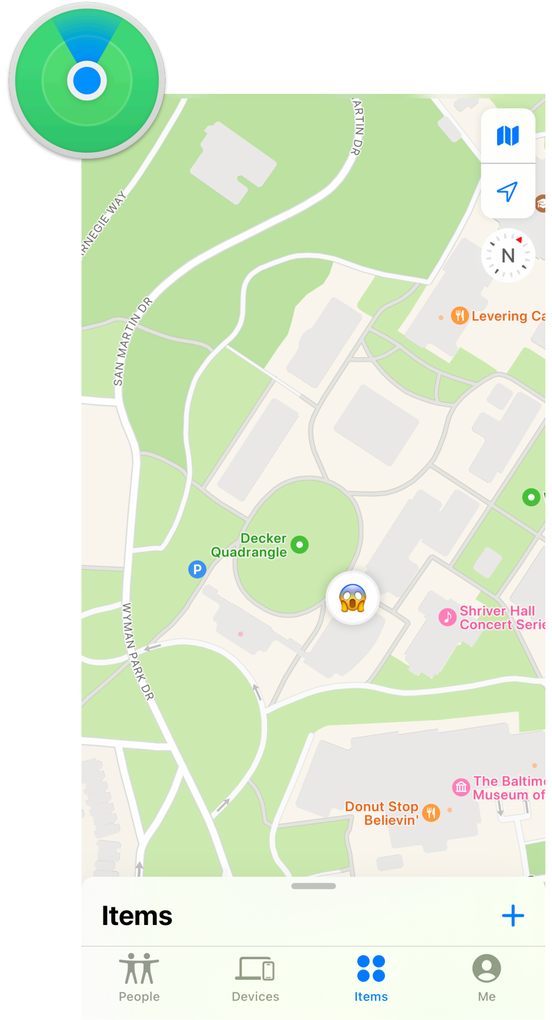
Abuse-Resistant Location Tracking: Balancing Privacy and Safety in the Offline Finding Ecosystem

Harry Eldridge Gabrielle Beck Matthew Green Nadia Heninger Abhishek Jain

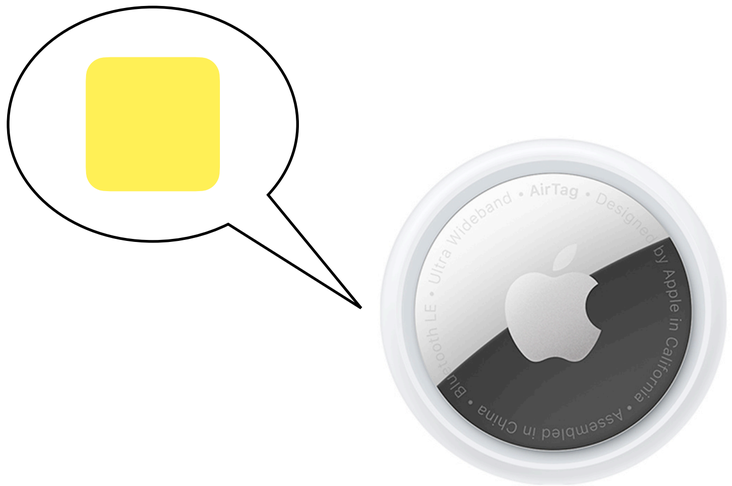
Location Tracking Accessories (LTAs)

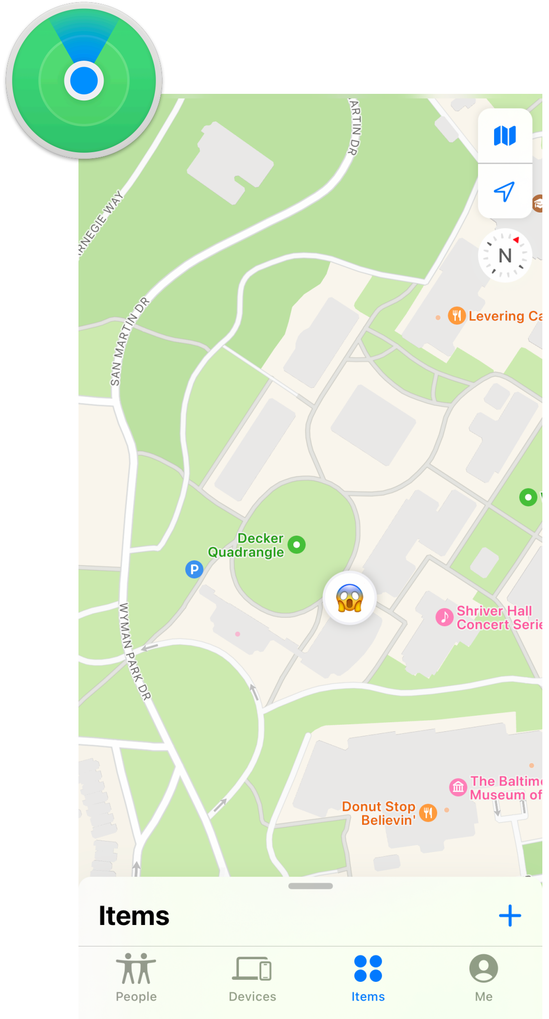
- Track physical objects: keys, luggage, pets, etc.
- Works via a *crowd-sourced* location tracking system



Location Tracking Accessories (LTAs)

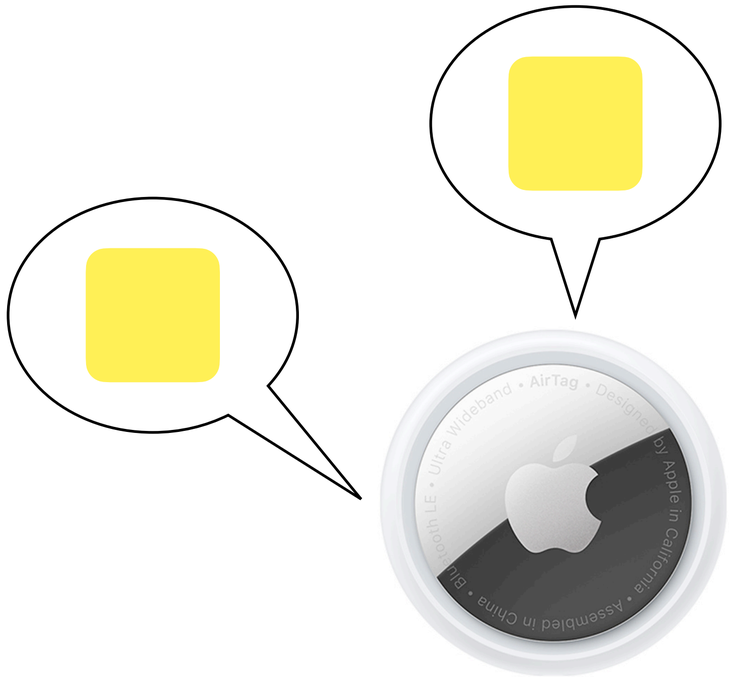
- Track physical objects: keys, luggage, pets, etc.
- Works via a *crowd-sourced* location tracking system

