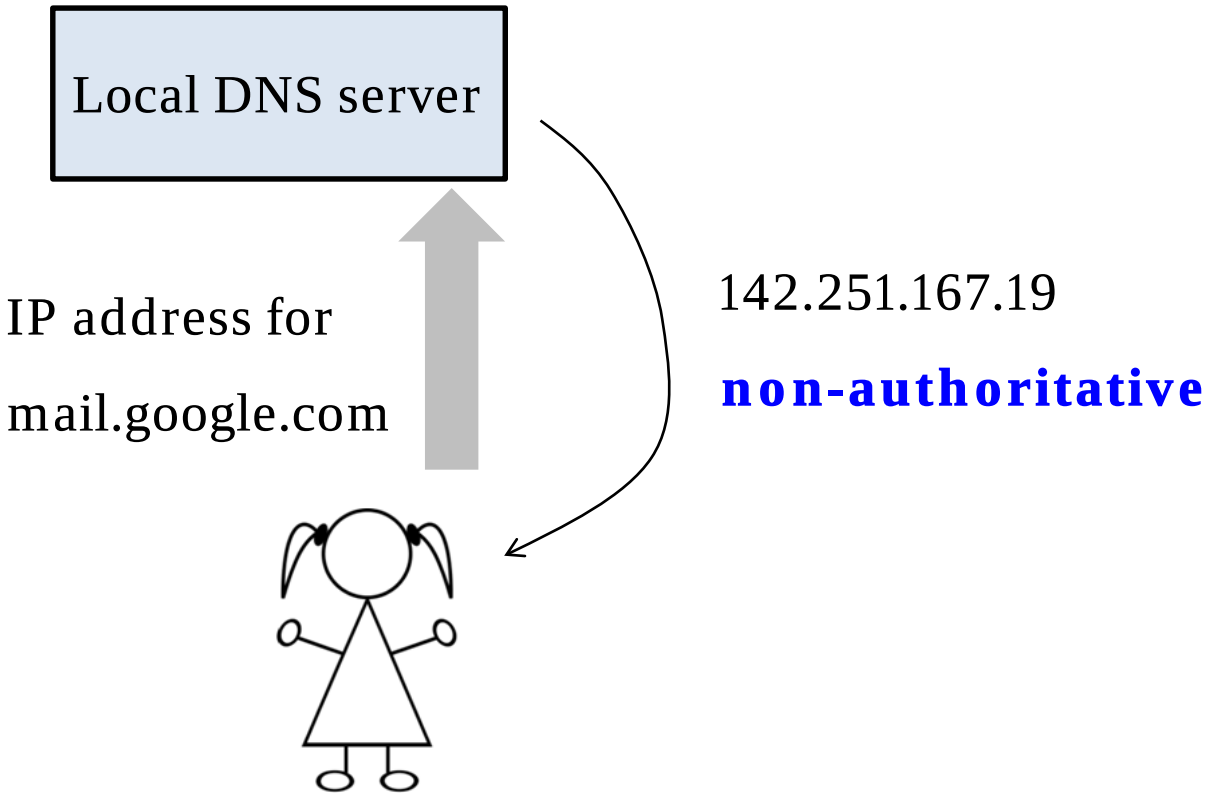
mail.google.com

DNS Recap


142.251.167.19
Local DNS server
ns1.google.com
IP address for
mail.google.com

DNS Recap

Cache info for future queries



DNS Cache Poisoning Attack

Kaminsky, 2008

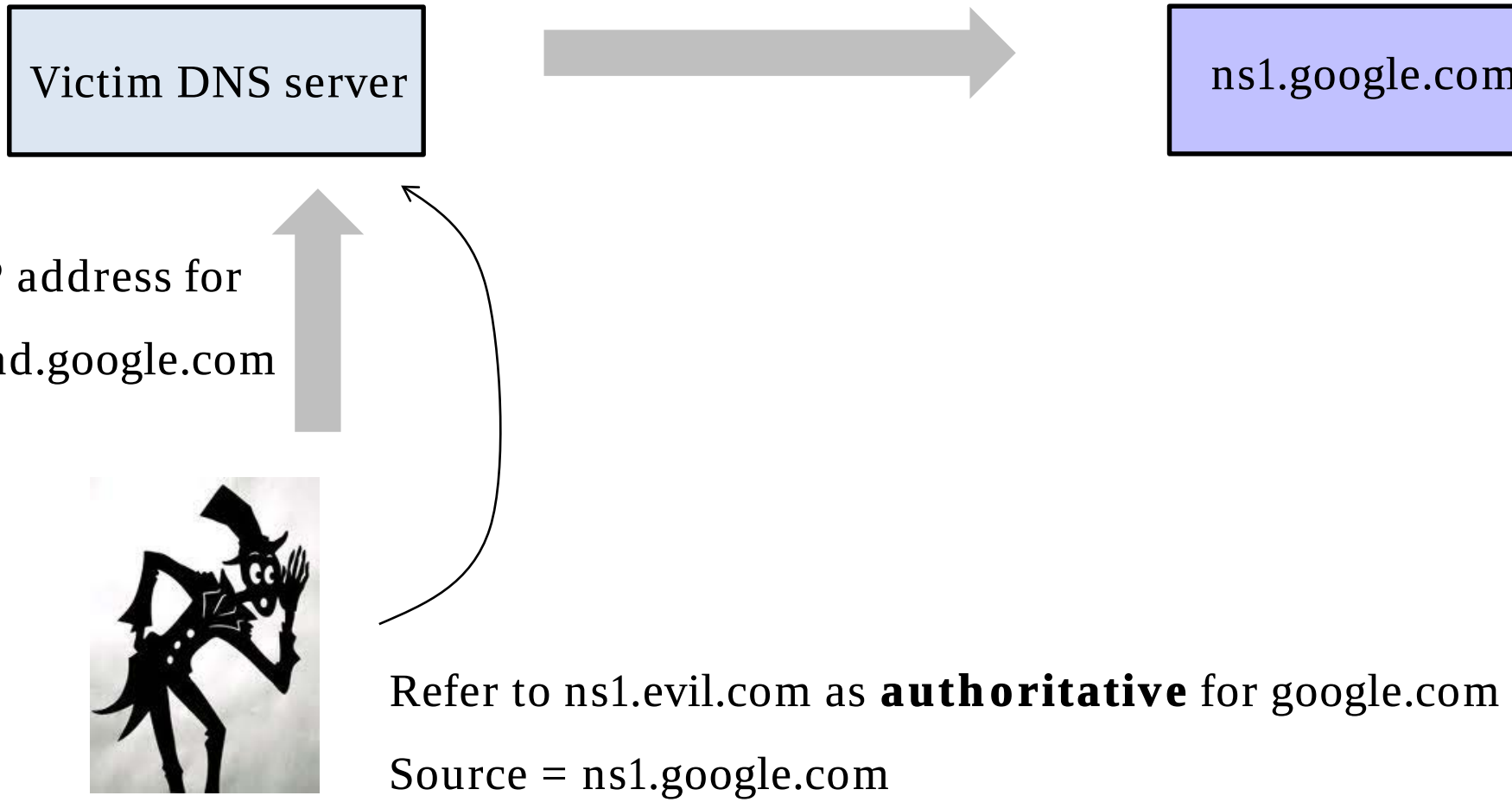
Victim DNS server

IP address for

bad.google.com

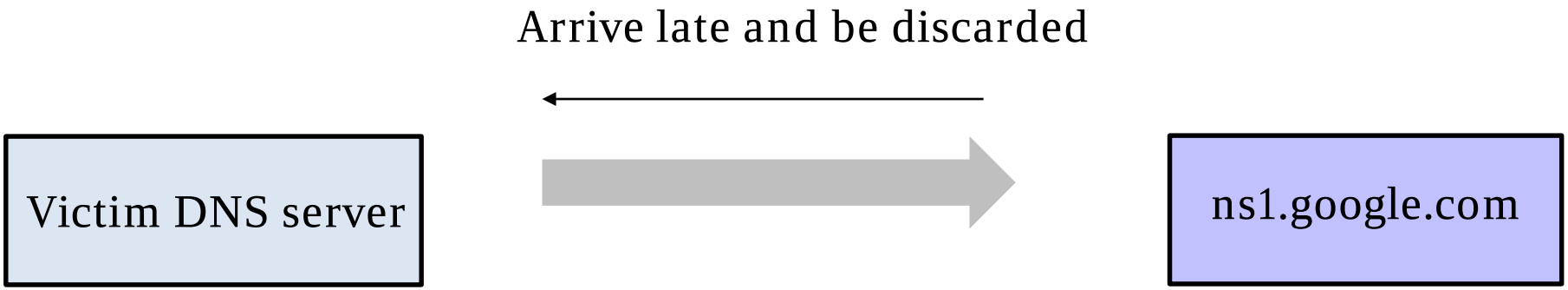
DNS Cache Poisoning Attack

Kaminsky, 2008



DNS Cache Poisoning Attack

