IoT: Security and Privacy

Dan Boneh

Stanford University

Private discovery via secret handshakes

attributes X

CA

Cert on attr. X

Cert on attr. Y

Attributes Y

only want to talk
to devices s.t. P(Y) = 1

only want to talk
to devices s.t. Q(X) = 1

problem: neither side wants to reveal its attributes

secret handshake protocol

key k only if P(Y)=1

key k only if Q(X) = 1

key confirmation

IoT Data Collection

Wearables

Home

Mobile devices

Data analysis for:
- Visualization
- Personalization
- Recommendation

Analysis of single user data:
- on premise

Analyzing data from multiple users?

Why?
- Build model of user behavior
- Use for recommendations, warnings, reputation

Social games
- Who walked the most today
- Who used the least energy

Cleartext data

Cloud

analysis results

The Cloud

Today: stores lots of (IoT) data in the clear

- A good target for attacks/subpoenas
- Some users will not use (context specific data)

Ideal solution:

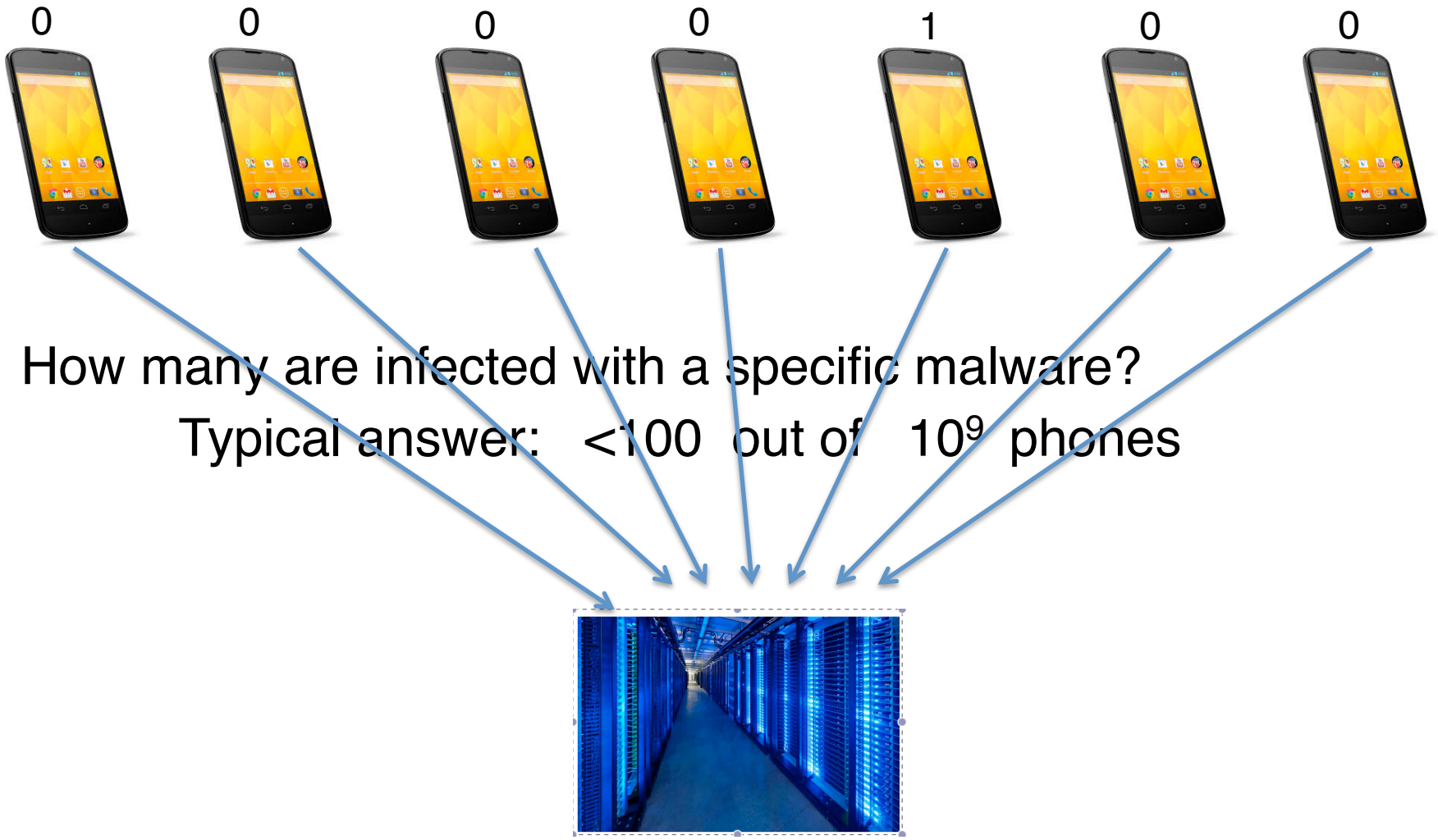
- Provide same services (recommendations, personalization)

