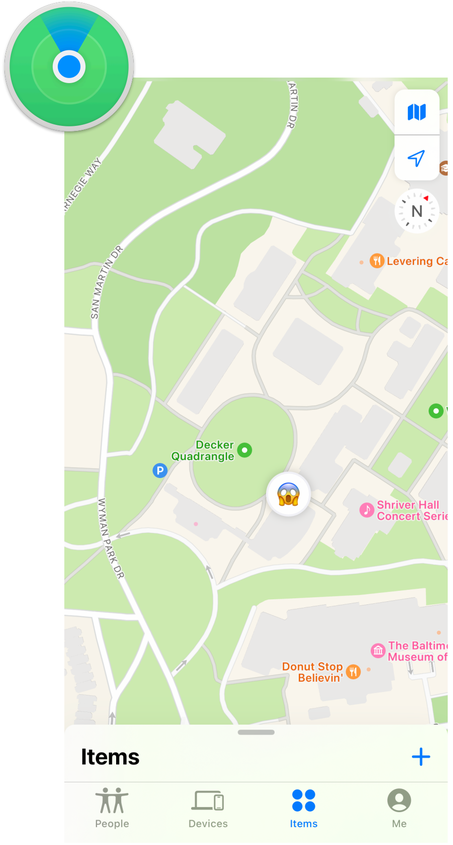
A way to achieve more private abuse-resistant location tracking

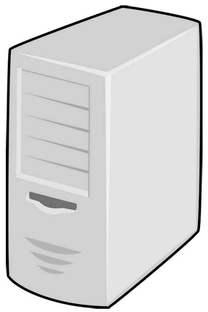
Based on paper by *Harry Eldridge,* ***Gabrielle Beck****, Matthew Green, Nadia Heninger, and Abhishek Jain.* **https://eprint.iacr.org/2023/1332.pdf**

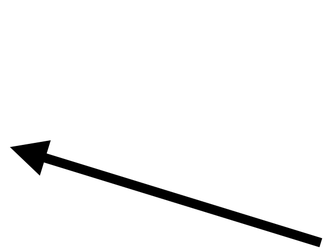
What are we talking about

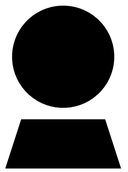
- Small computing devices that can help users find lost items
  - Known as tags/accessories
  - Make use of *crowd-sourced location tracking*
    - Only requires the tag to have access to BLE



