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 № 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

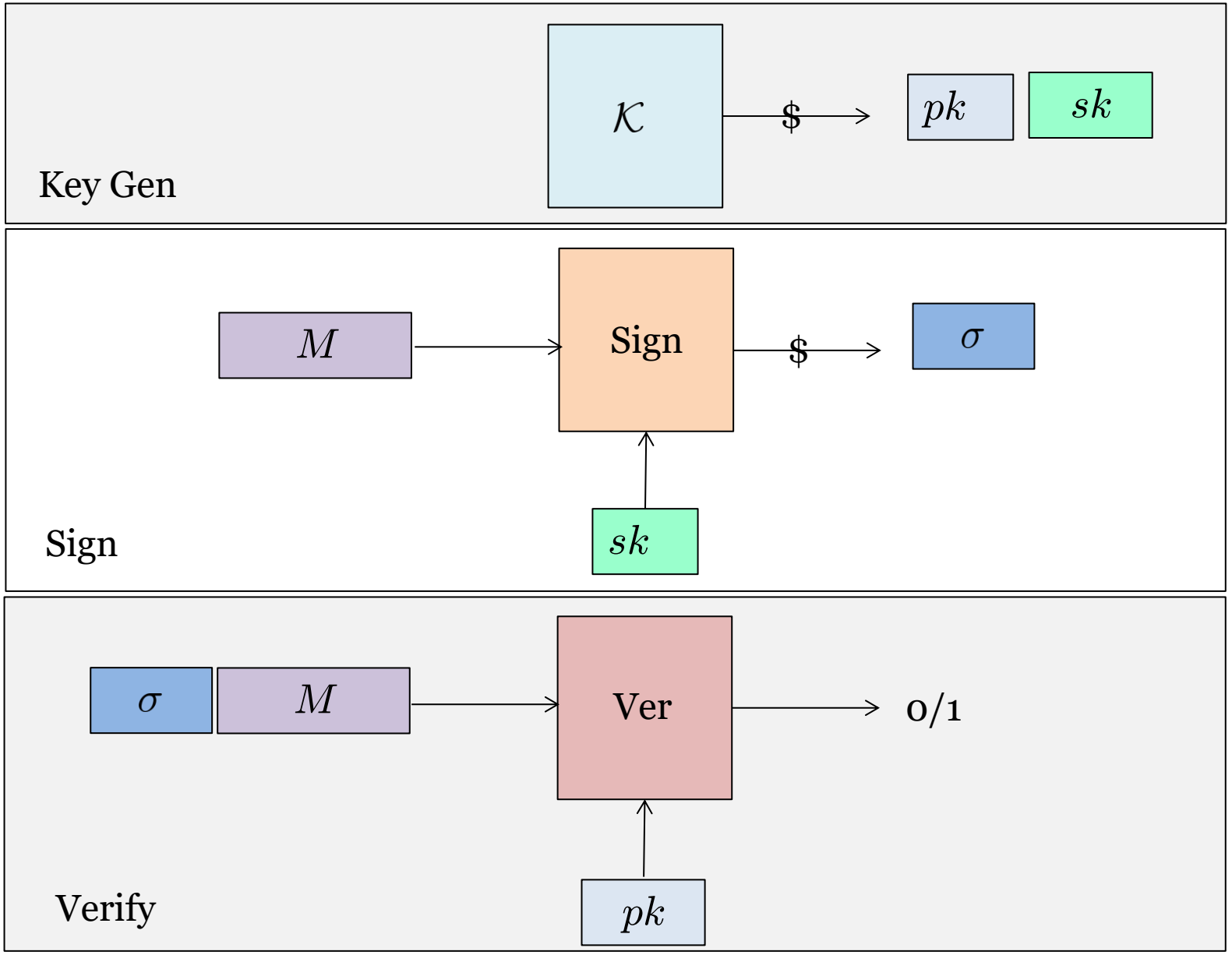
J. Smith
AUTHORIZED SIGNATURE

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

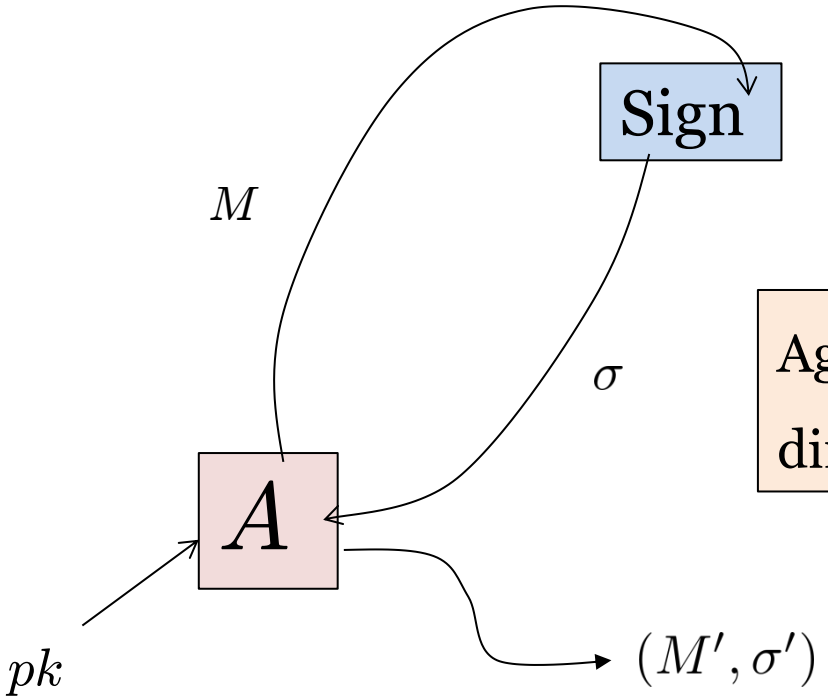
Digital Signature

- 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:

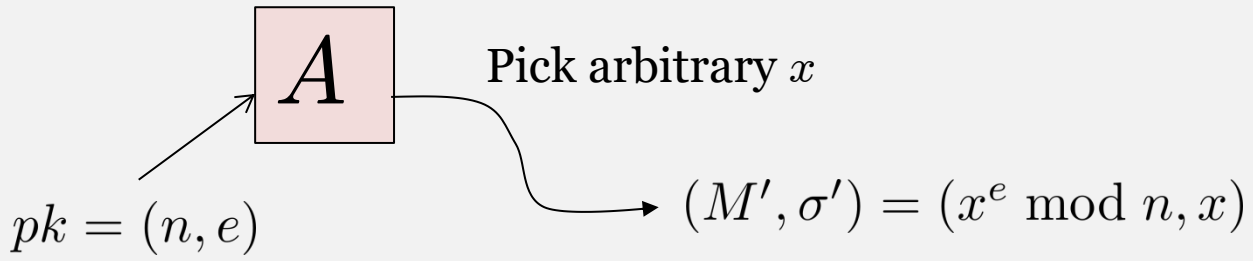
