

CIS 4360, SPRING 2026

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 NO 0007

DATE: Aug. 11, 2019

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

\$ 715,39
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.

Benton, Gwinnett
Lyman Hall,
Geo. Walton.

John Hooper
Joseph Hewes,
John Peleg

Edward Rutledge Jr.

Thosrd Haynes Jr.
Thomas Lynch Jr.
Arthur Middleton

John Hancock

Samuel Chase

Wm. Paca

Tho: Stone

Abner Gridley of Maryland

Edwrd

Livingston

John Morton

Geord

Smith

Thosrd

Taylor

James Wilson

Richrd

Stockton

Geord

Washington

Thosrd

Hancock

John Hart

Abra

Clark

Matthew Thornton

Oliver

Wolcott

John

Huntington

Geord

Williams

Oliver

Wolcott

Matthew

Thornton

John

Huntington

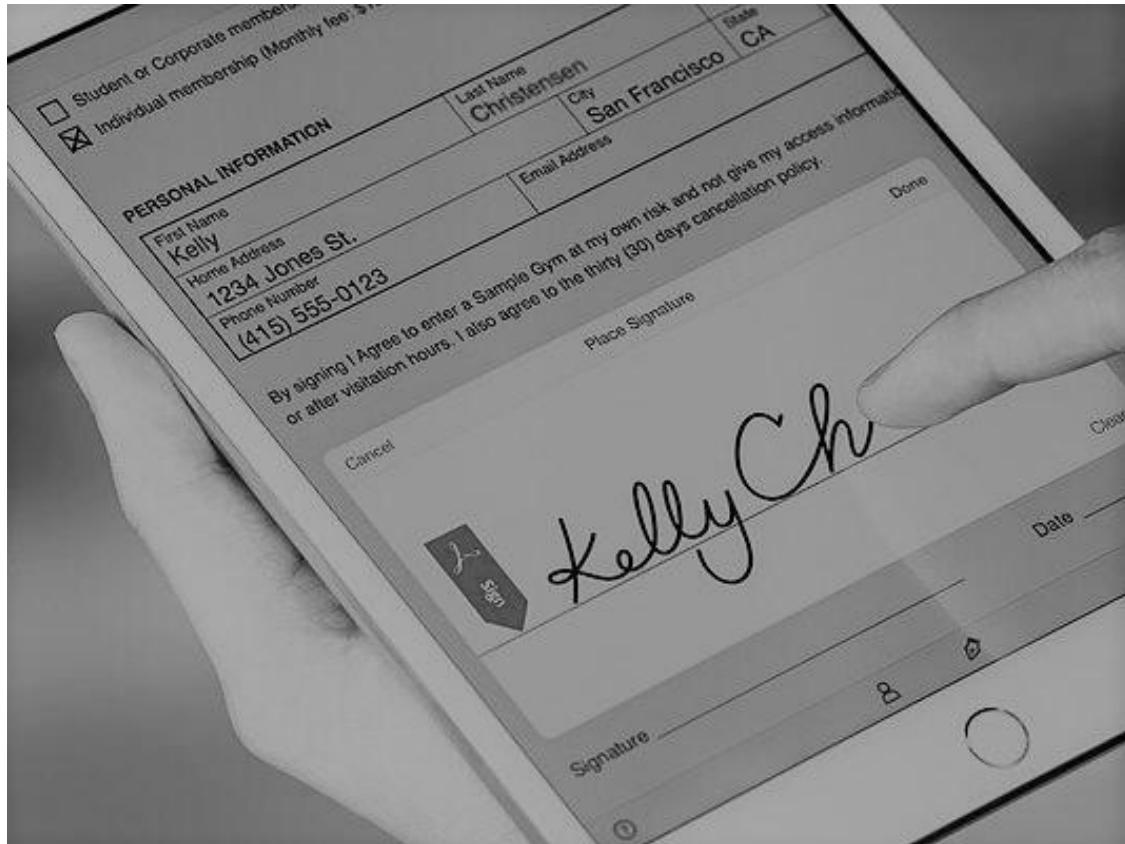
Geord

Williams

Oliver

Wolcott

How To Sign Electronically?