Existing Techniques: High Level Approach



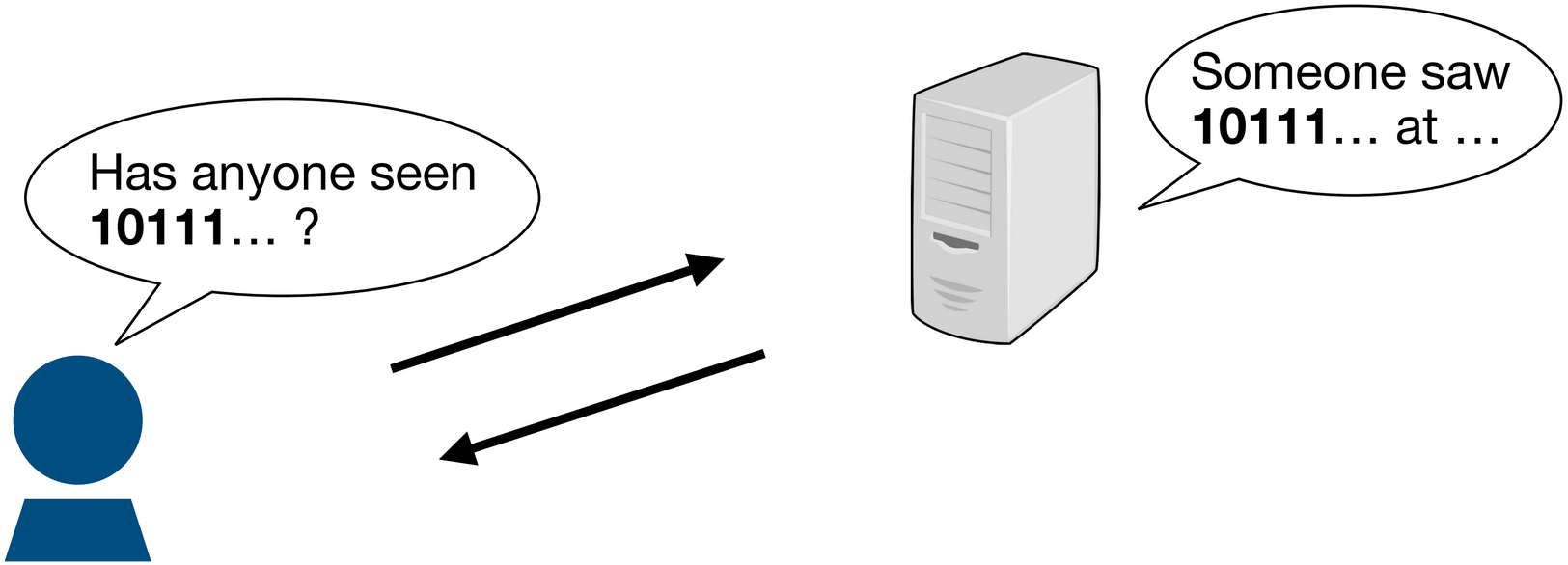




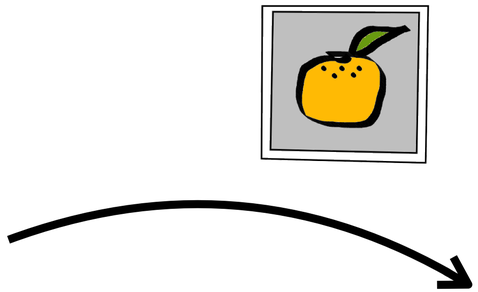
I saw **10111**…
at …

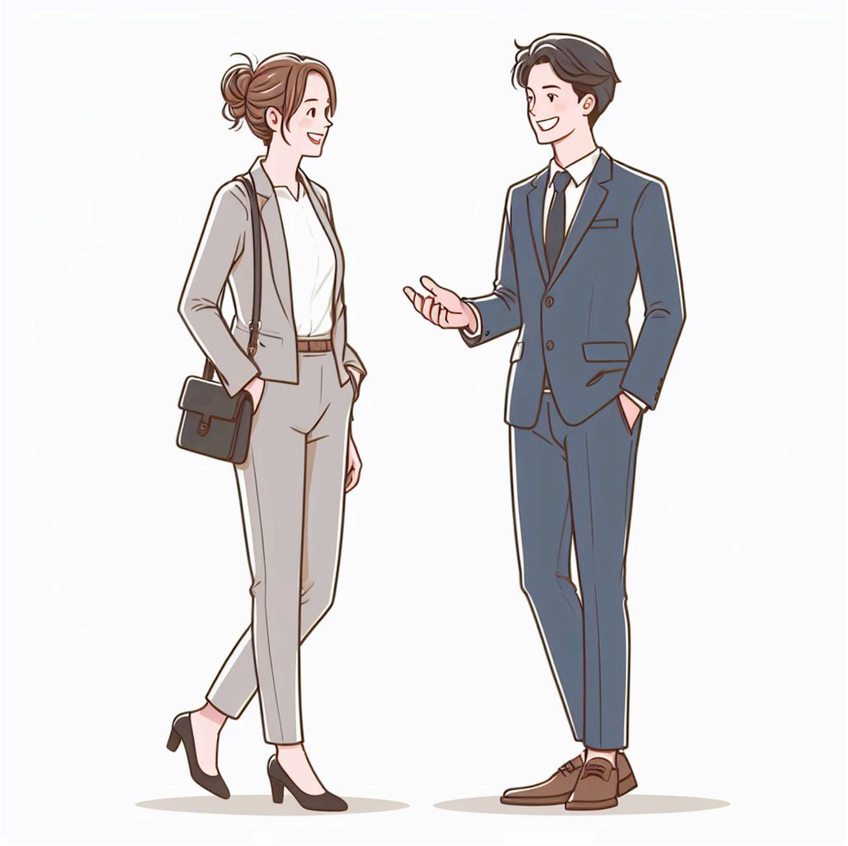
1011101111000101010…

1011101111… - Pseudorandom Identifier


Has anyone seen
10111… ?
Someone saw
10111… at …

Potential Safety Risks - Stalking?





Many, *many* real-life examples of failures

Two Women Sue Apple Over AirTag Stalking

One woman found an AirTag tracking device in the wheel well of her car and a second woman found an AirTag in her child's backpack, the lawsuit said.

TECHNOLOGY

AirTags are being used to track people and cars. Here's what is being done about it

February 18, 2022 · 5:37 PM ET
Heard on All Things Considered

By Michael Levitt

Ex-partner uses Apple AirTag to stalk Ahmedabad woman, device found hidden under driver's seat

Ex-partner exploits Apple AirTag technology for stalking a woman in Ahmedabad, India, marking the first case of such digital terror in the country.

BBC Sign in Home News Sport Reel Worklife T

NEWS

Home | War in Ukraine | Climate | Video | World | US & Canada | UK | Business | Tech | Science

Newsbeat

Apple AirTags: Love Island star says device used to stalk her

23 March

Android users have virtually no protection from AirTag stalking — and Apple needs to fix it

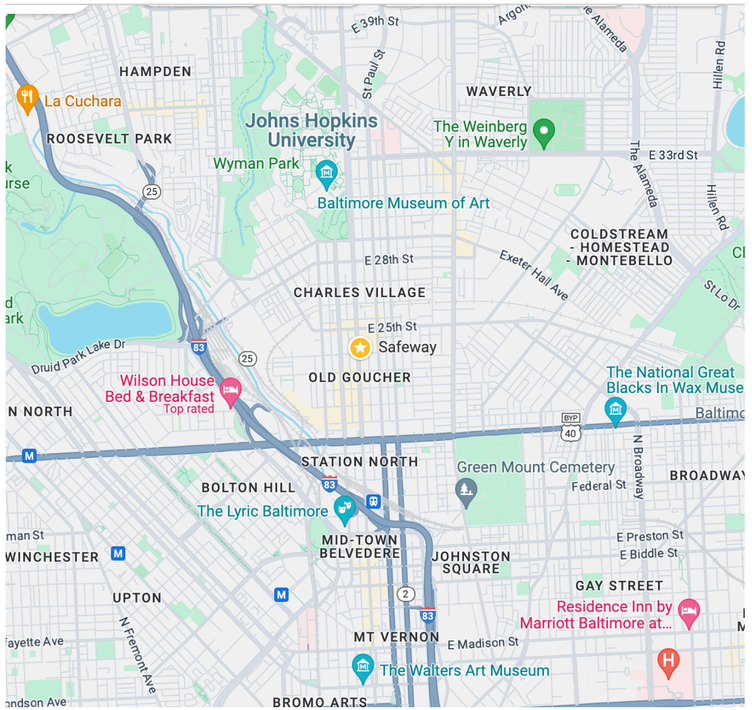
By Tom Pritchard published January 15, 2023

Apple needs to do more to protect Android users

Potential Safety Risks - Tracking?

