# Passive SSH Key Compromise via Lattices

Keegan Ryan[1], Kaiwen He[2], George Arnold Sullivan[1], Nadia Heninger[1]

[1] UC San Diego

[2] UC San Diego, MIT

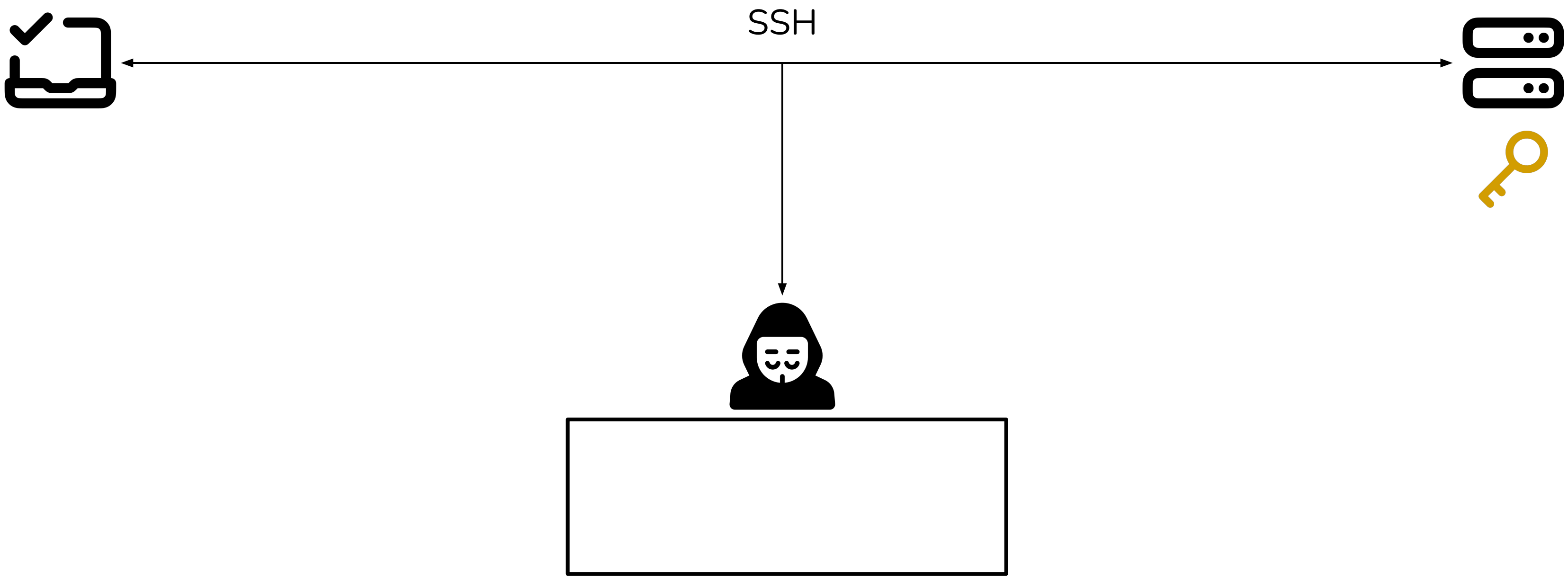
ACM CCS, November 2023

# Overview

1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?

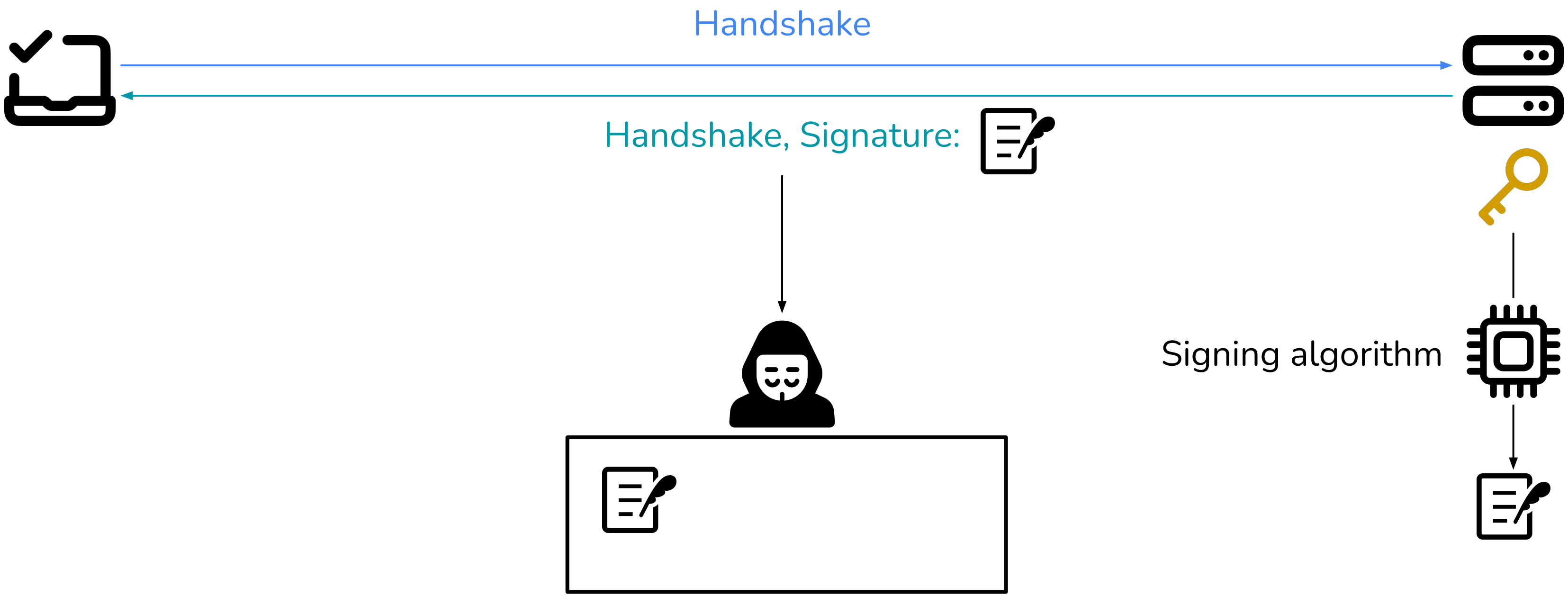
# Overview

1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?