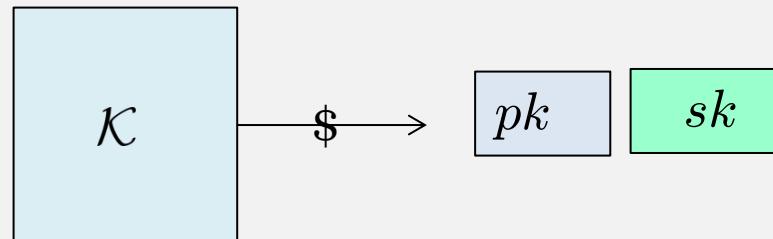


Lots of apps to digitize signatures

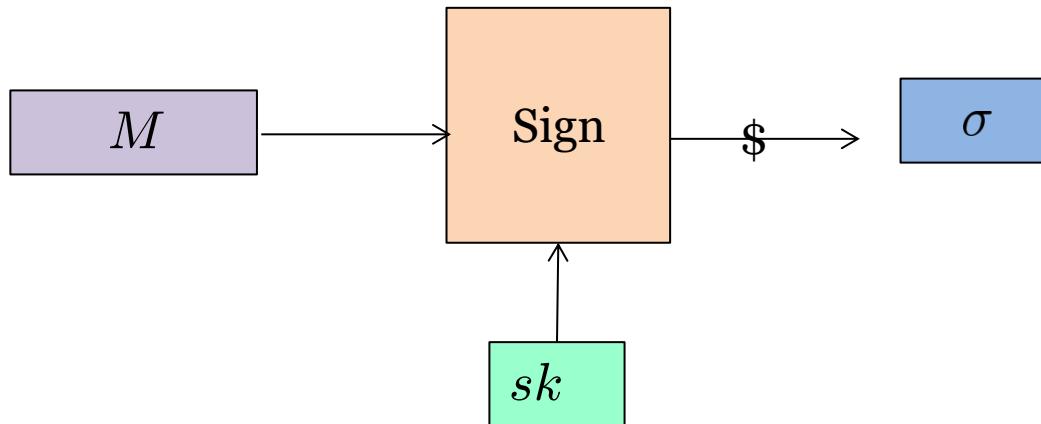
Problem: A digitized signature is easily copied → forgery

Digital Signature Scheme: Syntax

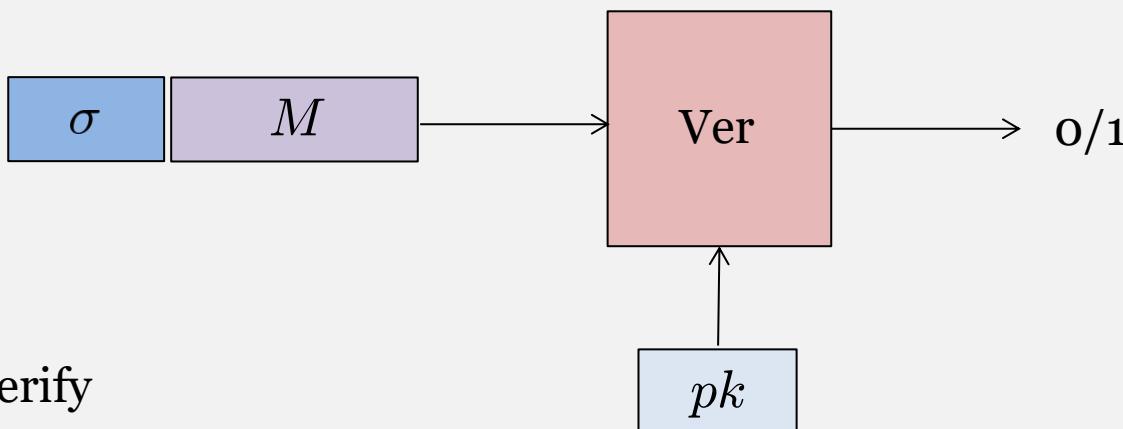
Key Gen



Sign



Verify



Digital Signature versus MAC

MAC

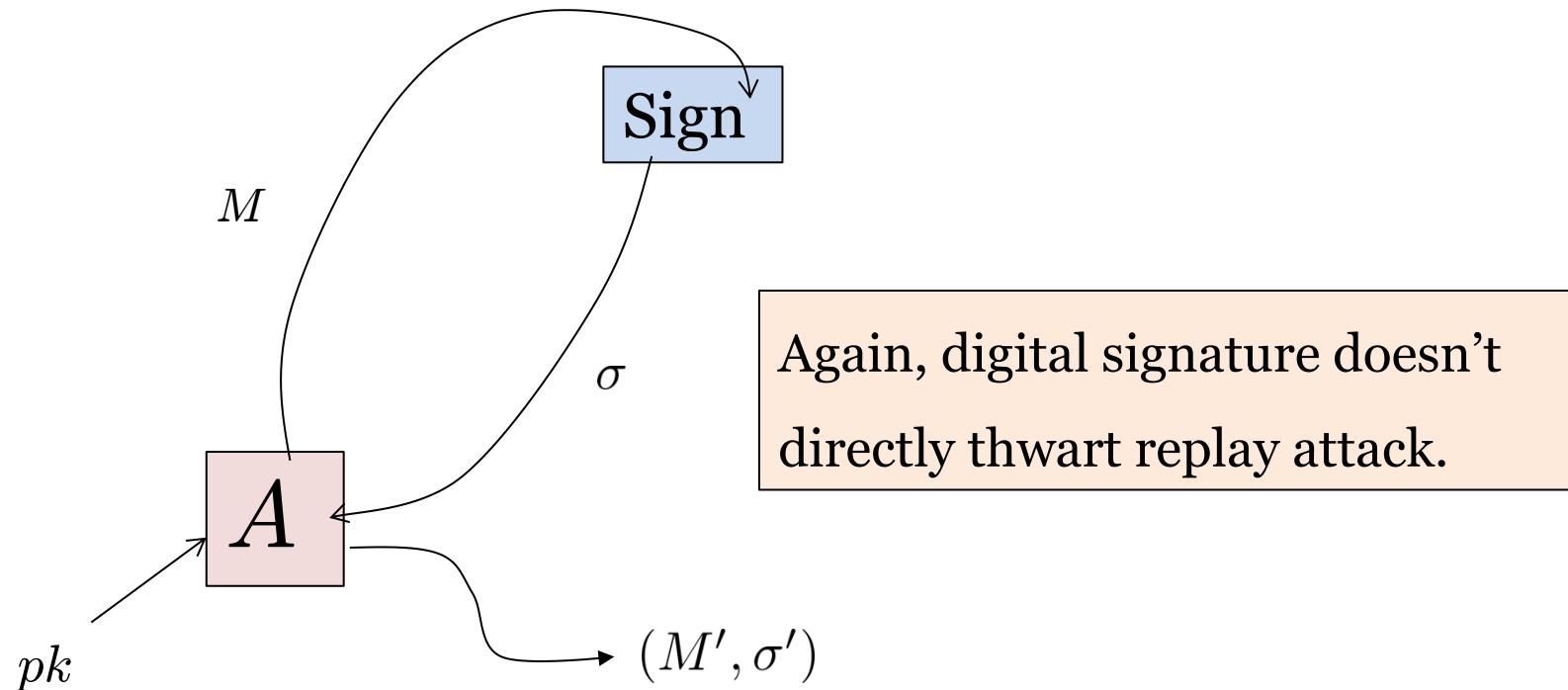
- Verifier needs to share a secret key with signer
- Verifier can impersonate signer