Kaminsky, 2008

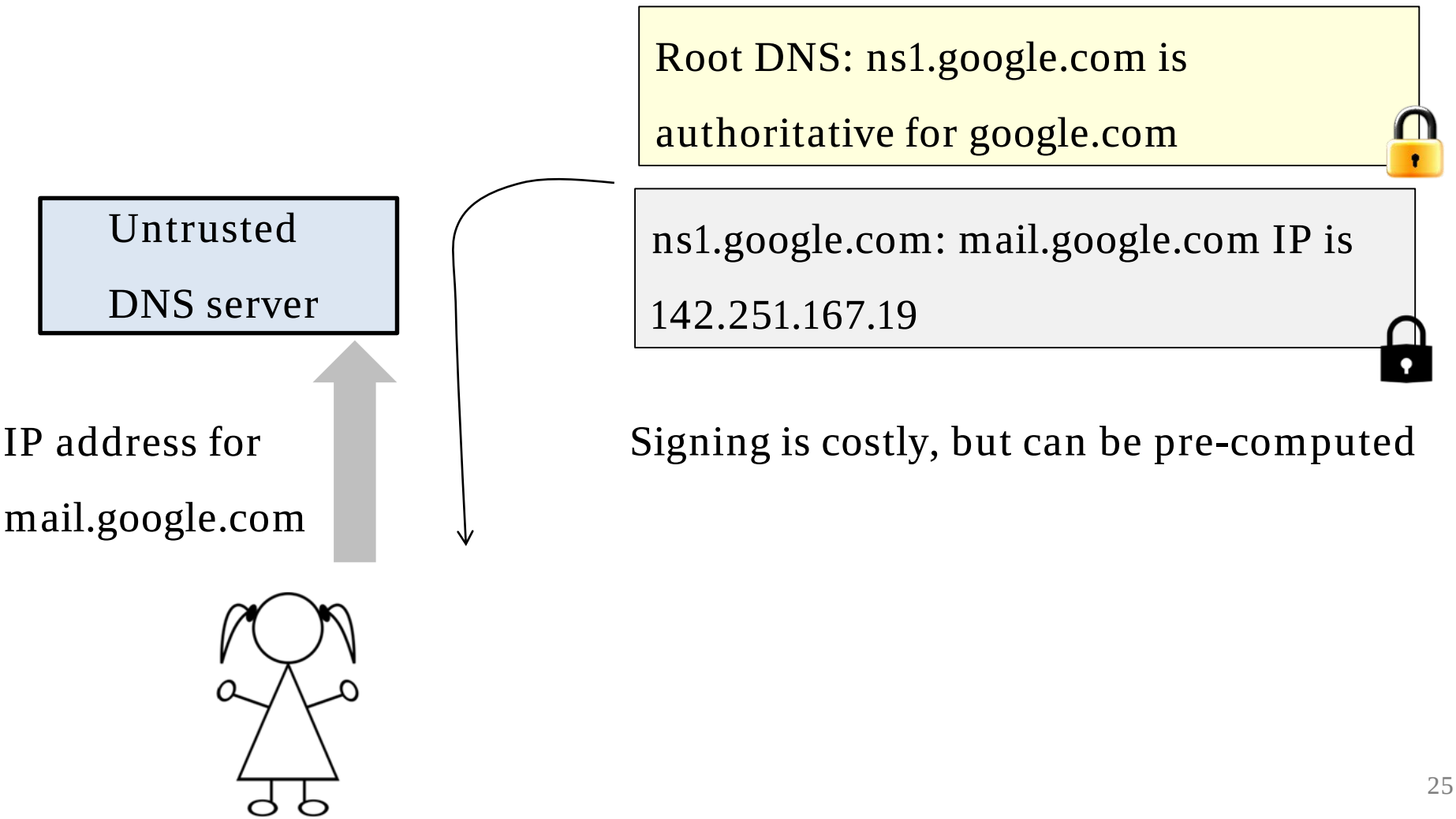


Cache: ns1.evil.com is

authoritative for google.com

The Fix: DNSSEC

DNS replies need to be signed by authority



Thwarting Cache Poisoning Attack

Victim DNS server

Incorrect signature, **reject**

IP address for

bad.google.com

Refer to ns1.evil.com as **authoritative** for google.com

Source = ns1.google.com

Issue: Prove Non-Existence

Untrusted DNS server

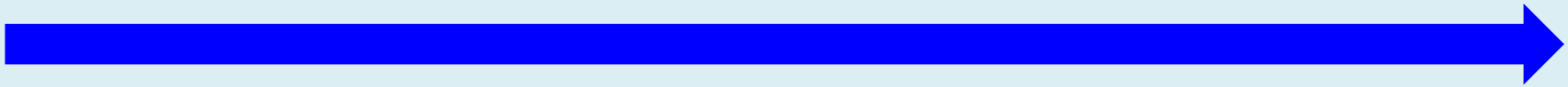
ns1.google.com

IP address for bad.google.com

How to prove non-existence that allows pre-computation?

Proving Non-Existence: Precomputation

Google sorts its subdomain names alphabetically



account chrome mail policies site

Sign every consecutive pairs

google.com account .google.com

account.google.com chrome .google.com

chrome.google.com mail .google.com

Proving Non-Existence: Respond to Query

Unsuccessful Binary Search