  … but without ever seeing user data in the clear

Can an IoT cloud provide services without seeing data in the clear?

An example: counting rare events

[MNB'15]

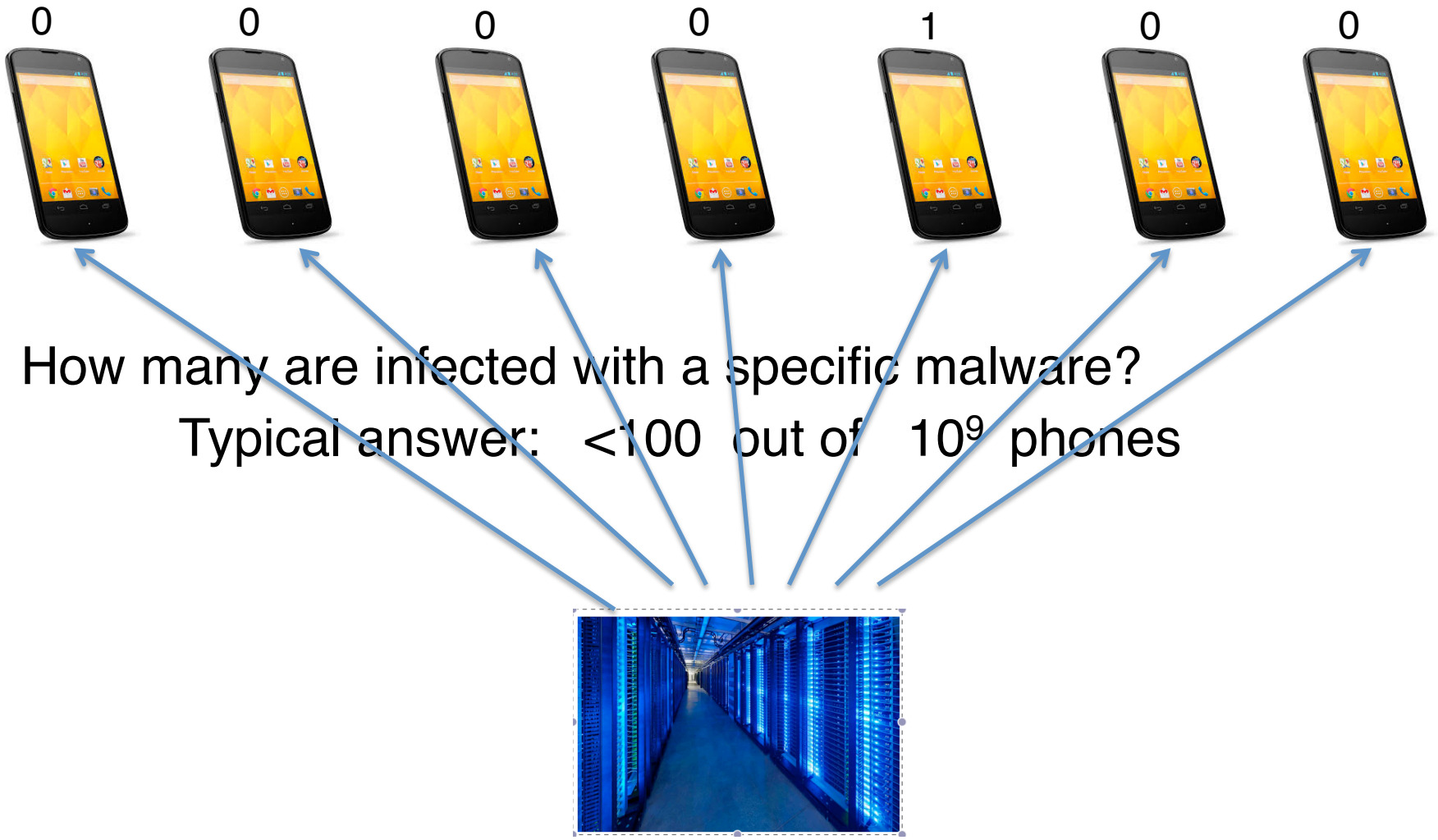


How many are infected with a specific malware?