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



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:

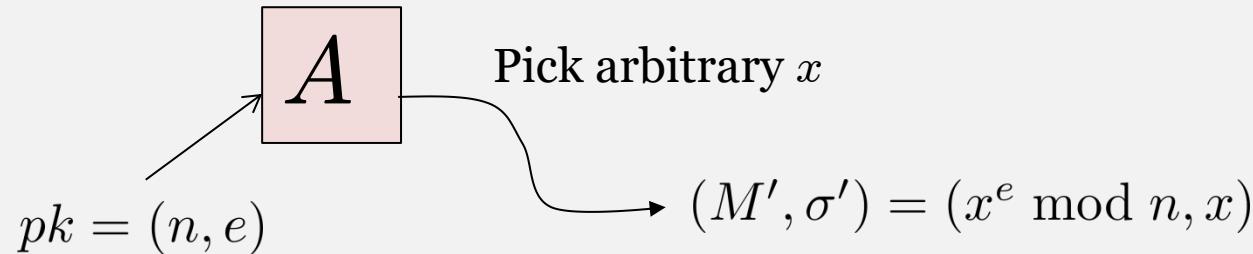
Verify:

- 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!

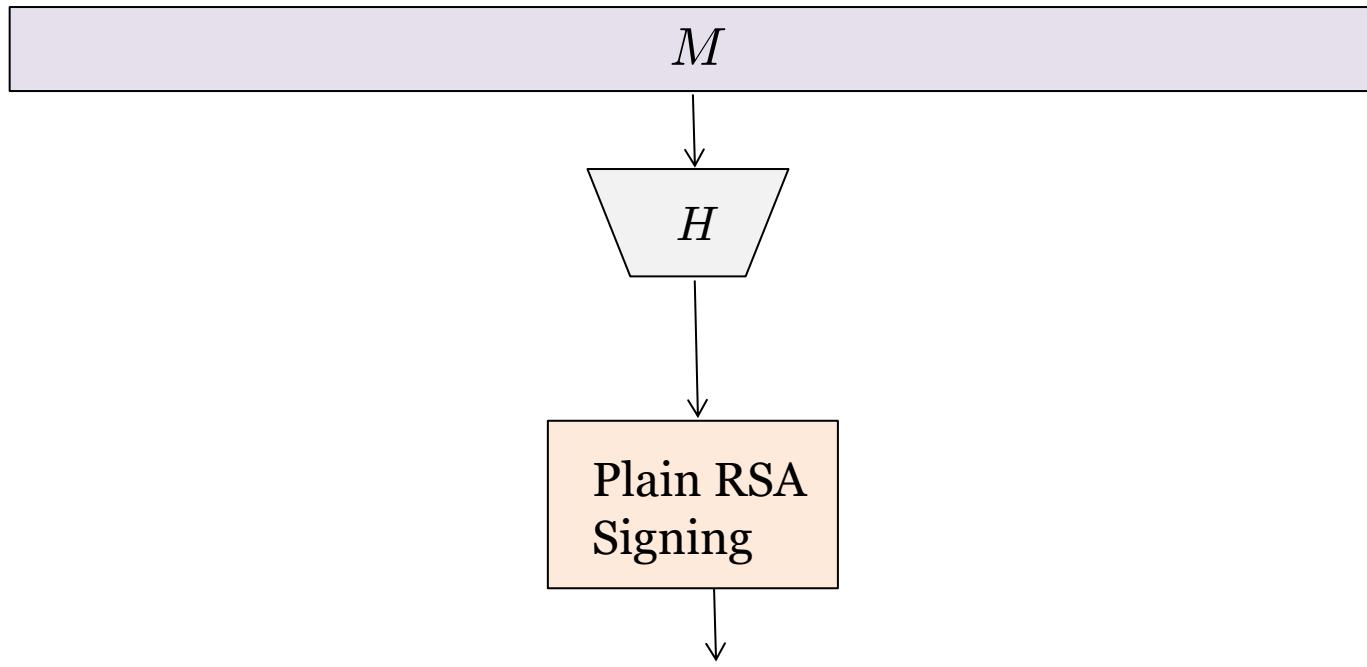


Hash-then-Sign Paradigm

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

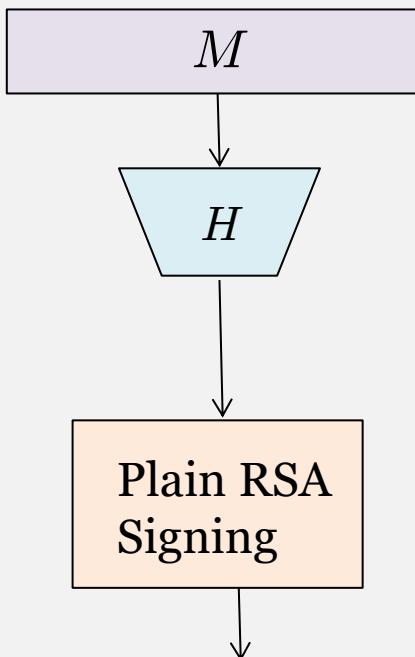
If $H(M) = H(M')$ then M and M' have the same signature