- To verify a signature, “encrypt” it and compare with the message

Issues with Plain RSA Signature

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

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

No sign query needed!

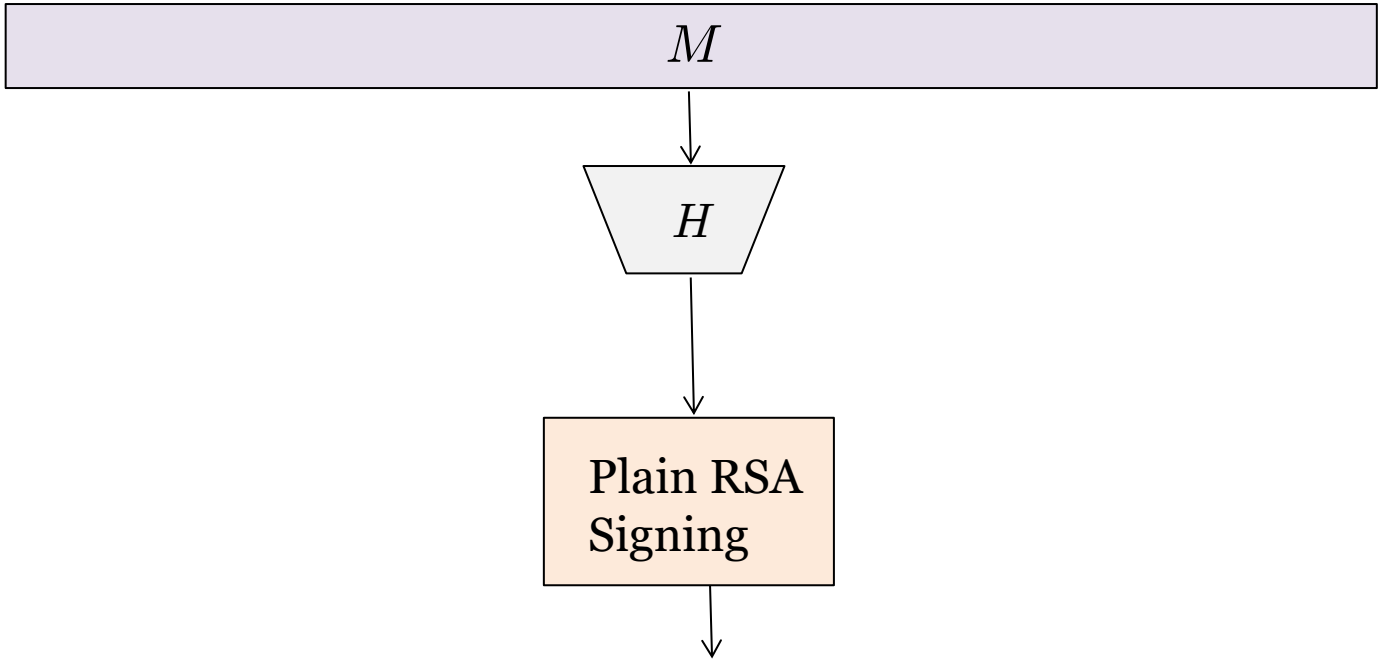


Hash-then-Sign Paradigm

Plain RSA Signature → Full Domain Hash (FDH)

Key generation: Like Plain RSA

Sign: To sign message M



Question: How to verify?

