SDDR: Light-Weight, Secure Mobile Encounters

Matthew Lentz, Viktor Erdélyi, Paarijaat Aditya
Elaine Shi, Peter Druschel, Bobby Bhattacharjee

University of Maryland

Max Planck Institute
for Software Systems

Mobile Social Applications

Services based on user context:

① **location** ② **activity** ③ **nearby peers**

Latitude

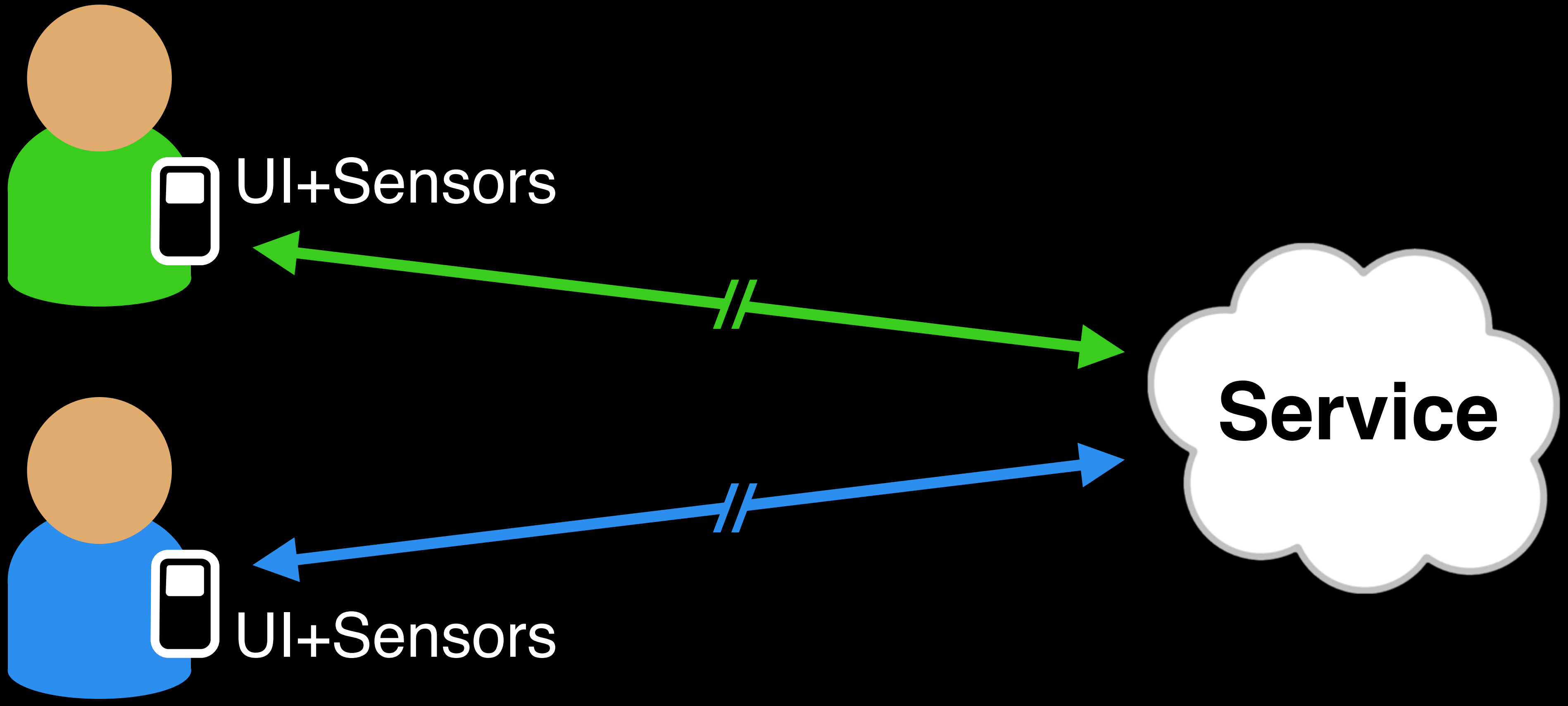
Foursquare

FireChat

Haggle

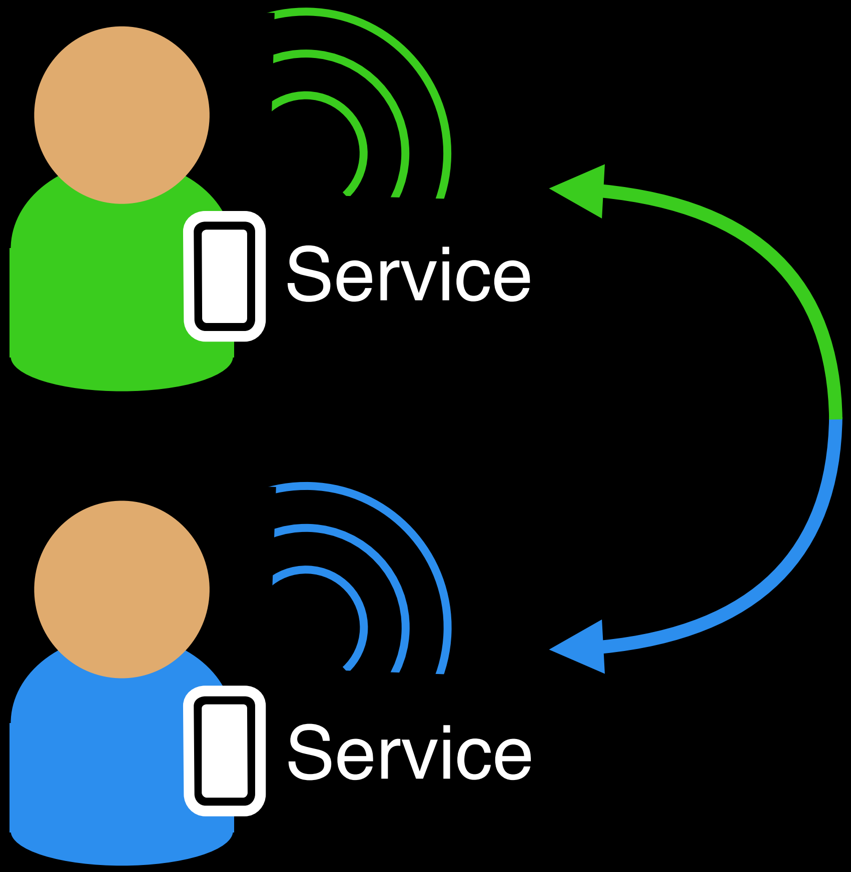
Highlight

Common: Centralized Service

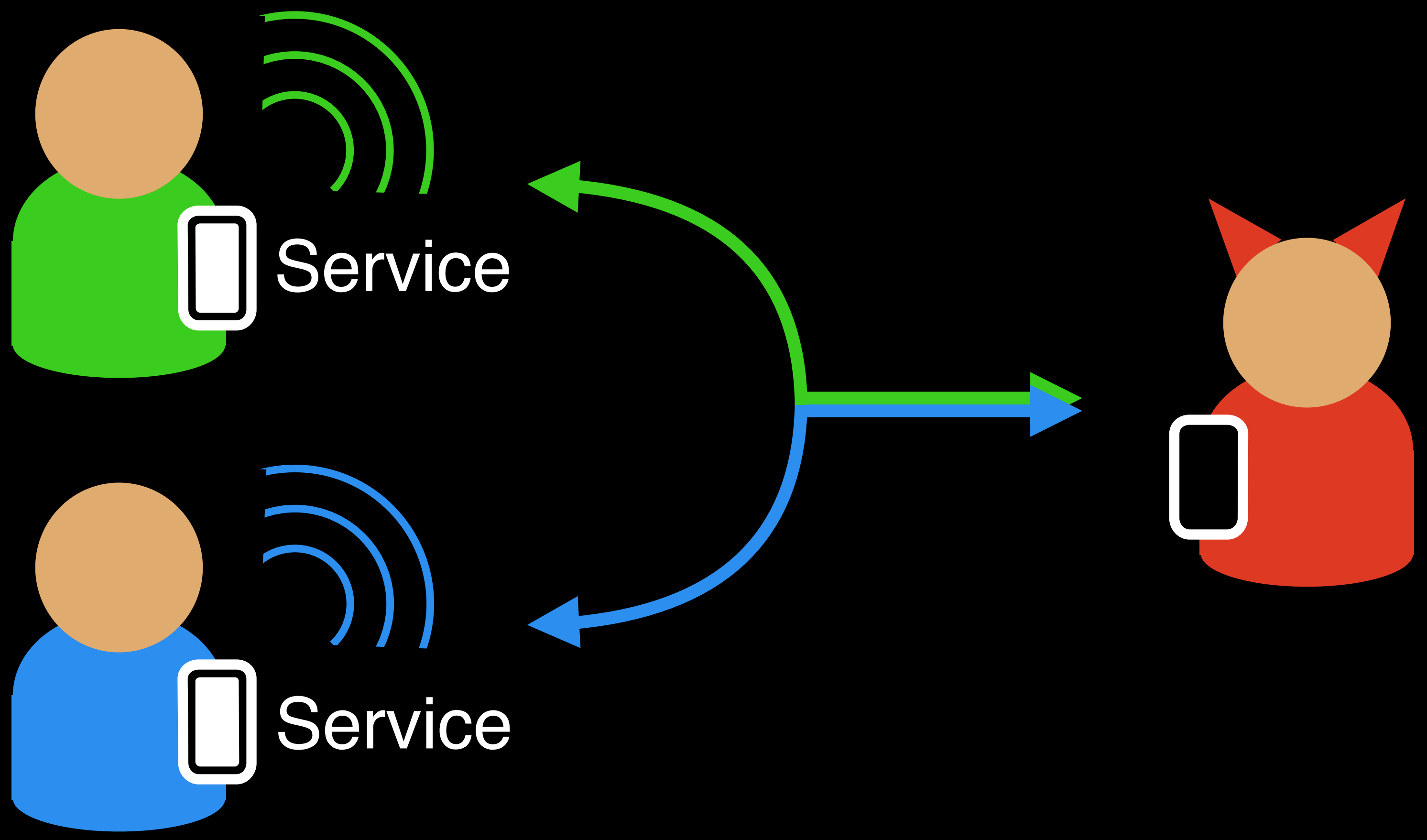


Involves a trusted third party

Alternate: Device-to-Device

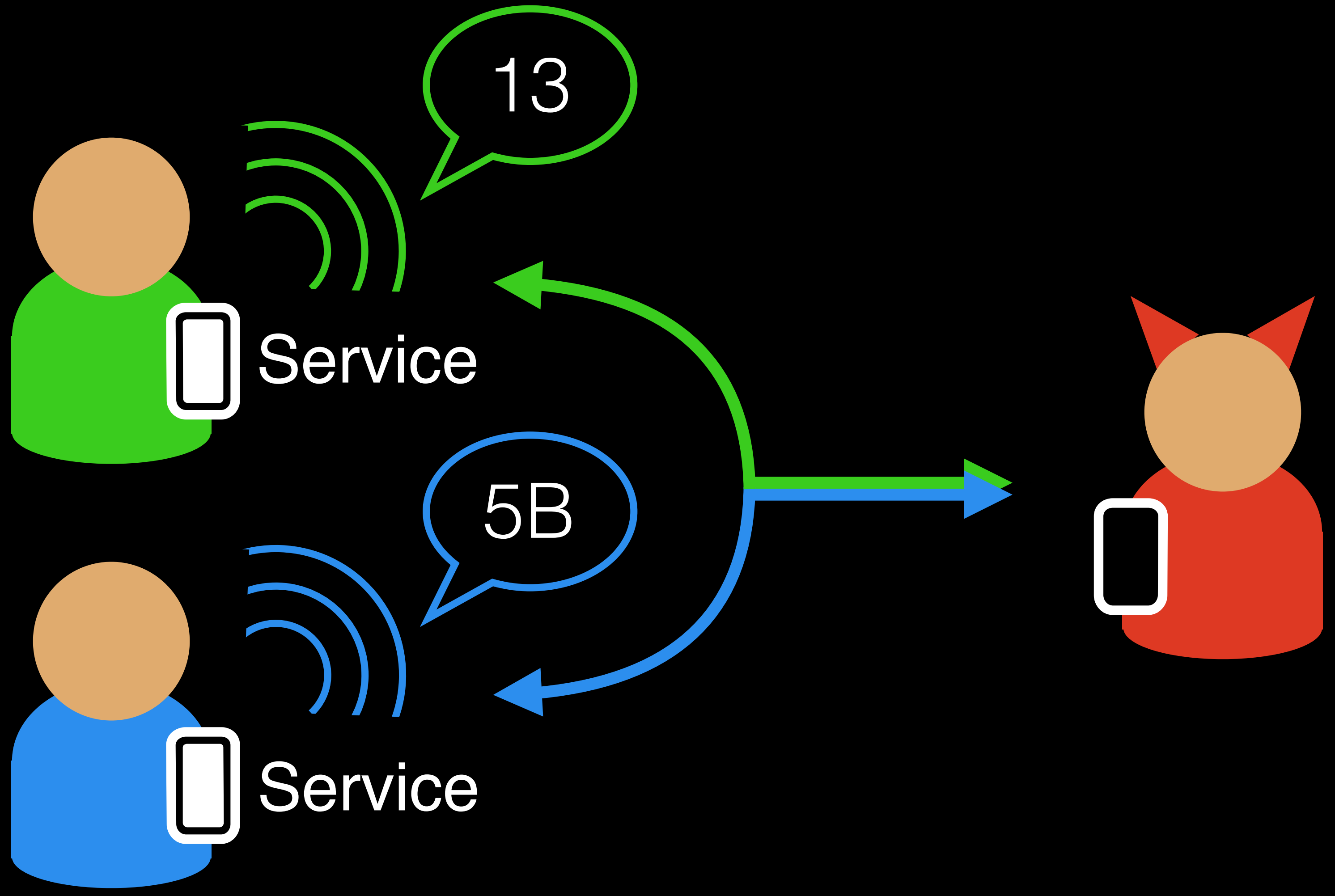


Alternate: Device-to-Device



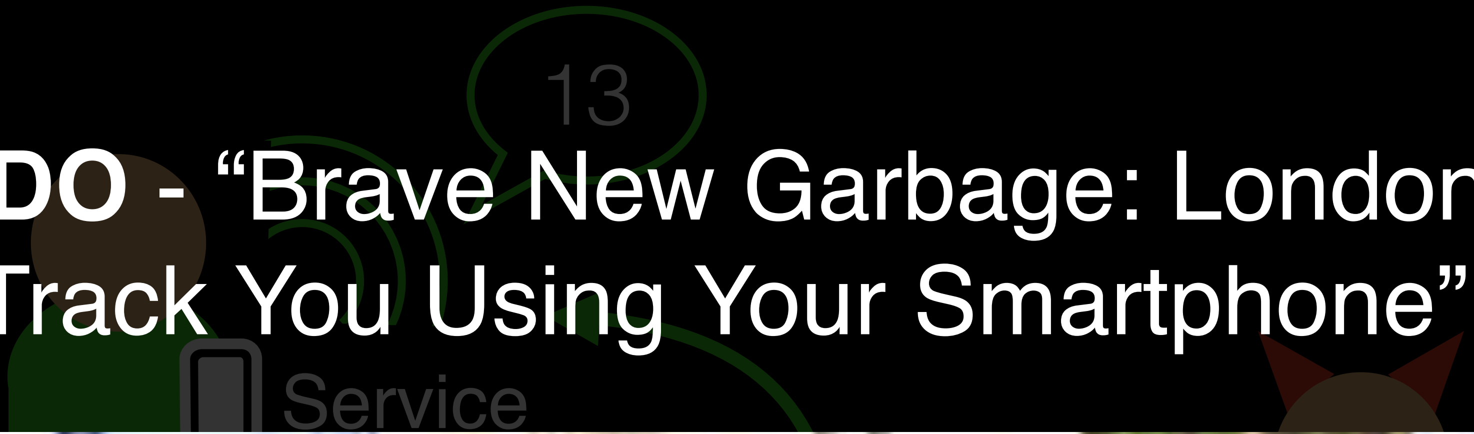
Enables tracking by adversaries

Alternate: Device-to-Device

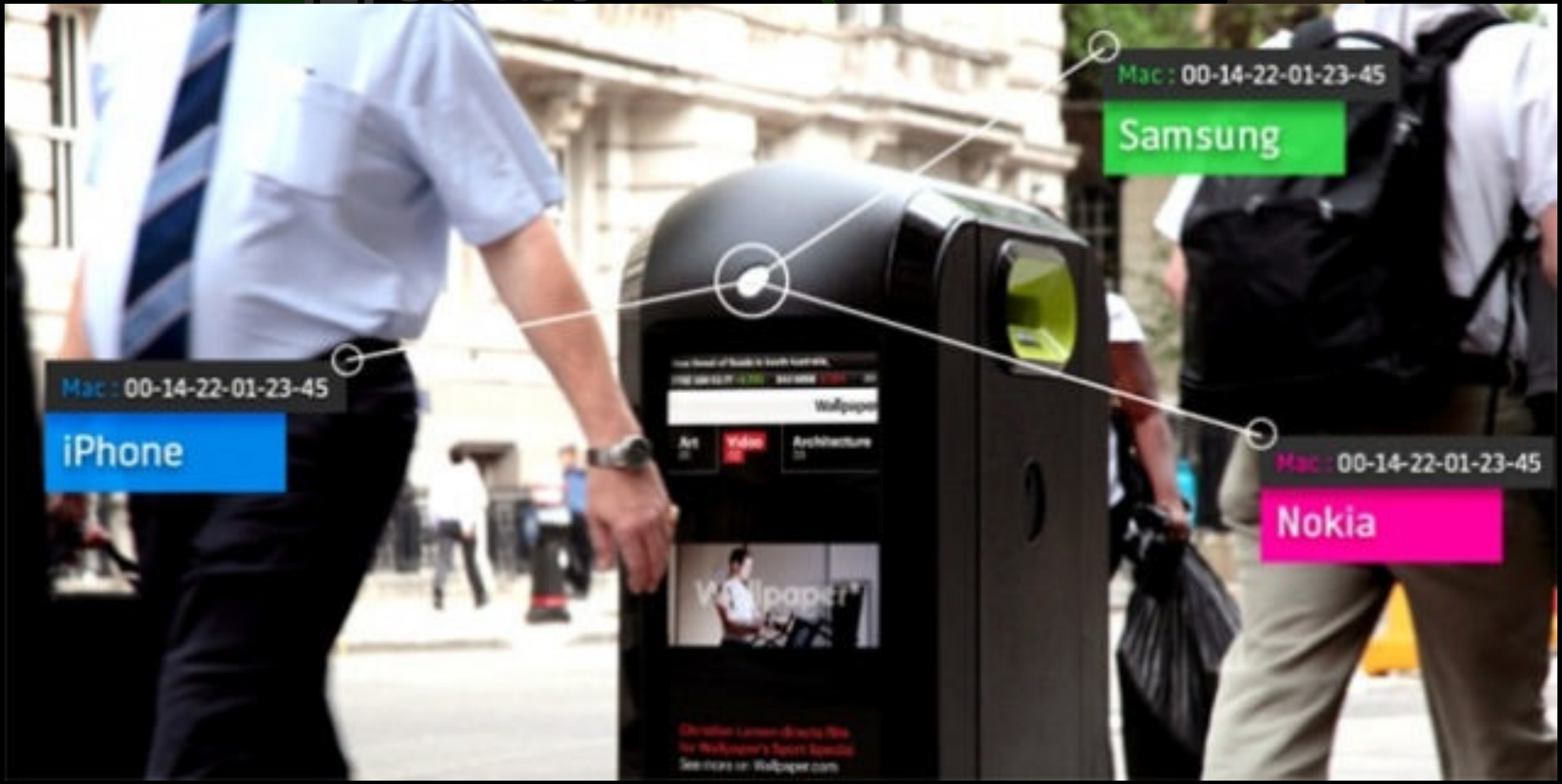


Enables tracking by adversaries

Alternate: Device-to-Device

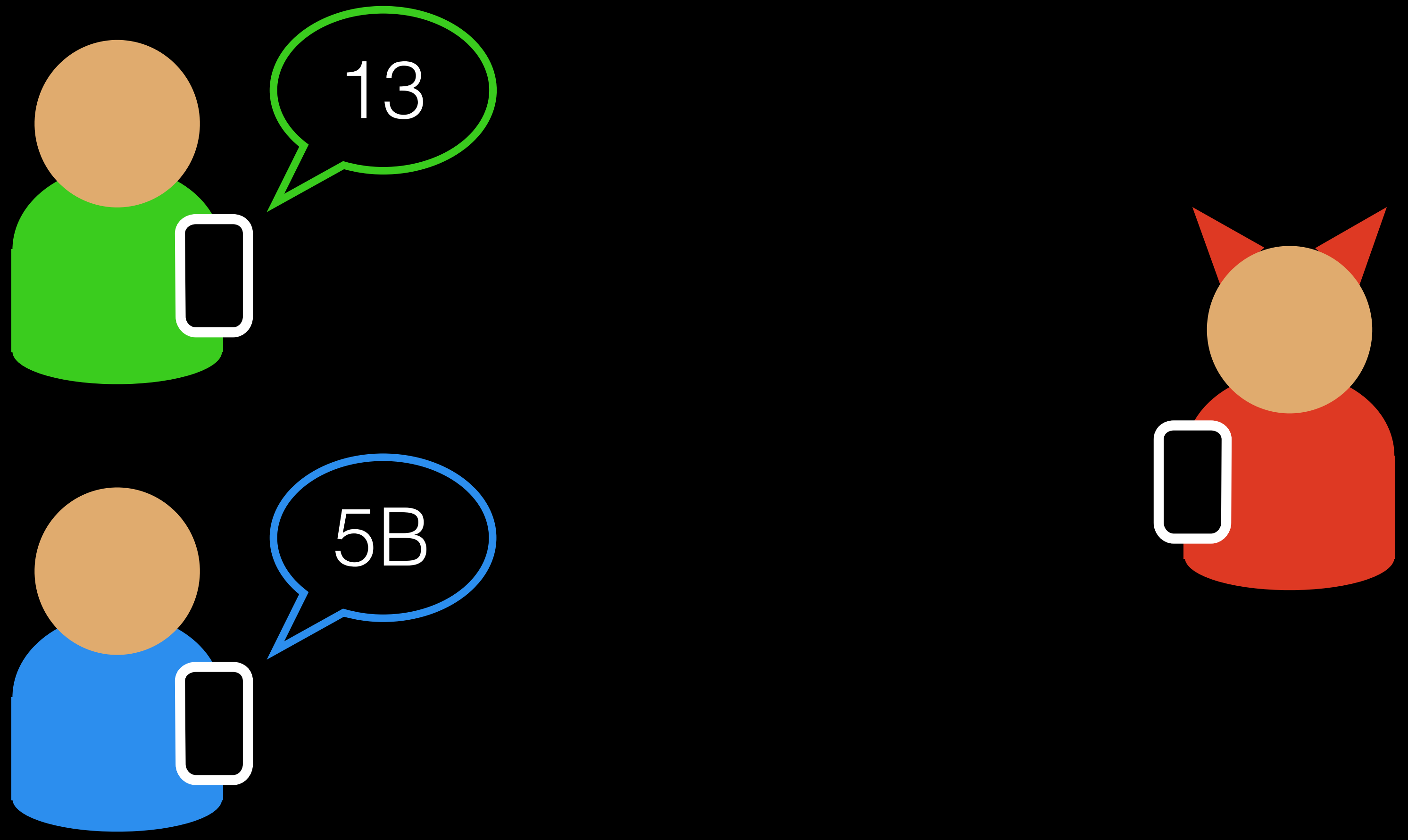


GIZMODO - “Brave New Garbage: London’s Trash Cans Track You Using Your Smartphone” (2013)