What proof requires: Hash is modeled as a random oracle

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

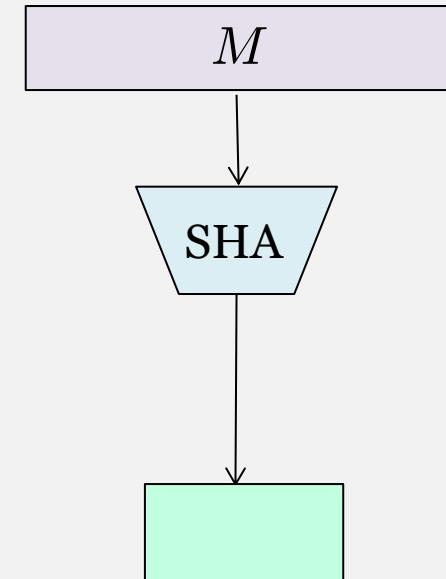
2048

bits of output

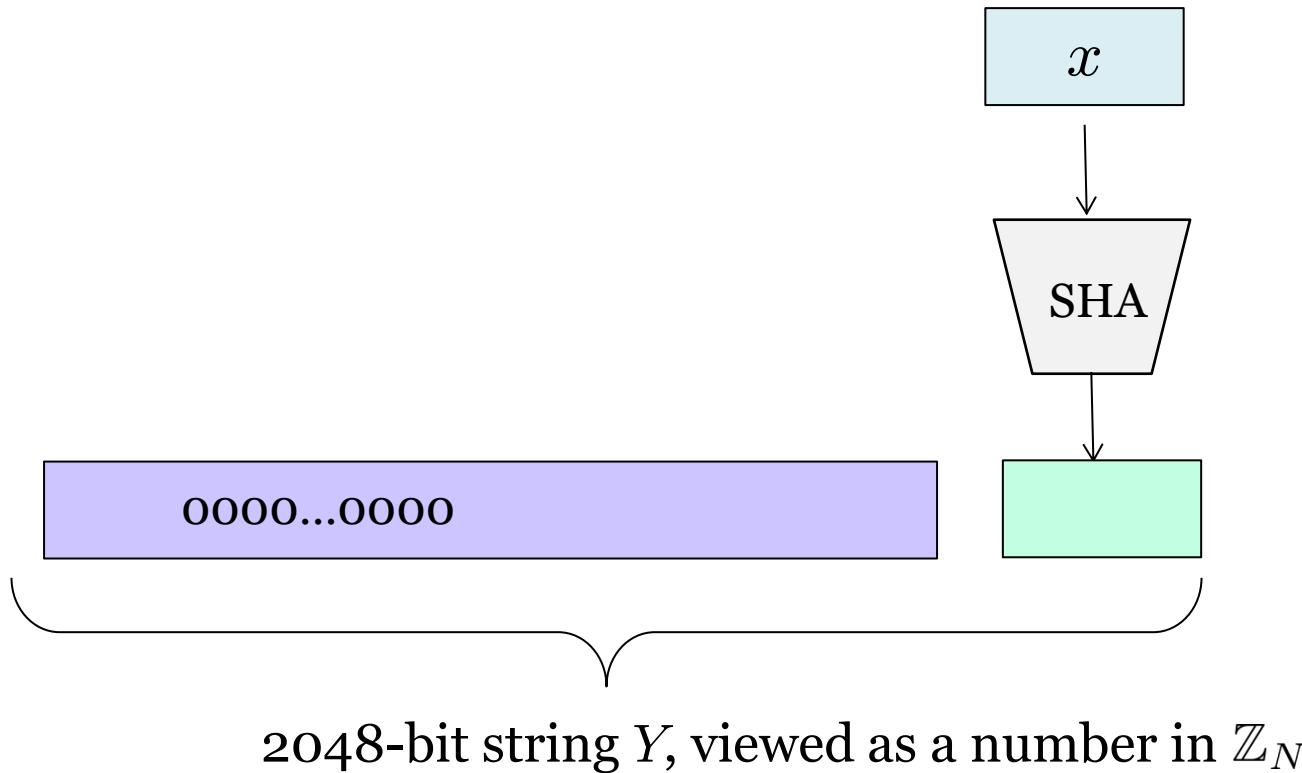


512

bits of output

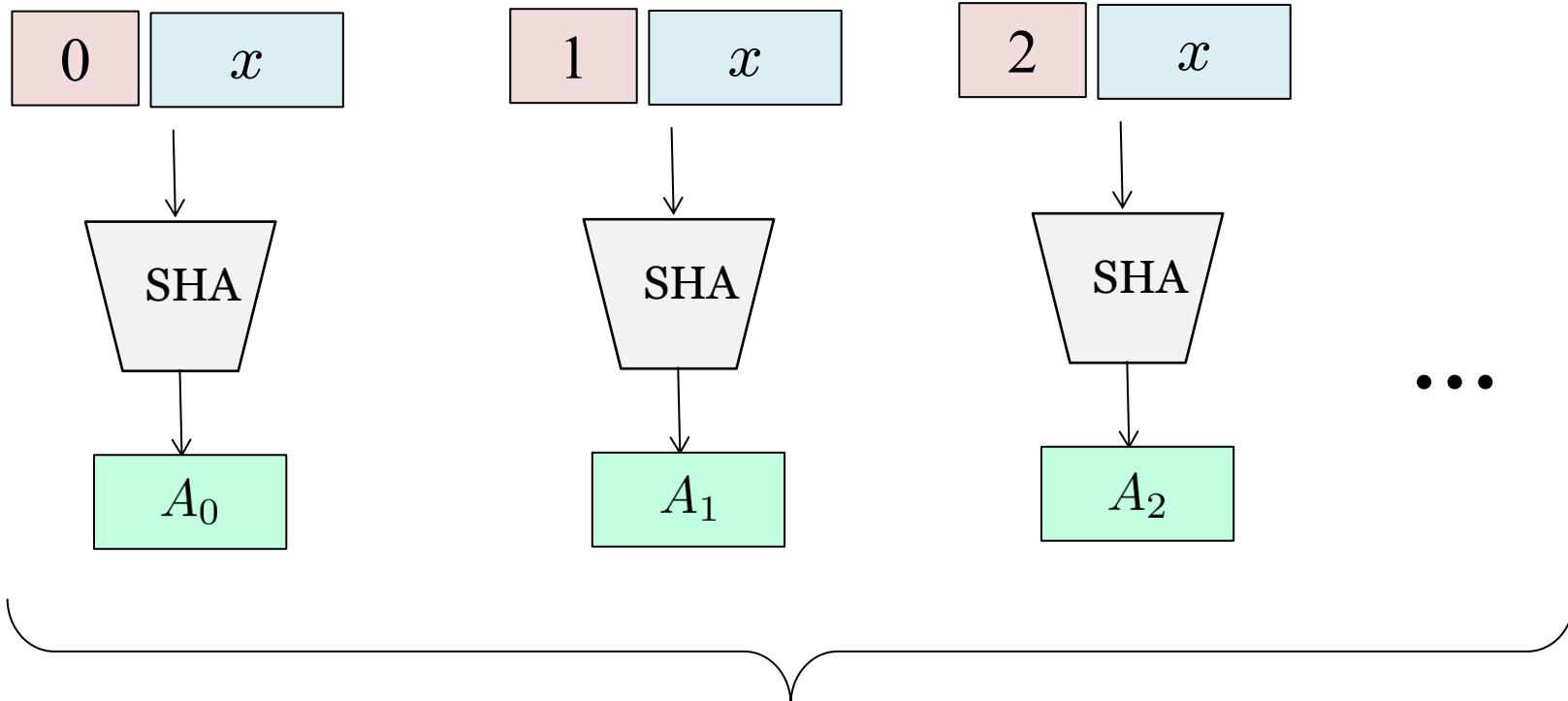


A Common Wrong Way to Hash



Broken by Desmedt and Odlyzko in 1985

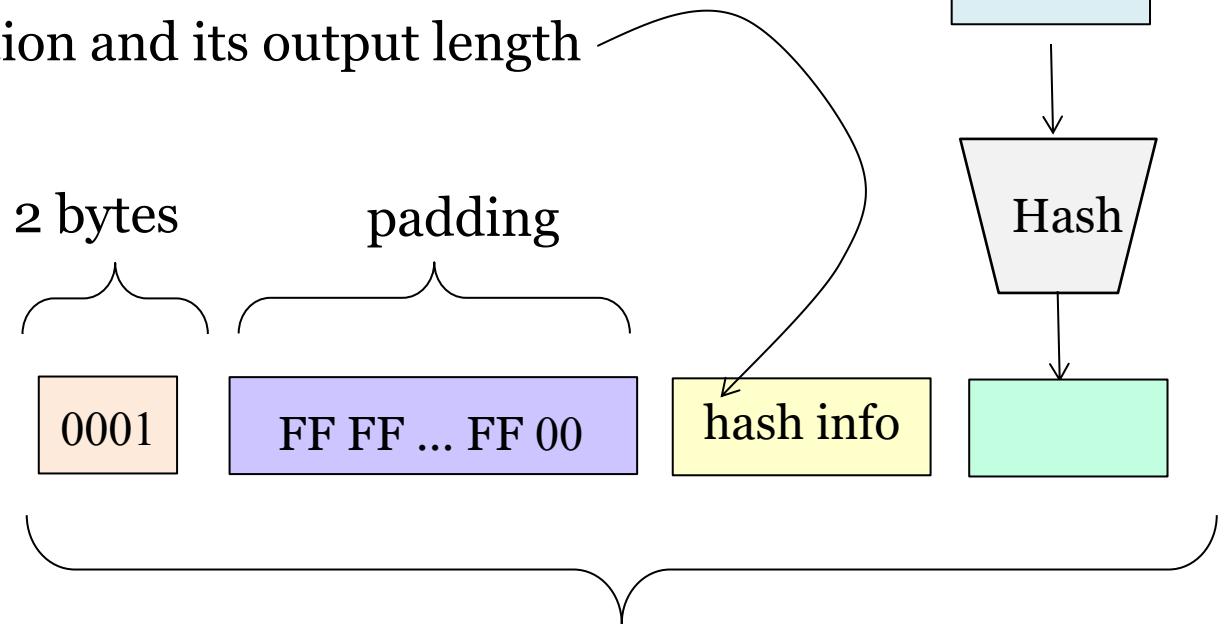