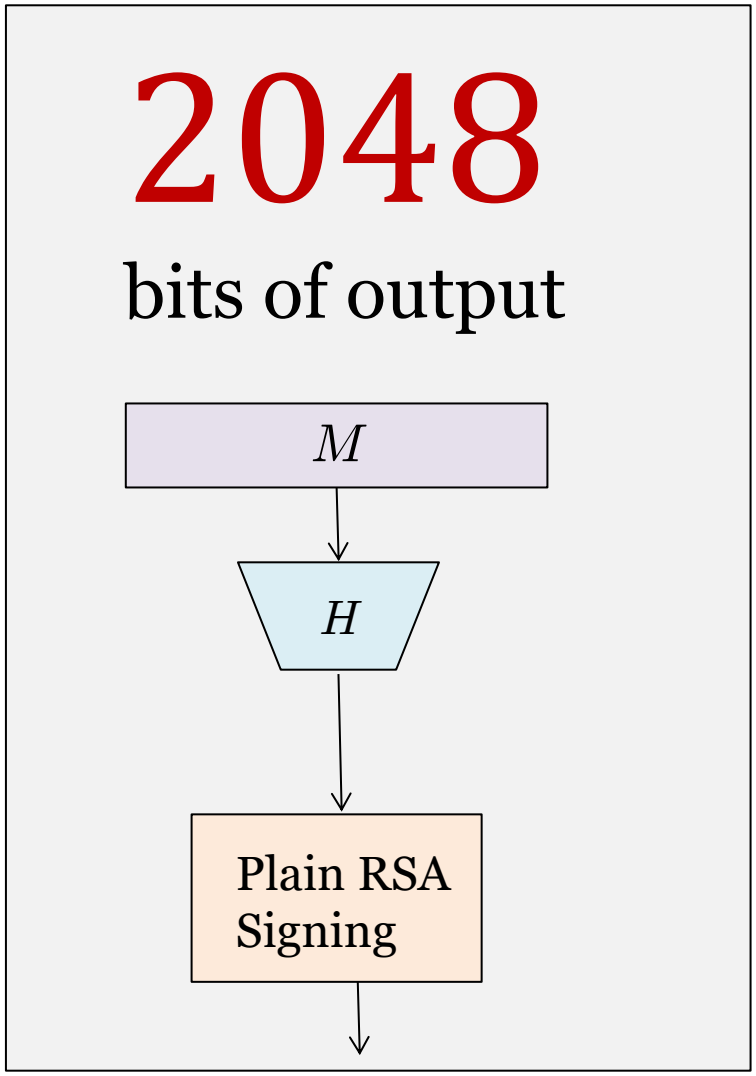
Security Requirement for Hash Function

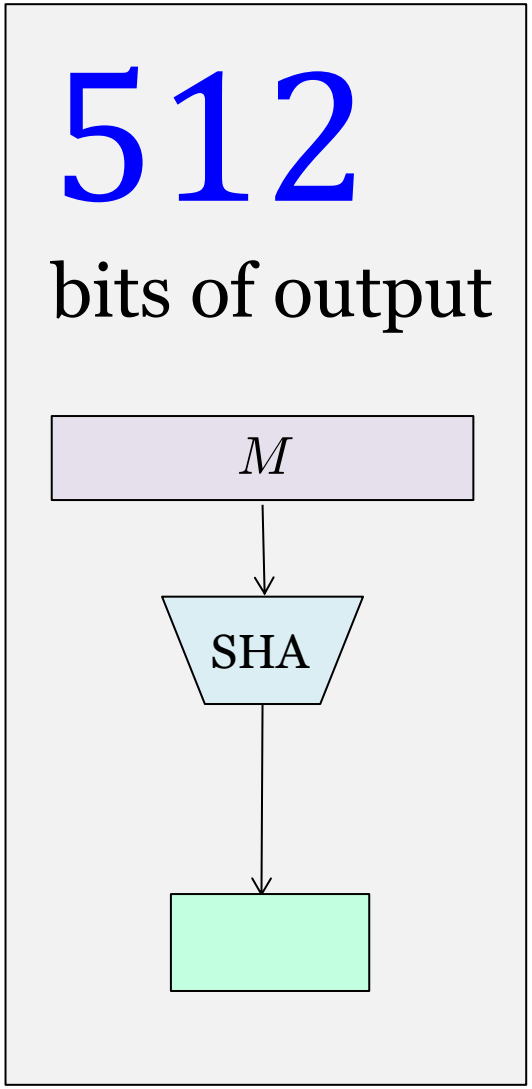
What intuition suggests: Hash must be collision-resistant