A *tracking* adversary who sees multiple bxs from the same device could **link** them together

Bxs:

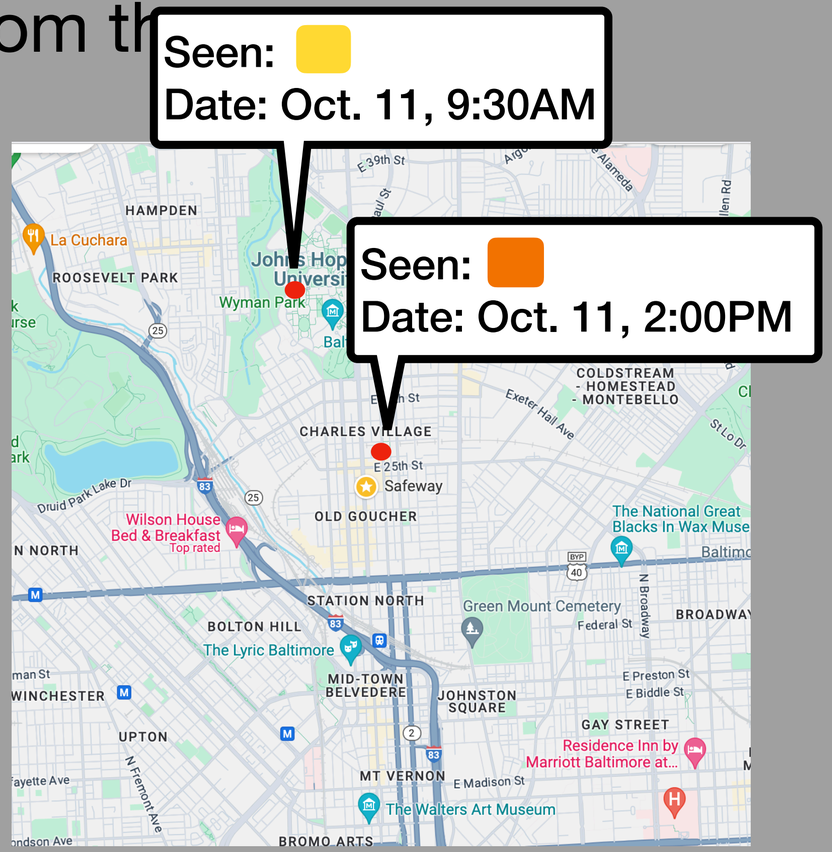


Potential Safety Risks - Tracking?

A *tracking* adversary who sees multiple bxs from th
device

Is this the same person?

Bxs:



Current Existing DULT Proposal [2]

- Based mainly off a design introduced by Apple
  - To combat *tracking* adversaries, identifier is **periodically** rotated
  - To combat *stalkers*, make identifiers rotate **slower** when disconnected from the owner

Current Existing DULT Proposal [2]

- Tags have two modes, **near-owner** and **separated**

Near-Owner	Separated
Identifiers rotate every **15** minutes	Identifiers rotate every **24** hours

Transitioning between **near-owner** and **separated** must happen within **30** minutes

Broadcasts made every **2-4** seconds

Disadvantages of approach

- One problem with the current approach is it could have better **privacy** for honest tag users
  - In **near-owner** mode, device still make broadcasts and owner can be tracked for 15 minute stretches
  - In **separated** mode, there is little to no privacy
    - If a friend takes your car and you had a tag in it, they can be tracked by **anyone**

Disadvantages of approach

- Things are even more complicated when accounting for transitions
  - Is it possible for a non-owner device to link **near-owner** and **separated** bxs from the same device?
  - Does transitioning from **separated** to **near-owner** to **separated**, in the same 24 hr window, result in the **same** identifier being transmitted?

Tension between privacy and stalker detection

- Difficult to achieve honest user privacy and stalker detection *simultaneously*
  - Seems like anything that prevents honest tag users from being tracked helps stalkers

> 2. It is not possible to correlate the public keys broadcast across multiple epochs without knowing the shared key SK, which is only know to the owner. However, an observer who sees multiple beacons within the same epoch can correlate them, as they will have the same Y_i. However, fast key rotation also makes it more difficult to detect unwanted tracking, which relies on multiple observations of the same identifier over time.

From [3]

Is there an alternative approach?

- Say tag produces y broadcasts in some window of time

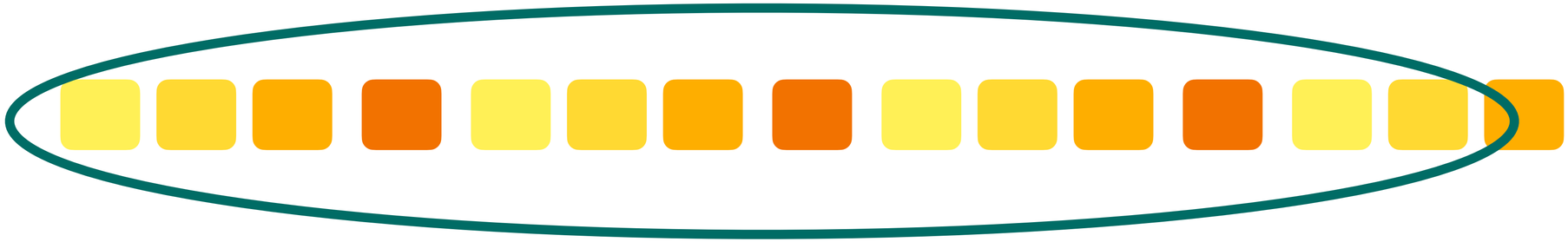
Bxs:

Is there an alternative approach?