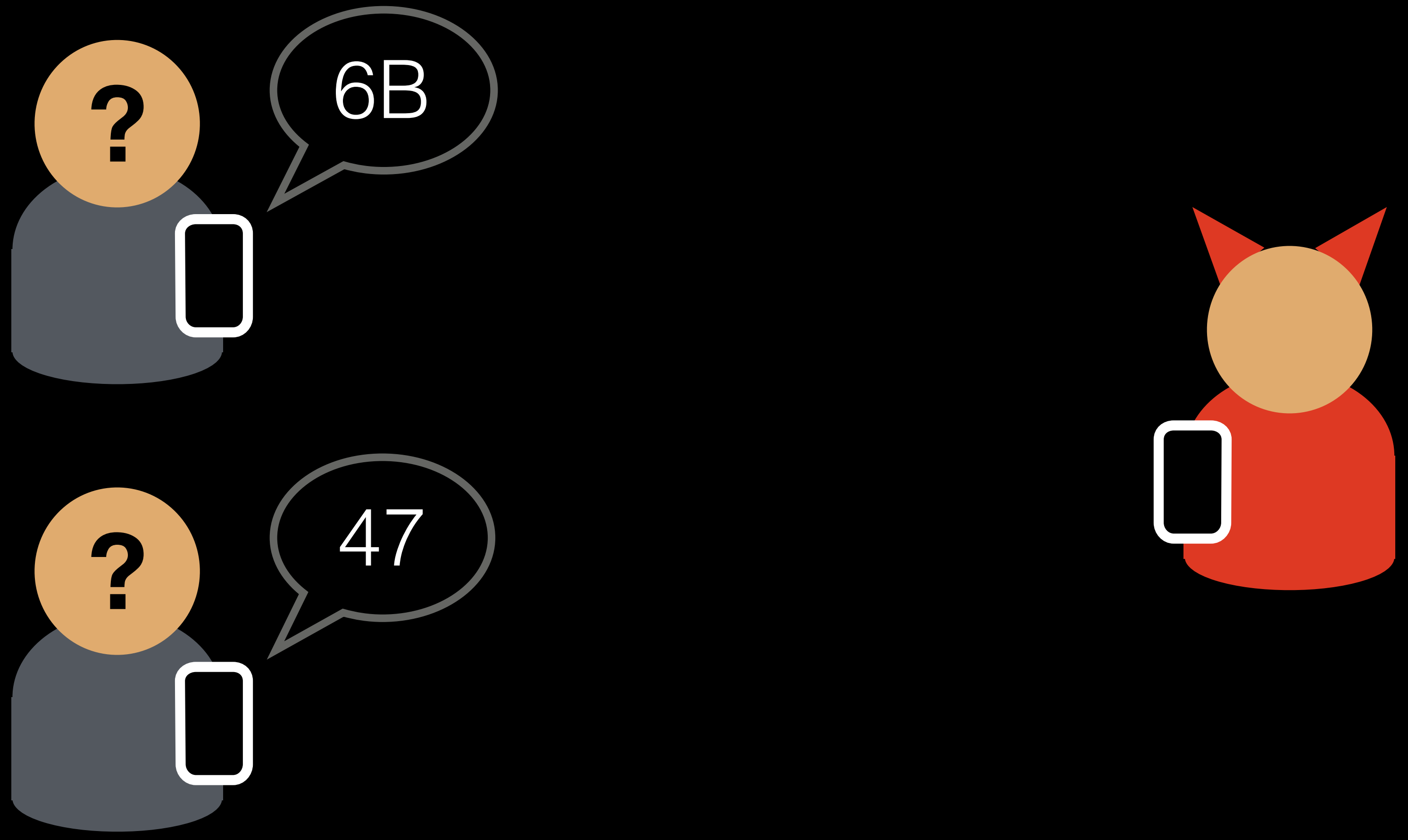


Credit: http://gizmodo.com/brave-new-garbage-londons-trash-cans-track-you-using-1071610114

Randomize Addresses?



Randomize Addresses?

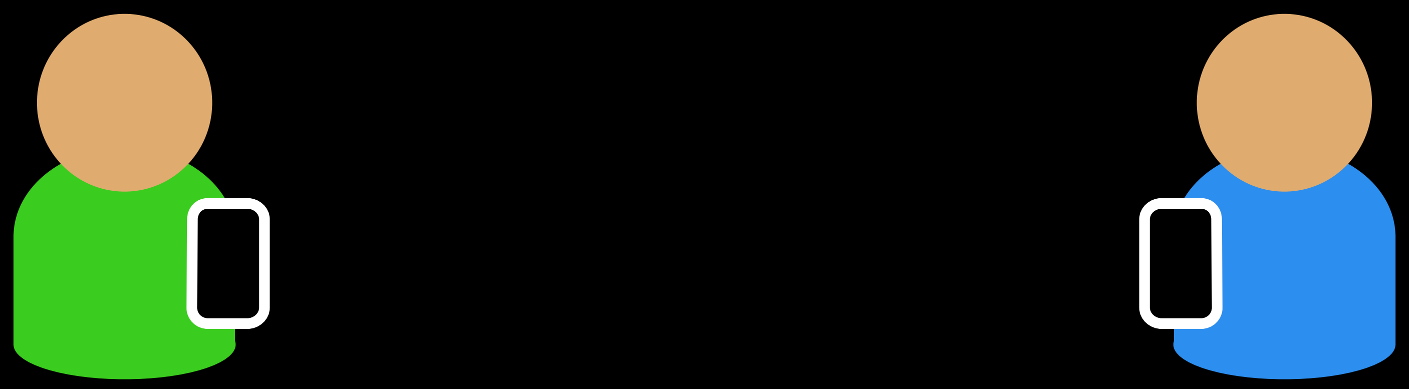


Unlinkable, but does not support **recognition**!

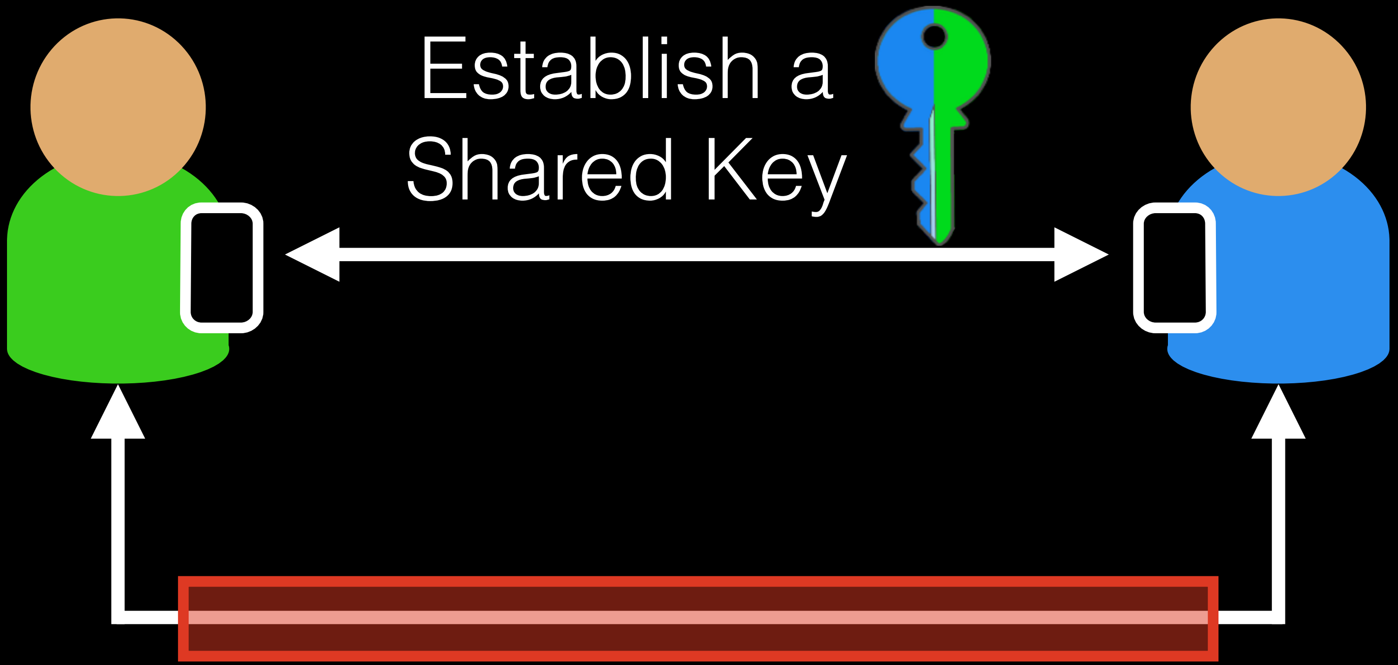
Secure Device Discovery and Recognition

1. Secure Encounter Primitive
2. Strawman Protocol
3. System Goals and SDDR Protocol
4. Evaluation and Concurrent Work

Secure Encounters



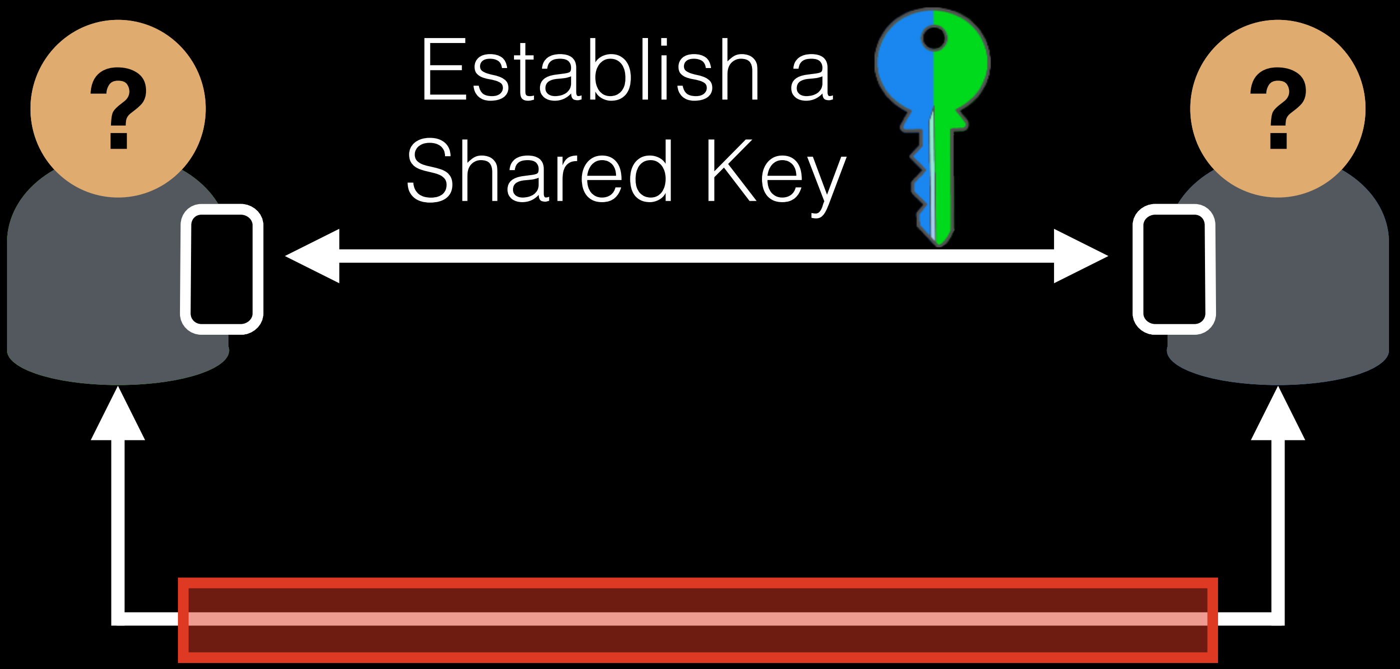
Secure Encounters



Establish a Shared Key

Secure communication through untrusted channel (e.g., pseudonymous email)

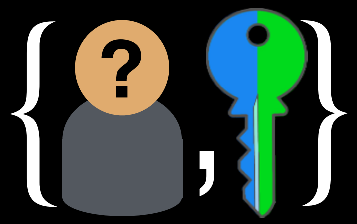
Secure Encounters



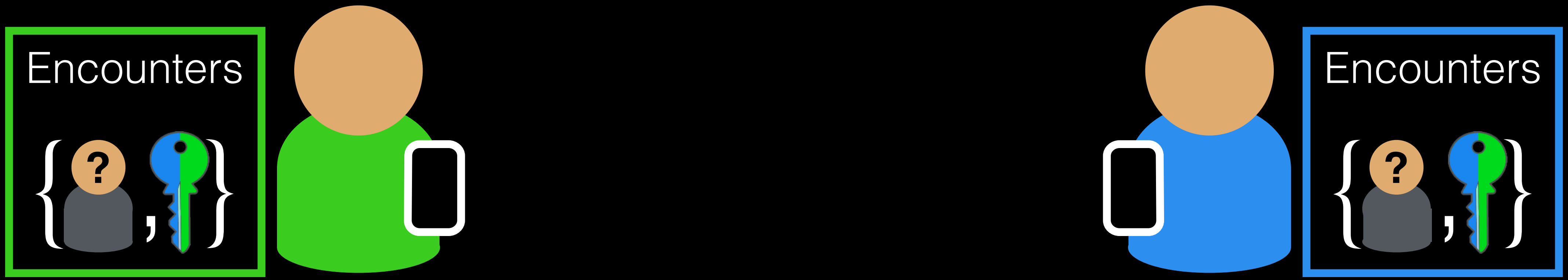
Establish a Shared Key

Secure communication through untrusted channel (e.g., pseudonymous email)

Unlinkable by default

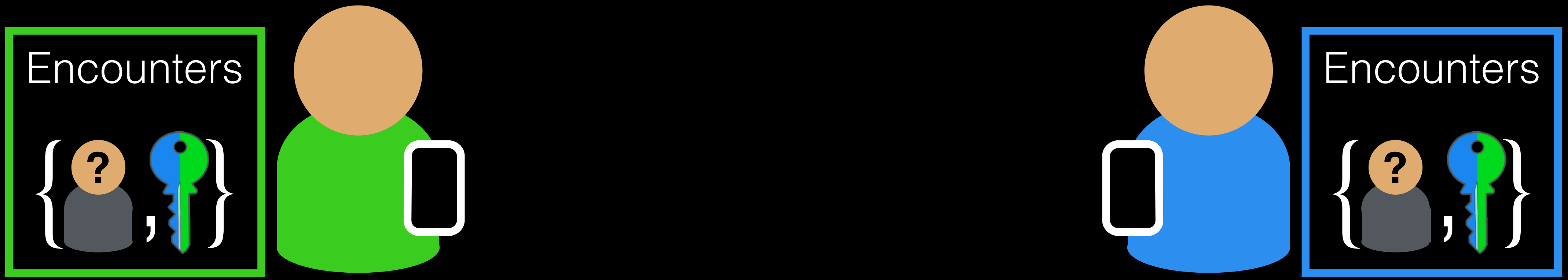


Recognition

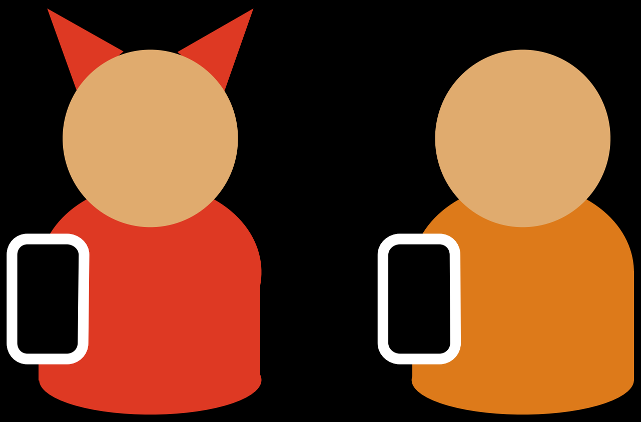


Want to **recognize** each other in encounters

Recognition

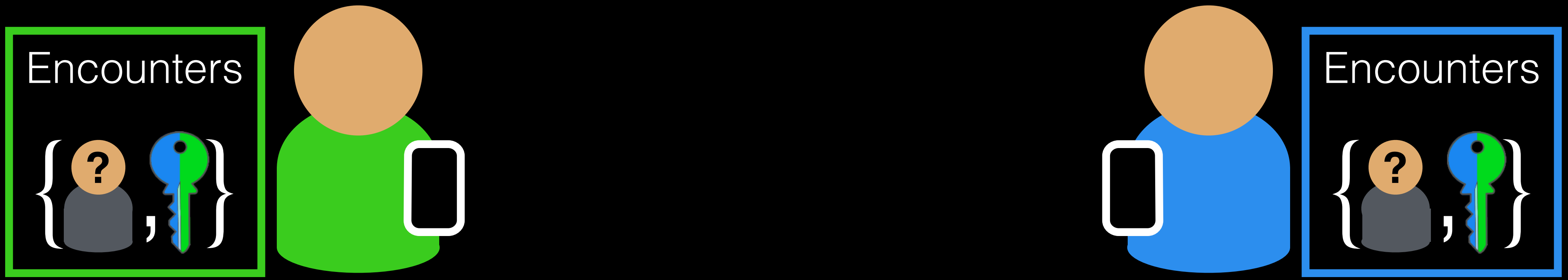


Want to **recognize** each other in encounters

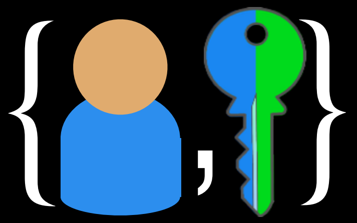


… while remaining **unlinkable** by others

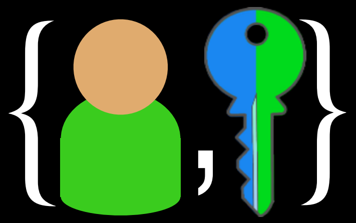
Recognition



Want to **recognize** each other in encounters



Map ephemeral pseudonyms to long-lived identities



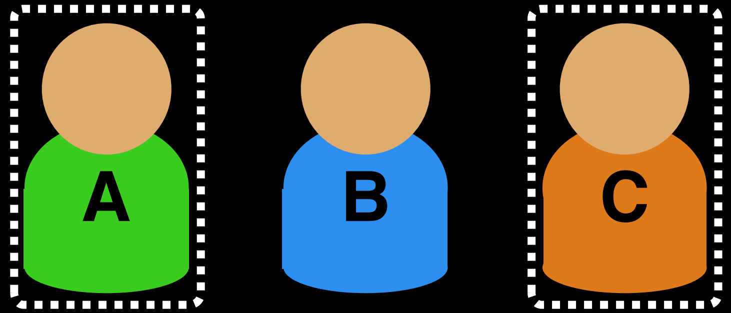
Revocation and Scoping

No Longer Friends

Temporary Friends

Only At Work

Only After 8pm



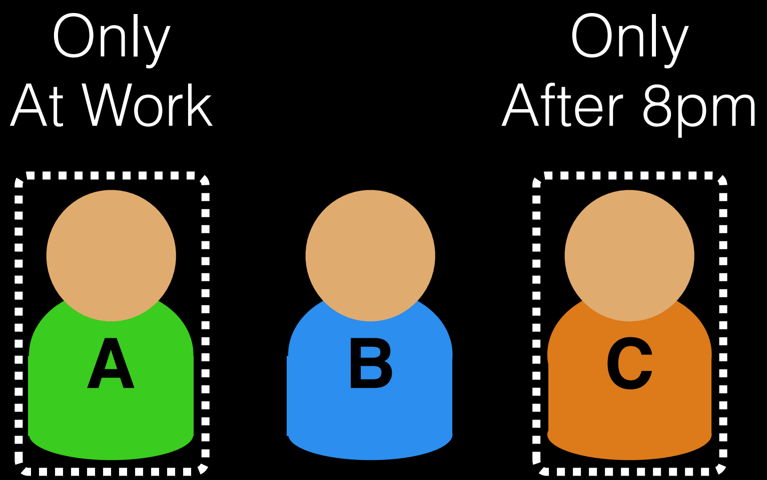
Context-based Scoping

Allow recognizability by friends using context-based constraints

Revocation and Scoping

No Longer Friends

Temporary Friends



Context-based Scoping

Allow recognizability by friends using context-based constraints

Efficient and **unilateral** revocation is required

Security Properties

Discover devices while preserving user privacy

Secure communication between encounter peers

Recognize peers with prior trust relations
and support efficient, unilateral **revocation**