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

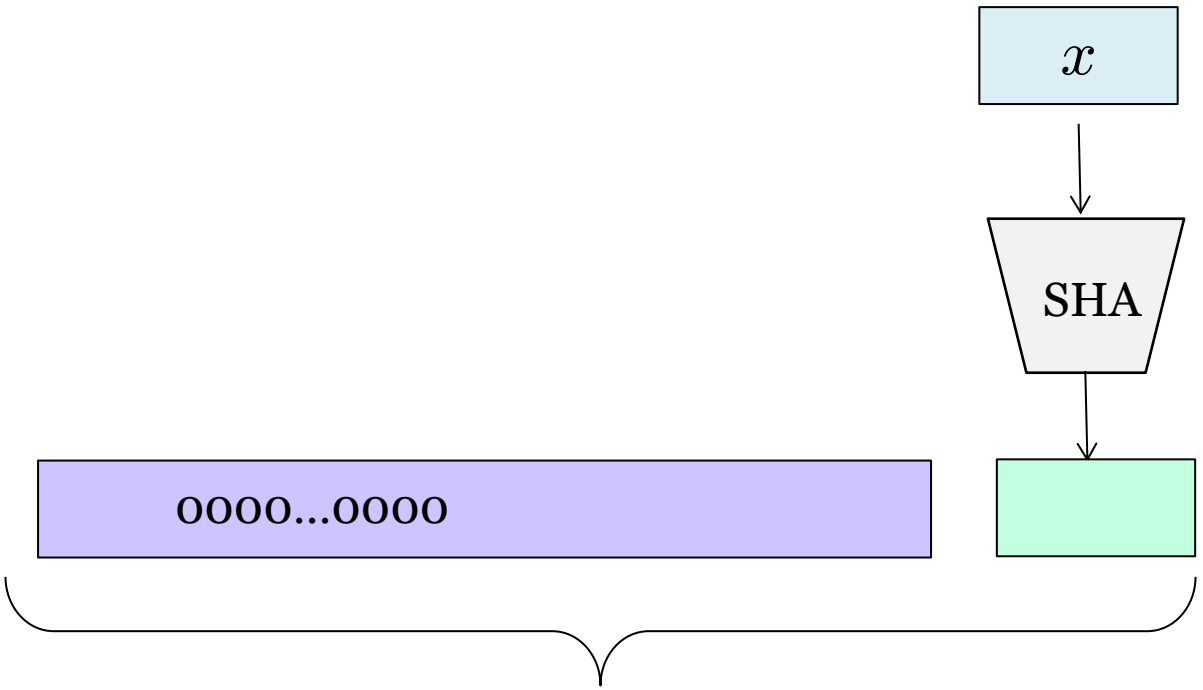
What proof requires: Hash is modeled as a random oracle