- If tag is placed on a person…

Seen by stalking victim

Bxs:



Is there an alternative approach?

- However, if someone tries to track an honest tag user…

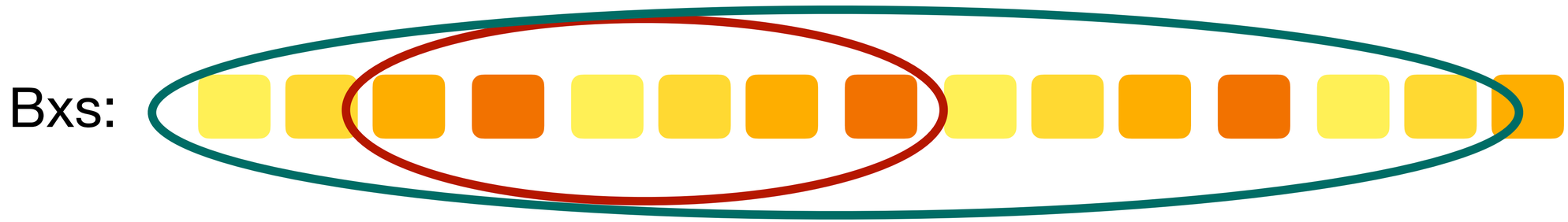
**assuming non-targeted, non-global tracking adversary

Is there an alternative approach?

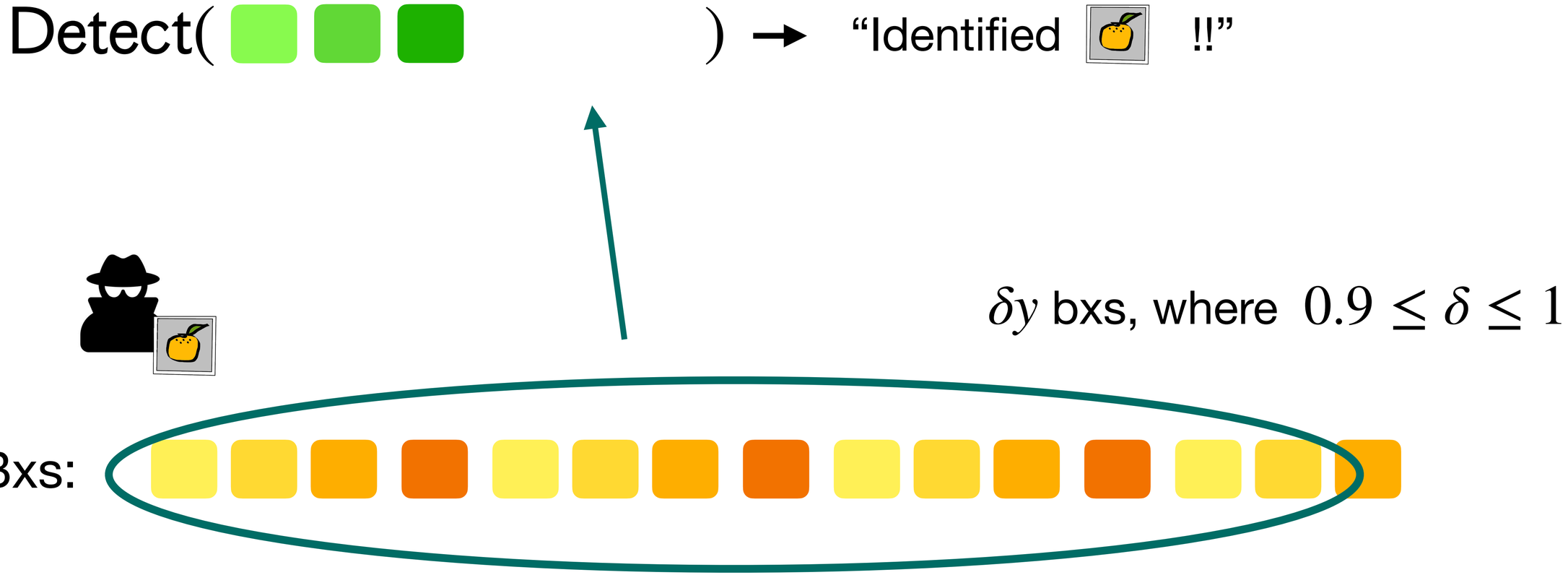
Observation: There is a difference in *resource capabilities* of stalking victims and tracking adversaries even if both parties have a similar de-anonymization goal!