Typical answer: <100 out of 10^9 phones

An example: counting rare events

[MNB'15]



How many are infected with a specific malware?

Typical answer: <100 out of 10^9 phones

An example: counting rare events

[MNB'15]

How many are infected with a specific malware?

Typical answer: <100 out of 10^9 phones

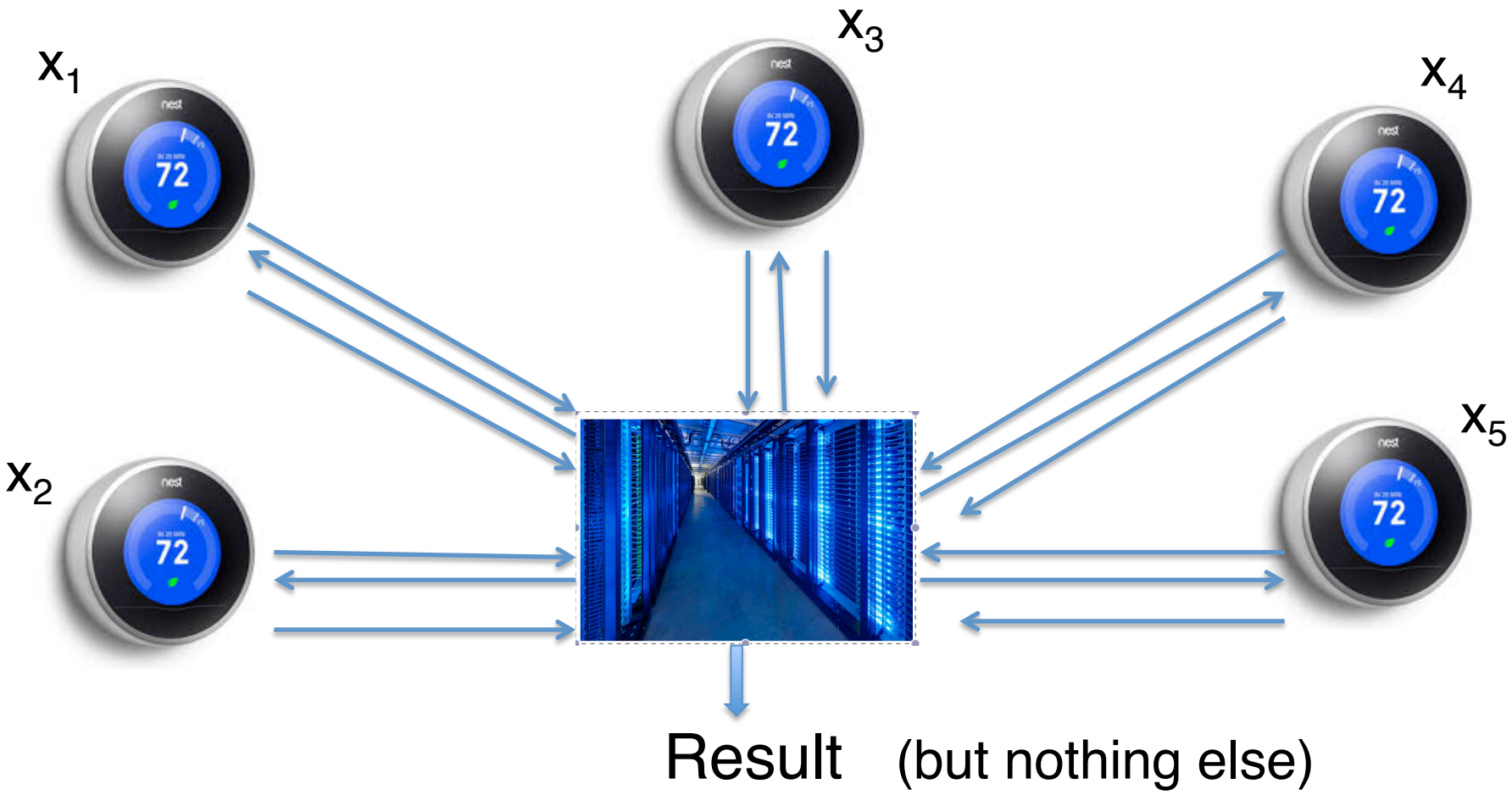
$\sum b_i$

(and nothing else)