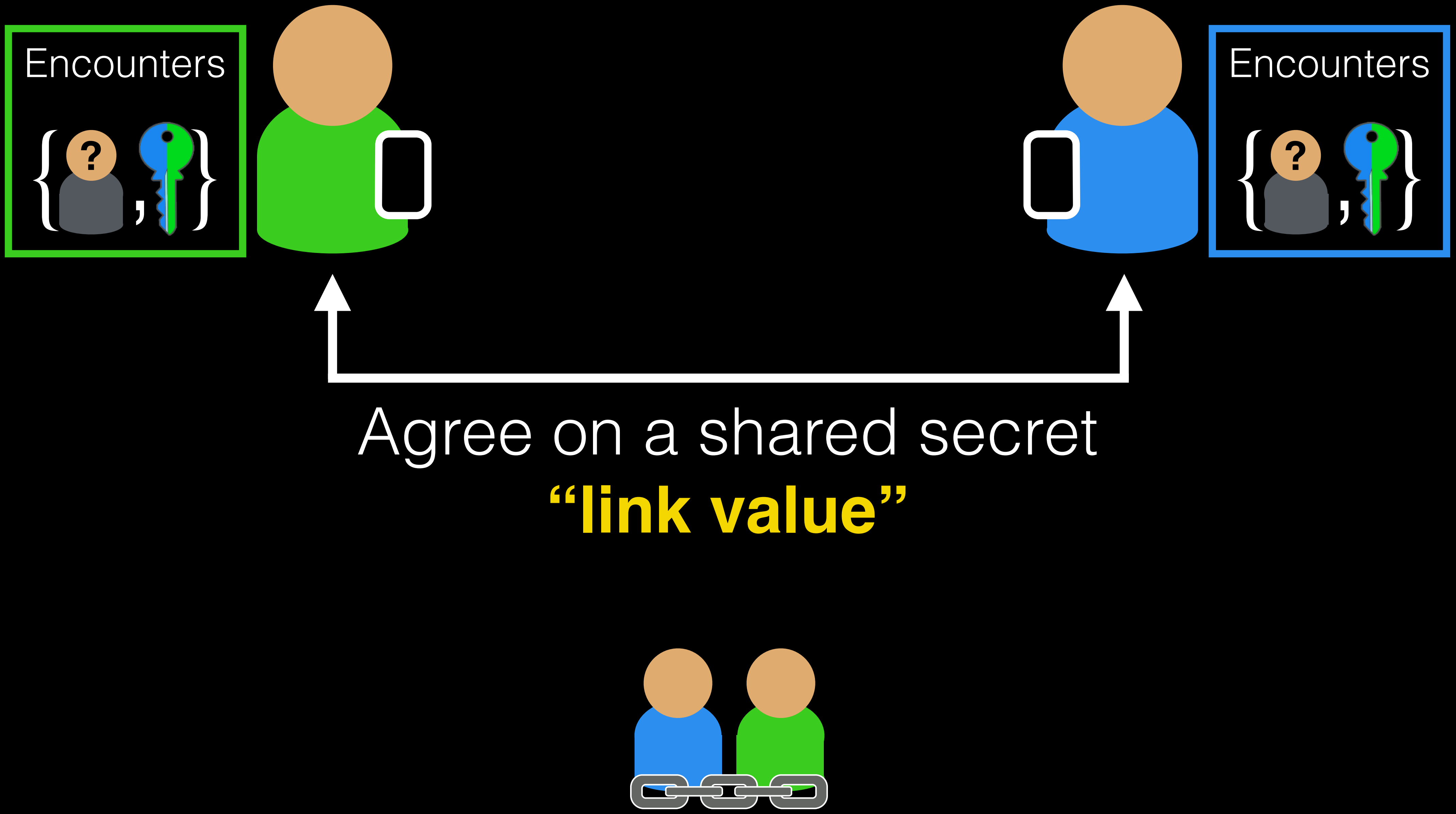
Threat Model

Trust OS and apps on your phone

No PHY layer attacks considered

Participate with all nearby devices
(*arbitrary* subset of colluding attackers)

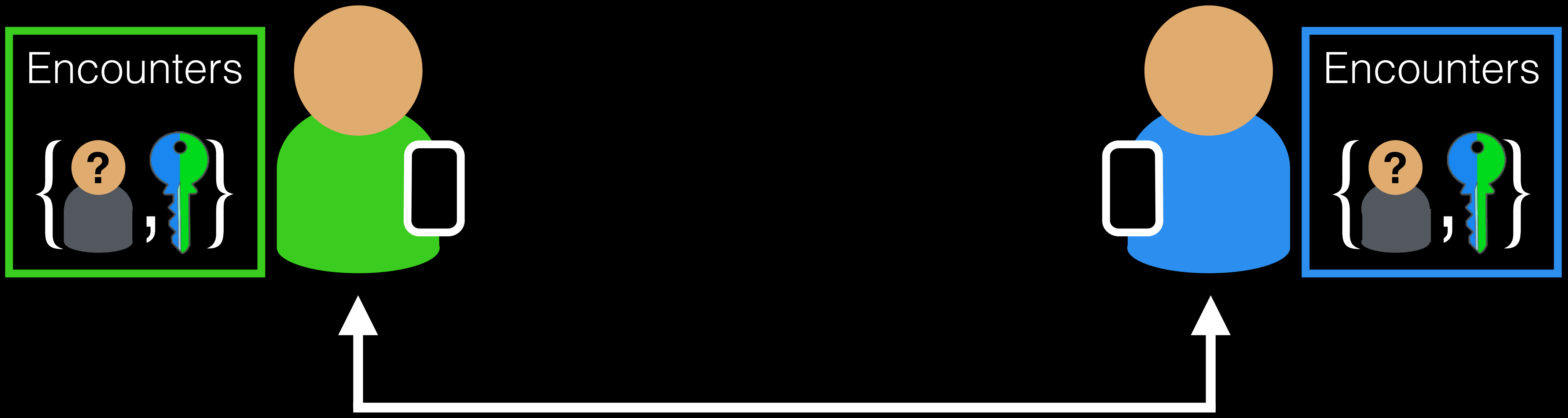
Enabling Recognition



Agree on a shared secret

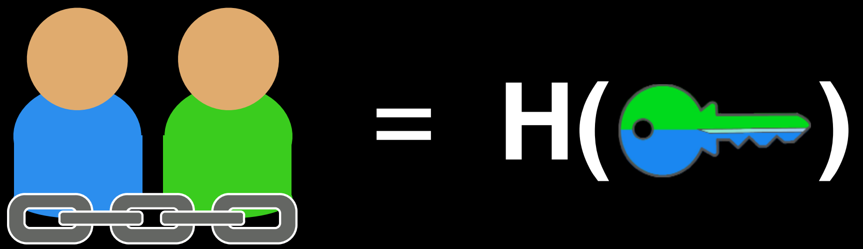
“link value”

Enabling Recognition

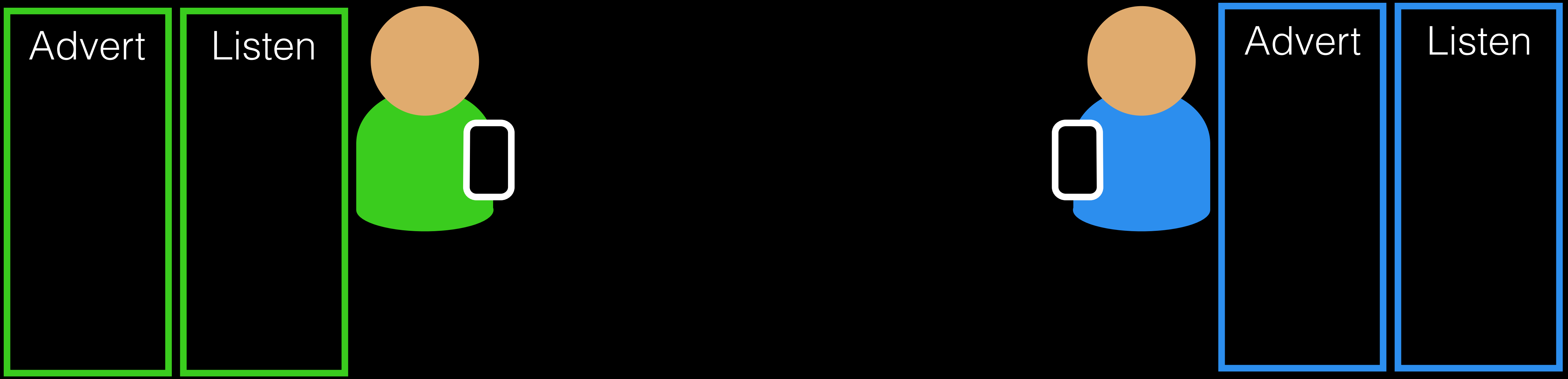


Agree on a shared secret

“link value”



Recognition and Revocation



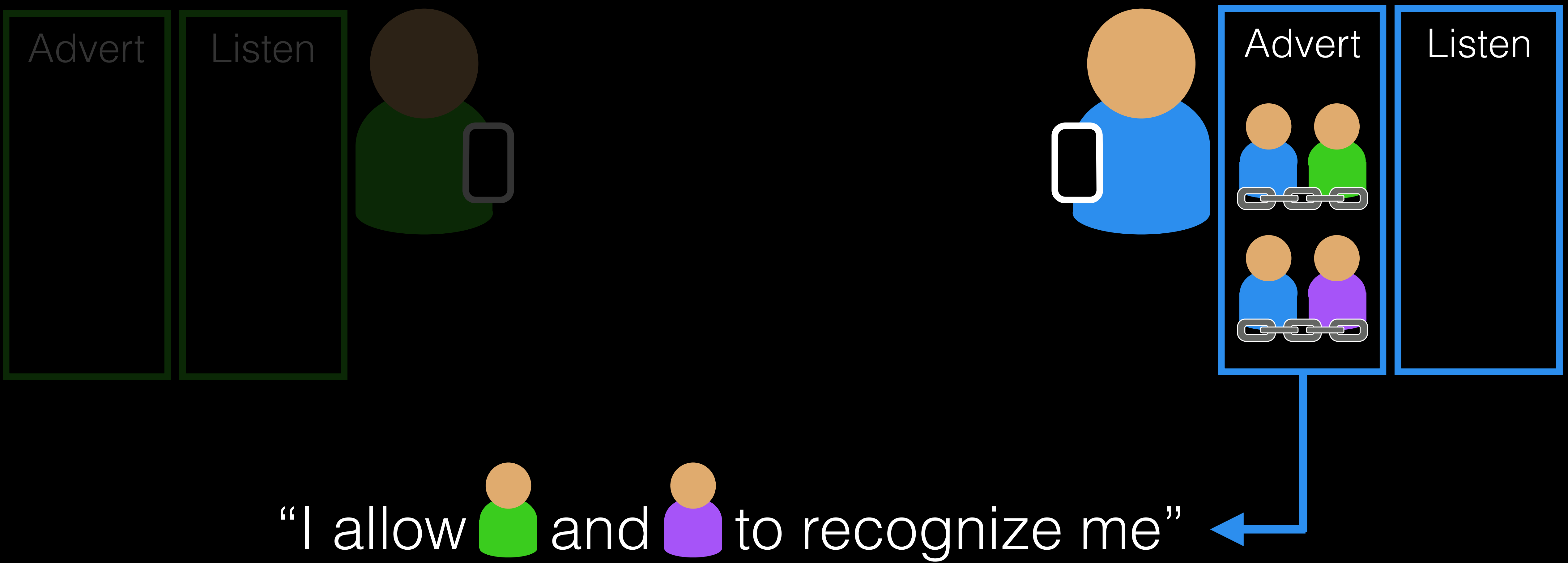
Advert

Listen

Advert

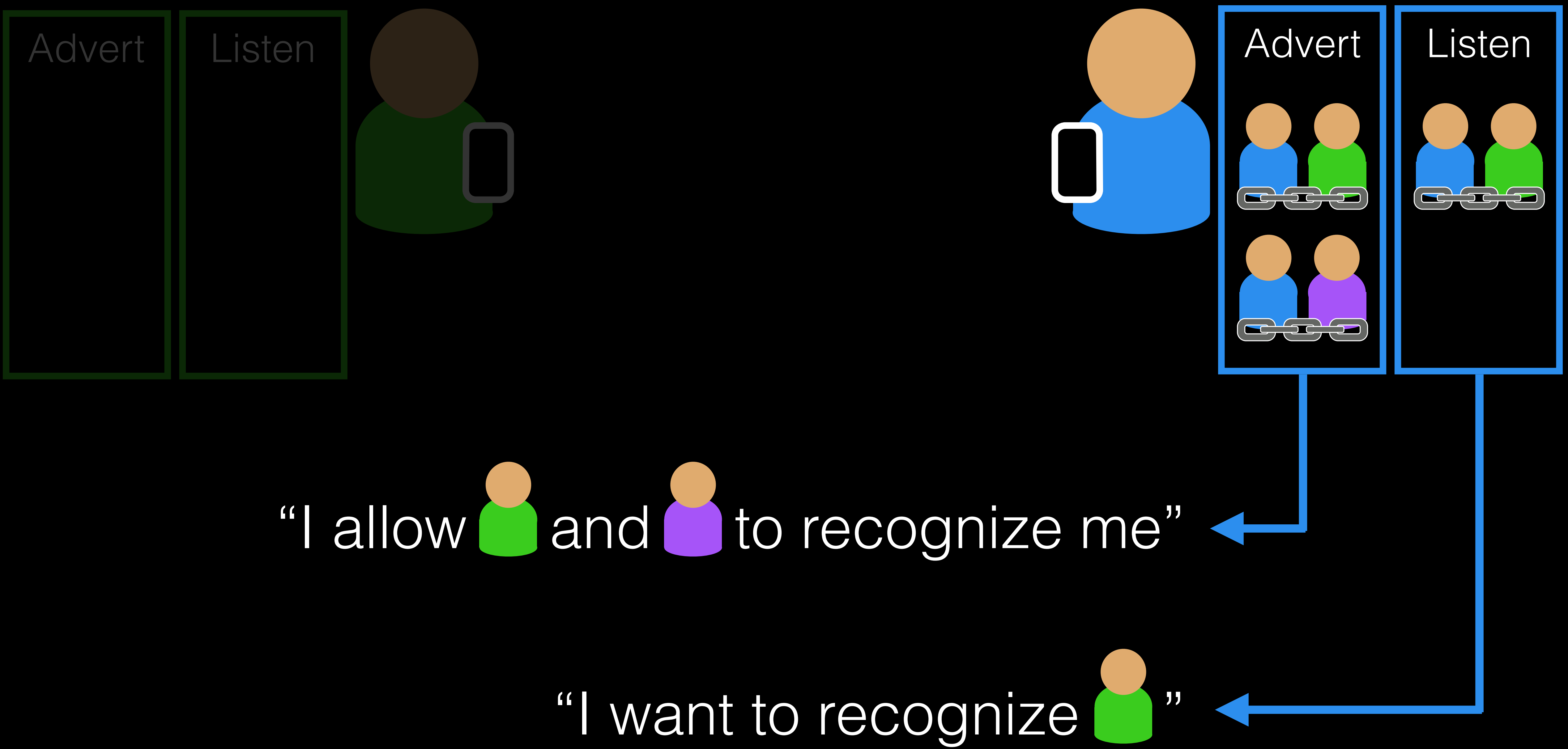
Listen

Recognition and Revocation



“I allow 🟩 and 🟪 to recognize me”

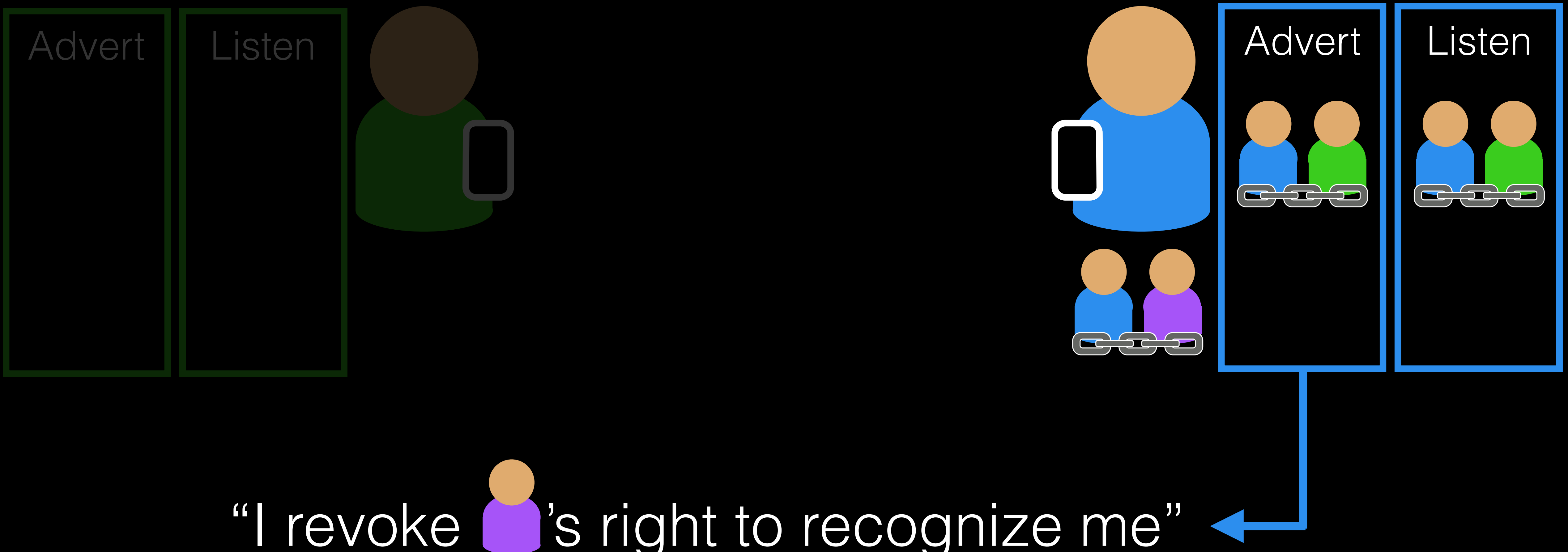
Recognition and Revocation



"I allow 🟩 and 🟪 to recognize me"

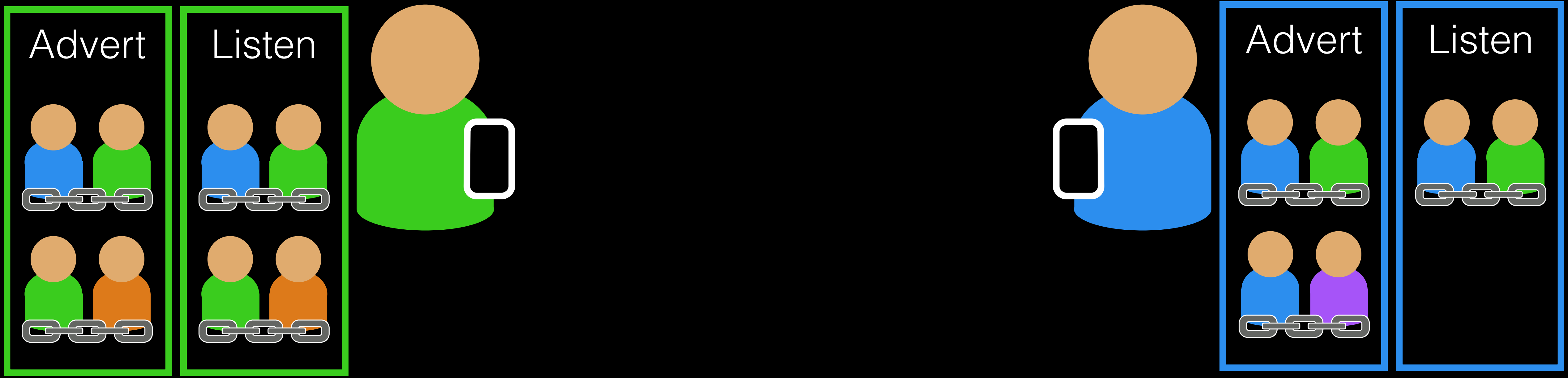
"I want to recognize 🟩"

Recognition and Revocation

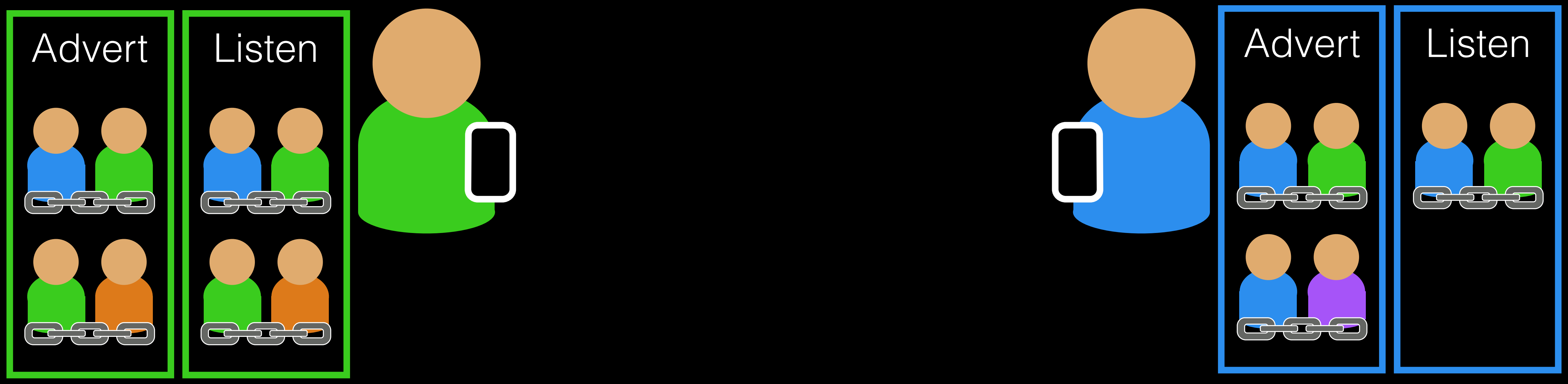


“I revoke 👤’s right to recognize me”