Seen by stalking victim

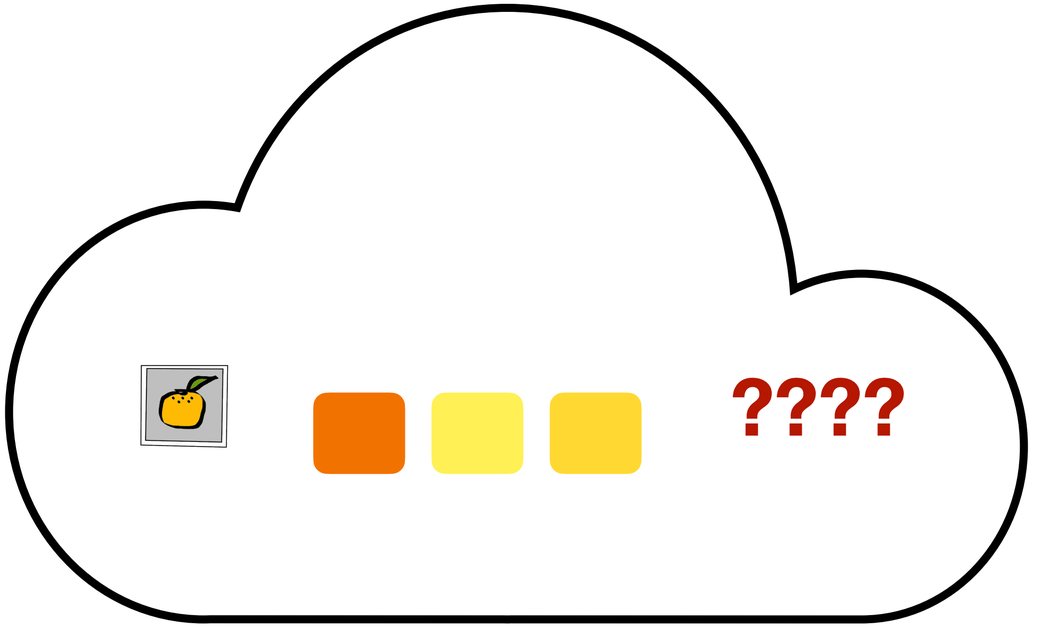
Seen by tracking adversary



What we achieve

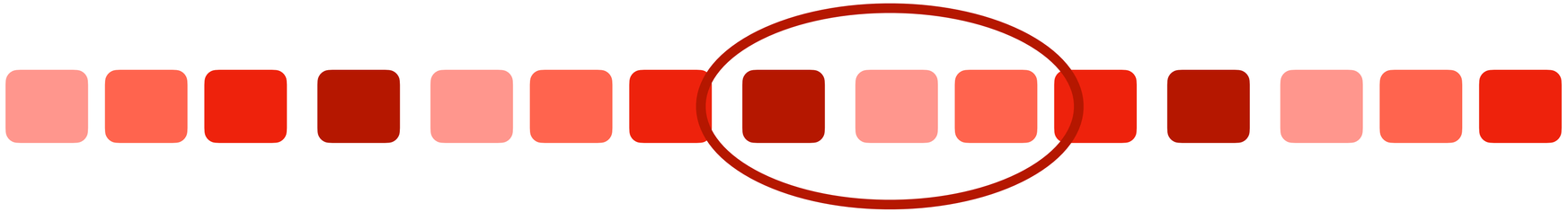


What we achieve

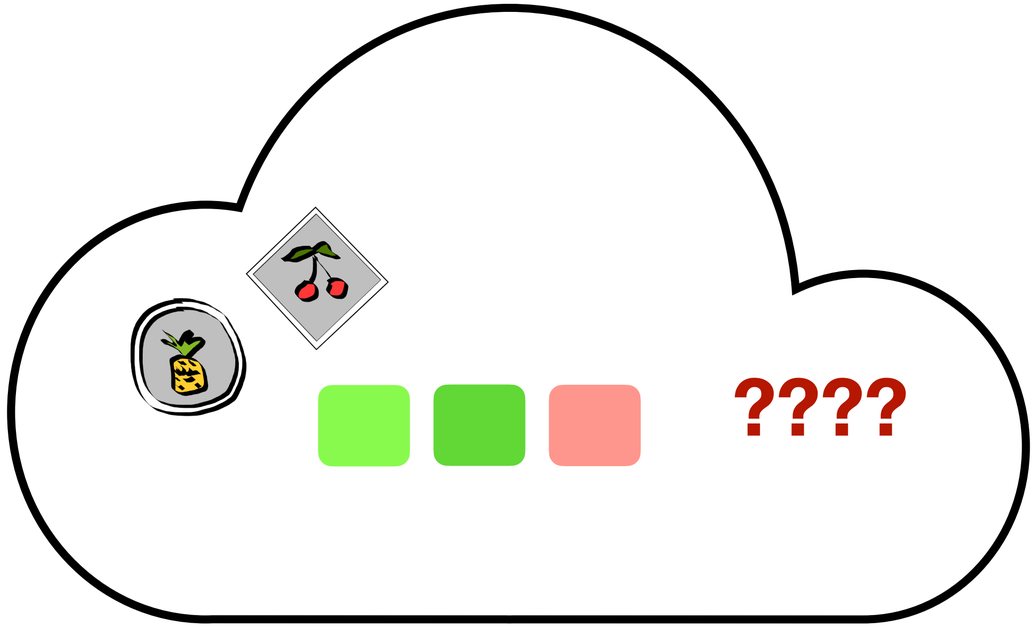


γy bxs, $0 \leq \gamma < \delta$,

Bxs:

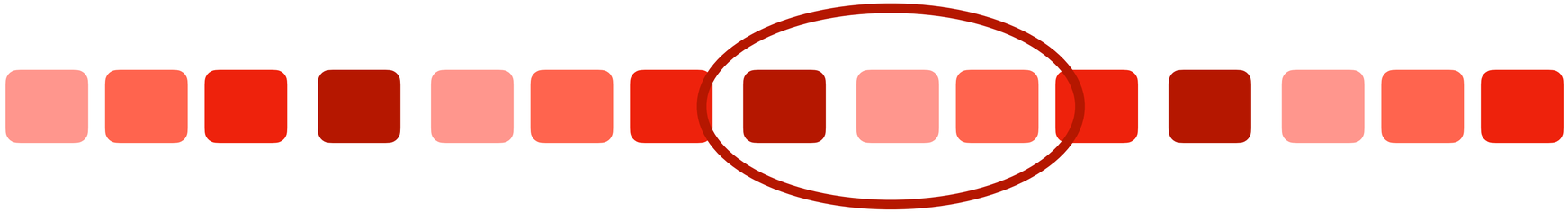


What we achieve



γy bxs, $0 \leq \gamma < \delta$,

Bxs:



How the approach works

- Tag sends out a bx every **2** seconds
  - Every other bx is the *identifier*
    - Not used for stalker detection, so rotates quickly
  - Other bxs solely for stalker detection
    - These also rotate quickly but are correlated in a way that is detectable if many bxs are collected

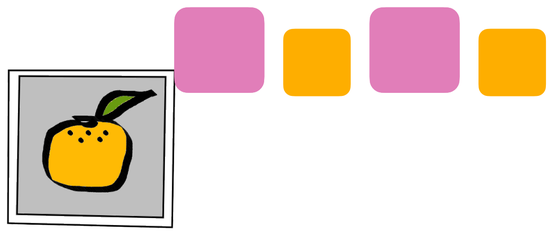
How the approach works

- The bxs and detection algorithm come from a multi-dealer secret sharing scheme (MDSS)
  - Bxs ≈ many different shamir secret shares
  - Detect algorithm is a list decoding algorithm for a type of RS code
  - If a secret is recovered from the detection algorithm it is used to contact the tag
  - Privacy holds due to MDSS *unlinkability,* detectability depends on list-decoding algorithm

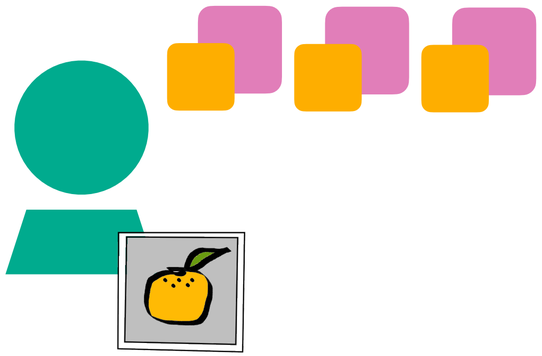
How the approach works

- identifier
- secret shares

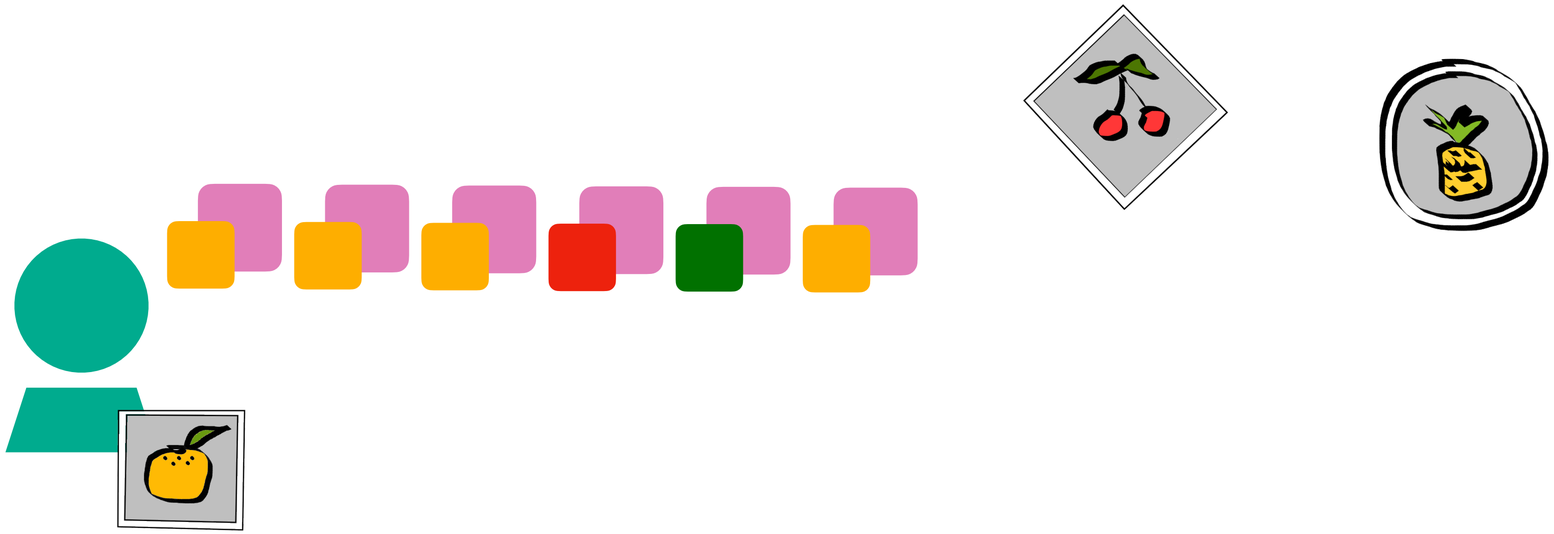
← 10011100...