More generally: keep data on IoT device

Current work:

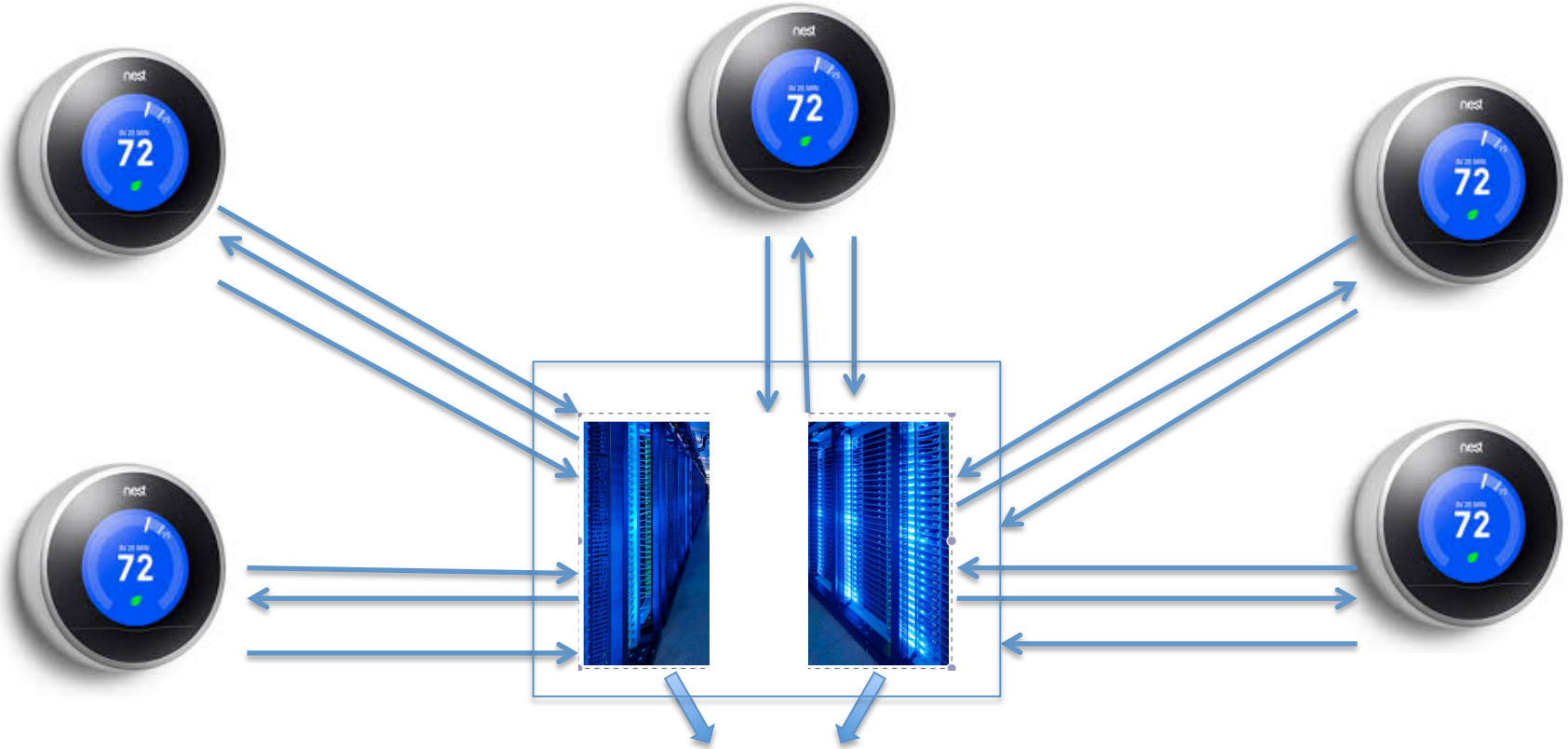
implementing secure computation with millions of devices



Improved efficiency with non-colluding clouds

Example: simple protocols for counting rare events

Is this a reasonable assumption?



THE END