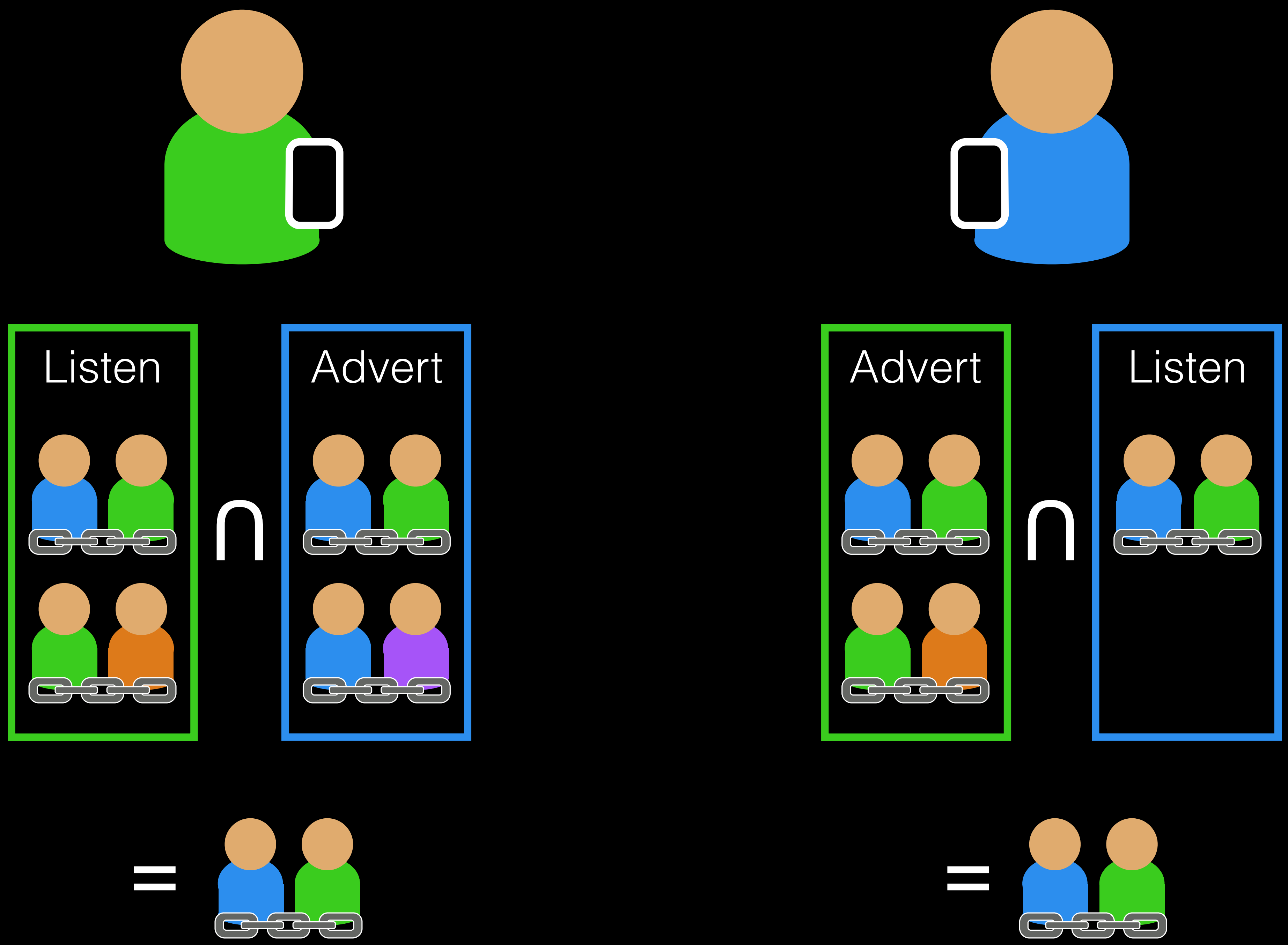
Recognition and Revocation



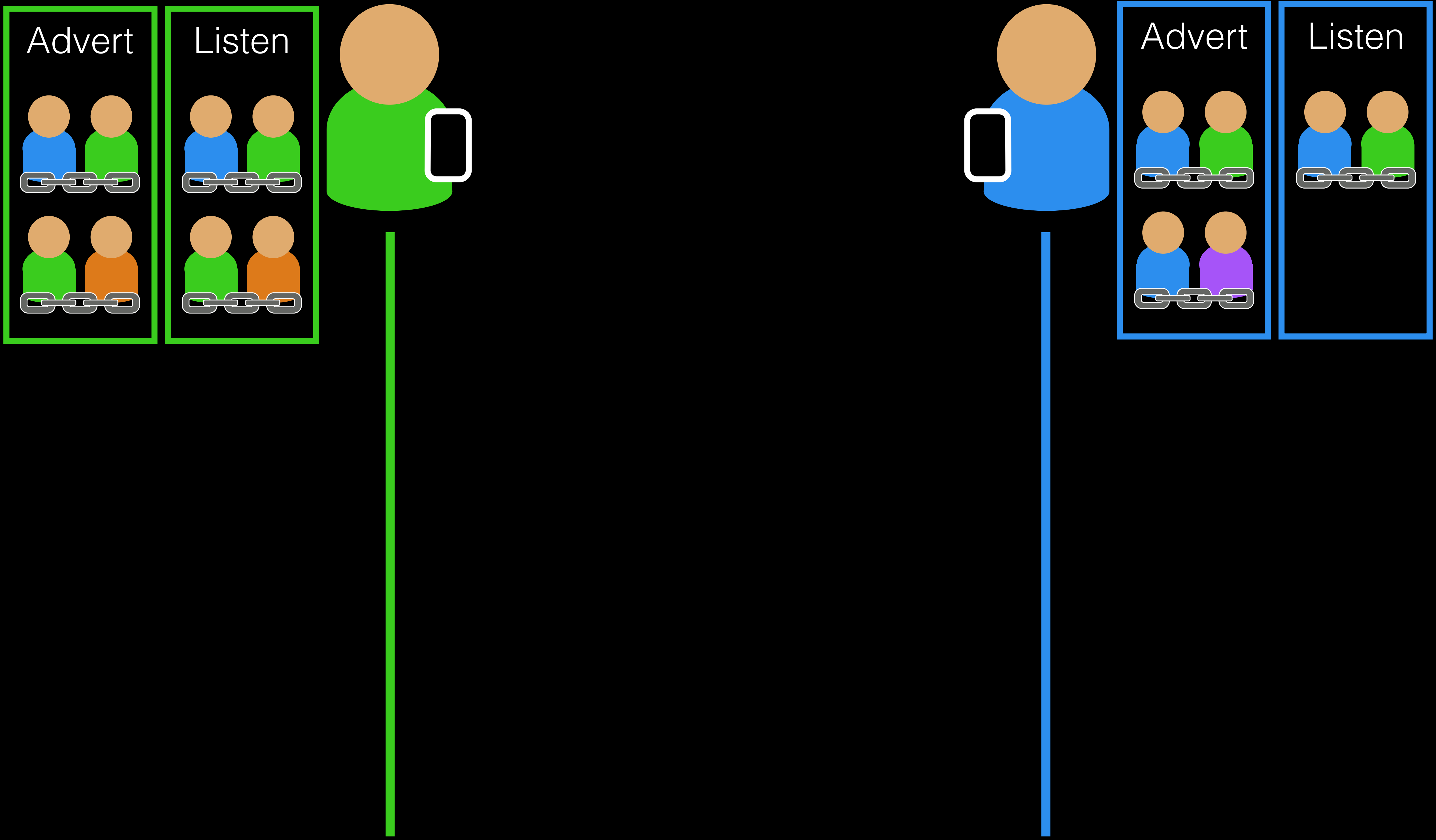
Recognition by Intersecting Sets



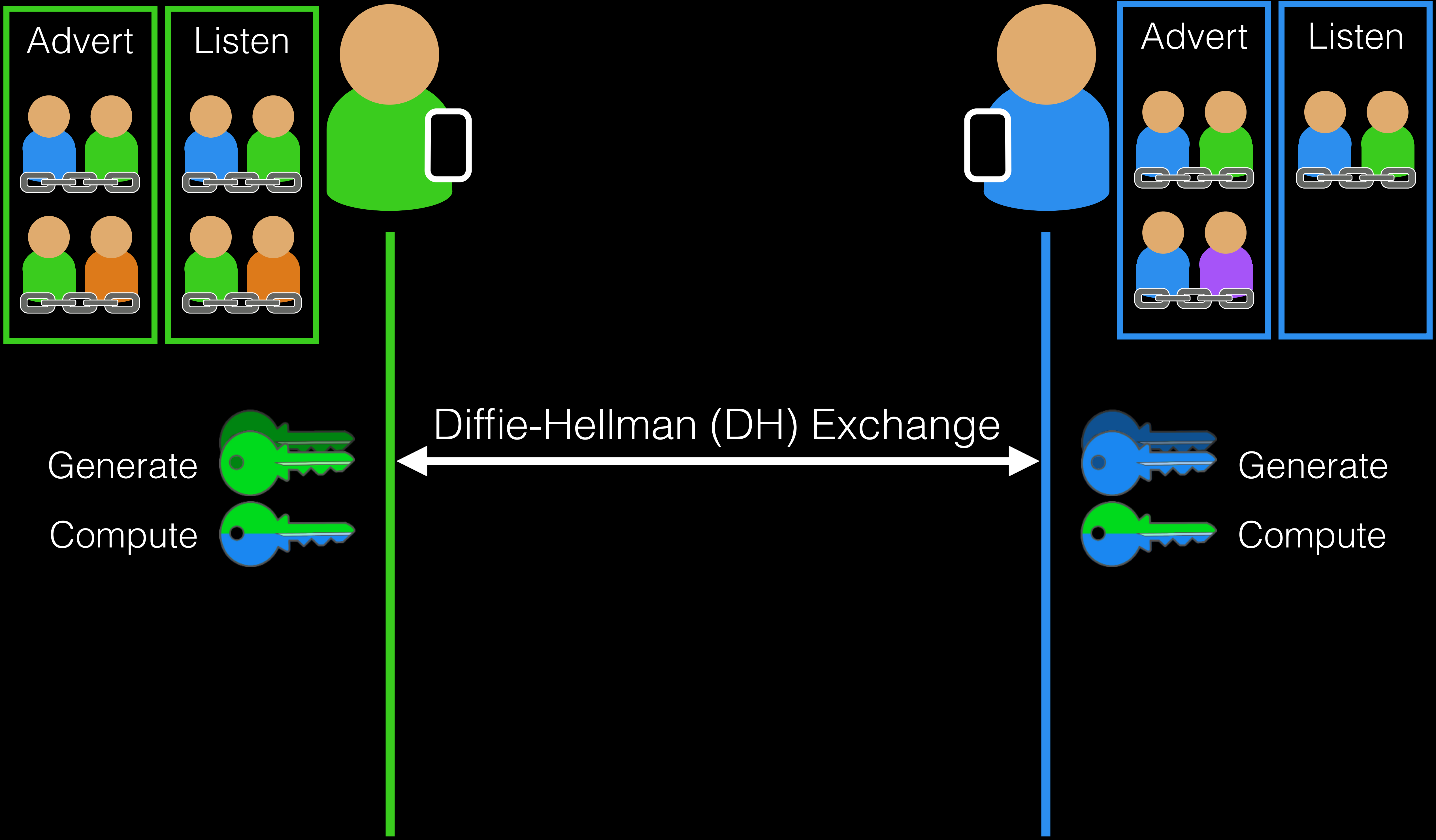
Recognition by Intersecting Sets



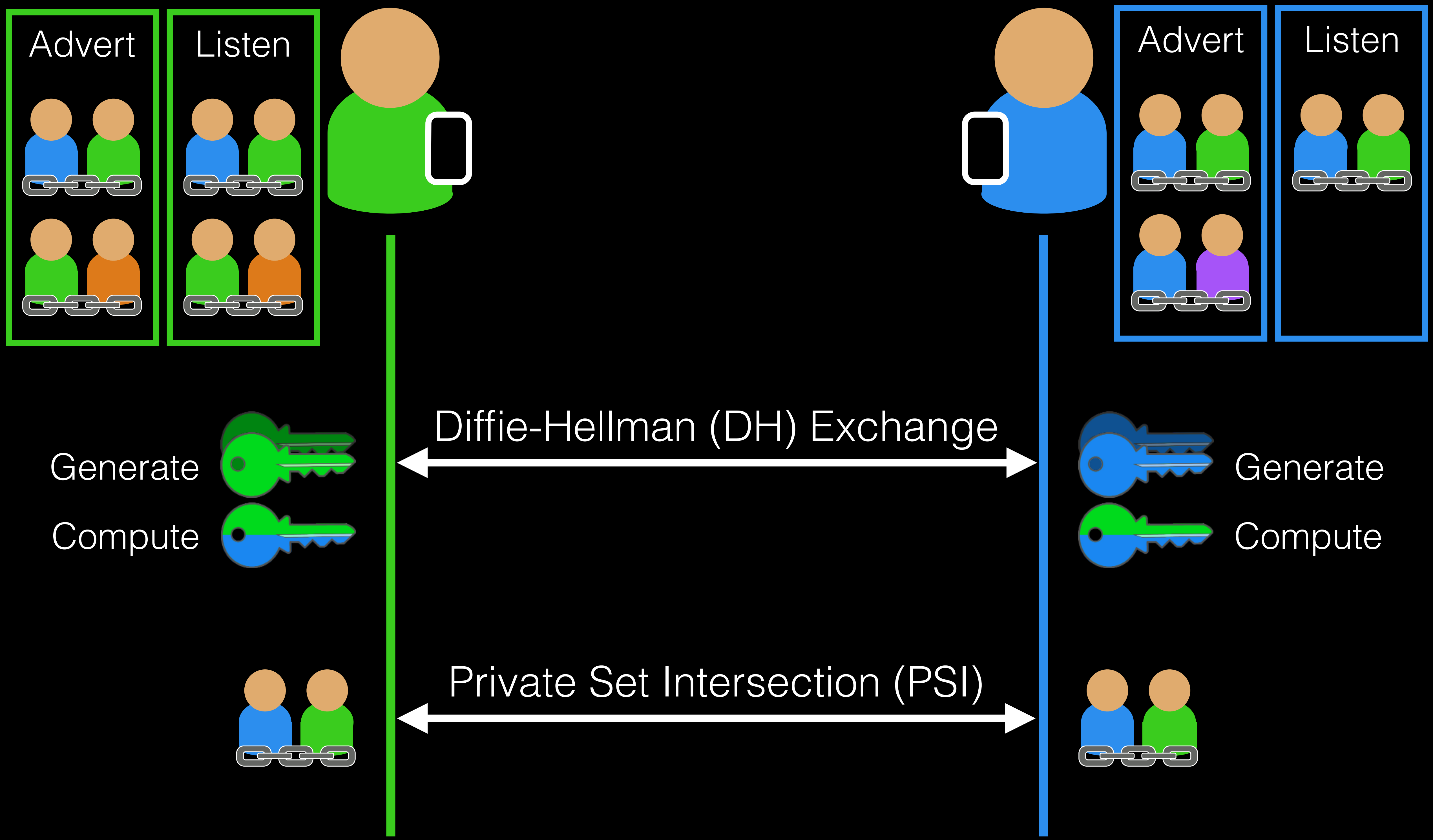
Strawman Protocol



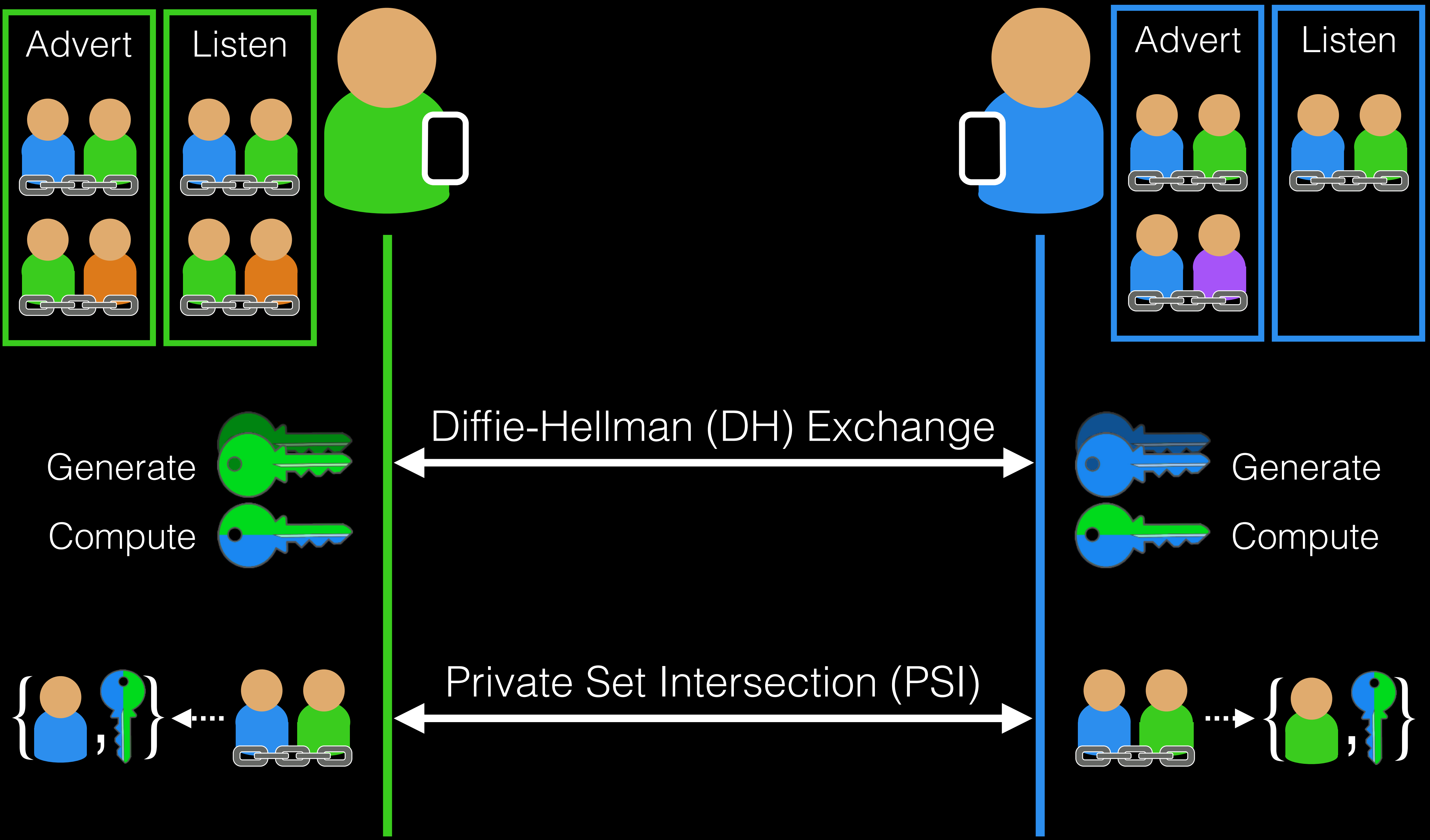
Strawman Protocol



Strawman Protocol



Strawman Protocol



Advert

Listen

Advert

Listen

Diffie-Hellman (DH) Exchange

Generate

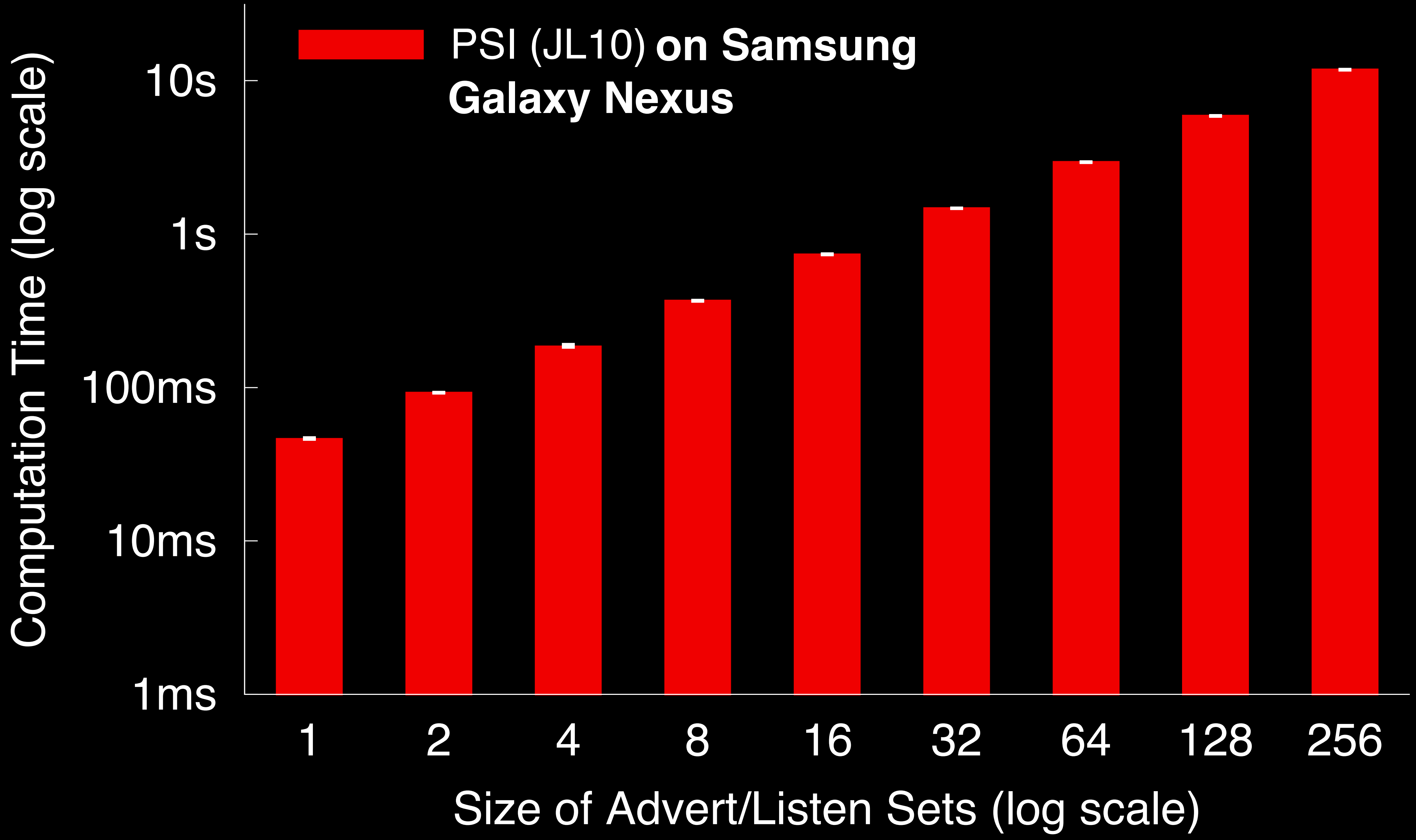
Compute

Generate

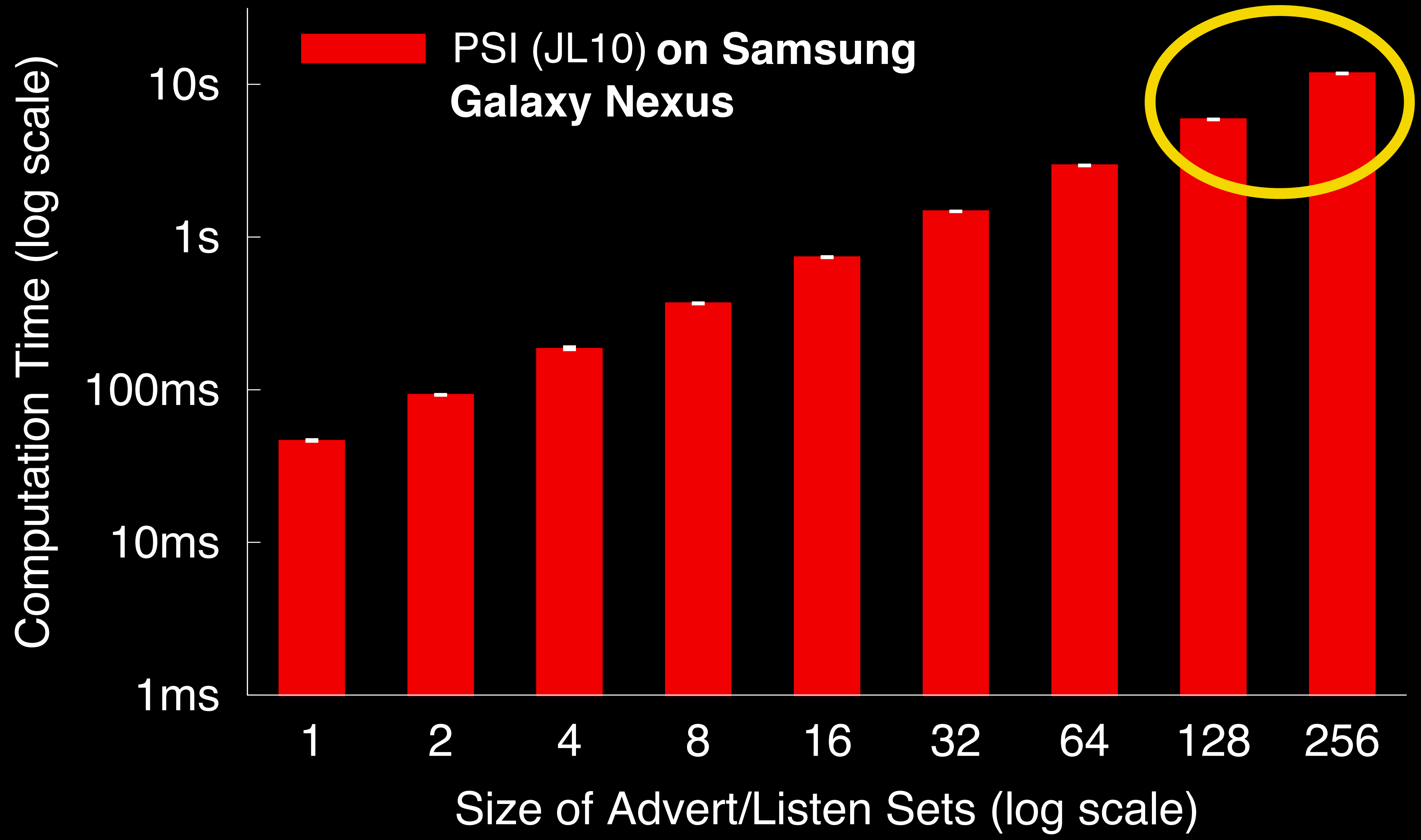
Compute

Private Set Intersection (PSI)