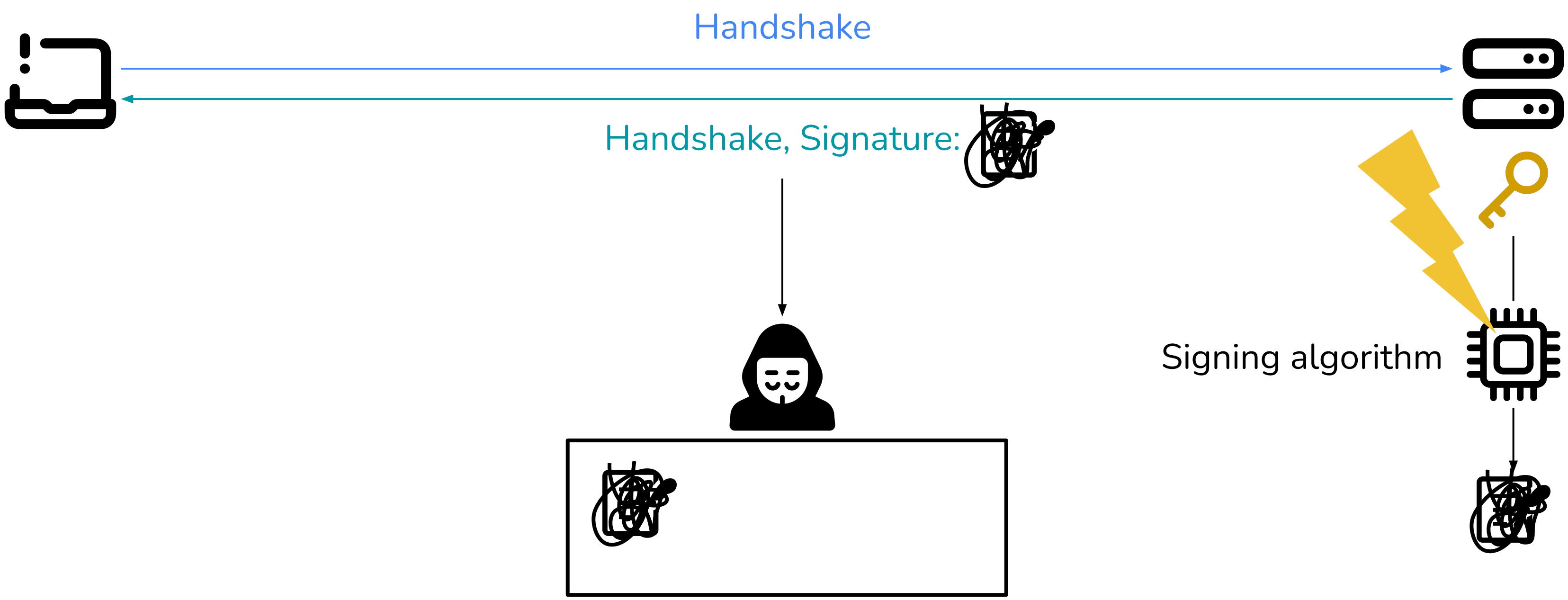
# Overview

1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?



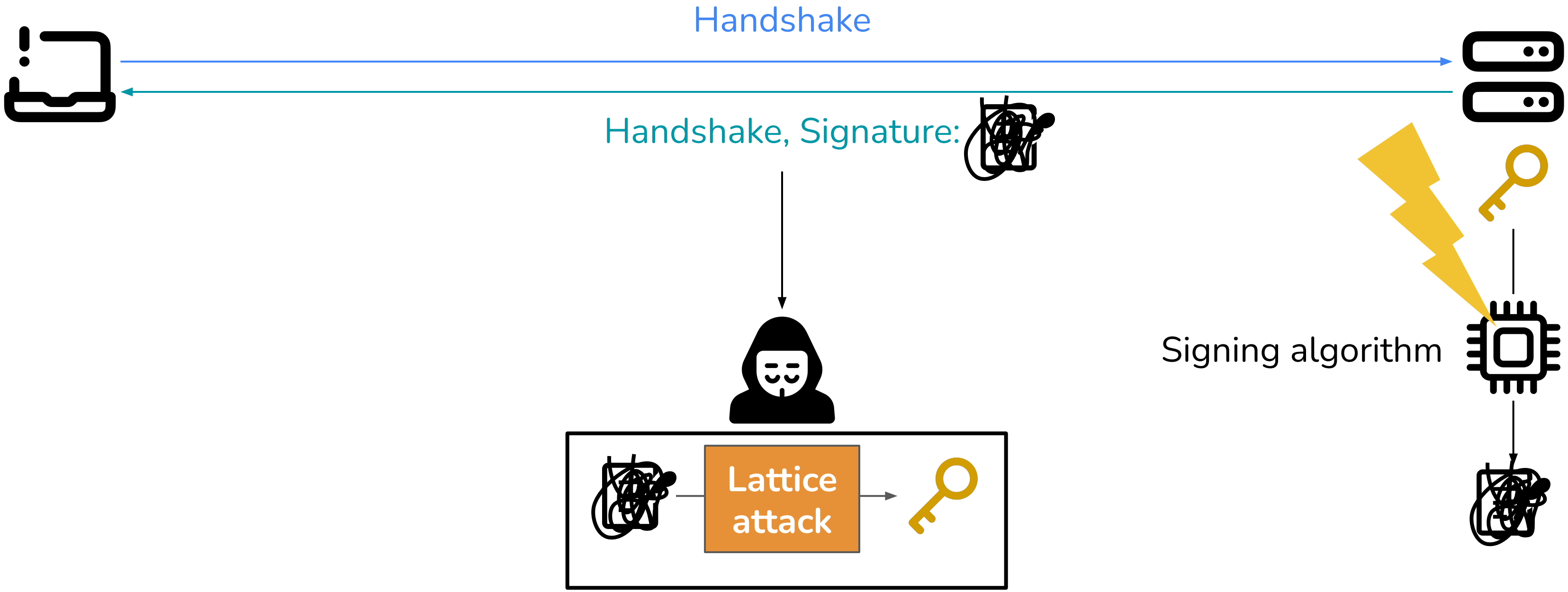
# Overview

1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?



# Overview

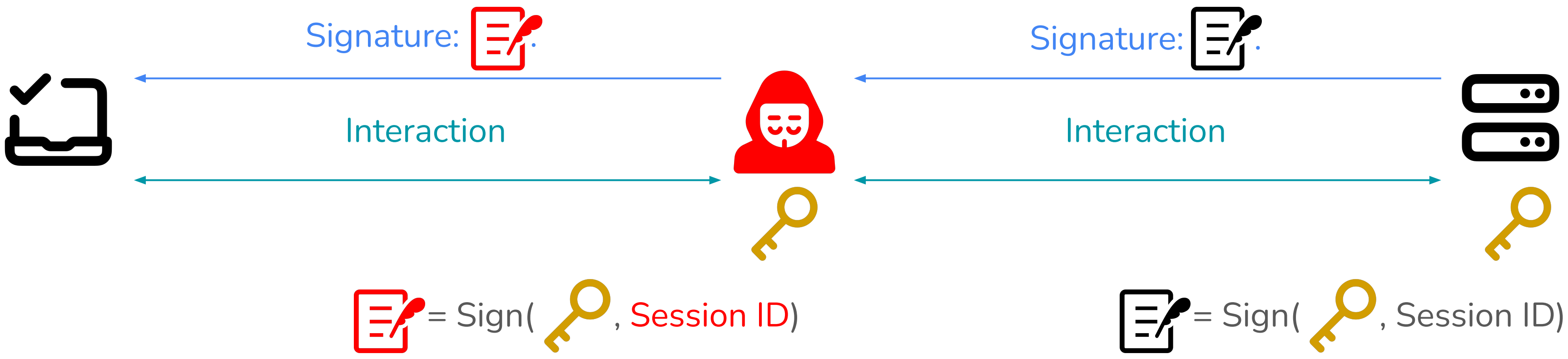
1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?