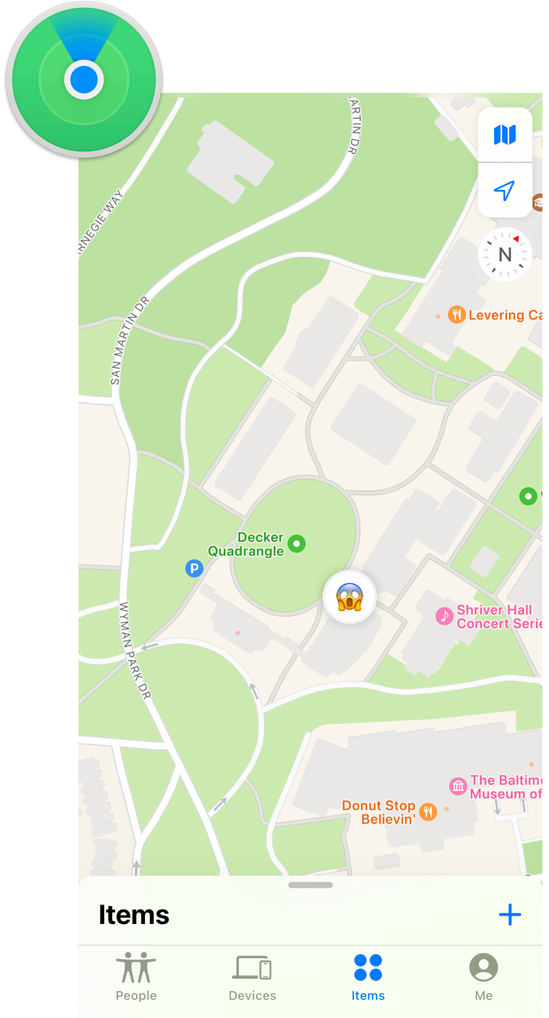




Location Tracking Accessories (LTAs)

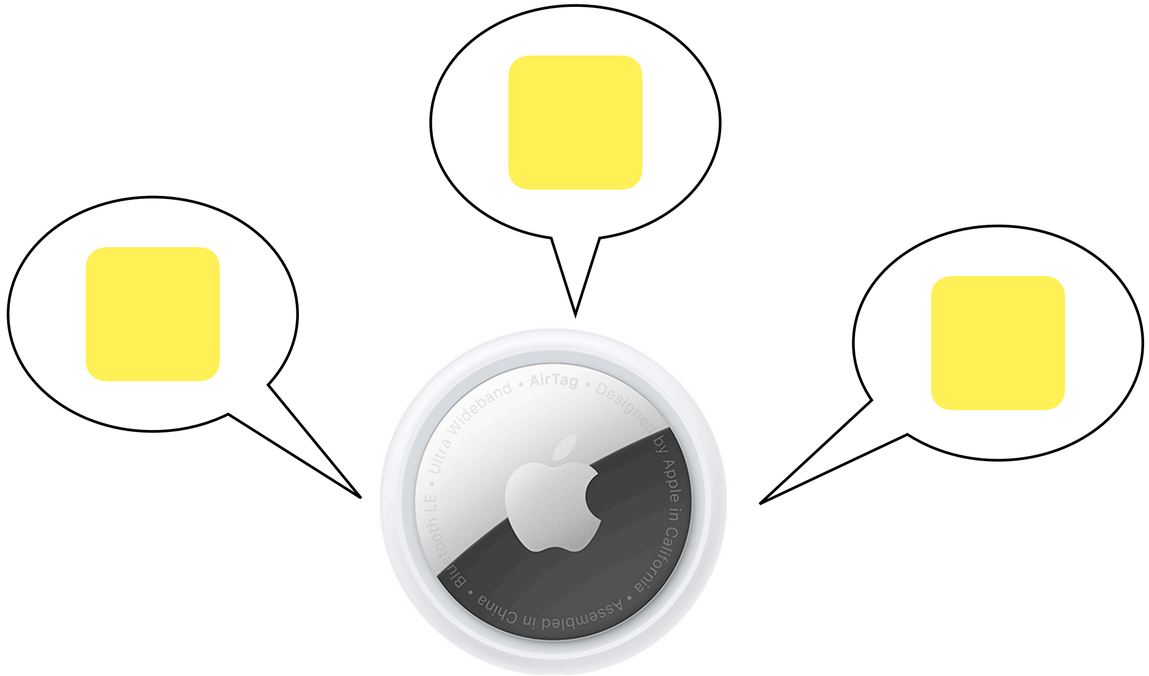
- Track physical objects: keys, luggage, pets, etc.
- Works via a *crowd-sourced* location tracking system