PSI is Prohibitively Slow



PSI is Prohibitively Slow



System Goals

Efficiency - Practical for resource-constrained devices

Scalability - Handle many peers (e.g., stadium)

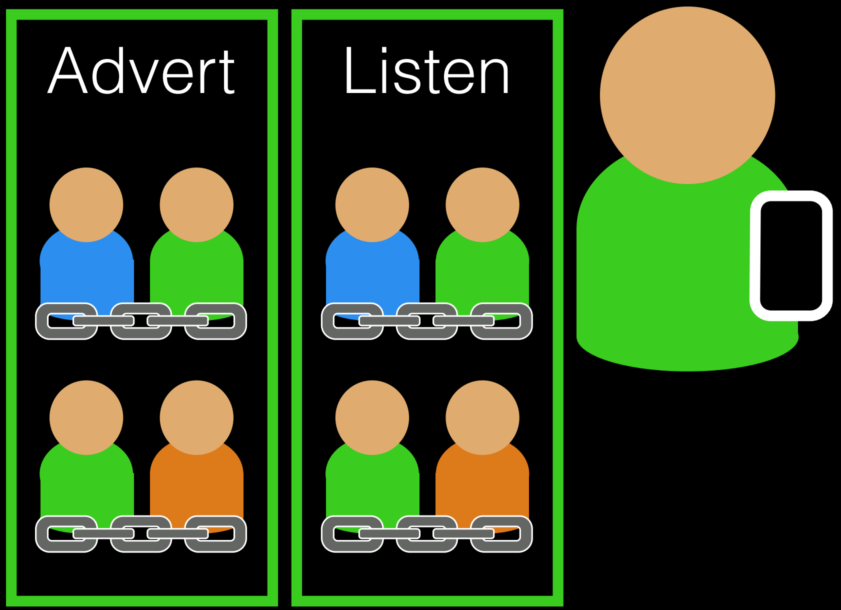
System Goals

Efficiency - Practical for resource-constrained devices

Scalability - Handle many peers (e.g., stadium)

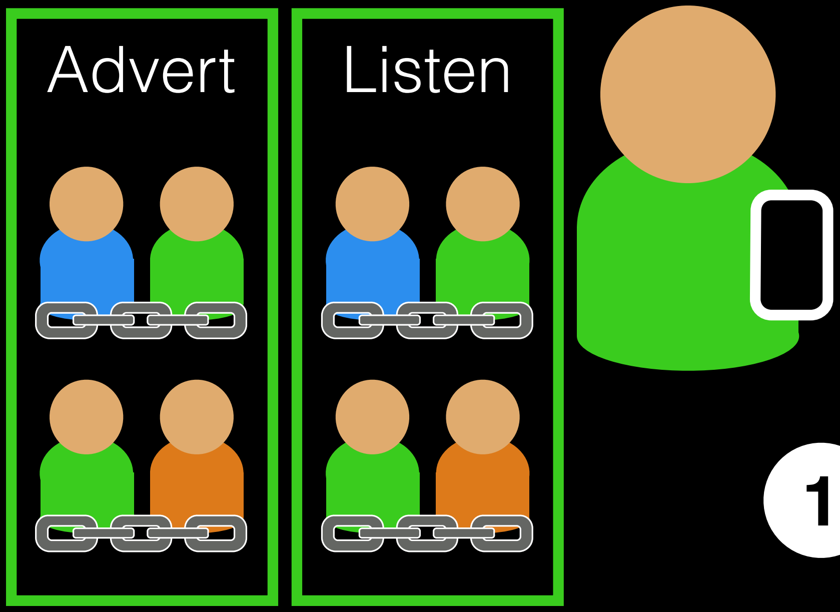
Need to develop secure protocols with energy efficiency as a first order goal

SDDR Protocol State



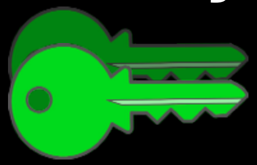
Divide time into discrete **epochs**, across which user is unlinkable.

SDDR Protocol State

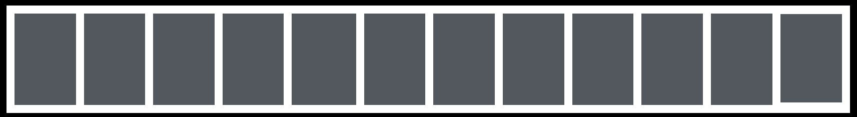


In each **epoch**, generate:

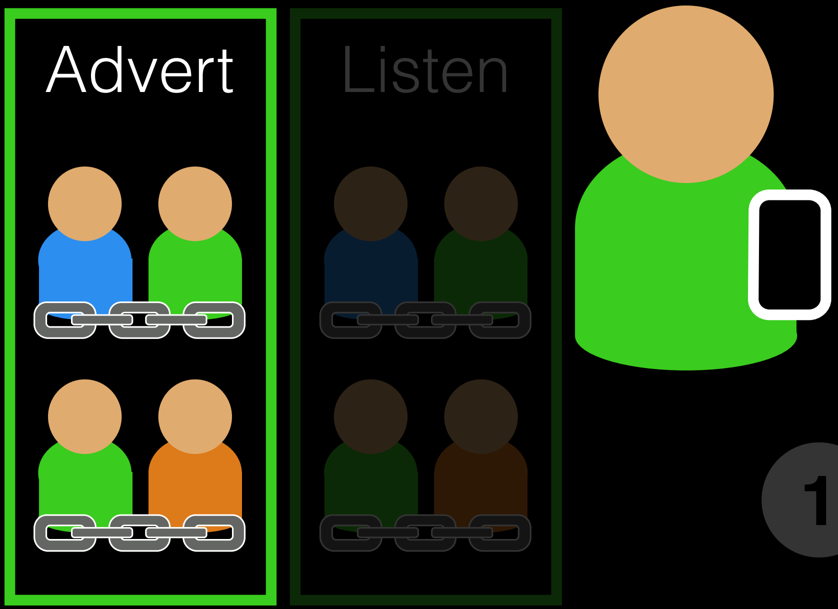
1 **DH Key Pair**



2 **Bloom Filter**



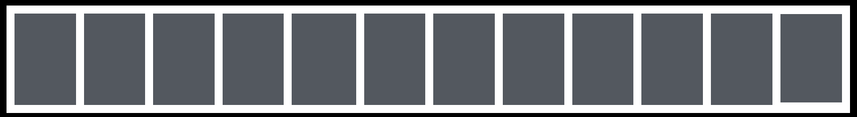
SDDR Protocol State



In each **epoch**, generate:

1 **DH Key Pair**

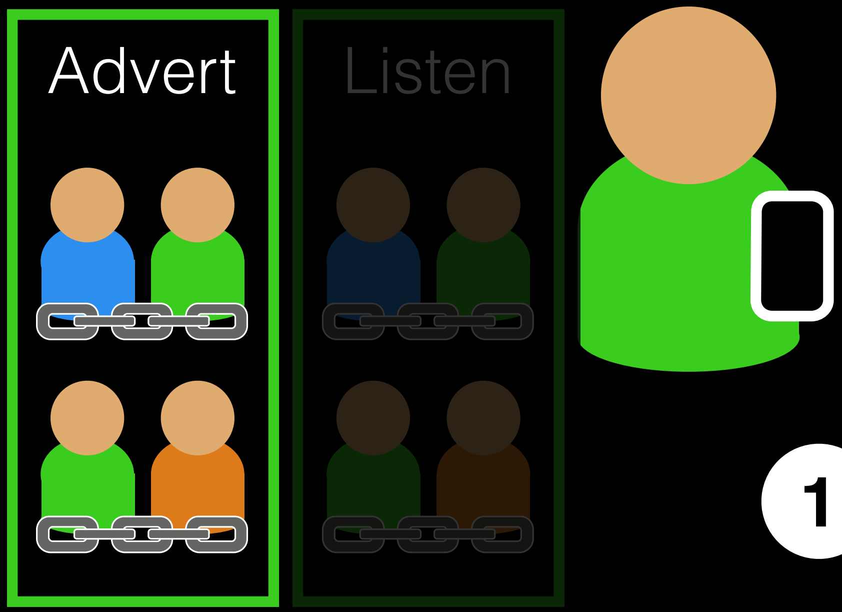
2 **Bloom Filter**



Probabilistic set digest for advertised link values

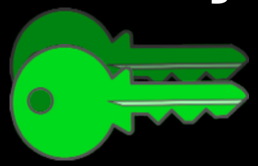
We use them for compactness, *not* security

SDDR Protocol State

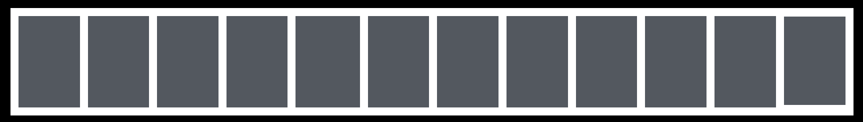


In each **epoch**, generate:

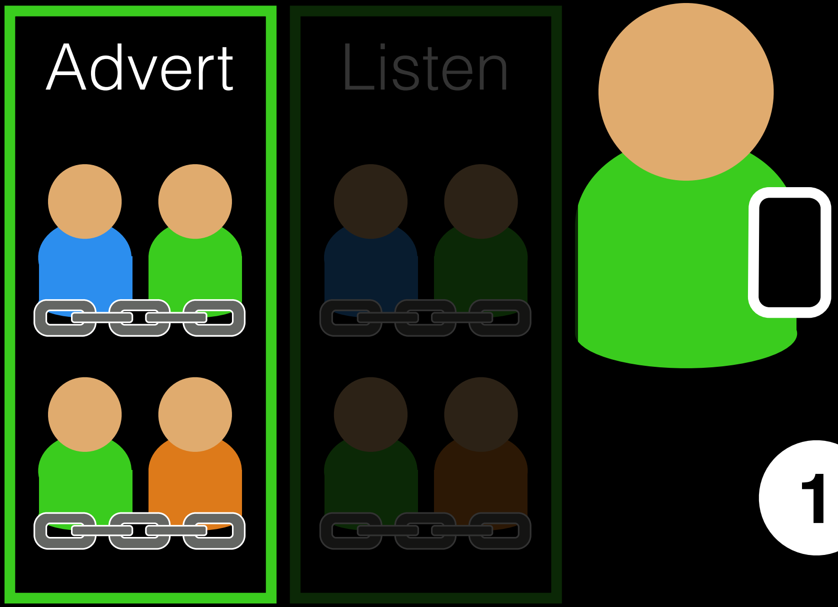
1 DH Key Pair



2 Bloom Filter

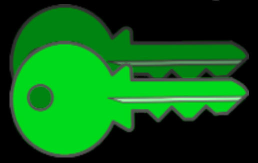


SDDR Protocol State

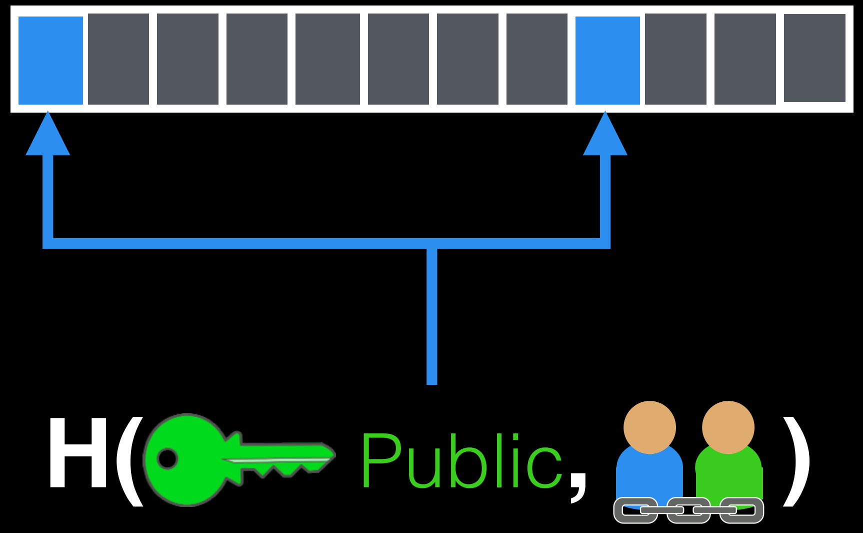


In each **epoch**, generate:

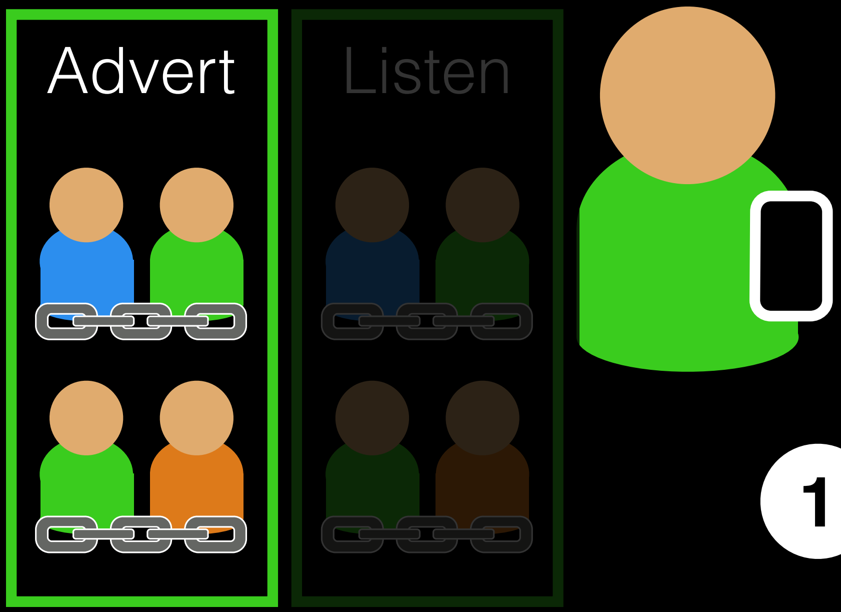
1 DH Key Pair



2 Bloom Filter

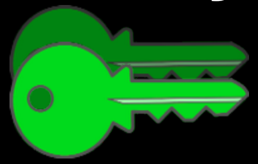


SDDR Protocol State

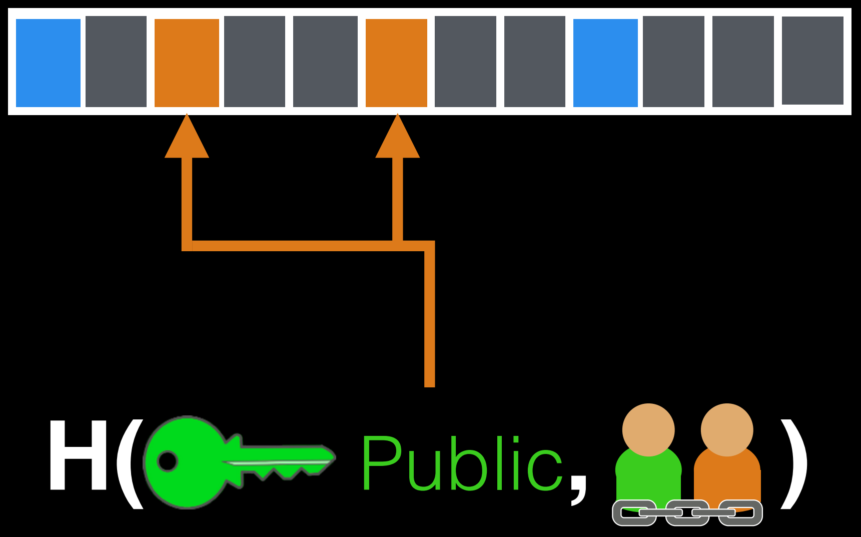


In each **epoch**, generate:

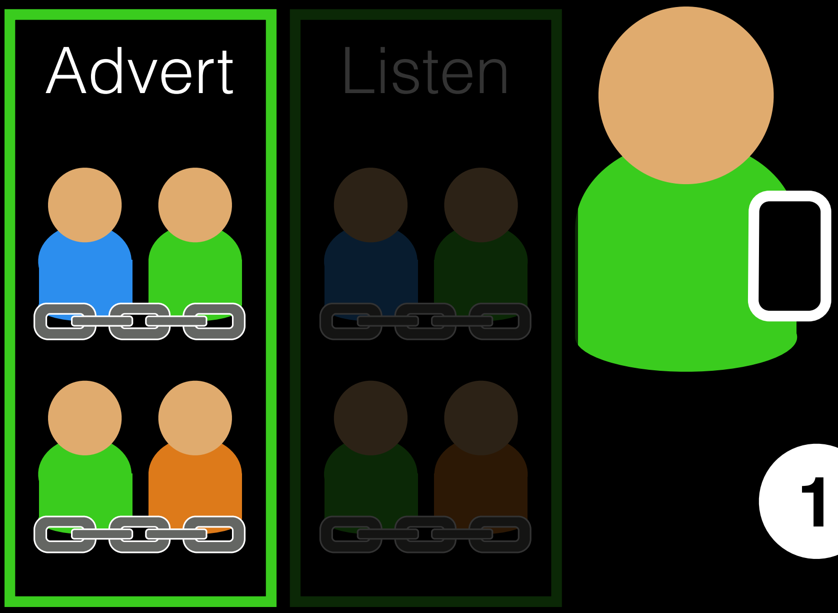
1 DH Key Pair



2 Bloom Filter

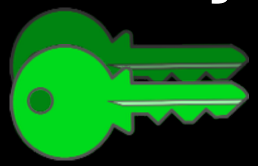


SDDR Protocol State



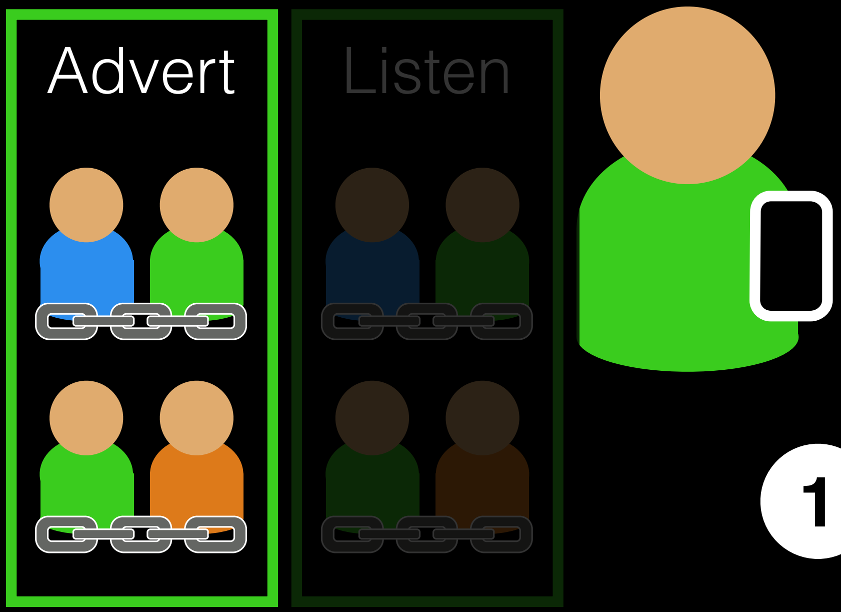
In each **epoch**, generate:

1 **DH Key Pair**



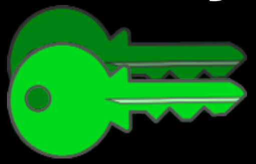
2 **Bloom Filter**

SDDR Protocol State

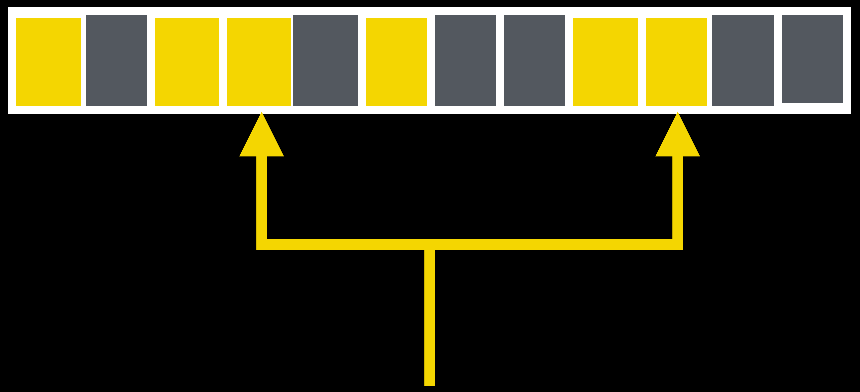


In each **epoch**, generate:

1 DH Key Pair

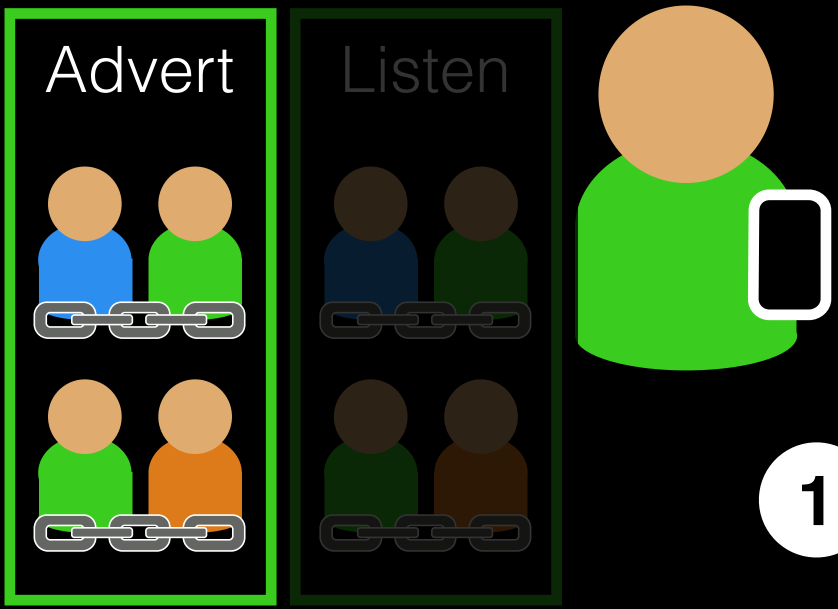


2 Bloom Filter

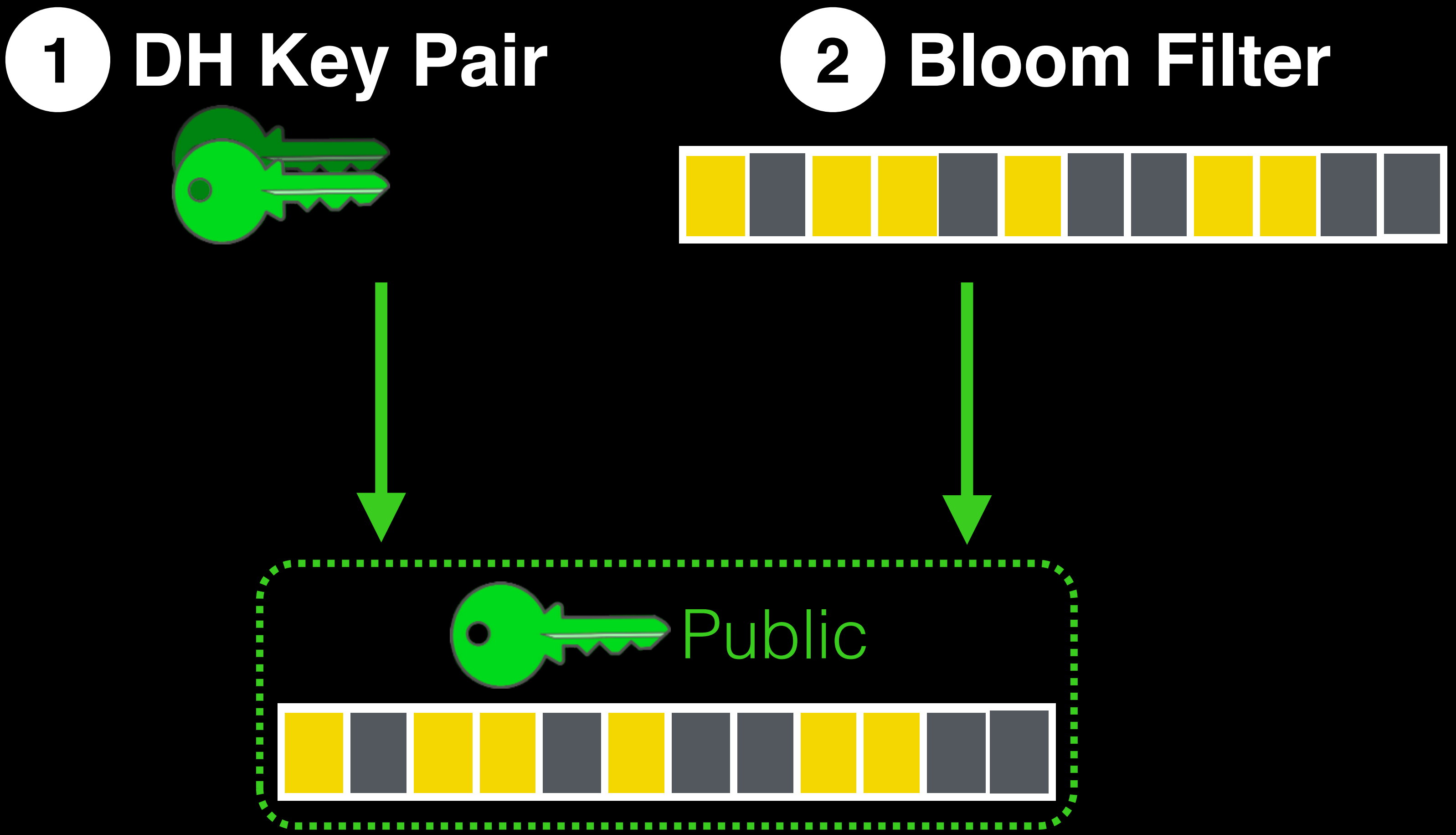


Random padding to global maximum size

SDDR Protocol State

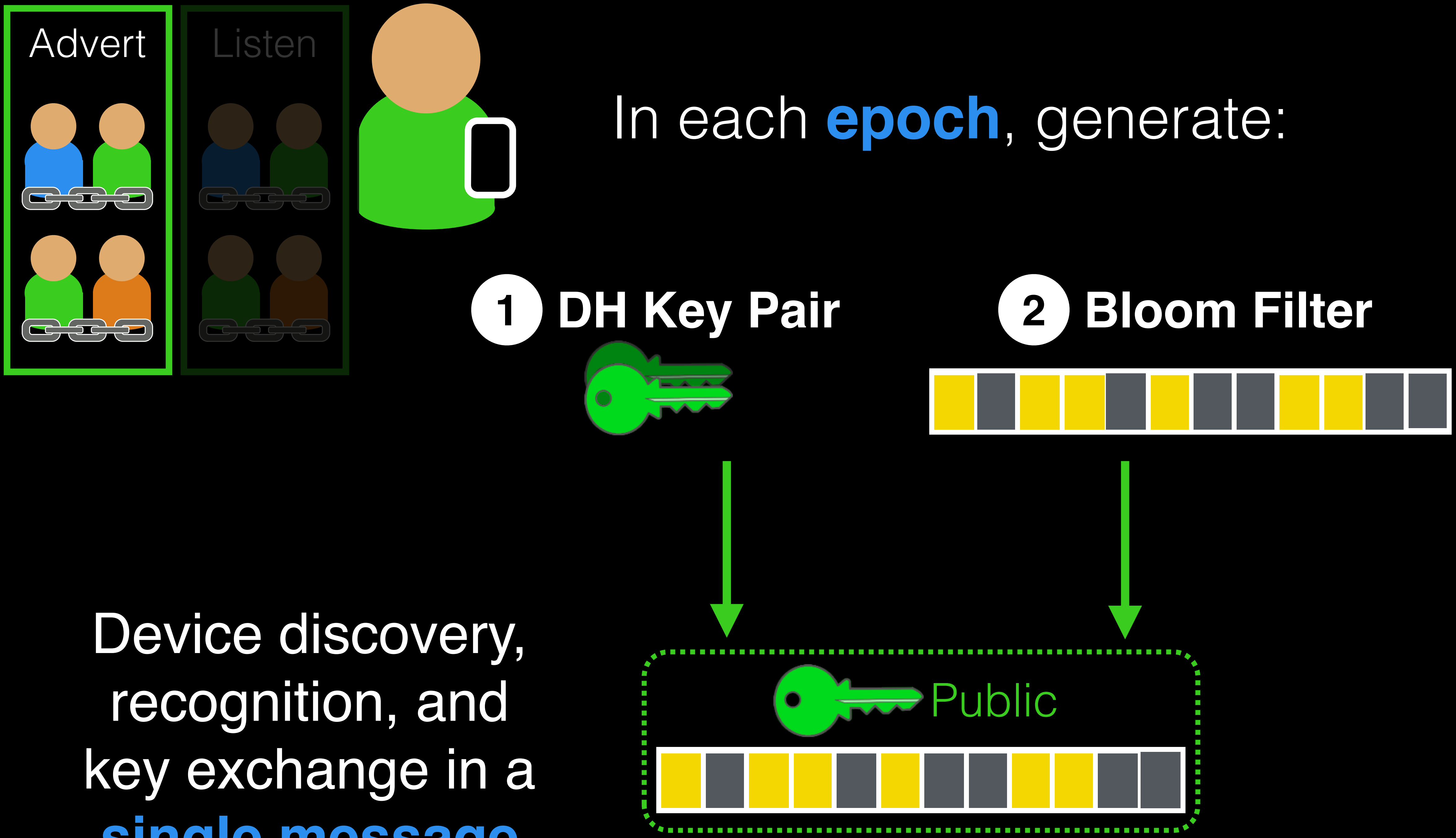


In each **epoch**, generate:



1. **DH Key Pair**
2. **Bloom Filter**

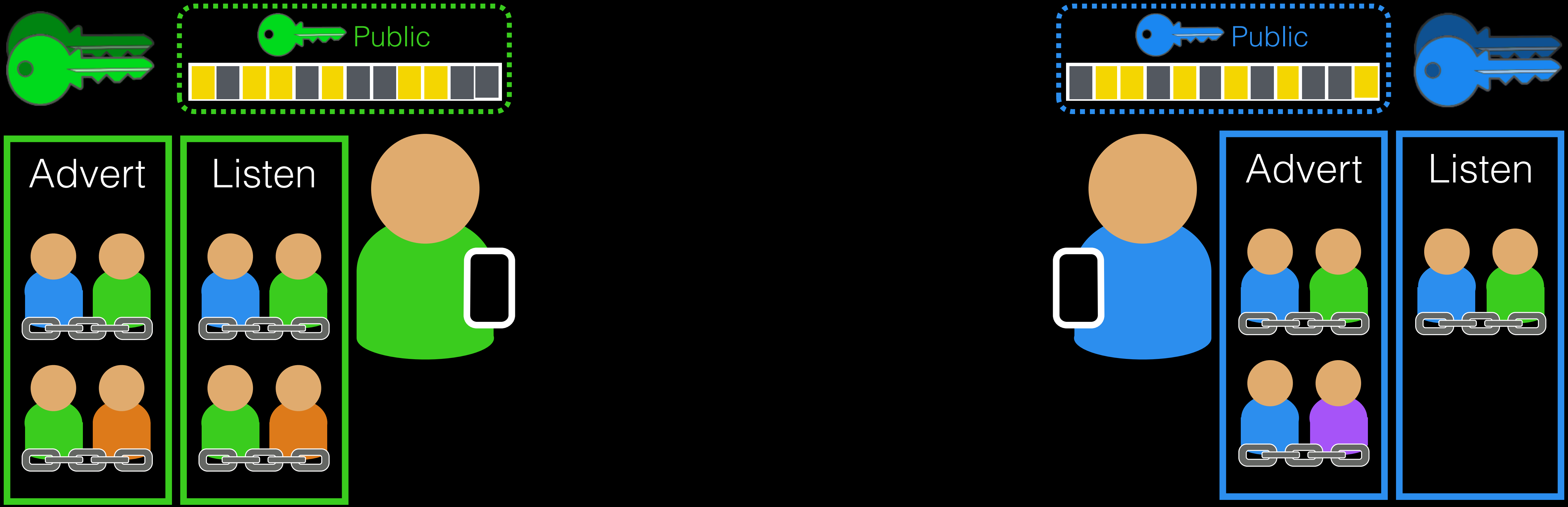
SDDR Protocol State



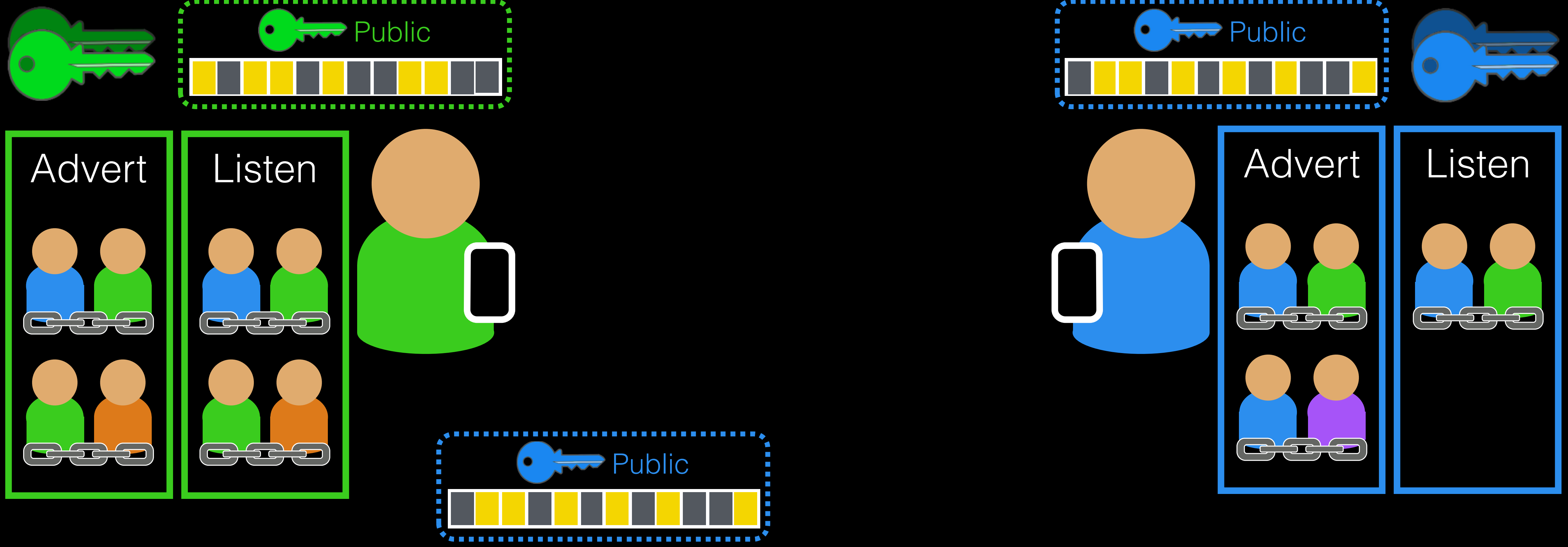
In each **epoch**, generate:

Device discovery, recognition, and key exchange in a **single message**

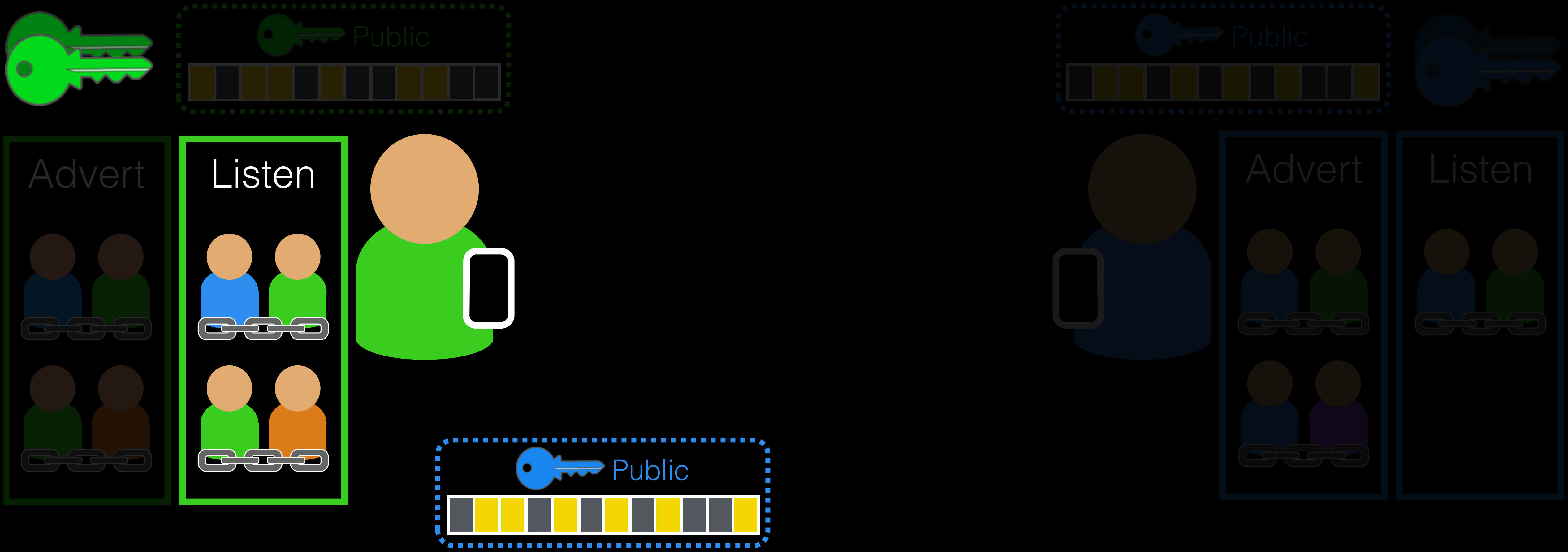
SDDR Protocol



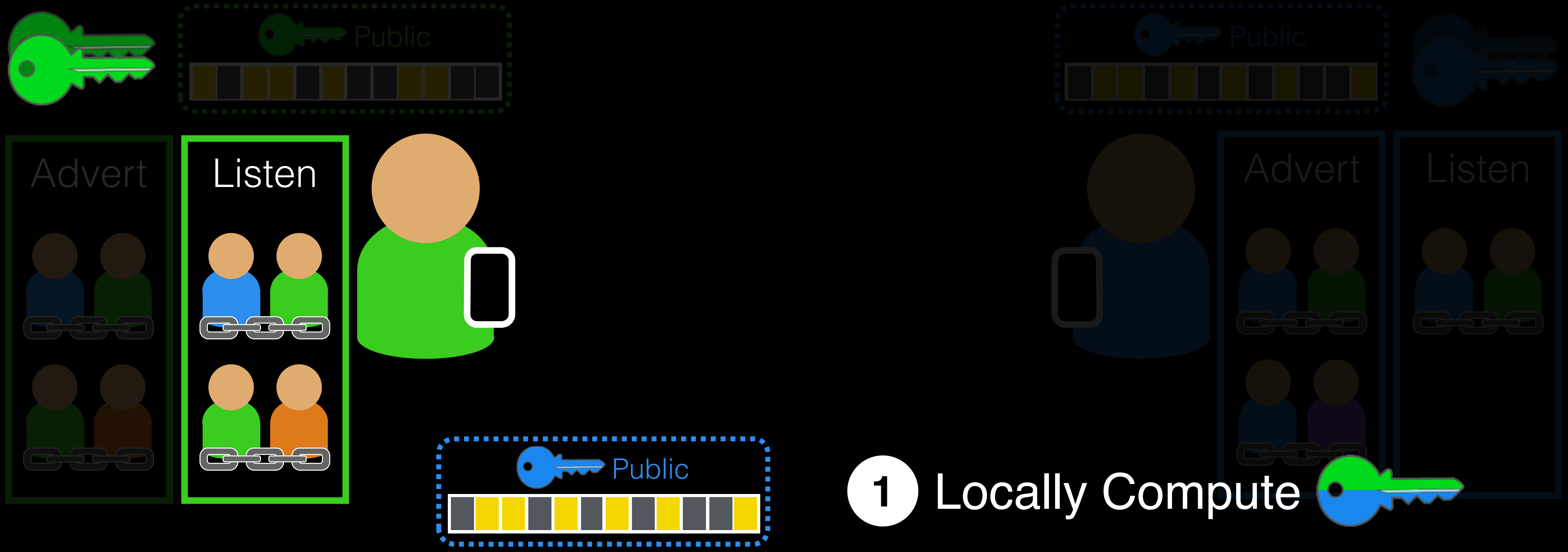
SDDR Protocol



SDDR Protocol

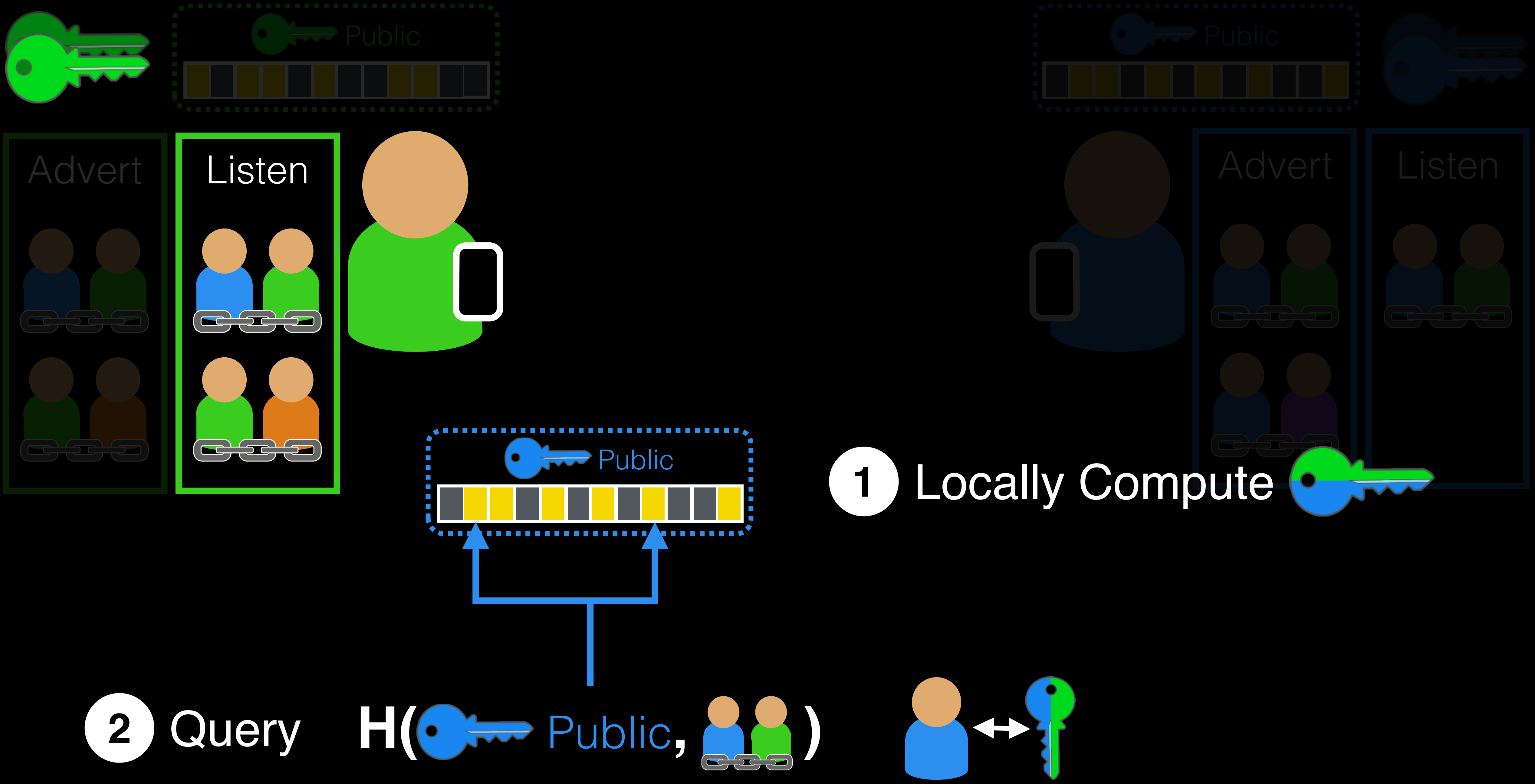


SDDR Protocol



1 Locally Compute

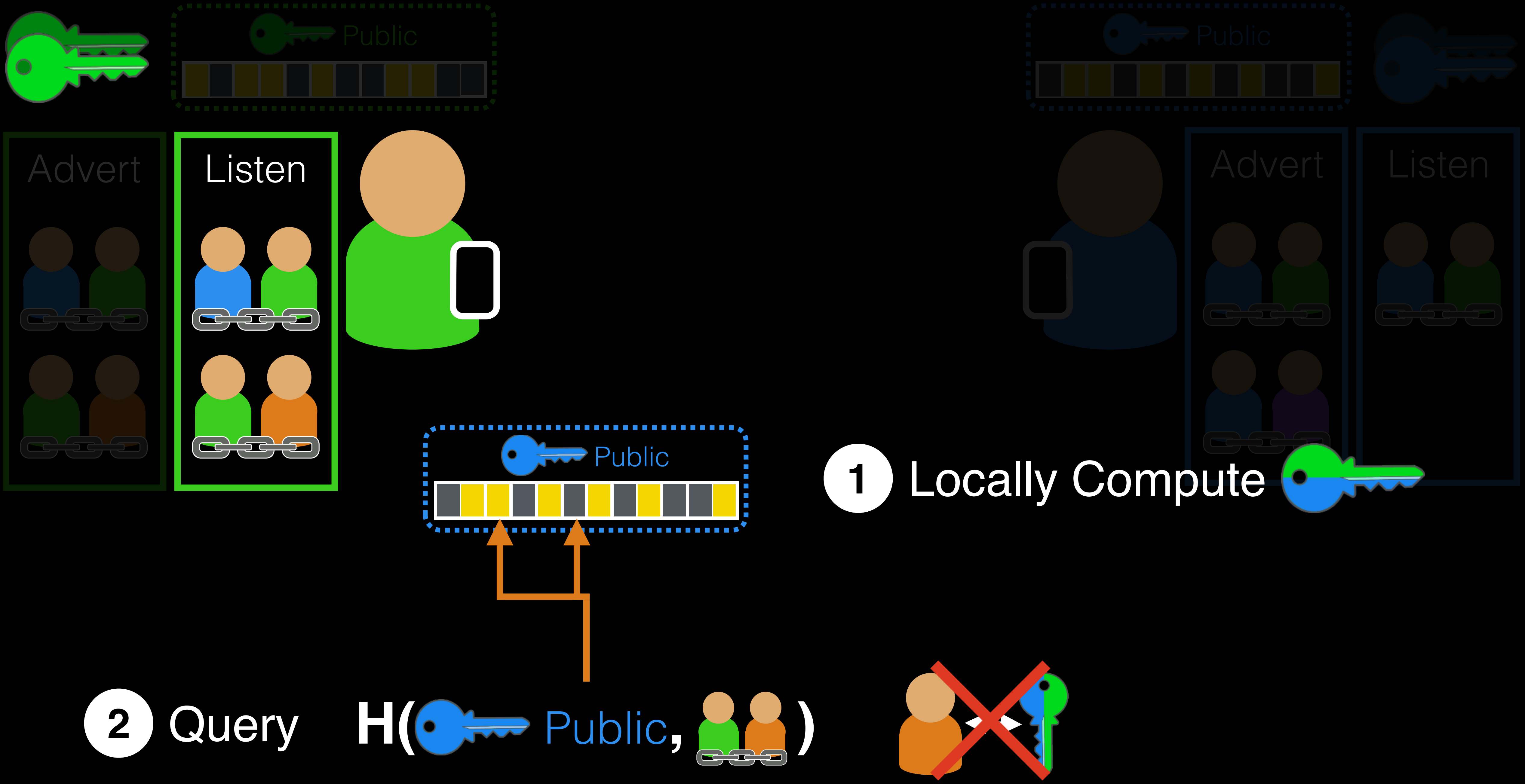
SDDR Protocol



1 Locally Compute

2 Query H(Public,)

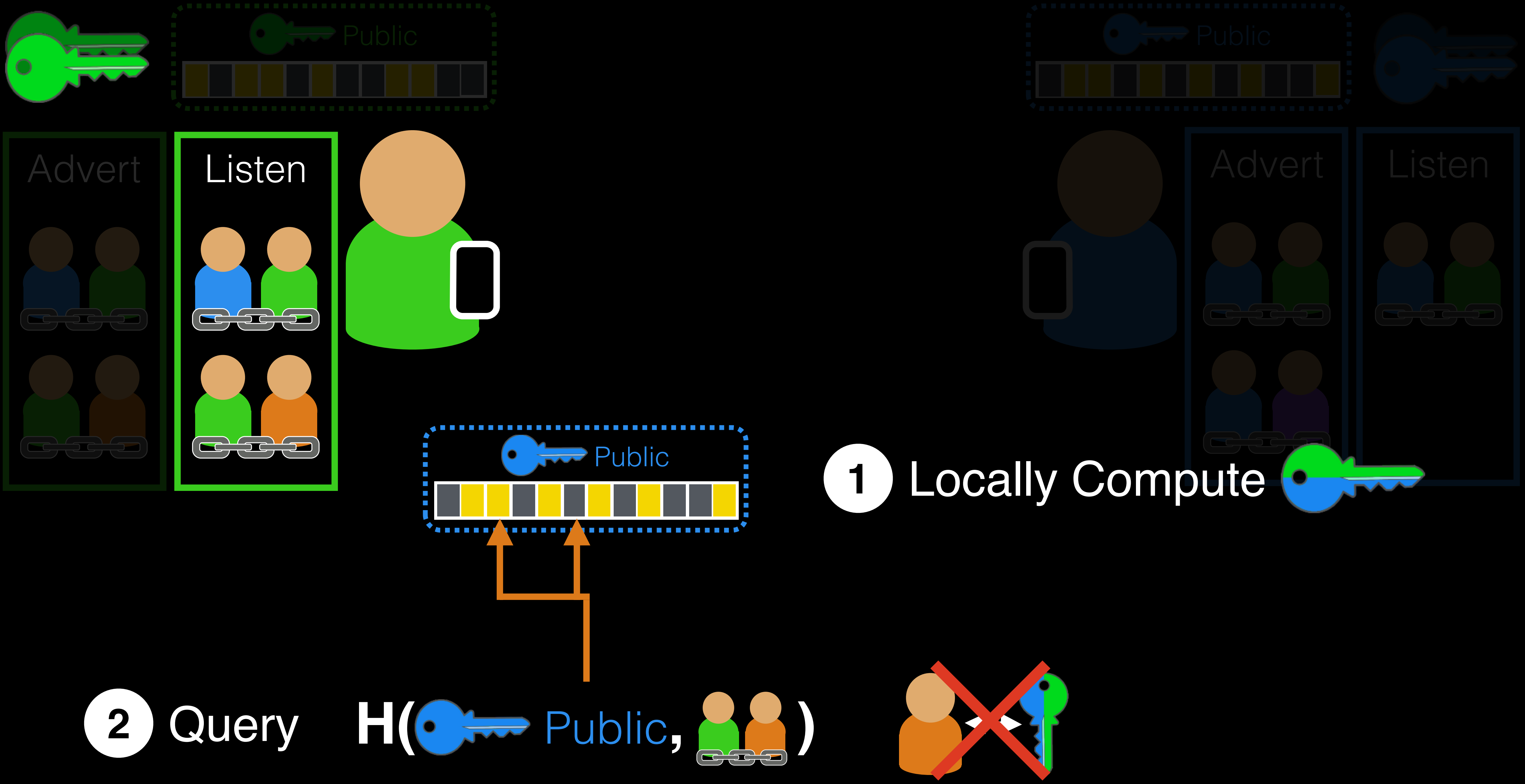
SDDR Protocol



1 Locally Compute

2 Query H(Public,)

SDDR Protocol

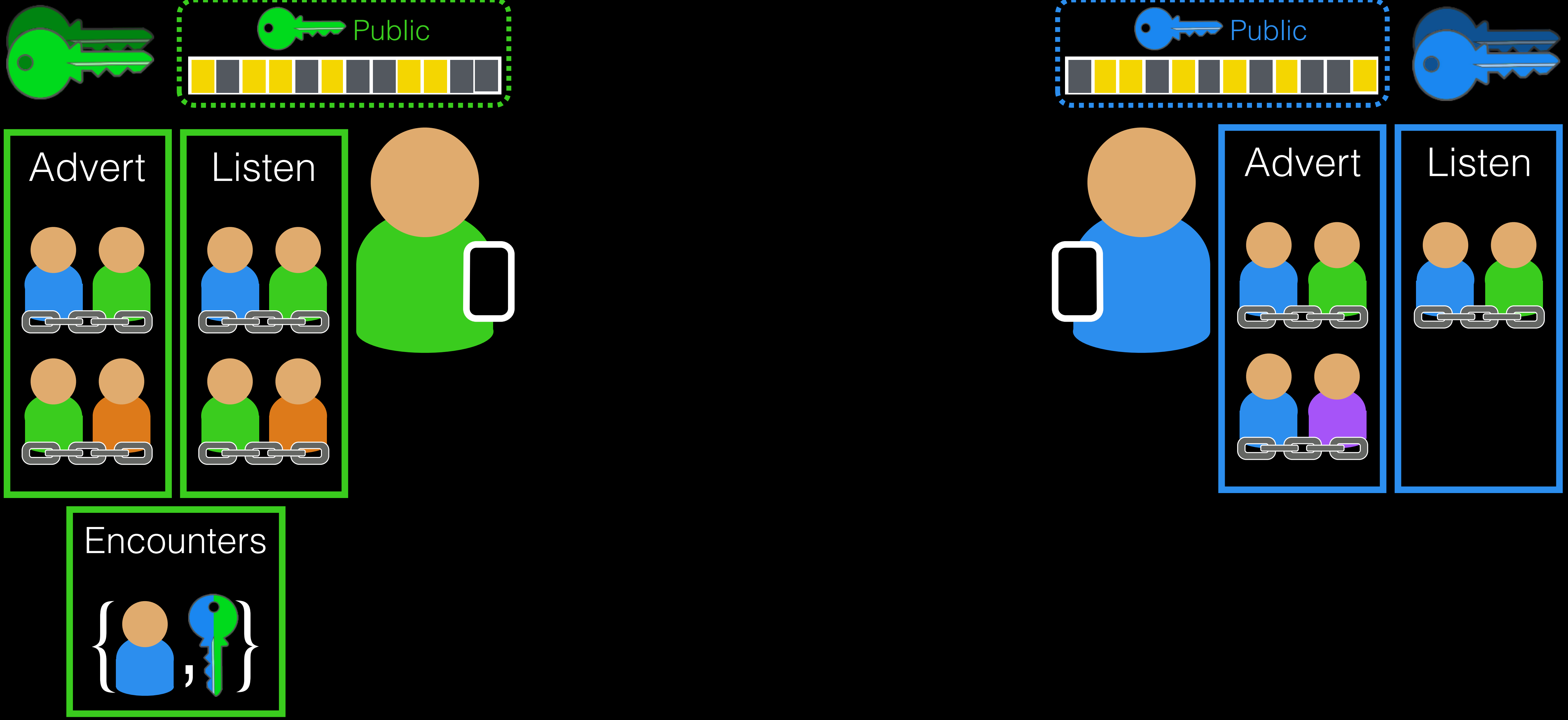


1 Locally Compute

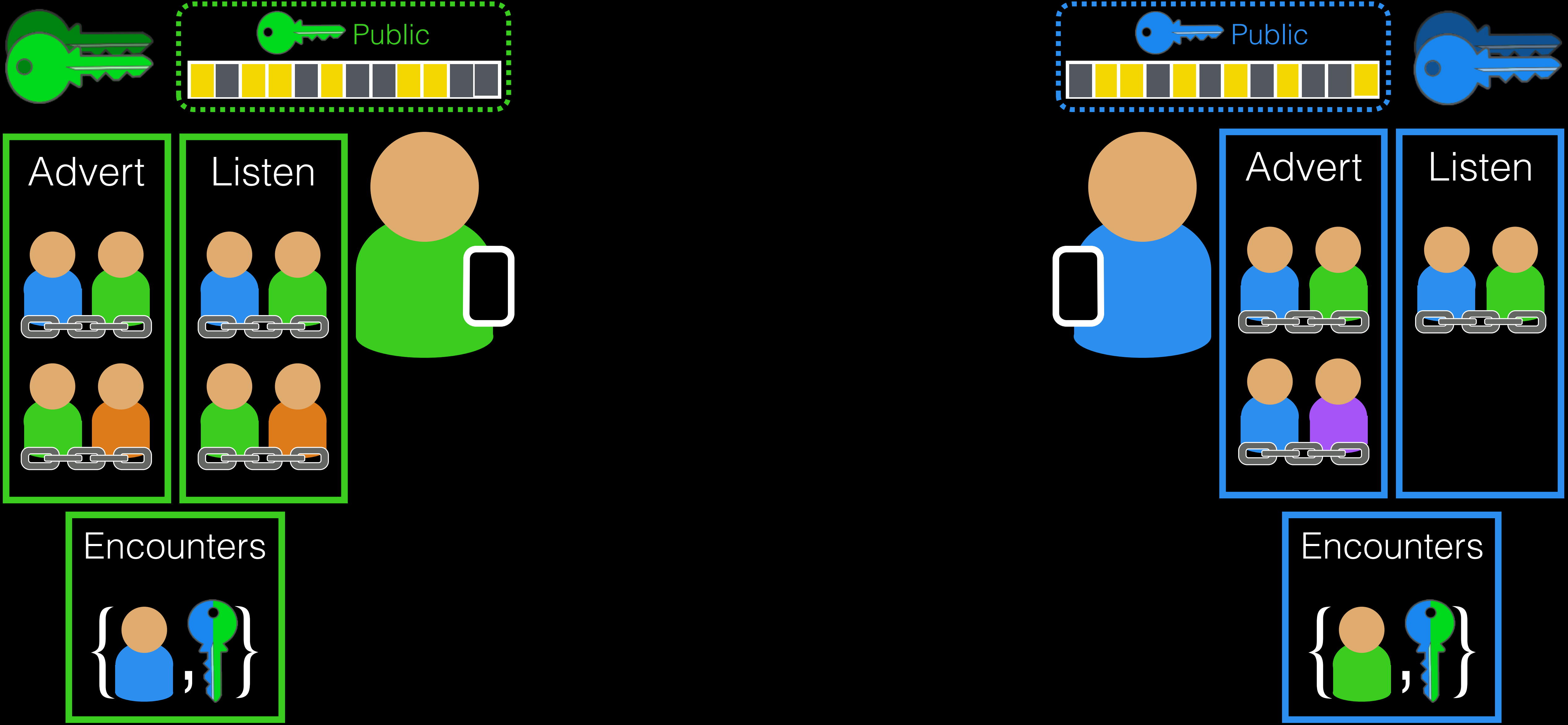
2 Query H(Public,)

Can mitigate false positives (Details in paper)

SDDR Protocol



SDDR Protocol



Public

Advert

Listen

Encounters

Public

Advert

Listen

Encounters

SDDR Implementation

Prototype for Android using Bluetooth 2.1

Developed/Evaluated on
Samsung Galaxy Nexus

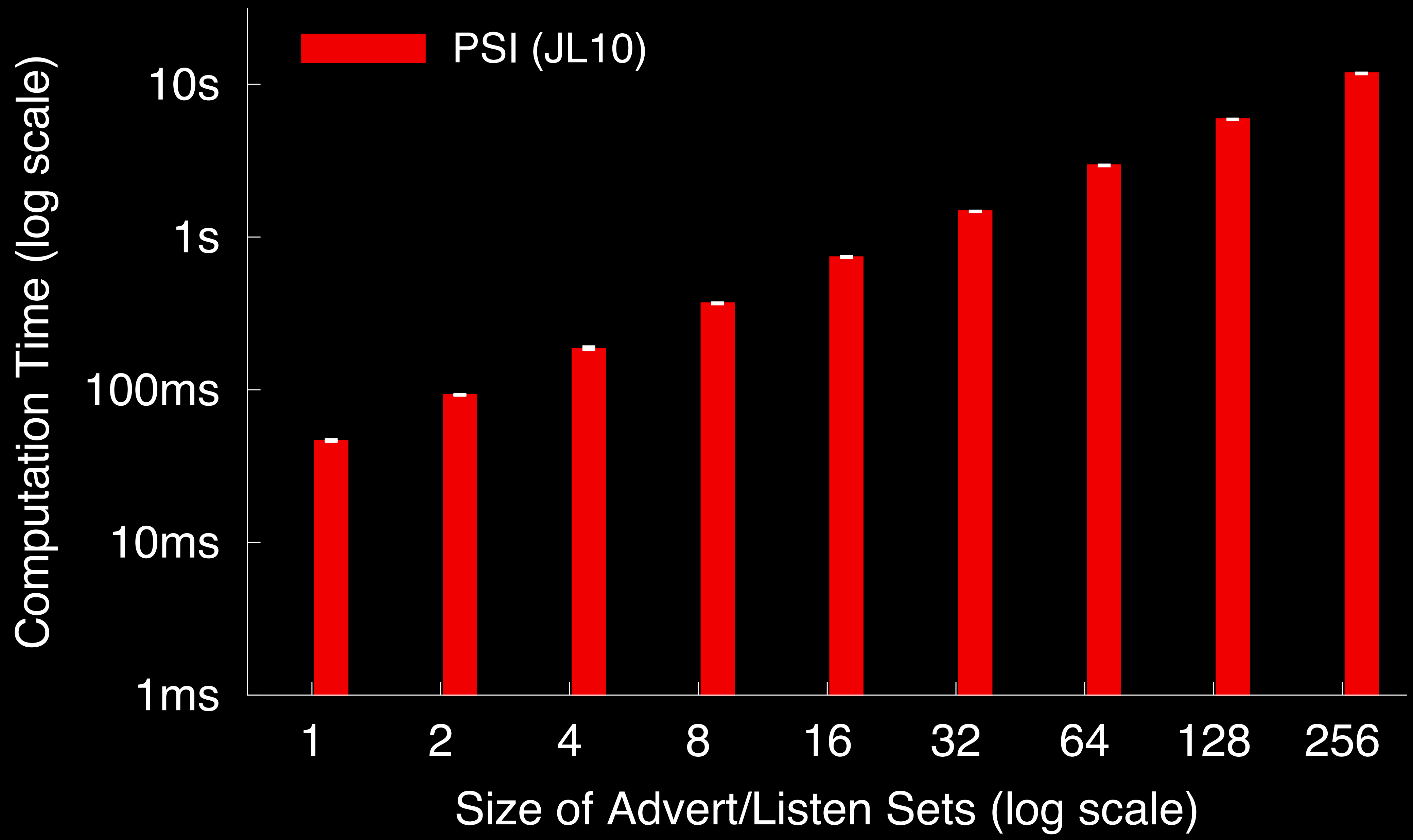
BattOr for Power
Measurements

System Goals

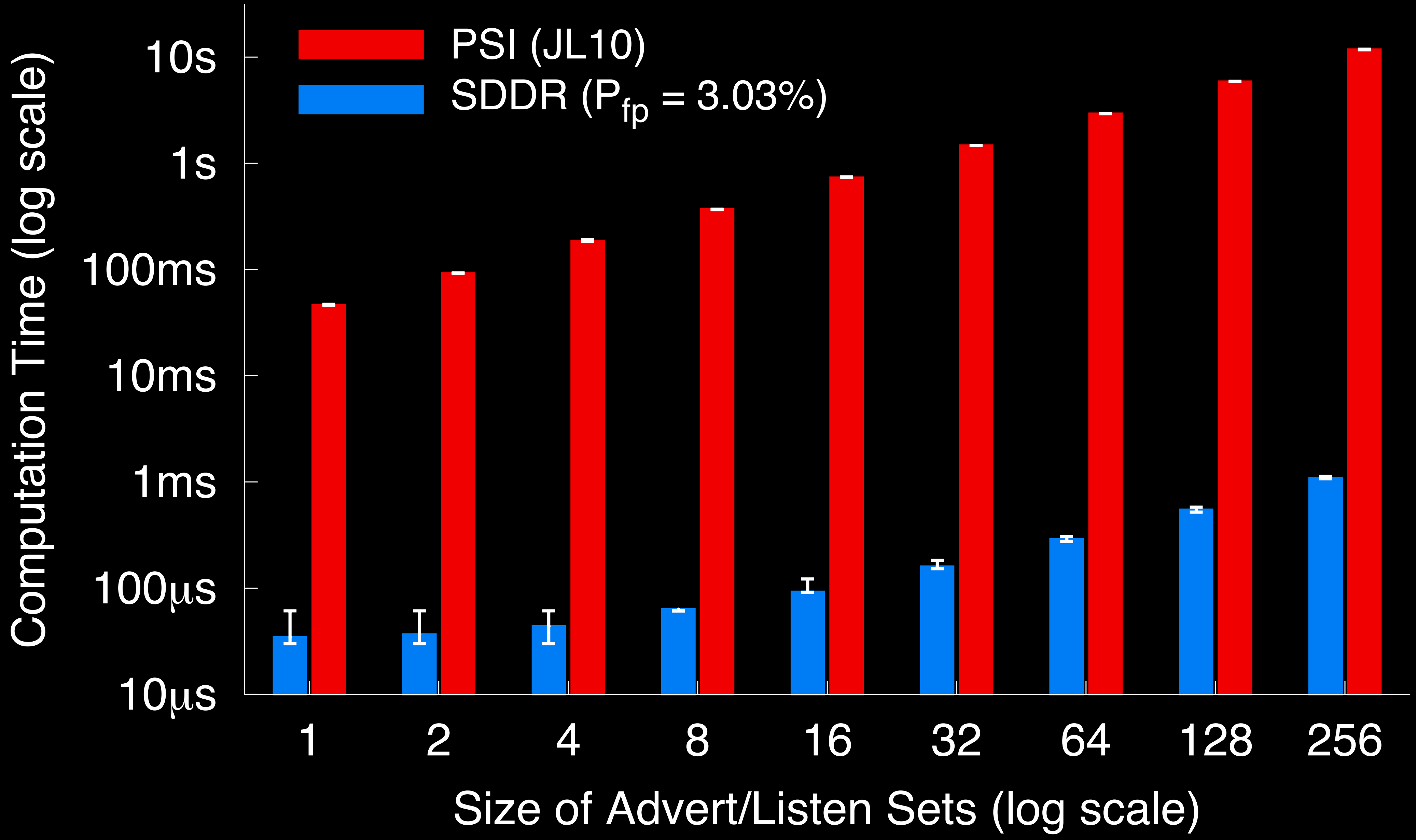
Efficiency - Practical for resource-constrained devices