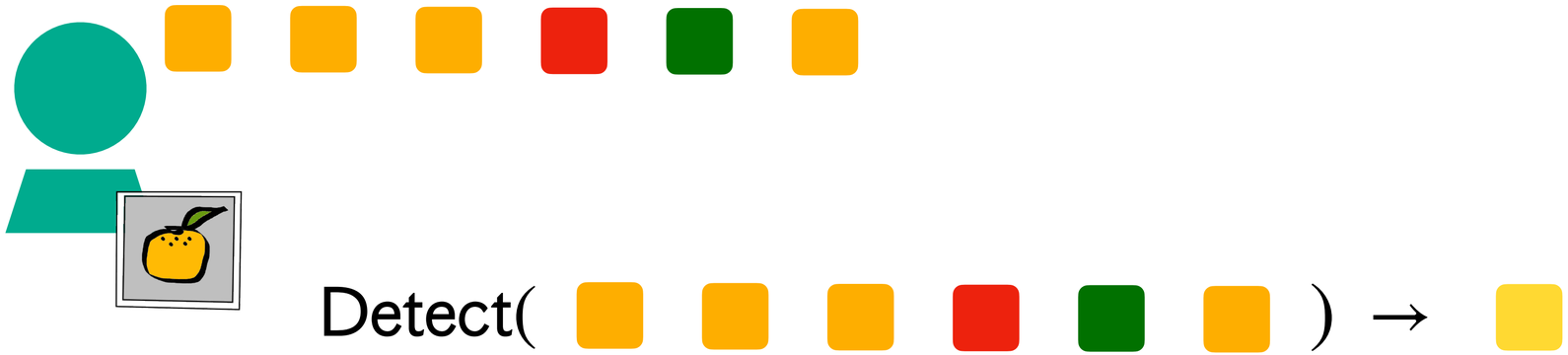
How the approach works



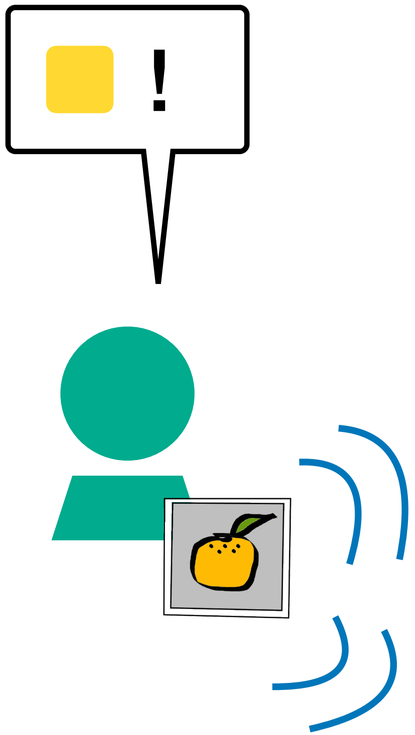
How the approach works



How the approach works



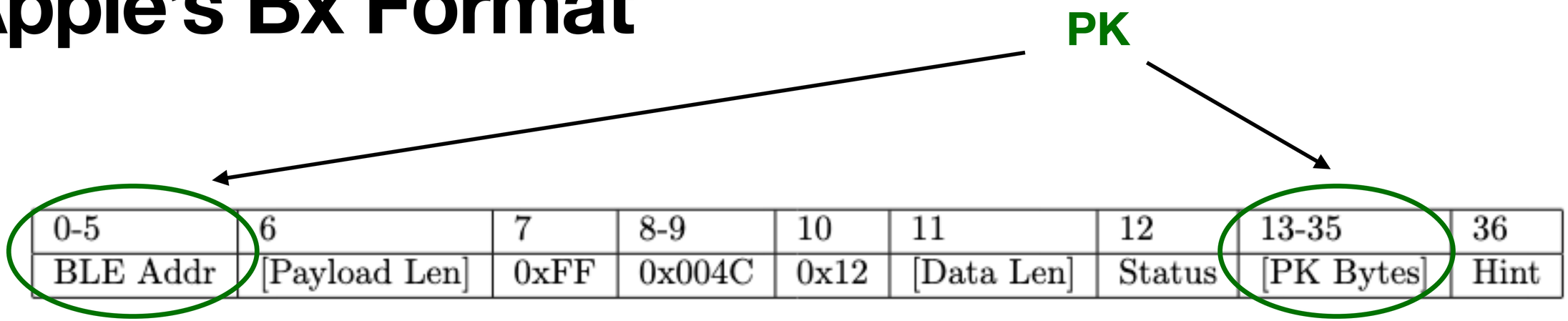
How the approach works



Analyzing approach

- **Advantages**
  - More privacy for honest tag users over existing solutions, while still retaining ability to detect stalking tags
- **Disadvantages**
  - Requires knowledge of environment conditions to achieve detection
    - Must have upper bound on number of tags to tolerate stalking one person and amount of “noise” from non-malicious tags

Apple’s Bx Format



0-5	6	7	8-9	10	11	12	13-35	36
BLE Addr	[Payload Len]	0xFF	0x004C	0x12	[Data Len]	Status	[PK Bytes]	Hint

- Pseudorandom identifier in Apple is a public key for a PKE
- PK is 28 bytes
  - 22 bytes + 2 bits of key are immediately after the “Status” byte
  - 5 bytes + 6 bits of key are in BLE Addr

From [4]

Proposed Bx Format

Replace with MDSS content

0-5	6	7	8-9	10	11	12	13-35	36
BLE Addr	[Payload Len]	0xFF	0x004C	0x12	[Data Len]	Status	[PK Bytes]	Hint