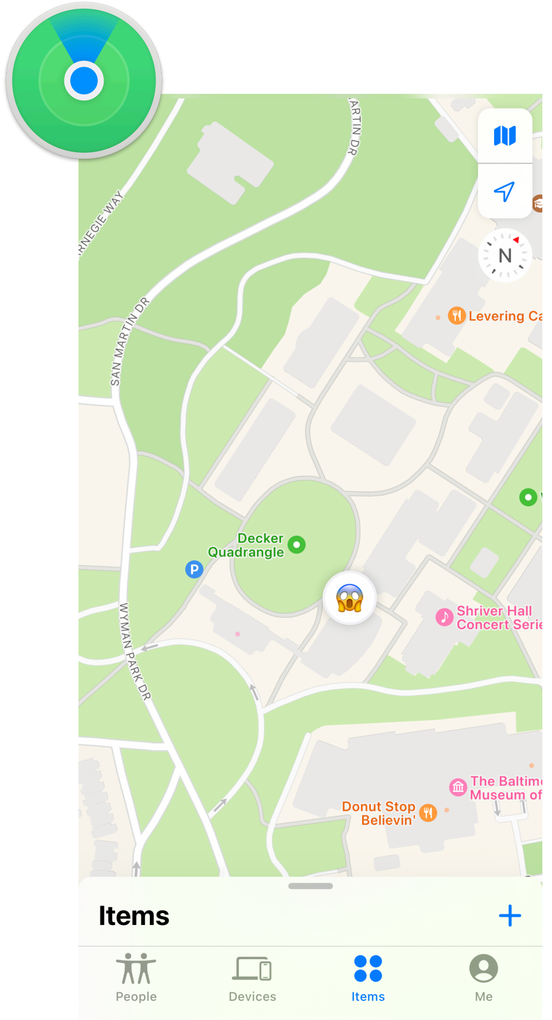




Location Tracking Accessories (LTAs)

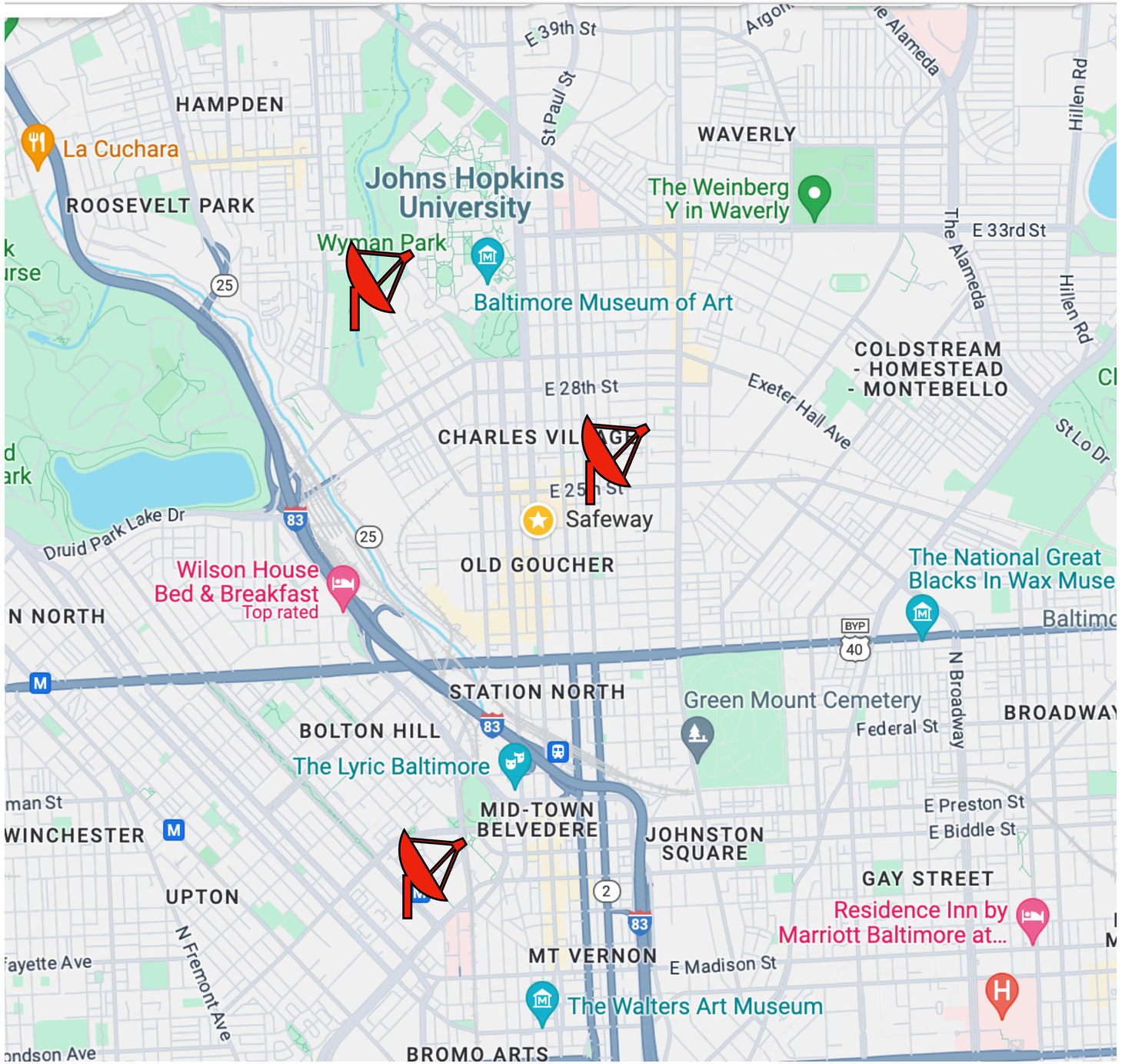
- Track physical objects: keys, luggage, pets, etc.
- Works via a *crowd-sourced* location tracking system