Scalability - Handle many peers (e.g., stadium)

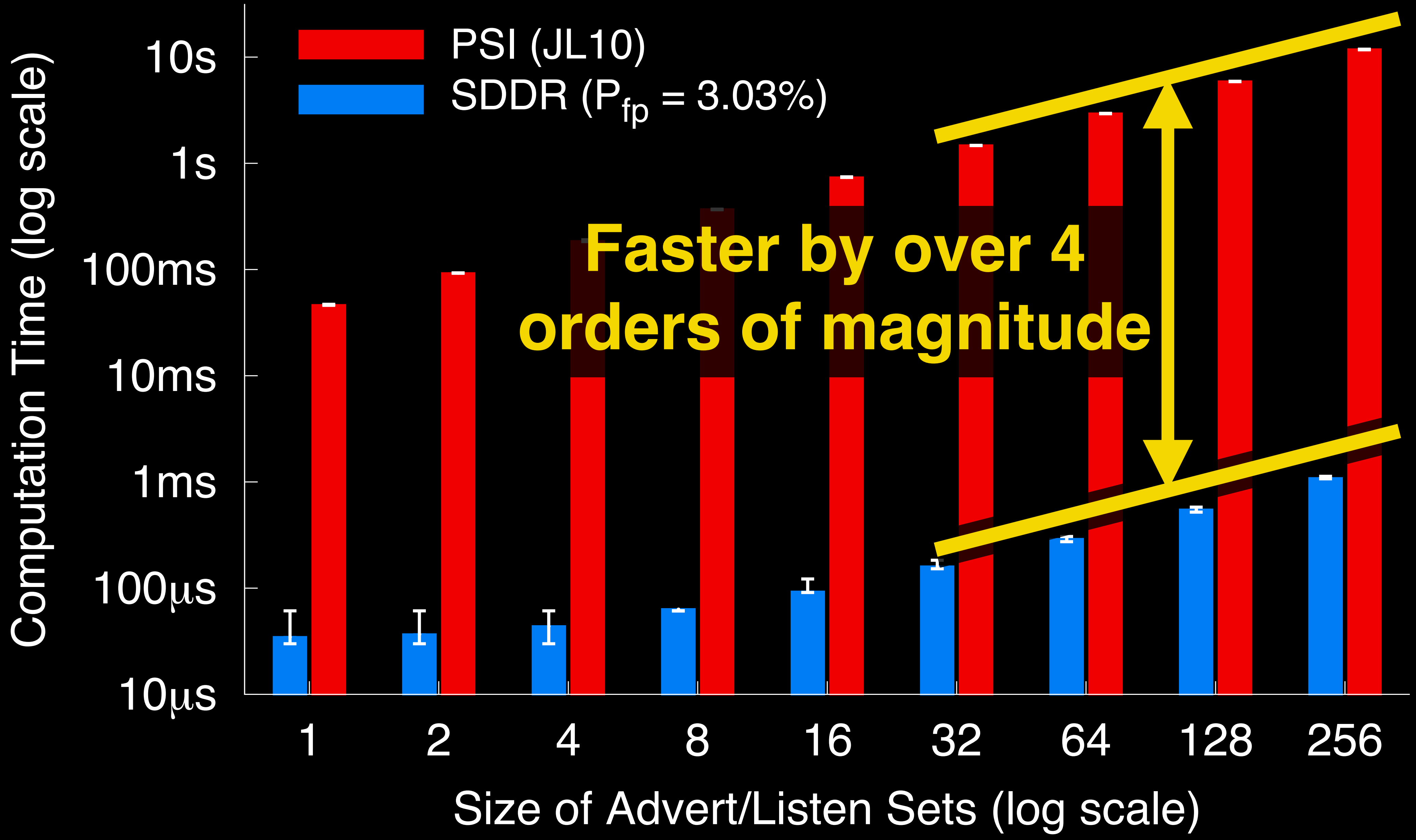
SDDR vs PSI - Computation



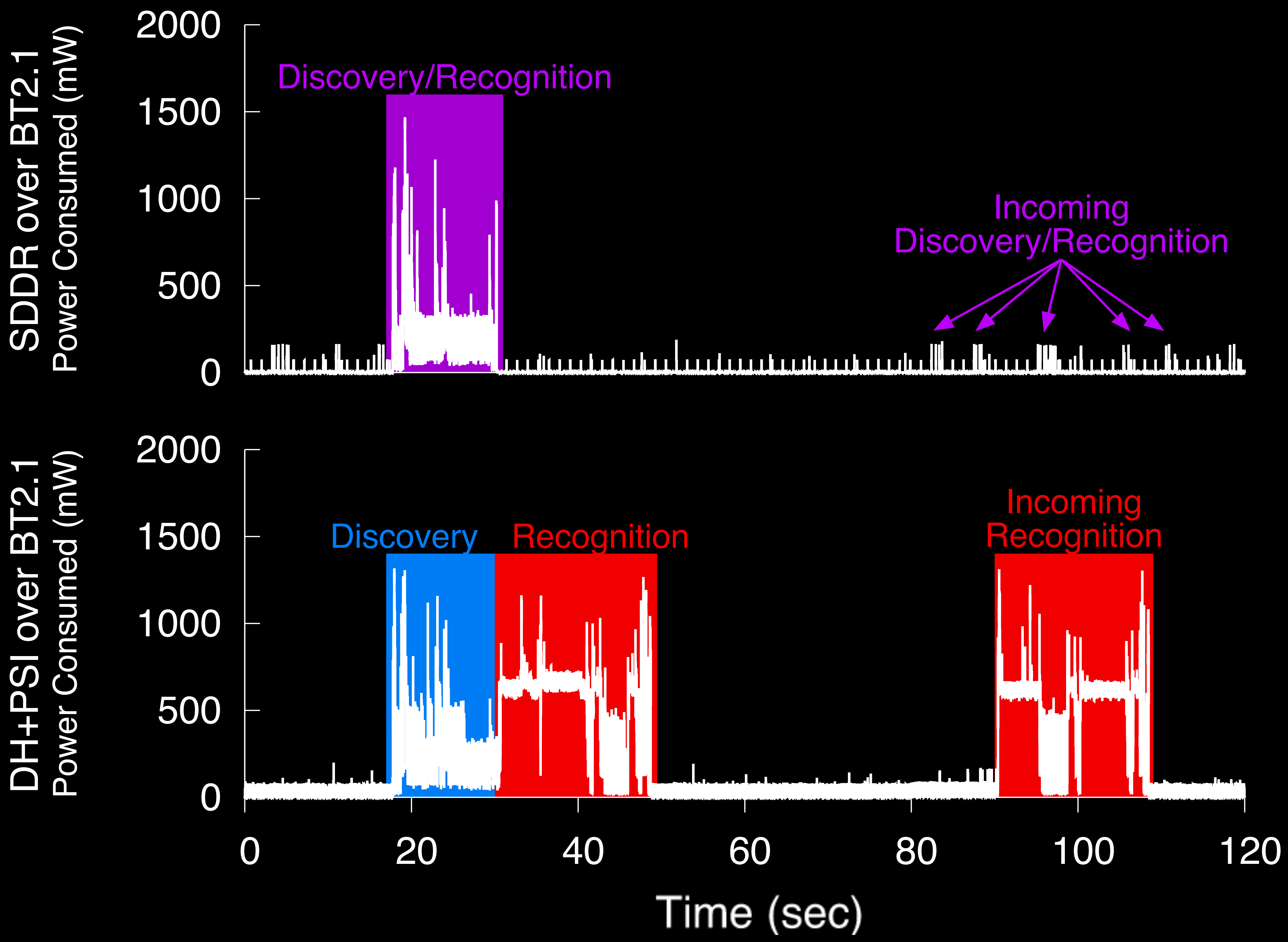
SDDR vs PSI - Computation



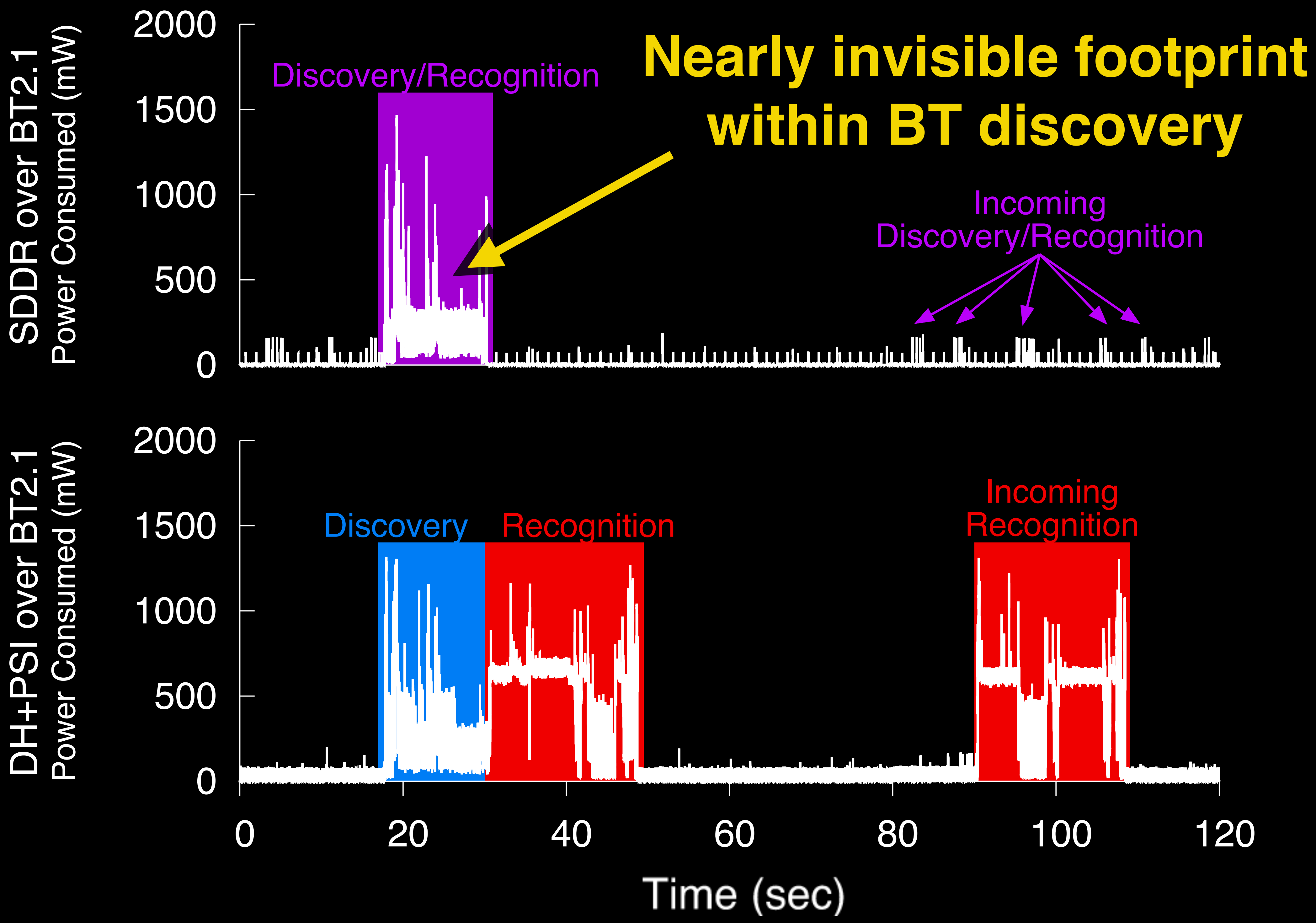
SDDR vs PSI - Computation



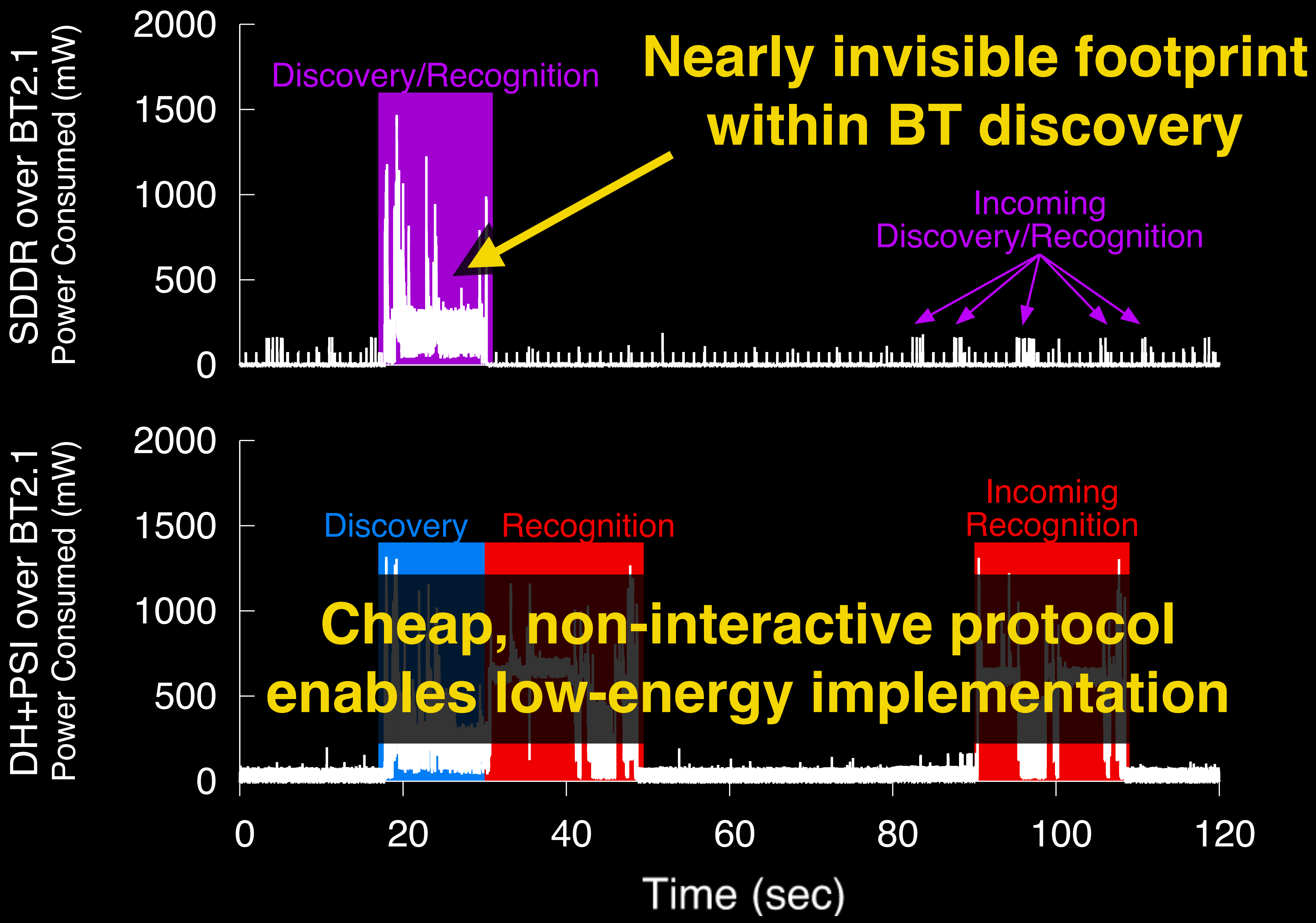
SDDR vs PSI - Power Traces



SDDR vs PSI - Power Traces



SDDR vs PSI - Power Traces



Nearly invisible footprint within BT discovery

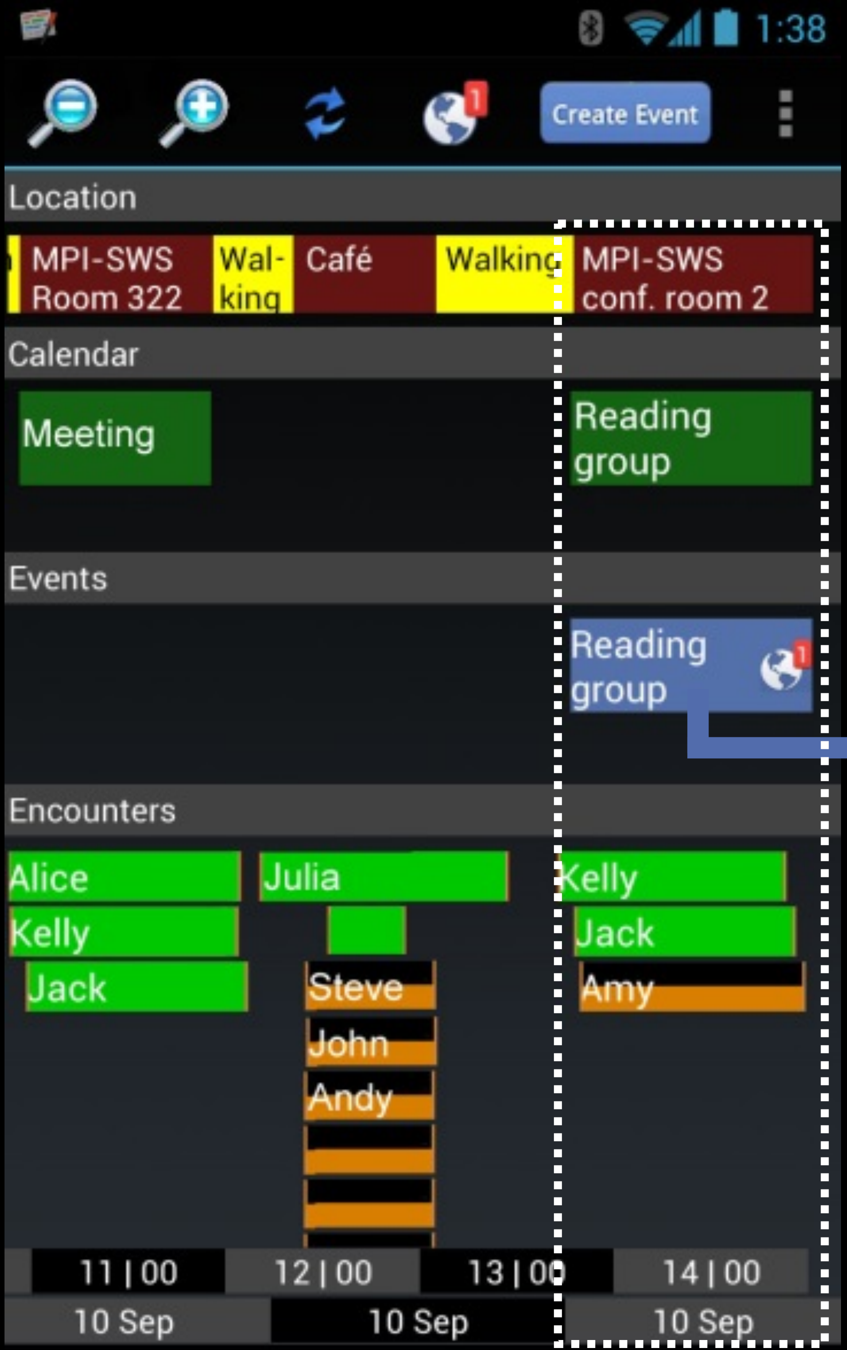
Cheap, non-interactive protocol enables low-energy implementation

SDDR Evaluation

- ✓ Time to Compute Recognizability
- ✓ Energy Consumption - Power Traces
- Energy Consumption - Micro-benchmarks
- Battery Life vs. # Nearby Devices

EnCore - Communication Platform

Appeared in MobiSys '14



Supports content sharing for groups of socially meaningful encounters

"Great discussion!" - Amy

Summary

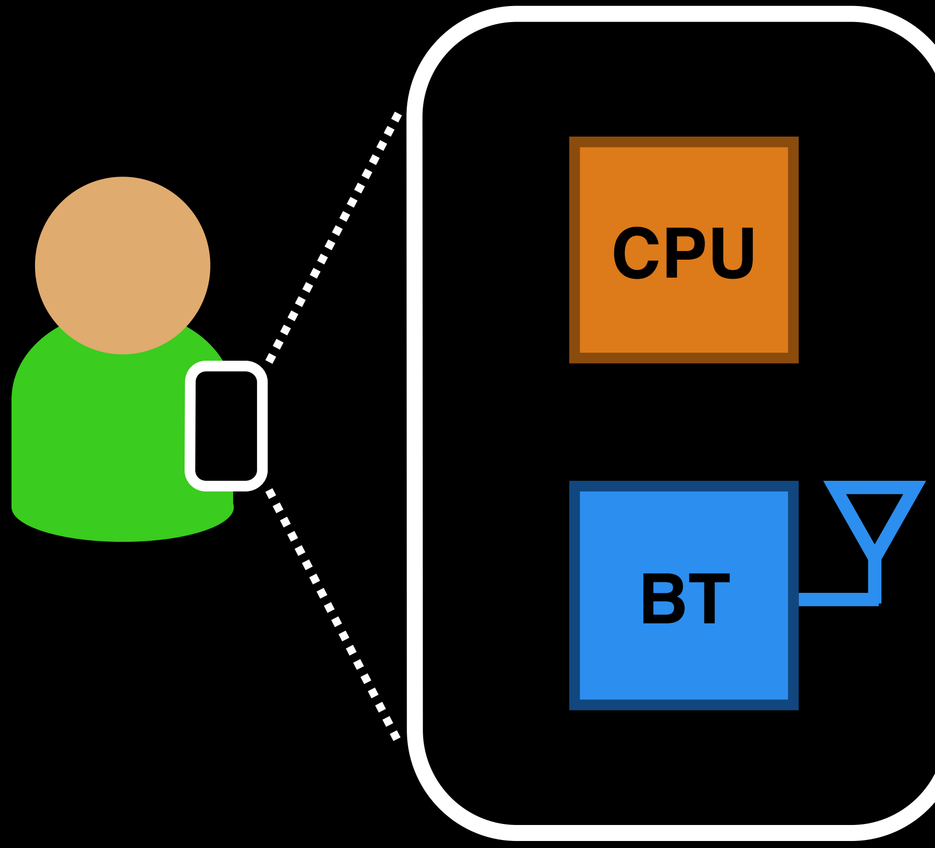
Mobile social applications have significant privacy challenges

SDDR provides secure encounter primitive

runs efficiently on mobile devices

www.cs.umd.edu/projects/ebn

SDDR over Bluetooth 2.1



Discoverable B

Responds to inquiry scan with address and beacon

Inquirer C B

Performs inquiry scan, receiving and processing nearby devices’ beacons

Change MAC address each epoch