# Implications of host key compromise

Active attacker with the key can impersonate the server

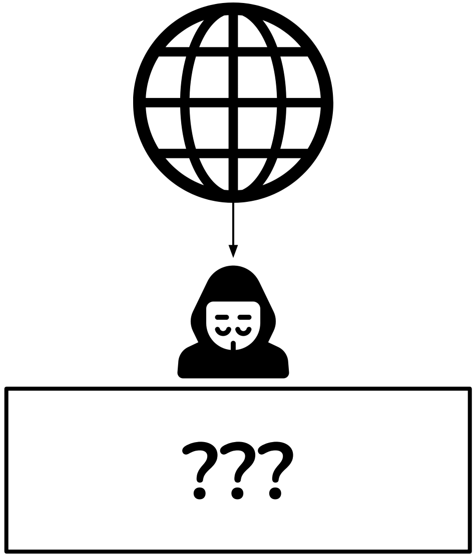
- Can then intercept and arbitrarily tamper with connection



# Overview

1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?

2. Are such keys leaked frequently over the internet?



# Overview

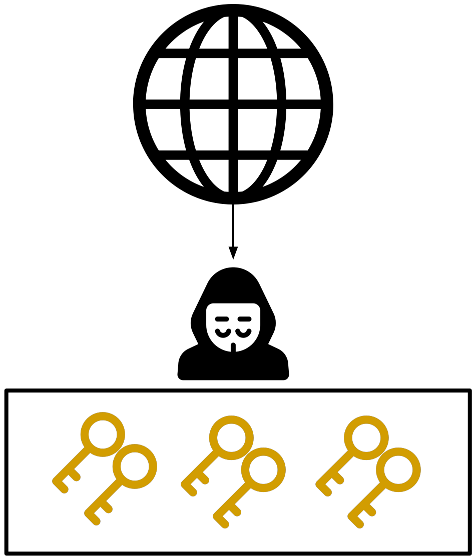
1. Can faulty RSA signatures reveal the private SSH host key to eavesdroppers?

2. Are such keys leaked frequently over the internet?

We analyzed **3.2 billion** SSH signatures on the internet

(1.2 billion *RSA signatures*)

**4,962** signatures: Revealed **private keys**



# History of signature fault attacks

1996-97

[Len96], [BDL97]: Error in RSA signature can reveal private key

# History of signature fault attacks

1996-97

[Len96], [BDL97]: Error in RSA signature can reveal private key

[Wei15]:
**Practical** signature fault attack on **TLS** in **active setting**
Believed **SSH** is not exploitable in **passive setting**

2015

[SSH+22]: **Practical** attack on **TLS** in **passive setting**

2022

# History of signature fault attacks

1996-97

[Len96], [BDL97]: Error in RSA signature can reveal private key

[Wei15]:
**Practical** signature fault attack on TLS in **active setting**

2015

[SSH+22]: **Practical** attack on TLS in **passive setting**

2022

# History of signature fault attacks

1996-97

[Len96], [BDL97]: Error in RSA signature can reveal private key
(only if signed message is **fully known**)

2015

[Wei15]:
**Practical** signature fault attack on **TLS** in **active setting**
Believed **SSH** is not exploitable in **passive setting**
Message hash includes **DH shared secret** → unknown to eavesdropper

2022

[SSH+22]: **Practical** attack on **TLS** in **passive setting**
Message fully computable by eavesdropper

# History of signature fault attacks

1996-97

[Len96], [BDL97]: Error in RSA signature can reveal private key
(only if signed message is **fully known**)

2015

[Wei15]:
**Practical** signature fault attack on **TLS** in **active setting**
Believed **SSH** is not exploitable in **passive setting**
Message hash includes **DH shared secret** → unknown to eavesdropper

2022

[SSH+22]: **Practical** attack on **TLS** in **passive setting**
Message fully computable by eavesdropper

2023

This work: **Practical** attack on **SSH** in **passive setting**

# History of signature fault attacks

1996-97

[Len96], [BDL97]: Error in RSA signature can reveal private key
(only if signed message is **fully known**)

2015

[Wei15]:
**Practical** signature fault attack on **TLS** in **active setting**
Believed SSH is not exploitable in **passive setting**
Message hash includes **DH shared secret** → unknown to eavesdropper

?