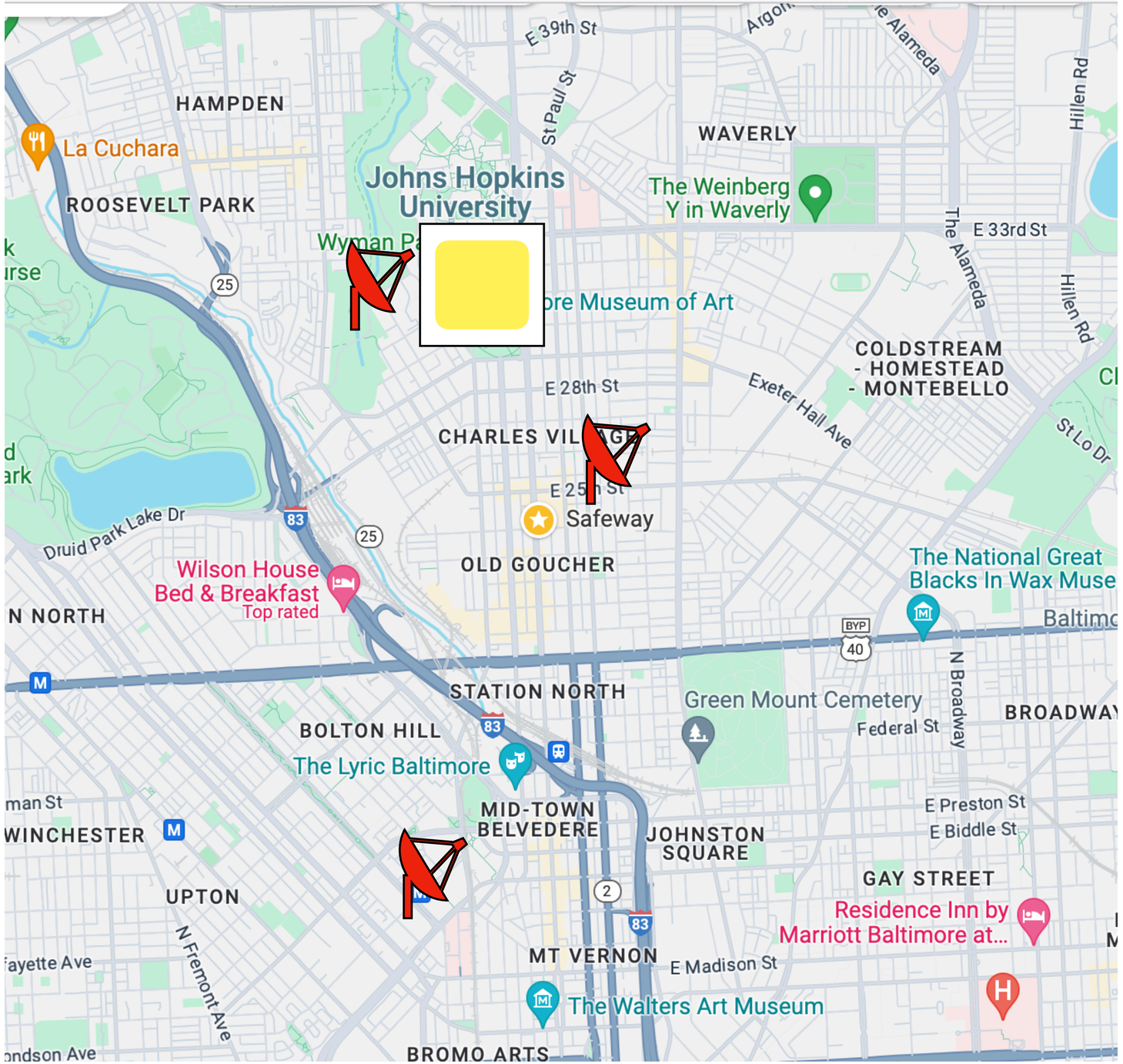
Tracking

- Adversaries with a network of Bluetooth receivers could track users by recognizing persistent nearby ID



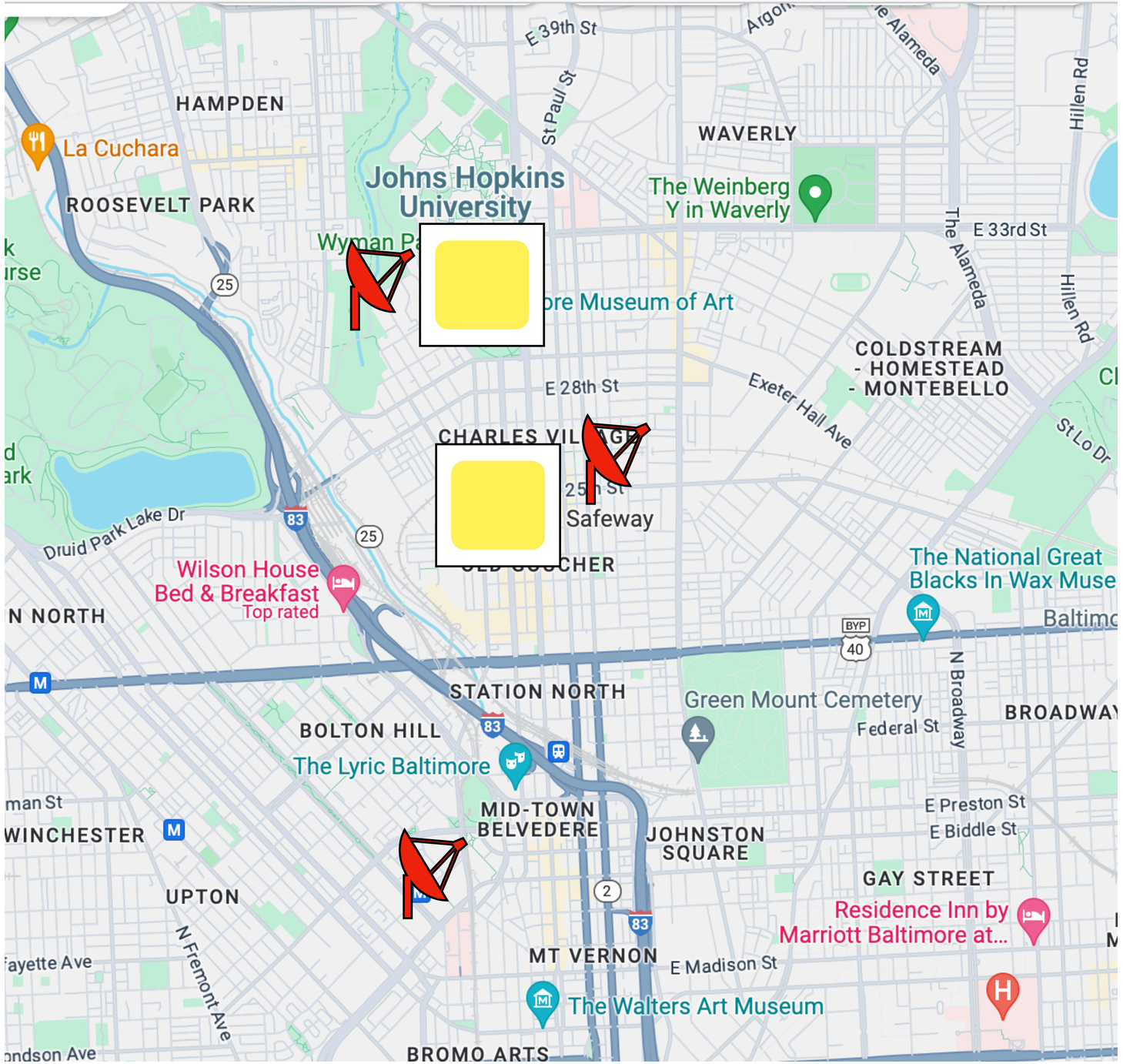
Tracking

- Adversaries with a network of Bluetooth receivers could track users by recognizing persistent nearby ID