A Gap of Demand and Supply





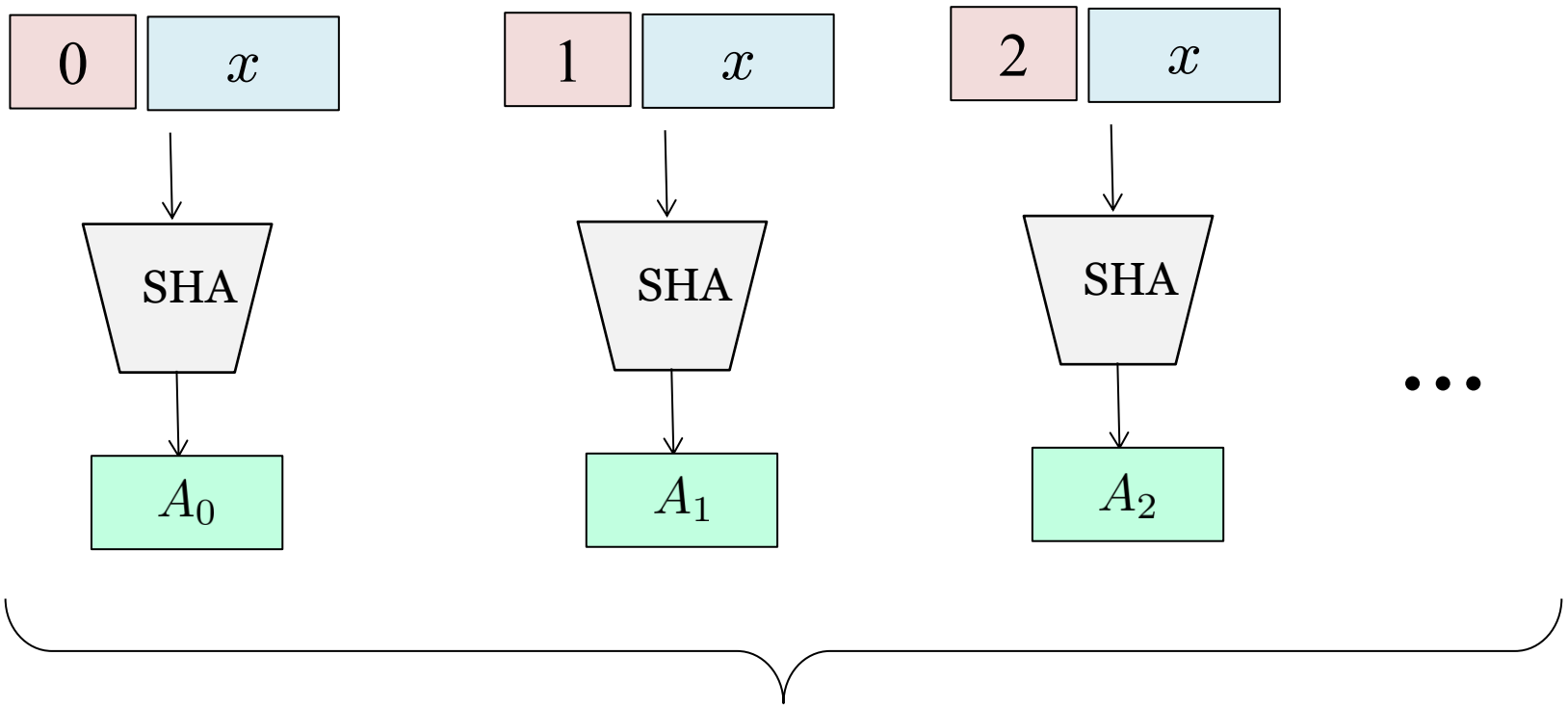
A Common Wrong Way to Hash



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

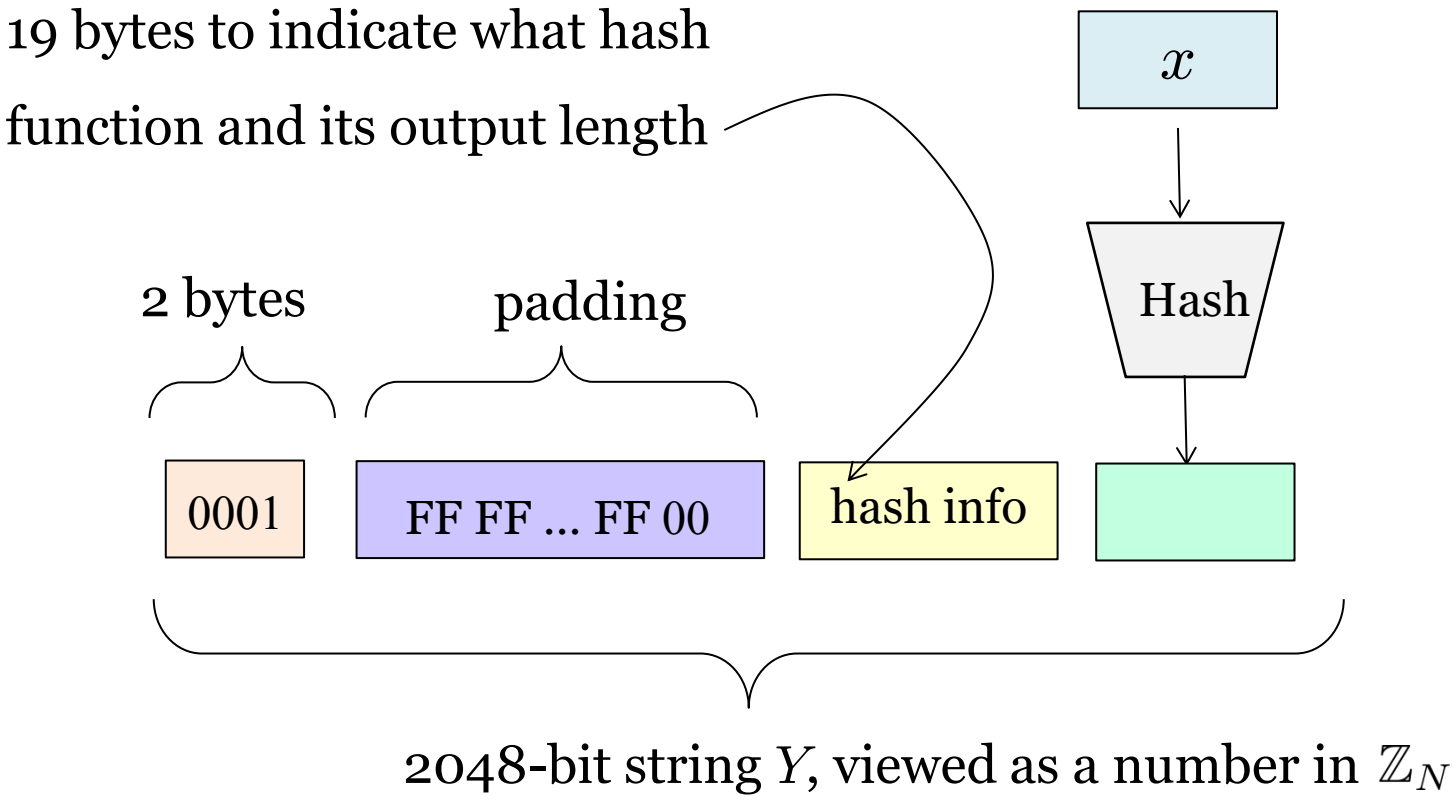
Broken by Desmedt and Odlyzko in 1985

How to Hash Properly



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