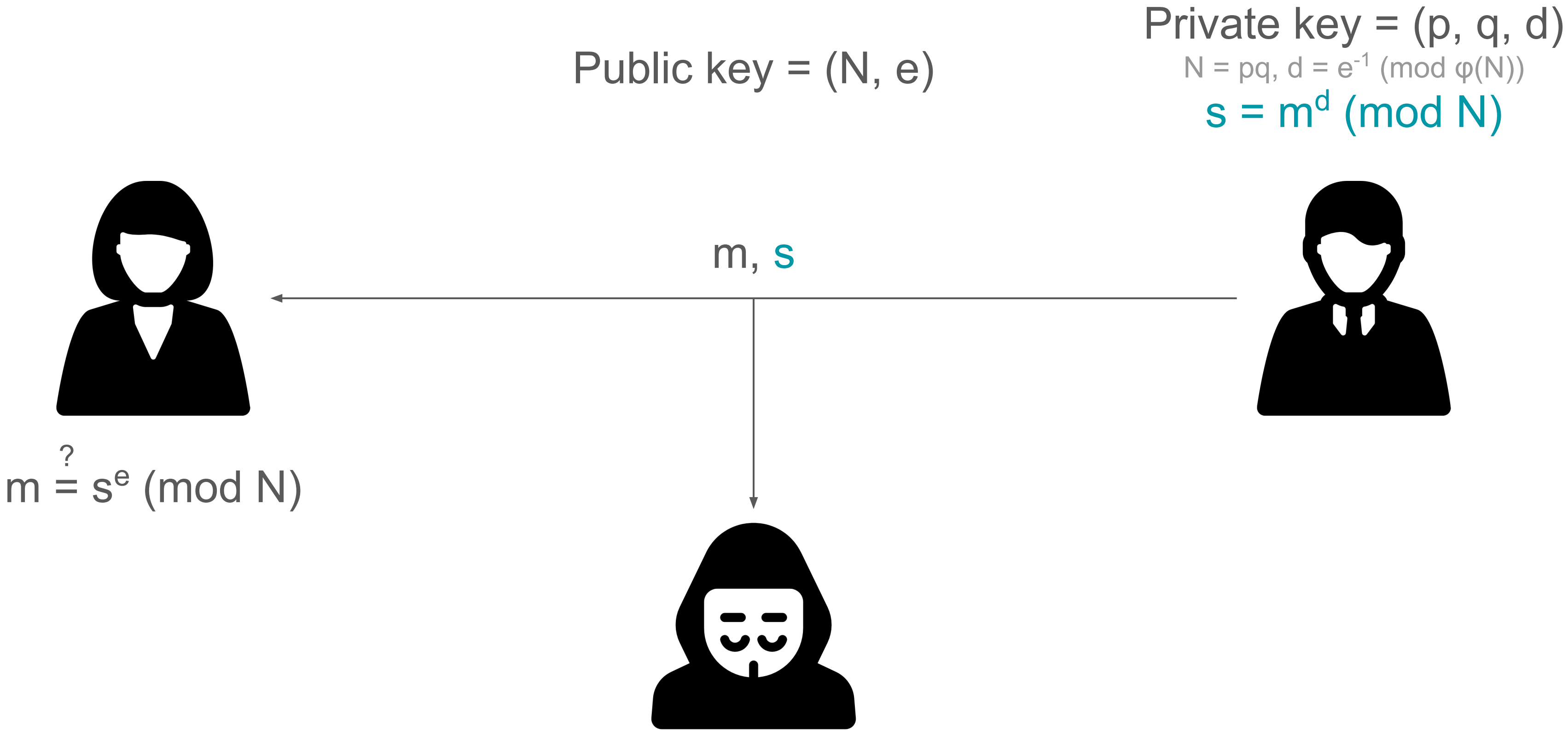
2022

[SSH+22]: **Practical** attack on **TLS** in **passive setting**
Message fully computable by eavesdropper