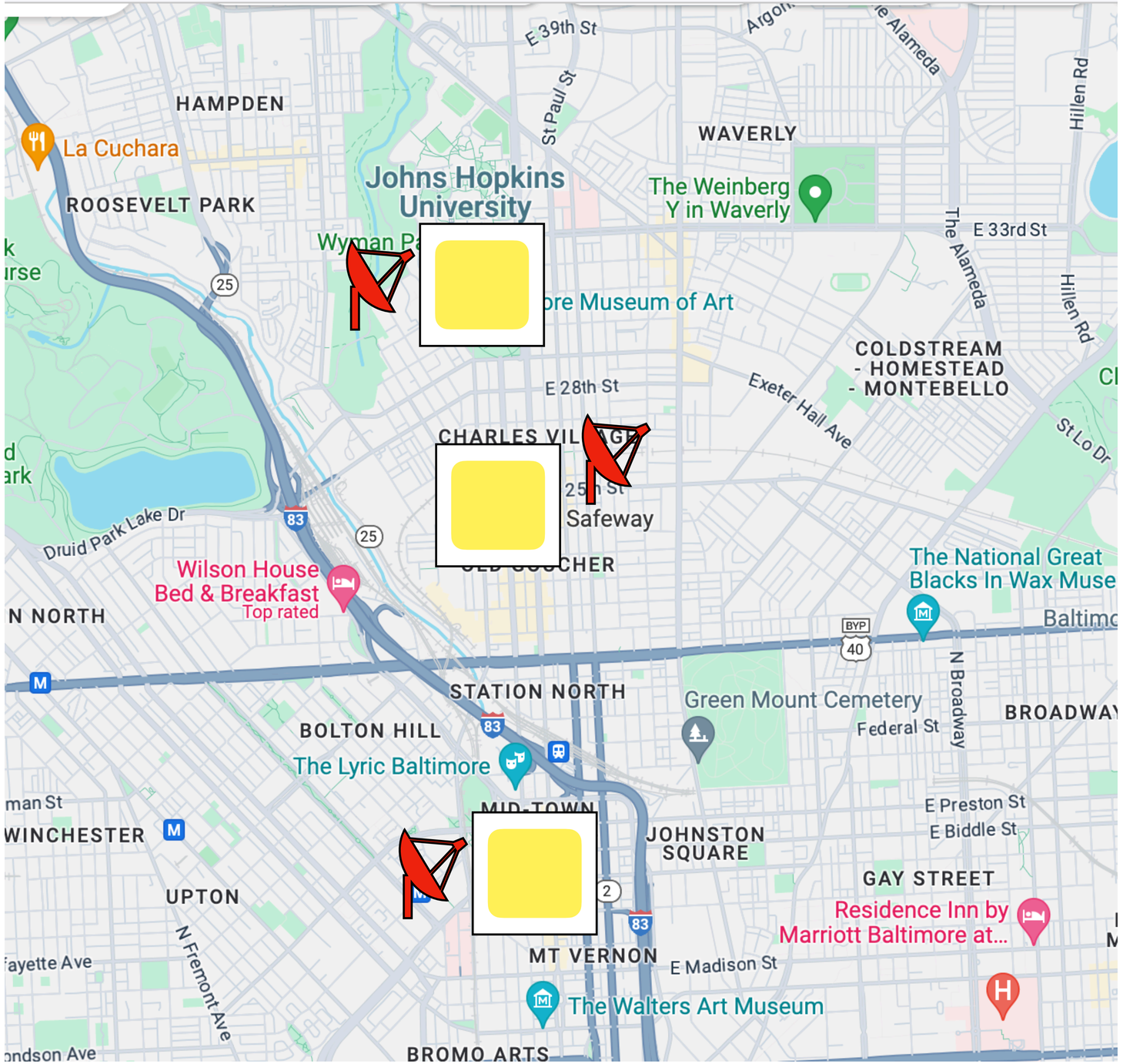
Tracking

- Adversaries with a network of Bluetooth receivers could track users by recognizing persistent nearby ID