How to Hash Properly



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

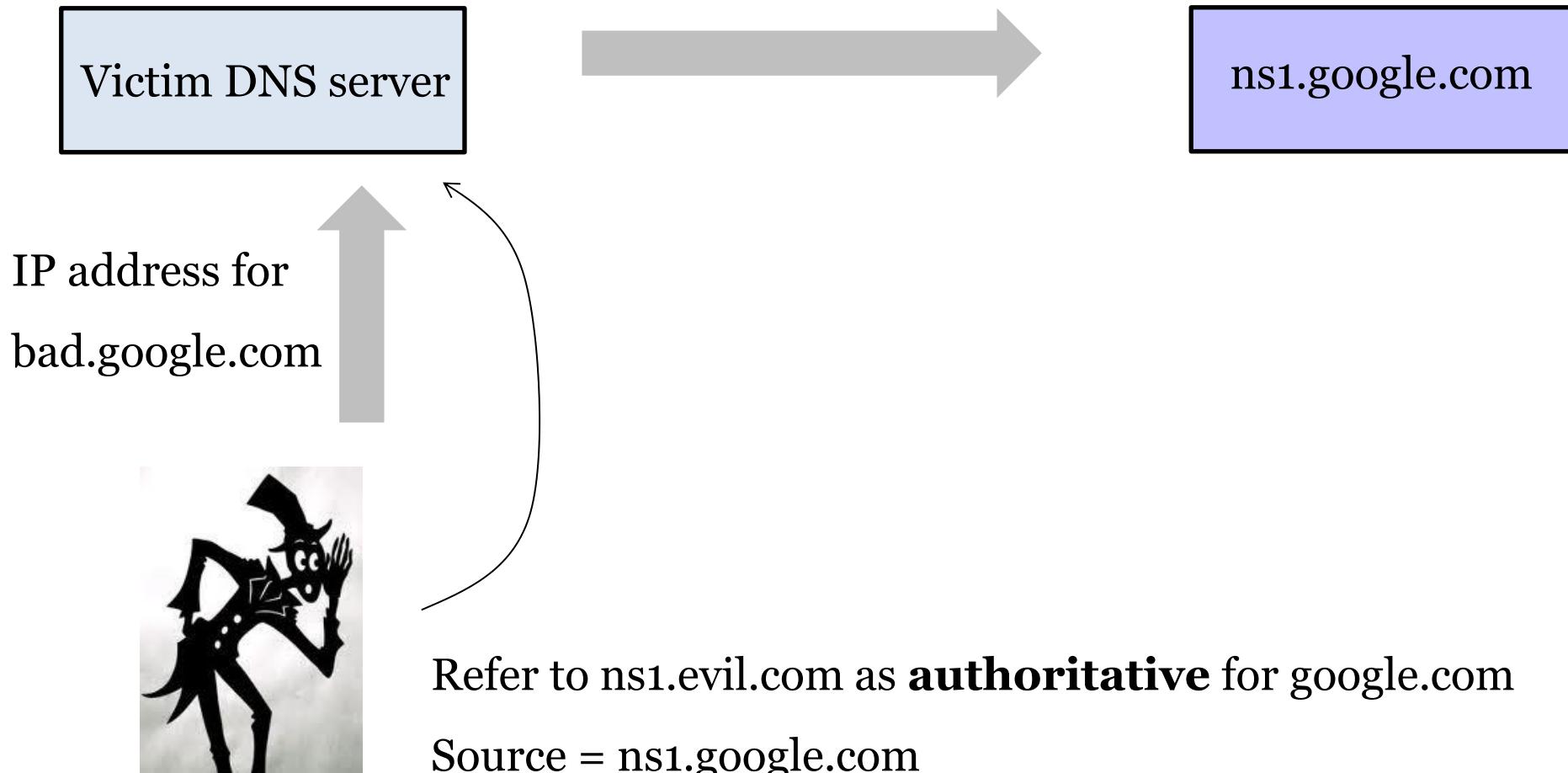


Agenda

1. High-level Overview
2. Building Signature Scheme