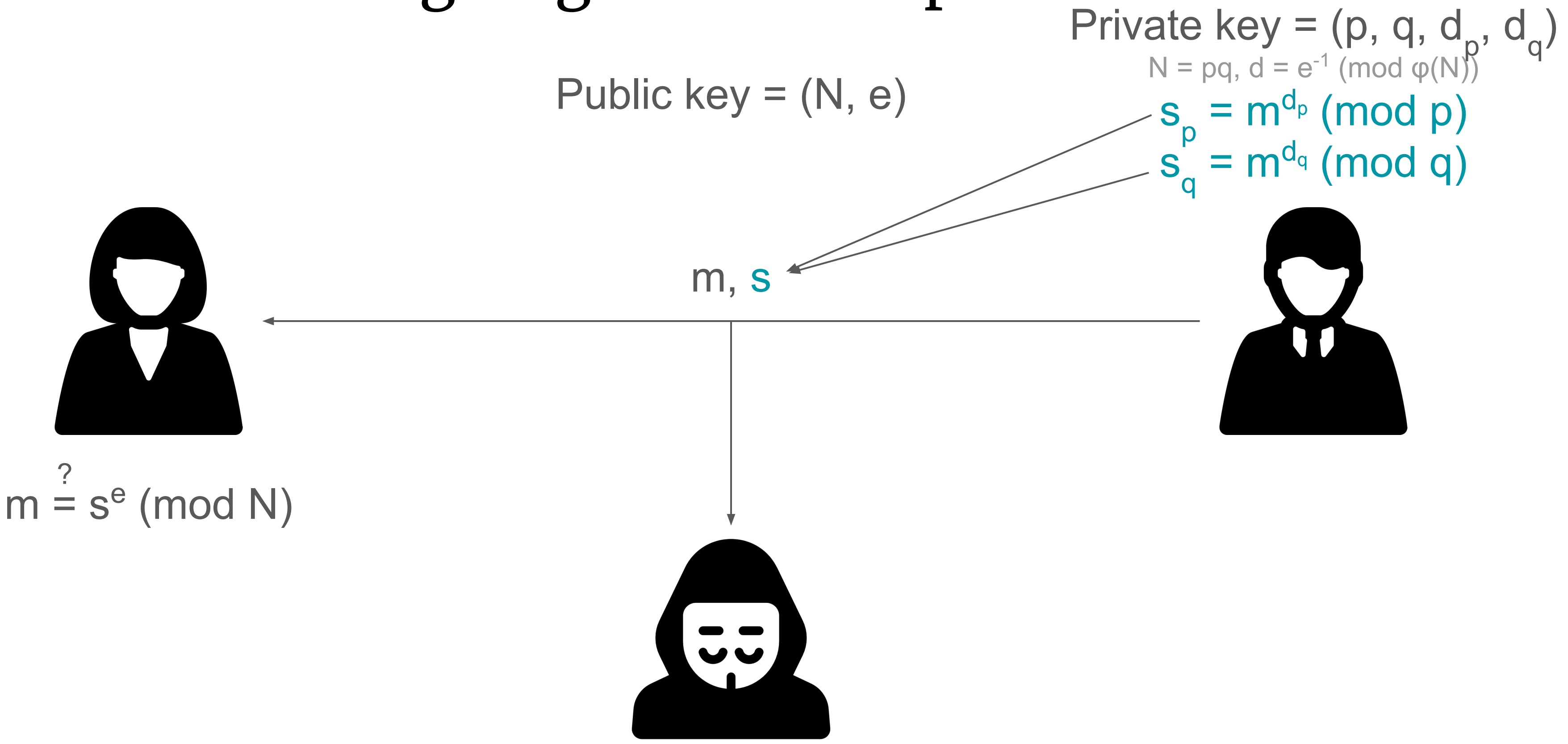
2023

This work: **Practical** attack on **SSH** in **passive setting**

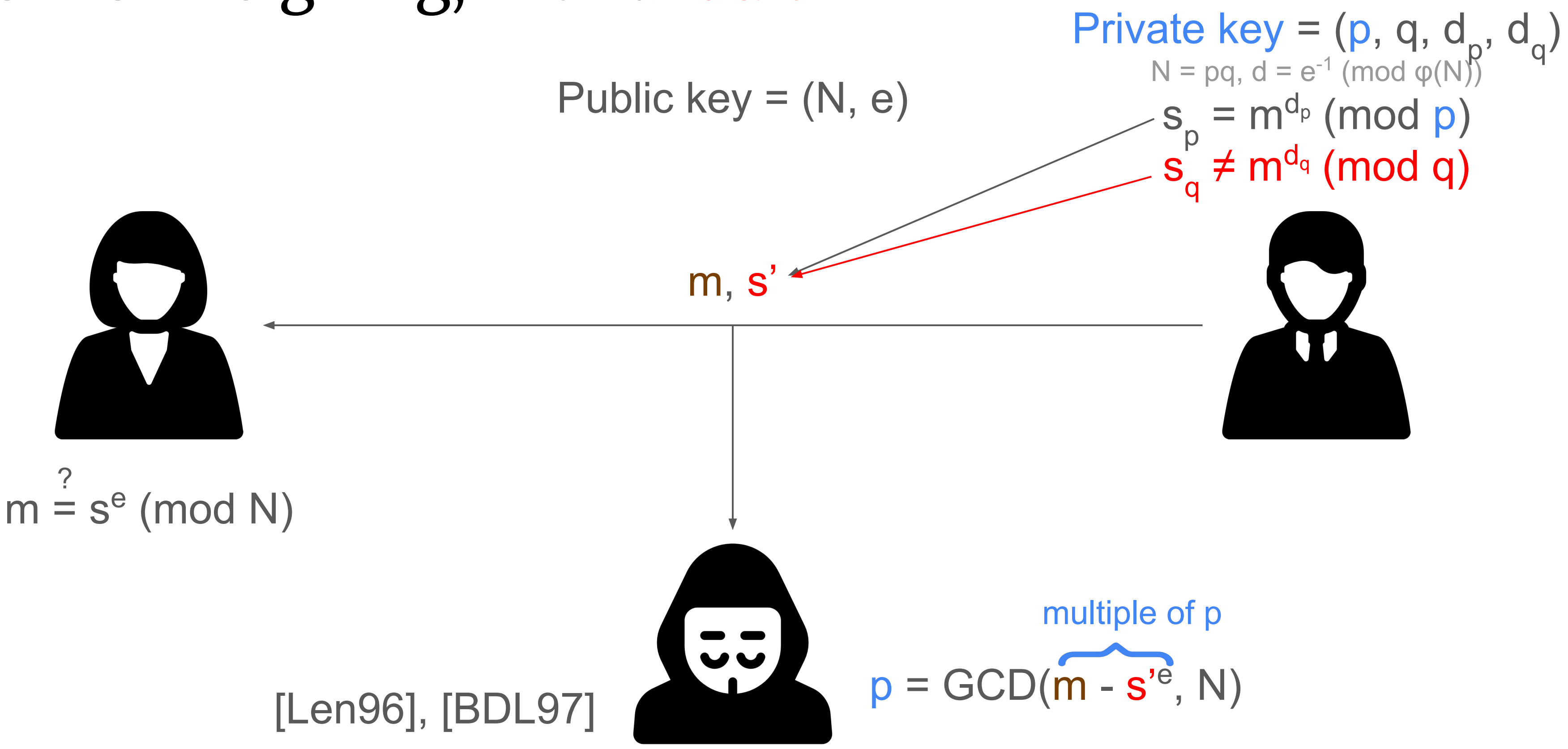
# Textbook RSA signing



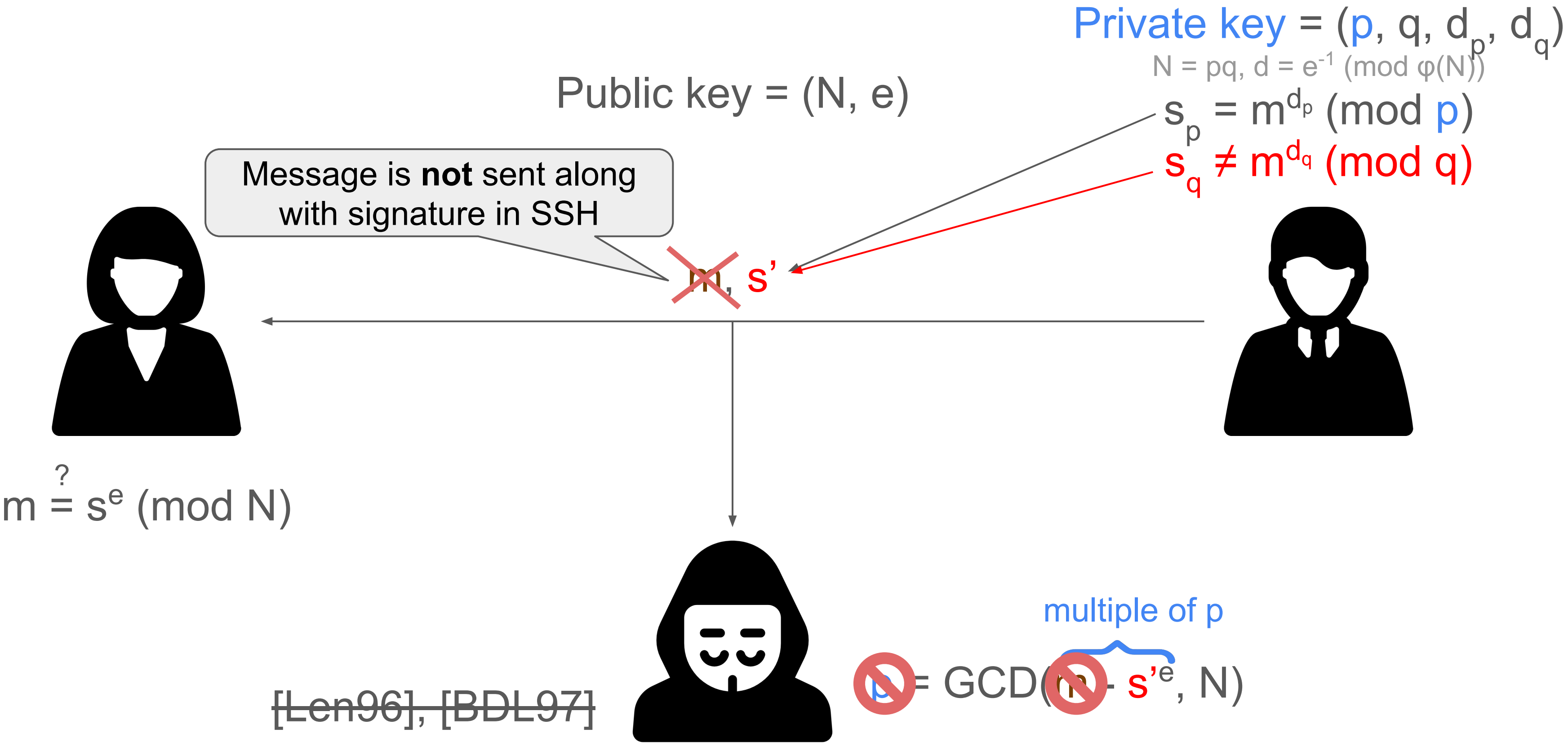
# Textbook RSA signing with CRT optimization



# RSA-CRT signing, with a fault



# RSA-CRT fault in SSH



# PKCS#1 v1.5 RSA signature padding

Message format for SSH:
m = 0x0001FF…FF00 {hash algorithm} {hash}

- Padding is deterministic and known to the attacker
- Attacker knows almost all of message m, except for the hash