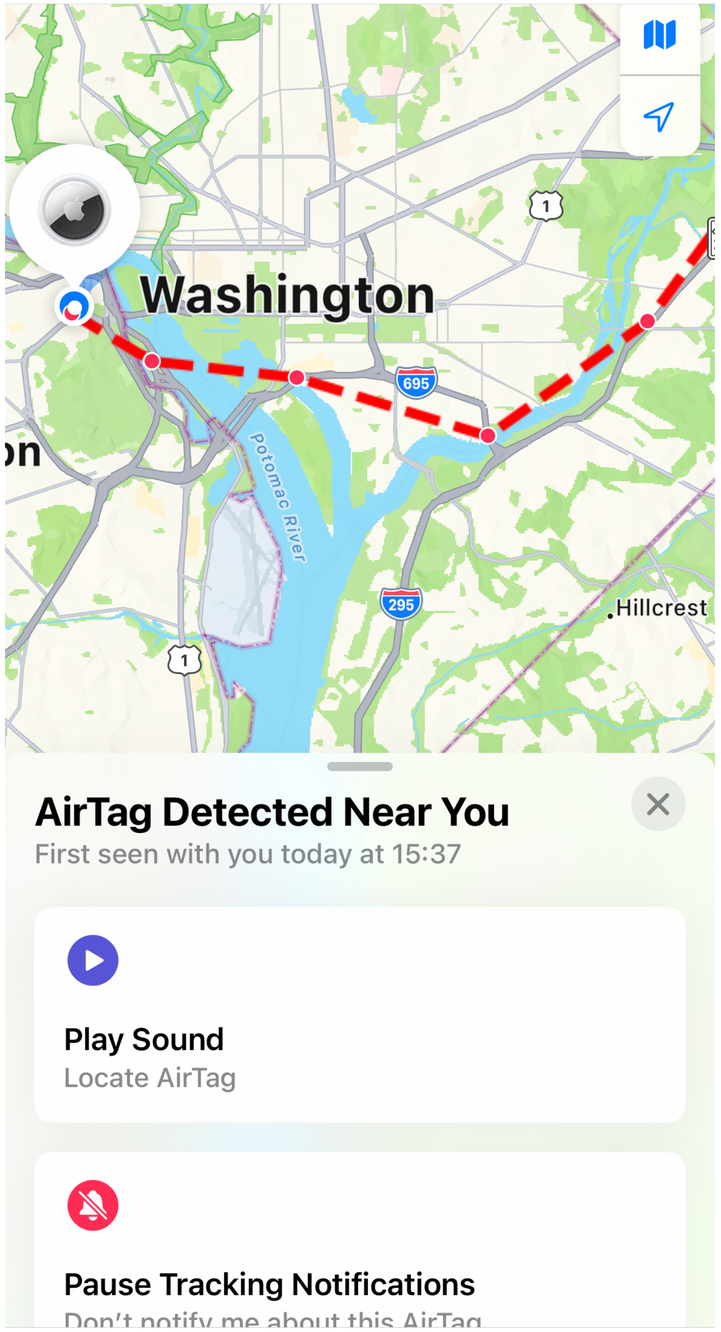
Tracking

- Adversaries with a network of Bluetooth receivers could track users by recognizing persistent nearby ID



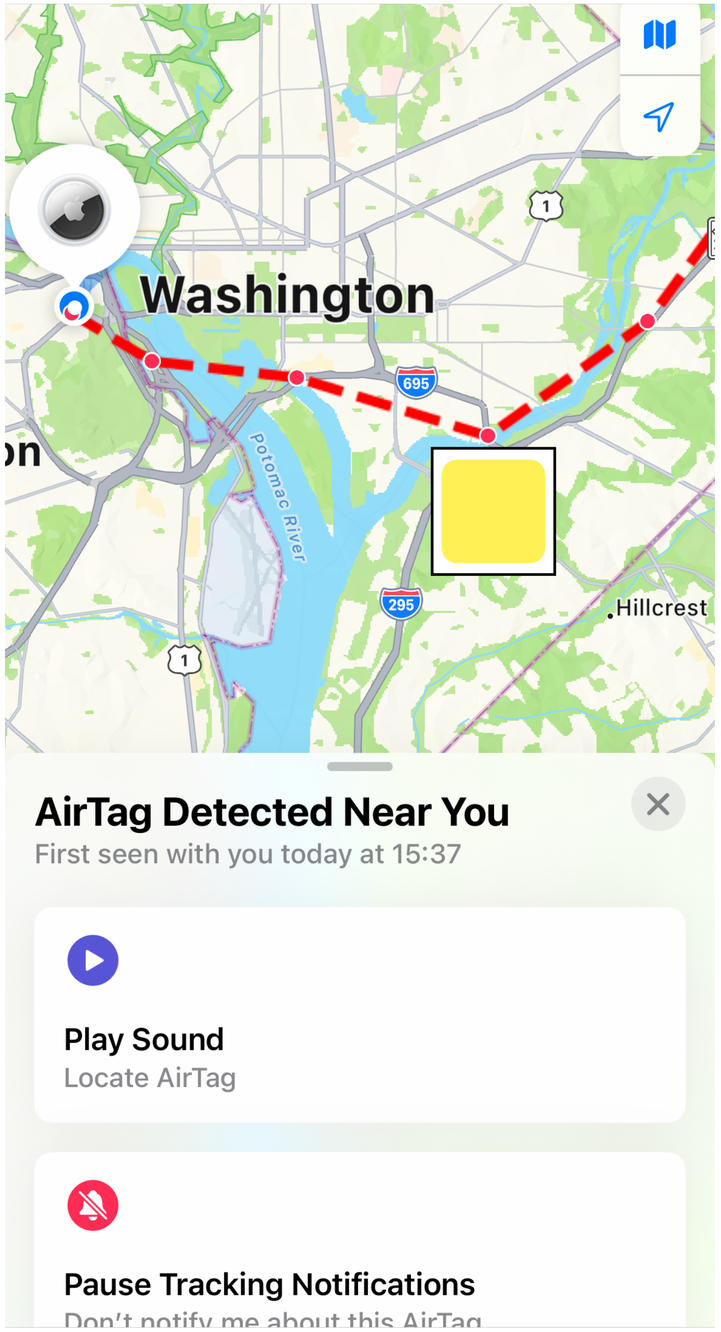
Stalking

- Secretly place an LTA **you own** on a person's belongings, follow their movement.
- Detected by recognizing a persistent nearby ID