- New broadcast has similar format to the old one
  - Keeping the address and other important fields in tact, we can afford **25 bytes = 200 bits** for the MDSS content

Parameters - High Level

- When attempting to deploy MDSS in this setting, implementors must consider…
  - Identifier rotation rate*
  - The environment
    - max number of stalking tags expected to be placed on a victim
    - max amount of bxs expected from honest tags

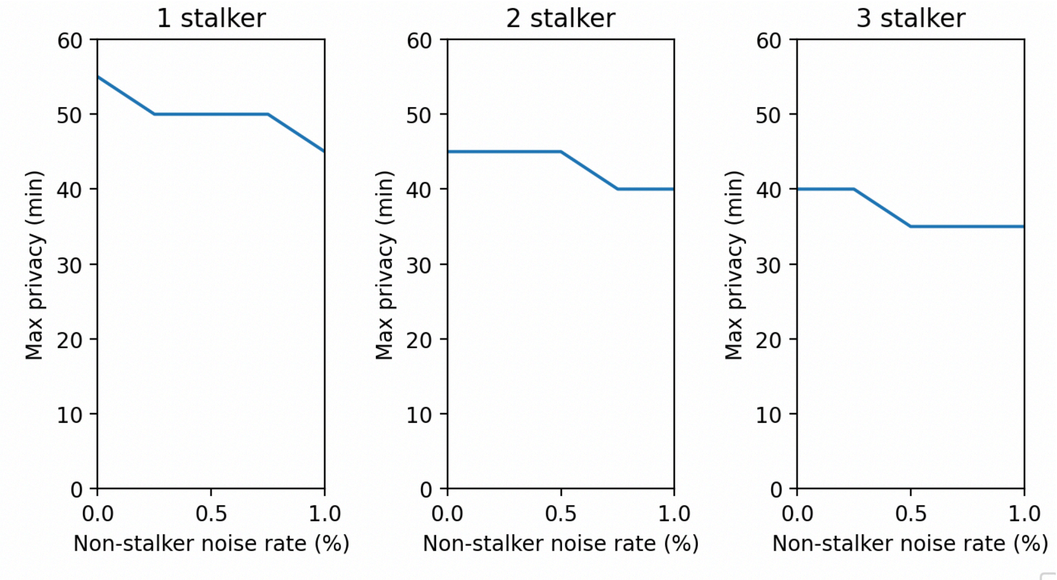
* - there is no point in rotating shares faster than this rate because a non-changing address makes a device's bxs linkable

Parameters - High Level

- Faster identifier rotation means…
  - More unique broadcasts given to detection algorithm
    - This will make detection algorithms slower
  - better privacy is achievable (typically)

Parameters - High Level

- If more stalkers and noise must be tolerated from other tags
  - Privacy for honest users will likely degrade
  - Detection algorithms may also be slower



Parameters - High Level

- Packet size also effects achievable privacy and can also effect algorithm running time
    - The larger the packets, the better the privacy parameter can be made (subject to identifier rotation rates)
    - Detection is slower in most if not all cases

ID rotation rate	Privacy (min)	MDSS Content (bits)
every 5 min	35	168
	40	260
	45	315

Choosing Parameters

- We assume…
  - pre BLEv5 limits on packet size
  - stalkers should be detected in an hour
  - there are at most…
    - 3 tags placed on individual from a stalker
    - “noise” from honest tags equal to 1/2 the broadcasts made by a single stalking tag

Choosing Parameters

ID rotation rate	Privacy for honest users (min)	Bx Size (bits)
every 5 min	35	168
every 10 min	30	200
every 15 min	30	170

Note: All sizes are below or at the 200 bit limit

An aside on rotation rate

- Bluetooth core specification [1] describes two types of random private addresses, non-resolvable and resolvable
  - Resolvable are generated using an algorithm involving an identity resolving key and hashing
  - Non-resolvable are set according to the host, but must have two MSBs set to 0

An aside on rotation rate

- The Bluetooth core spec recommends rotating a private addresses only every 15 minutes, it *is* possible to rotate them faster
  - Change GAP profile parameter that has suffix PRIVATE_ADDR_INT
    - It’s unclear - to me - why 15 is the default

Benchmarking

Epoch duration	# Unique bxs received	Detection runtime (no stalkers)	Detection runtime (stalkers present)	Polynomial recovery (all stalkers)
5 min	42	10 ms	20 ms	30 ms
10 min	21	10 ms	10 ms	20 ms
15 min	14	10 ms	10 ms	10 ms

Table 1: Benchmarks for detection on a MacbookPro, assuming broadcasts are being received at a rate that is equivalent to the number that would be produced by 3 tags.

Detection algorithms are faster than in paper because rotation period is much longer, meaning there are less unique points

Further Considerations

- Benchmarking does not take into account malicious security against rogue tags
  - If you want to combine this solution with BlindMy would require further work
- Experiments would need to be re-done to figure out what reasonable amount of noise is in given environments for a particular rotation rate
  - May be able to do additional filtering because of longer rotation periods

References

- [1] https://www.bluetooth.com/specifications/specs/core-specification-amended-5-0/
- [2] https://datatracker.ietf.org/doc/draft-ledvina-dult-accessory-protocol/
- [3] https://datatracker.ietf.org/doc/draft-fossaceca-dult-finding/
- [4] Heinrich et al. AirGuard - Protecting Android Users From Stalking Attacks By Apple Find My Devices. https://arxiv.org/pdf/2202.11813