# RSA-CRT fault in SSH, passive attack

Private key = $(p, q, d_p, d_q)$

$N = pq,\ d = e^{-1} \pmod{\varphi(N)}$

Public key = $(N, e)$

$s_p = m^{d_p} \pmod{p}$

$s_q \neq m^{d_q} \pmod{q}$

$s'$

Message format for SSH: (PKCS#1 v1.5)

m = 0x0001FF…FF00 {algorithm} {hash}

[CJK+09]

Knows that $m = \overbrace{a}^{\text{known}} + \overbrace{r}^{\text{small unknown}}$

$p$ = **Approx**-GCD$(a - s'^e, N)$

# Lattice attack

Message format for SSH: (PKCS#1 v1.5)
m = 0x0001FF…FF00 {hash algorithm} {hash} < N

Experimented with attacking faulty SSH signatures:

- Generated instances that correspond to SSH parameter choices
    - e.g., RSA-2048, SHA-256

For all common parameter choices (RSA modulus length > 4 × hash length):

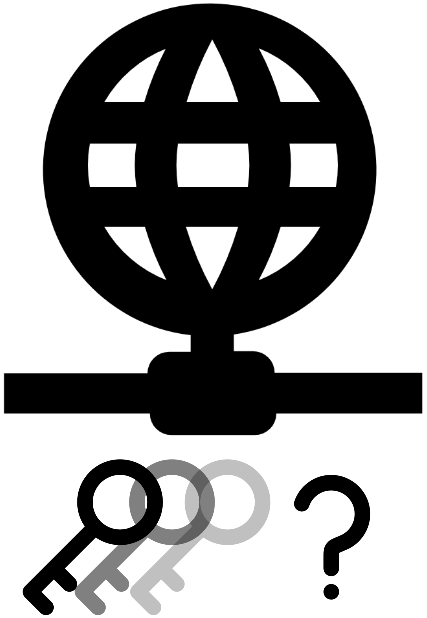
- Attack averages under 0.2 seconds per signature
- Recovers correct key for every generated signature

# Key leakage in the wild

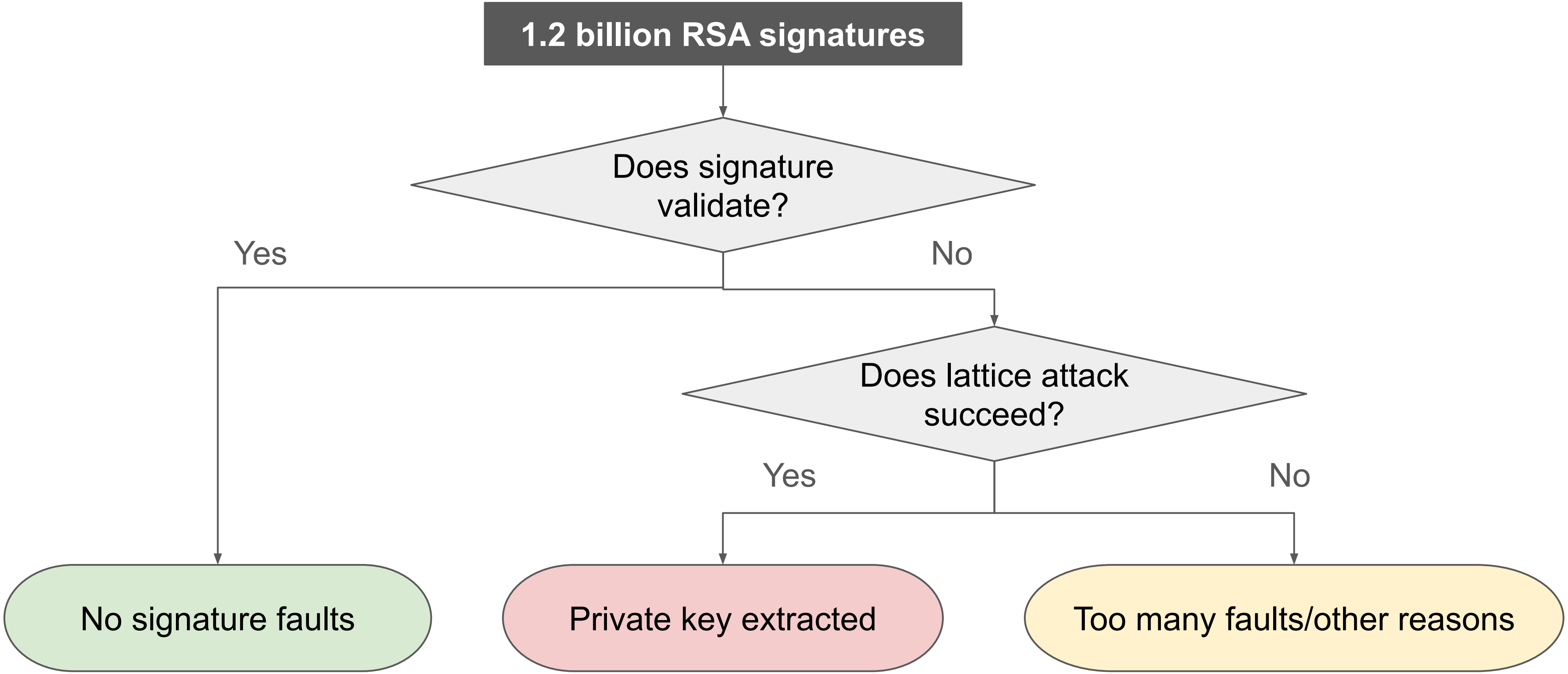
How frequently do keys leak on the internet?

We analyzed data from:

- Zmap scans performed at UCSD
- Passive network traffic through UCSD
- Censys
- University of Michigan