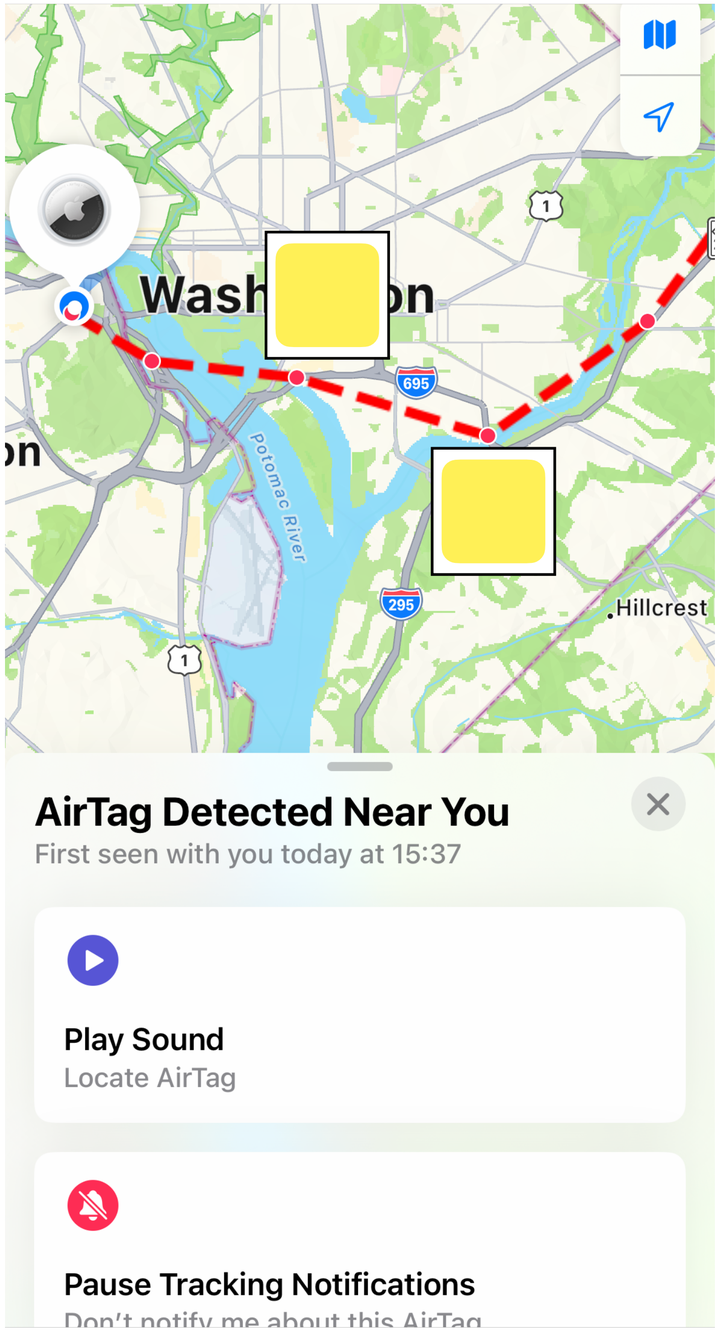
Stalking

- Secretly place an LTA **you own** on a person's belongings, follow their movement.
- Detected by recognizing a persistent nearby ID



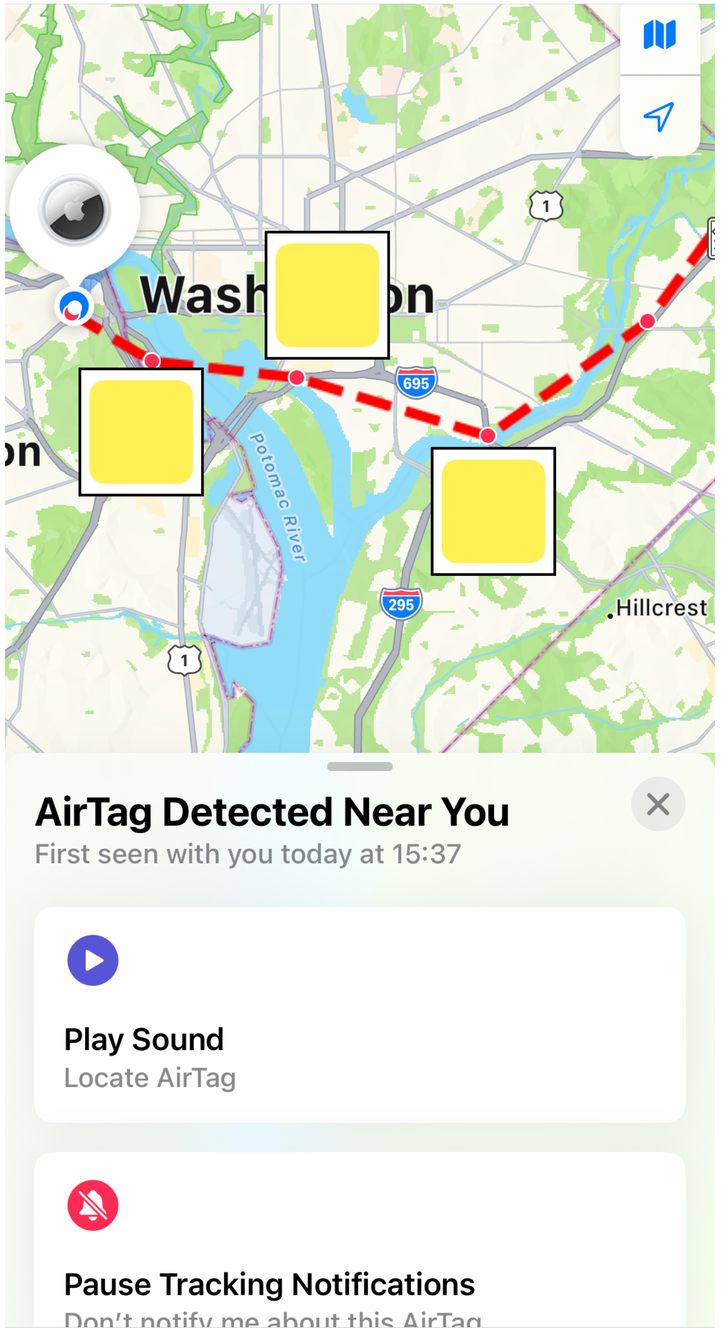
Stalking

- Secretly place an LTA **you own** on a person's belongings, follow their movement.
- Detected by recognizing a persistent nearby ID



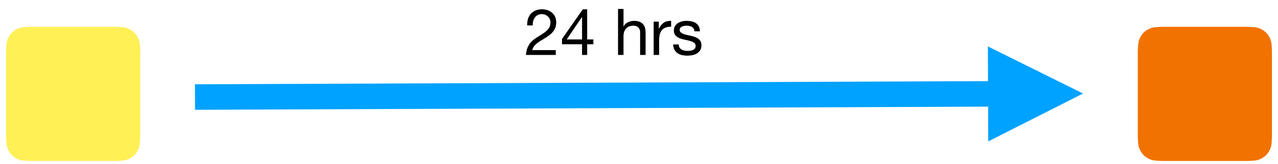
Stalking

- Secretly place an LTA **you own** on a person's belongings, follow their movement.
- Detected by recognizing a persistent nearby ID



Mitigations

- Apple’s current approach is to rotate the ID every 24 hours
- This means **honest** users can be **tracked** for 24 hours
- Can we do better?