Hashing in PKCS#1



Agenda

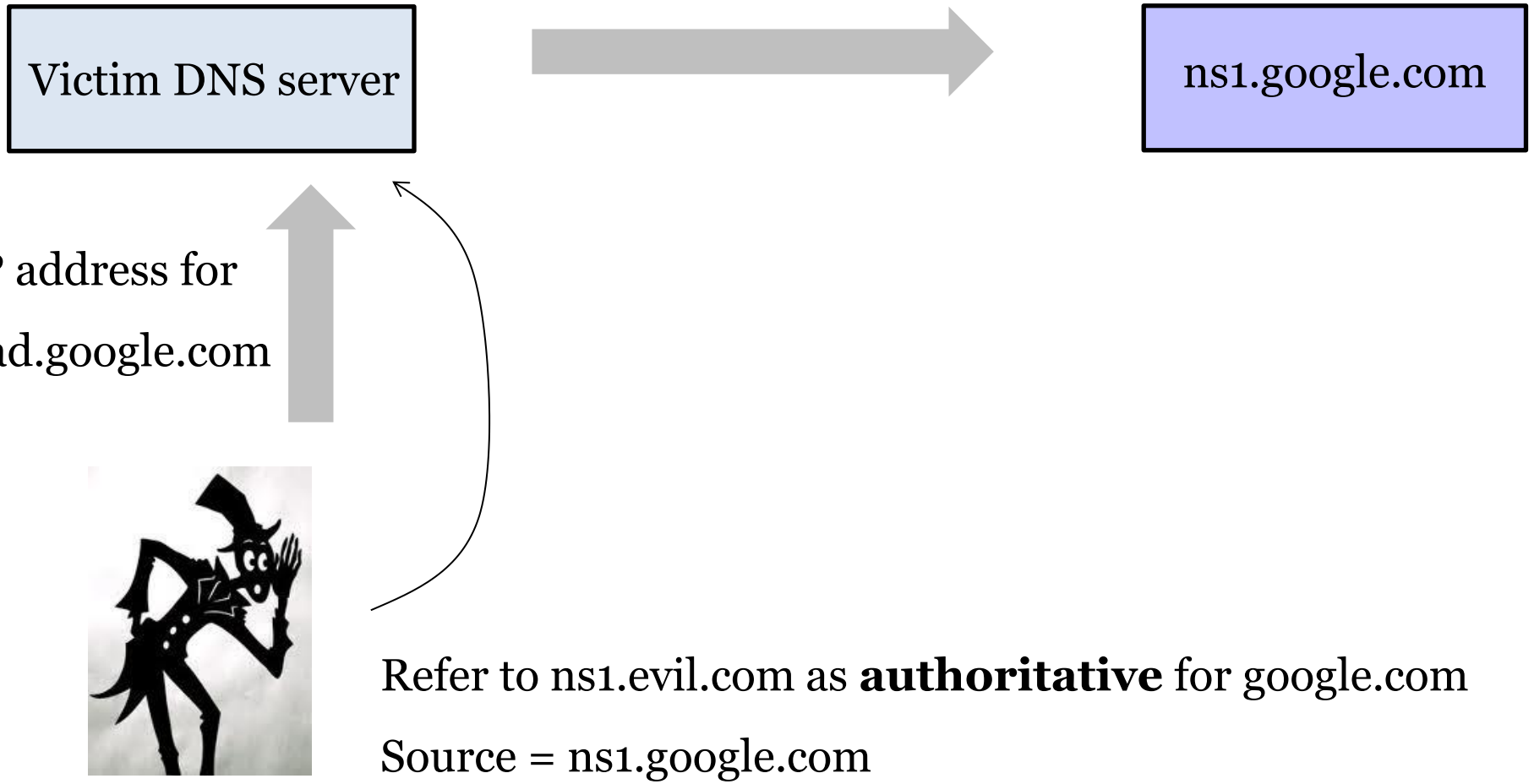
1. High-level Overview

2. Building Signature Scheme

3. Application: DNSSEC

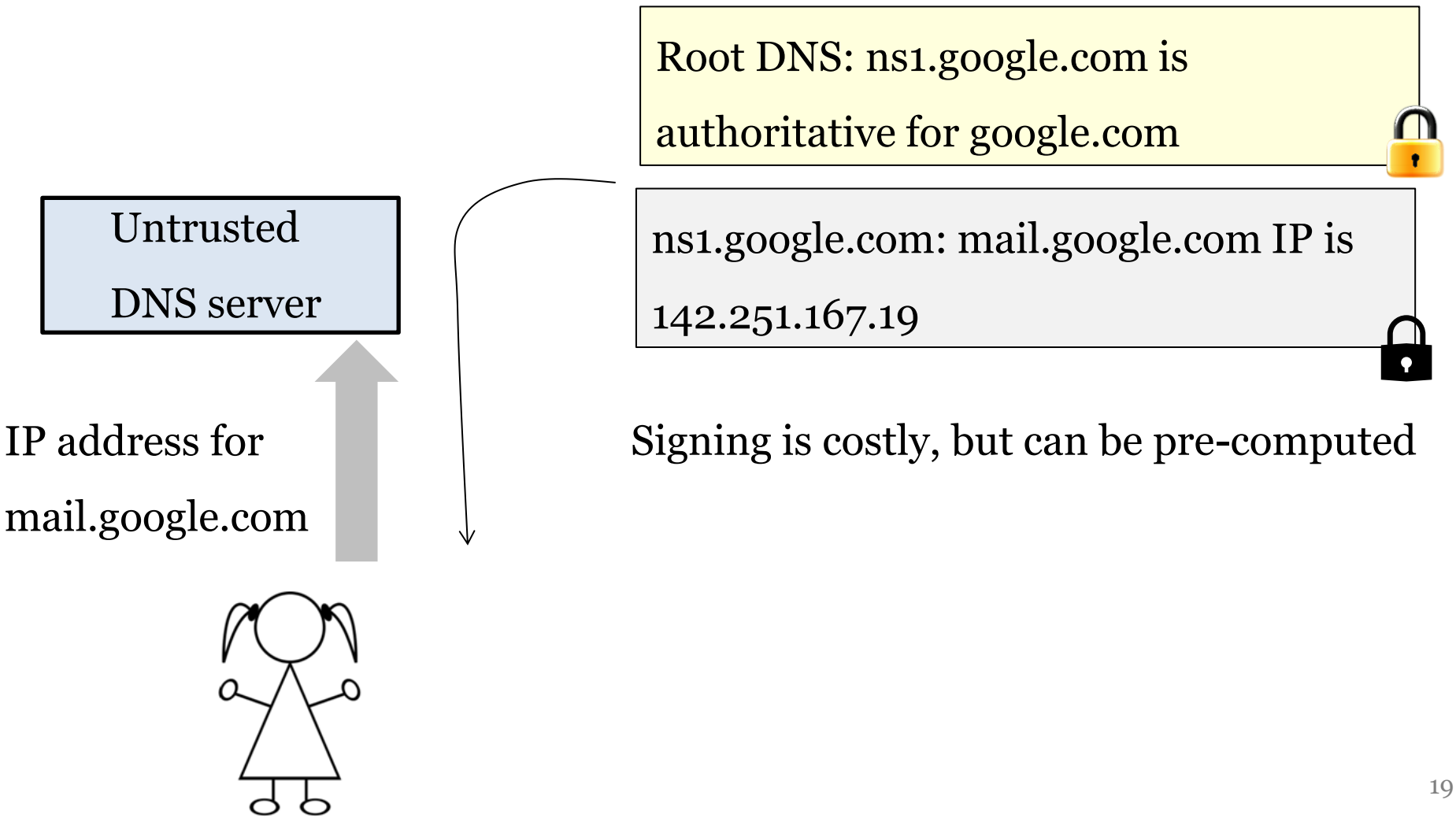
Recap: DNS Cache Poisoning Attack

Kaminsky, 2008



The Fix: DNSSEC