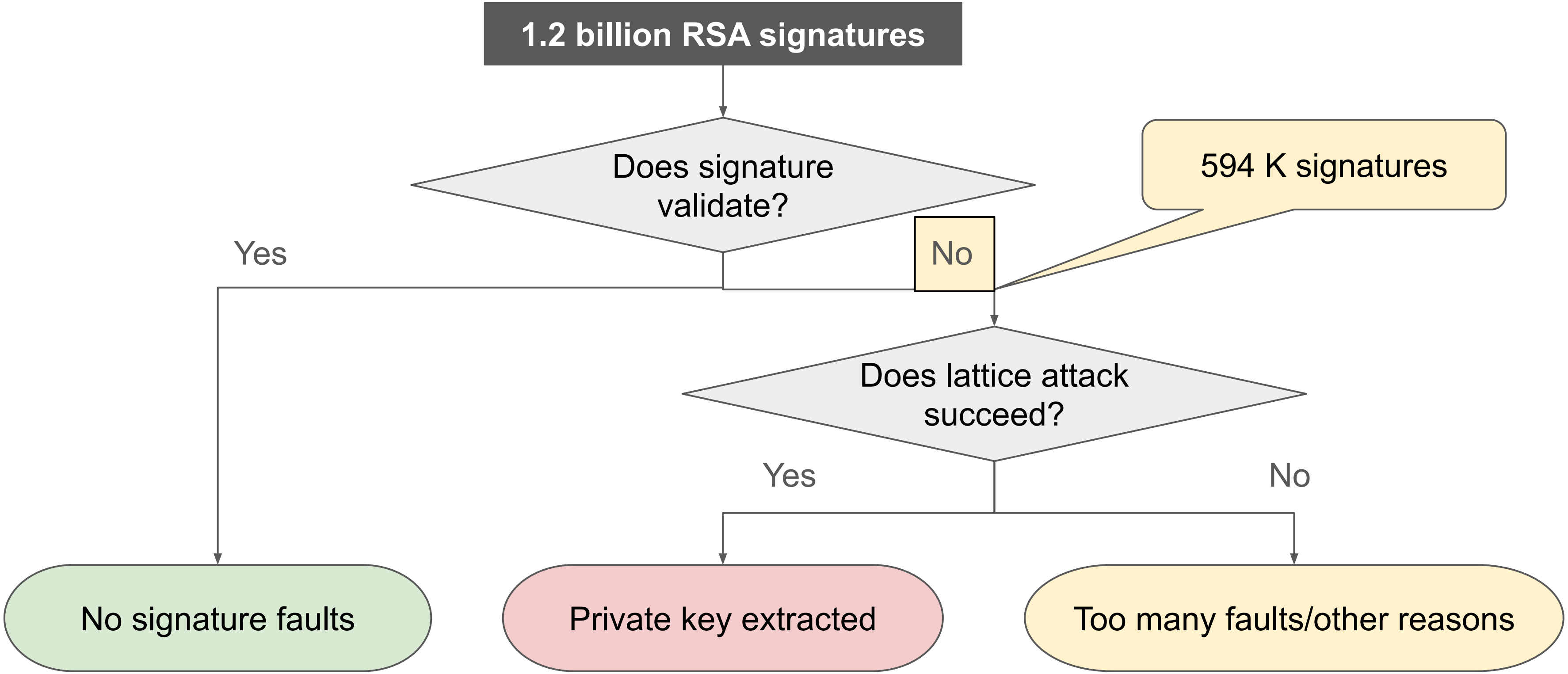


# Analysis



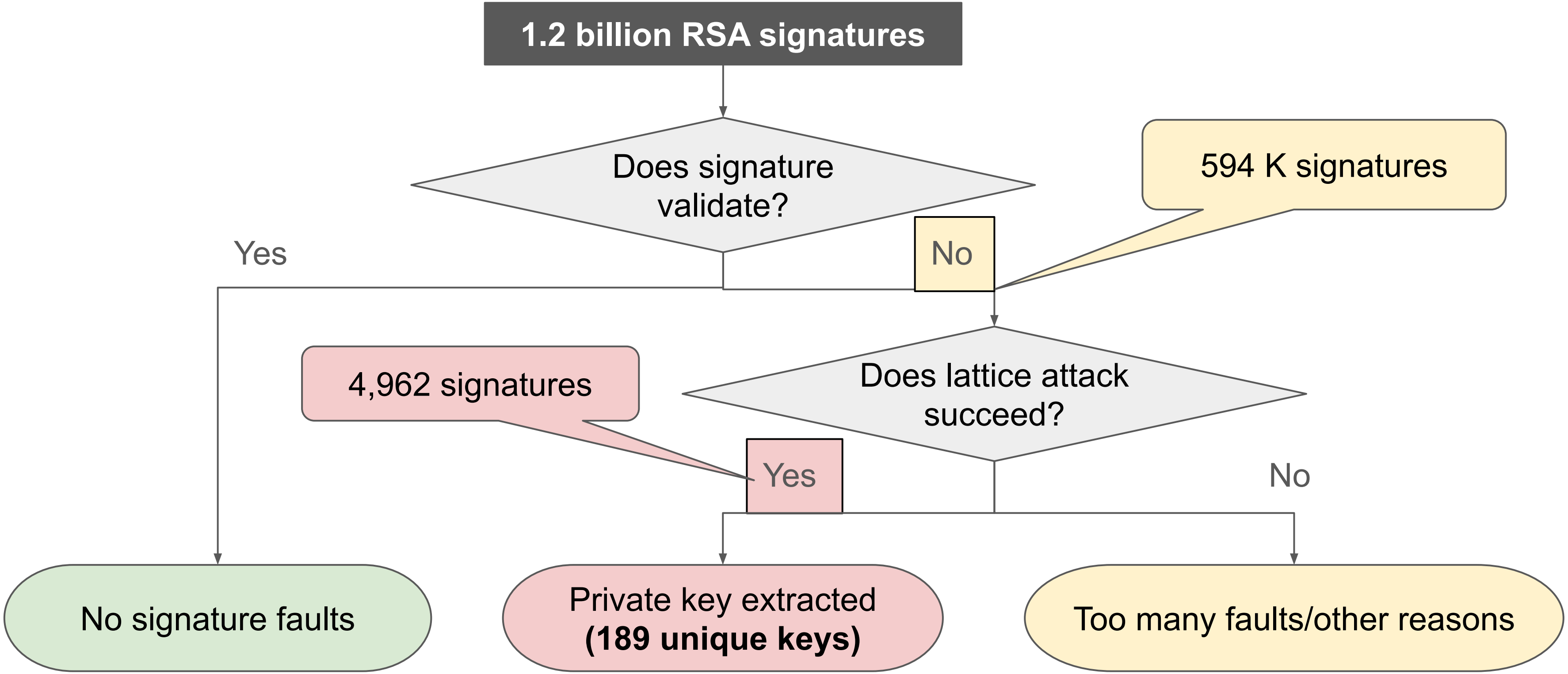
1.2 billion RSA signatures
Does signature validate?
Yes
No
Does lattice attack succeed?
Yes
No
No signature faults
Private key extracted
Too many faults/other reasons