3. Application: DNSSEC

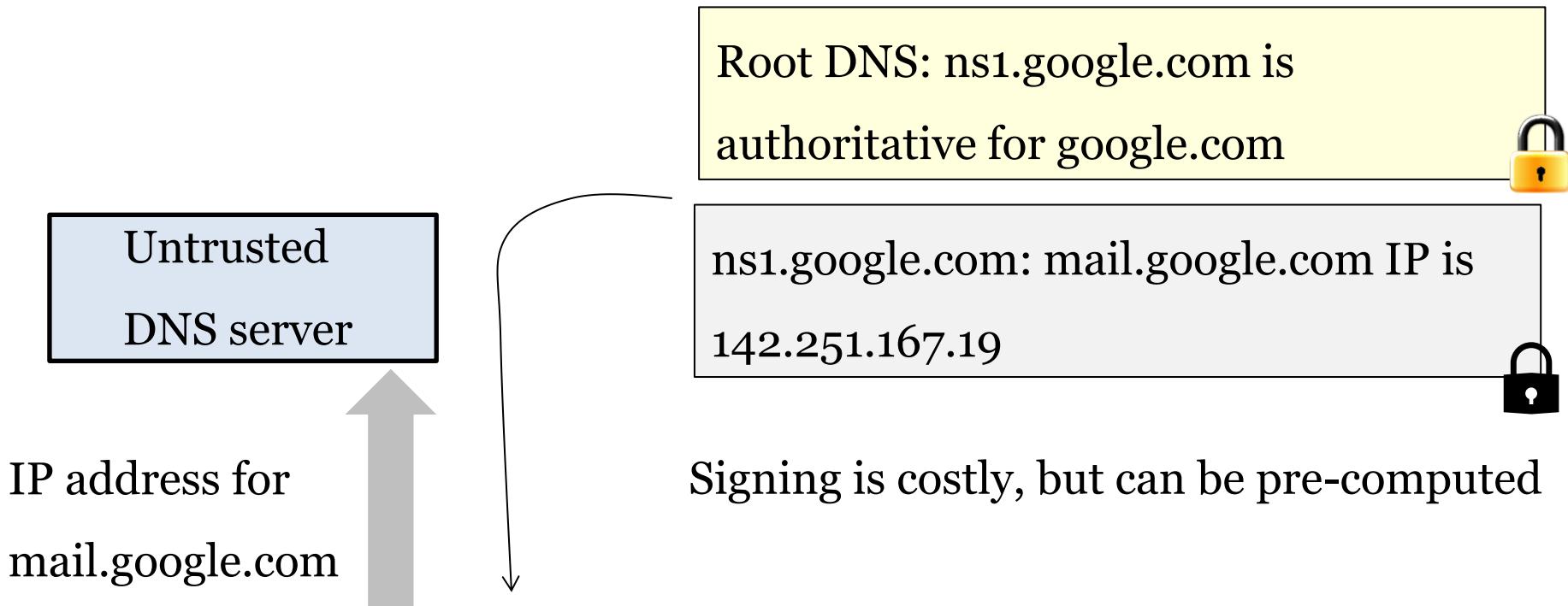
Recap: DNS Cache Poisoning Attack

Kaminsky, 2008

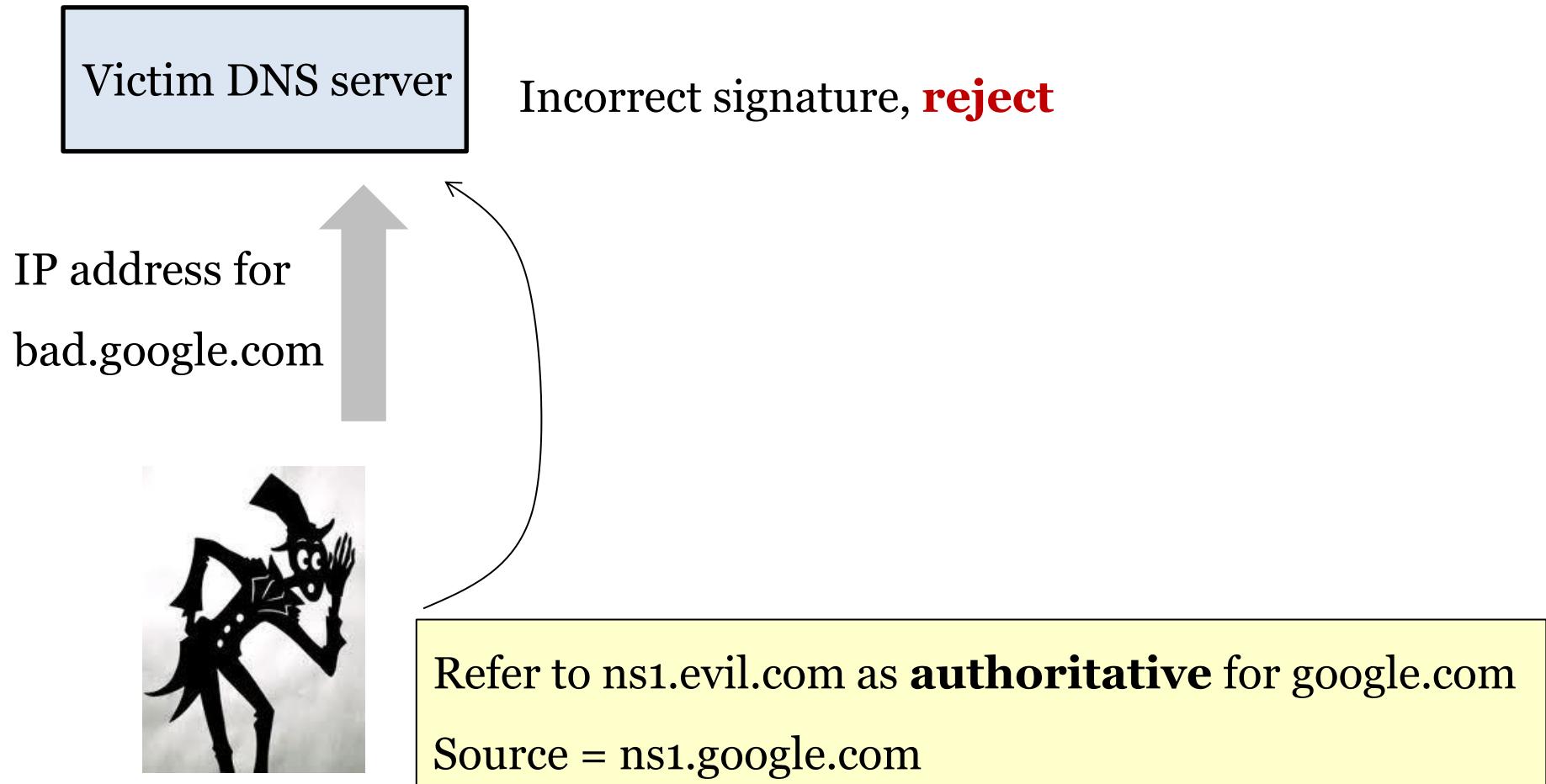


The Fix: DNSSEC