DNS replies need to be signed by authority



Thwarting Cache Poisoning Attack

Victim DNS server

Incorrect signature, **reject**

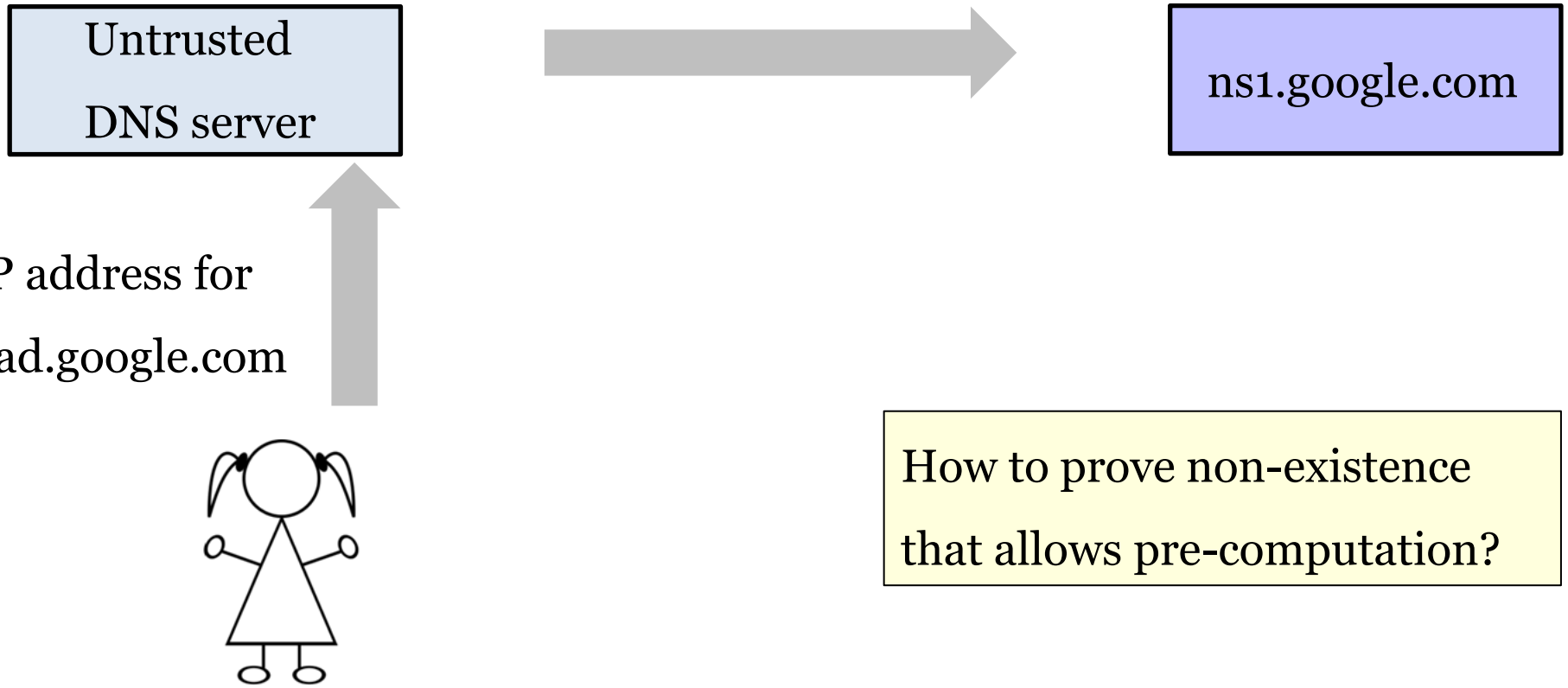
IP address for

bad.google.com

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

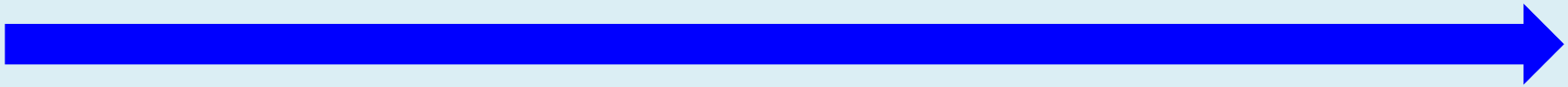
Source = ns1.google.com