# Analysis

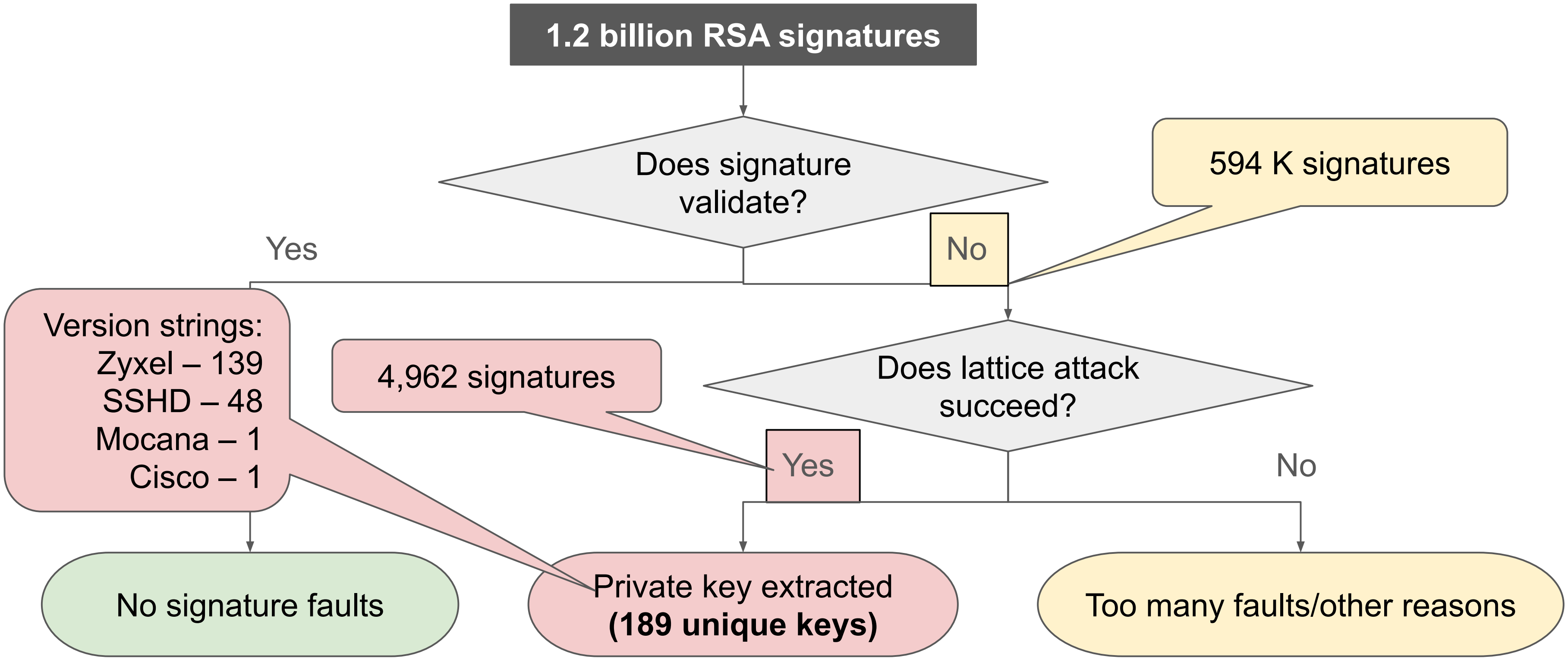


1.2 billion RSA signatures
Does signature validate?
594 K signatures
Yes
No
Does lattice attack succeed?
Yes
No
No signature faults
Private key extracted
Too many faults/other reasons

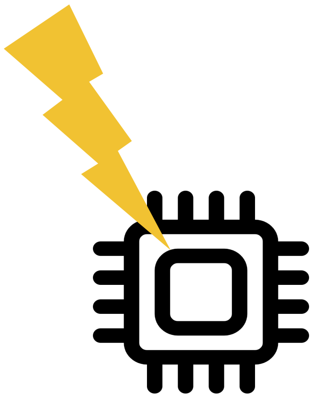
# Analysis


1.2 billion RSA signatures
Does signature validate?
594 K signatures
Yes
No
4,962 signatures
Does lattice attack succeed?
Yes
No
No signature faults
Private key extracted
(189 unique keys)
Too many faults/other reasons

# Analysis


1.2 billion RSA signatures
Does signature validate?
594 K signatures
Yes
No
Version strings:
Zyxel – 139
SSHD – 48
Mocana – 1
Cisco – 1
4,962 signatures
Does lattice attack succeed?
Yes
No
No signature faults
Private key extracted
(189 unique keys)
Too many faults/other reasons

# Lessons



Hypothesis: signature faults originate from hardware failures

Include random hardware faults in the threat model

**Countermeasure**: Validate signatures before sending

- OpenSSL and derivatives include this check
- Vulnerable implementations we observed do not have this countermeasure

# Future directions

- SSH: Collect `rsa-sha2-*` signatures
  - Potentially more vulnerable hosts are out there
- Collect more data passively
- Study similar key leaks on IPsec
  - Our visibility into IPsec hosts is limited

# Summary

**A single faulty signature reveals the private SSH host key to eavesdroppers**

- Private host key allows attacker to later impersonate server
- About 1 out of 1 million analyzed signatures on the internet are vulnerable

We disclosed the vulnerability to device vendors:

- Mitigations confirmed for Cisco, Zyxel, and Hillstone Networks
- Unable to contact Mocana

# Passive SSH Key Compromise via Lattices

https://ia.cr/2023/1711

Keegan Ryan[1] kryan@ucsd.edu
Kaiwen He[2] khe01@mit.edu
George Arnold Sullivan[1] gsulliva@ucsd.edu
Nadia Heninger[1] nadiah@cs.ucsd.edu

[1] UC San Diego

[2] UC San Diego, MIT

ACM CCS, November 2023

# References

[BDL97]: Dan Boneh, Richard A. DeMillo, and Richard J. Lipton. 2001. On the Importance of Eliminating Errors in Cryptographic Computations. Journal of Cryptology 14, 2 (March 2001), 101–119. https://doi.org/10.1007/s001450010016

[CJK+09]: Jean-Sébastien Coron, Antoine Joux, Ilya Kizhvatov, David Naccache, and Pascal Paillier. 2009. Fault Attacks on RSA Signatures with Partially Unknown Messages. Cryptology ePrint Archive, Report 2009/309. https://eprint.iacr.org/2009/309.

[How01]: Nick Howgrave-Graham. 2001. Approximate Integer Common Divisors. In *Cryptography and Lattices*, Joseph H. Silverman (Ed.). Springer Berlin Heidelberg, Berlin, Heidelberg, 51–66.

[Len96]: Arjen K Lenstra. 1996. Memo on RSA signature generation in the presence of faults. Technical Report. EPFL. https://infoscience.epfl.ch/record/164524.

[SSH+22]: George Arnold Sullivan, Jackson Sippe, Nadia Heninger, and Eric Wustrow. 2022. Open to a fault: On the passive compromise of TLS keys via transient errors. In 31st USENIX Security Symposium (USENIX Security 22). USENIX Association, Boston, MA, 233–250. https://www.usenix.org/conference/usenixsecurity22/presentation/sullivan

[Wei15]: Florian Weimer. 2015. *Factoring RSA Keys With TLS Perfect Forward Secrecy*. Technical Report. Red Hat. https://www.redhat.com/en/blog/factoring-rsa-keys-tls-perfect-forward-secrecy.