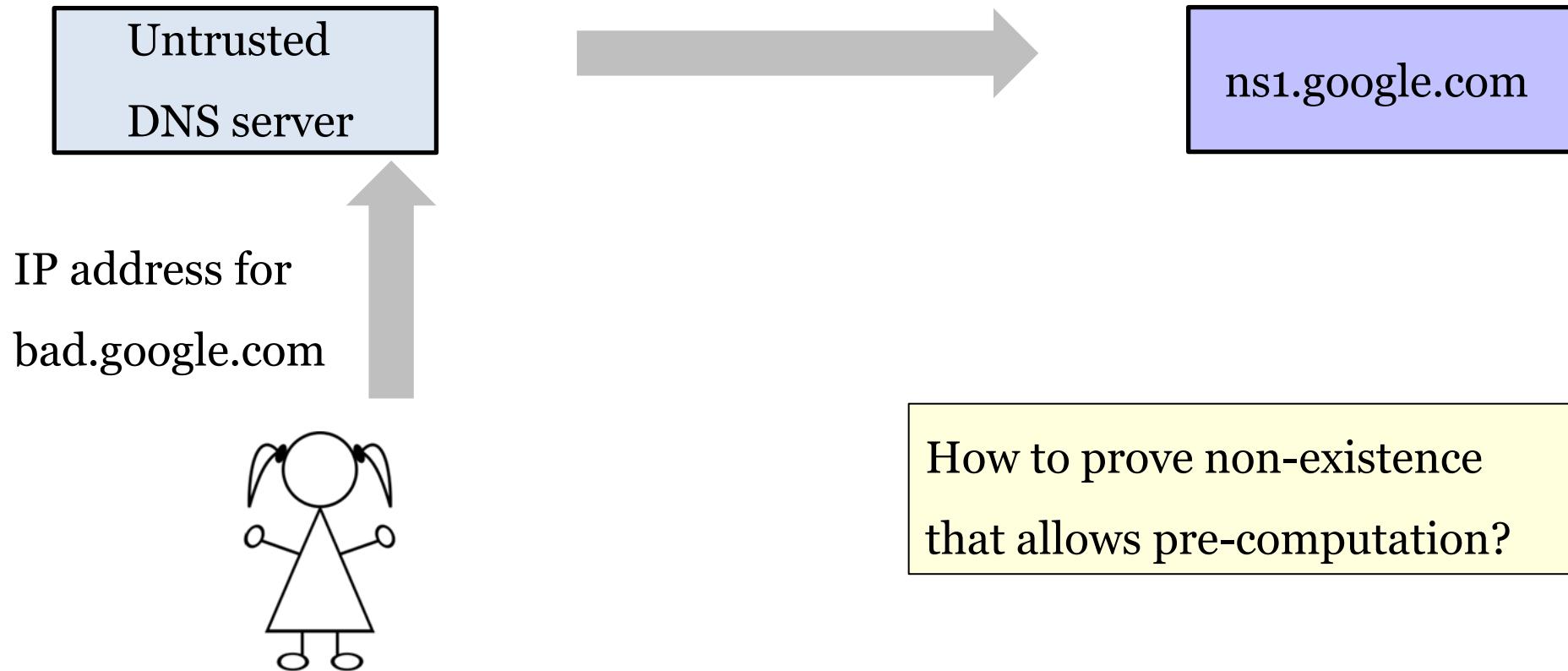
DNS replies need to be signed by authority



Thwarting Cache Poisoning Attack



Issue: Prove Non-Existence



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