Issue: Prove Non-Existence



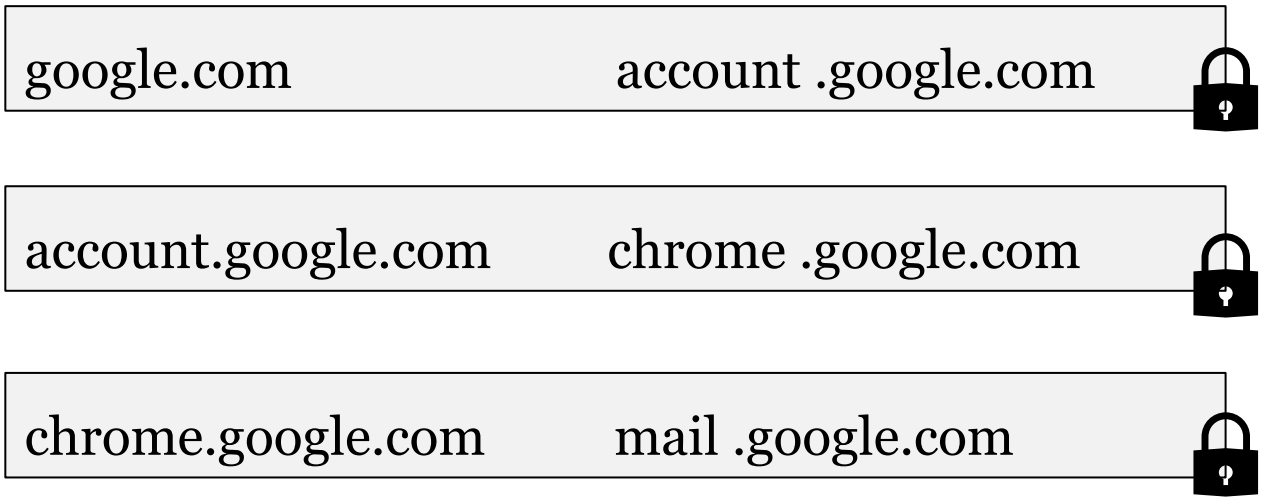
Proving Non-Existence: Precomputation

Google sorts its subdomain names alphabetically



account chrome mail policies site

Sign every consecutive pairs



Proving Non-Existence: Respond to Query

Unsuccessful Binary Search