Hope

Hope

Stalking victims will be in
continuous proximity to an LTA

Hope

Stalking victims will be in **continuous proximity** to an LTA

Tracking adversaries will only see broadcasts in short bursts

Hope

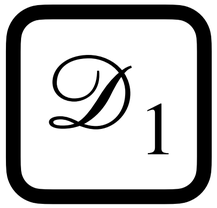
Stalking victims will be in **continuous proximity** to an LTA

Tracking adversaries will only see broadcasts in short bursts

We want a scheme where you can only **link** broadcasts together if you have **seen enough of them**

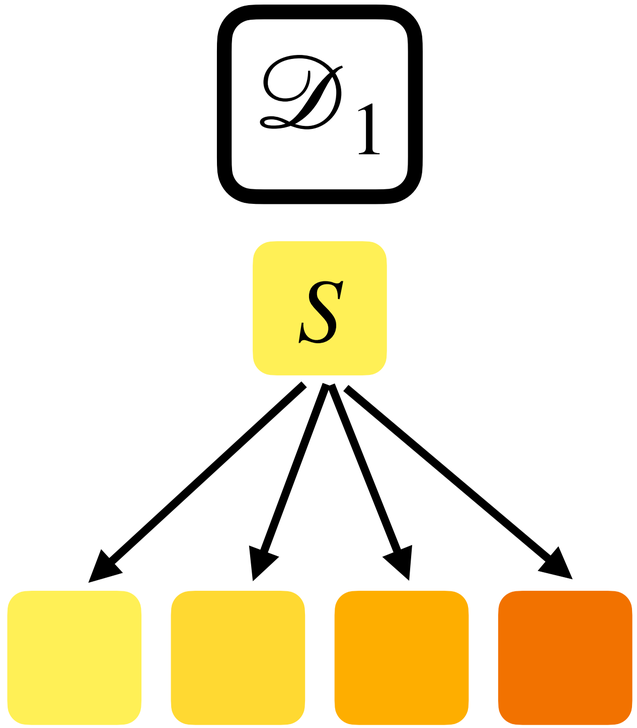
Secret Sharing

Secret Sharing

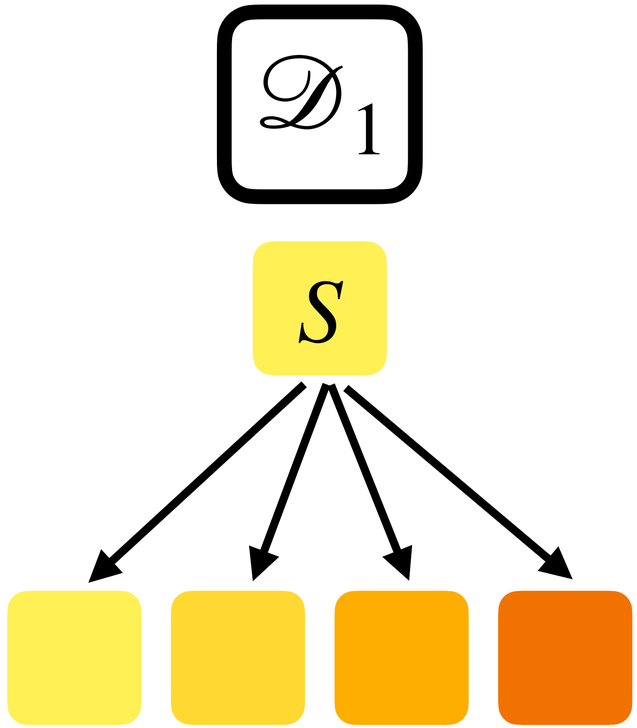


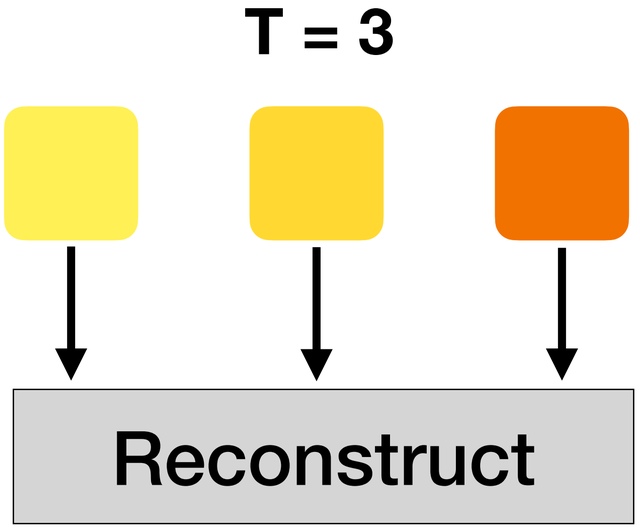
S

Secret Sharing

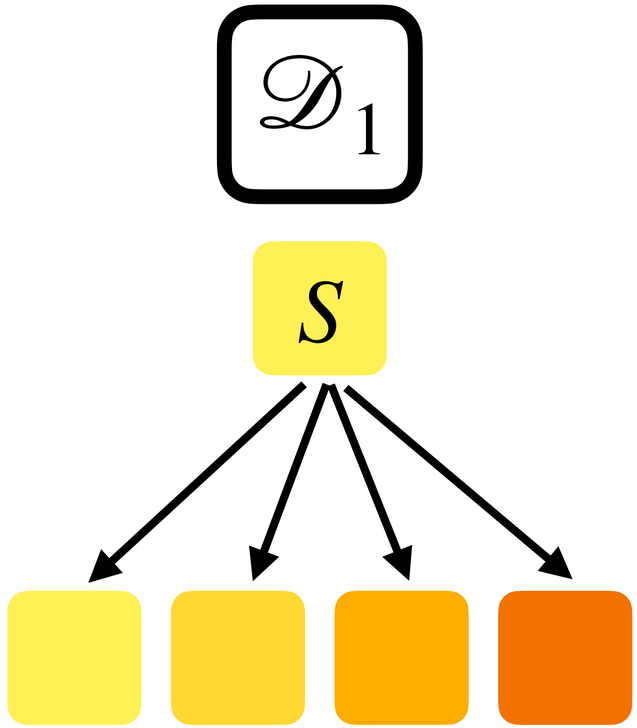


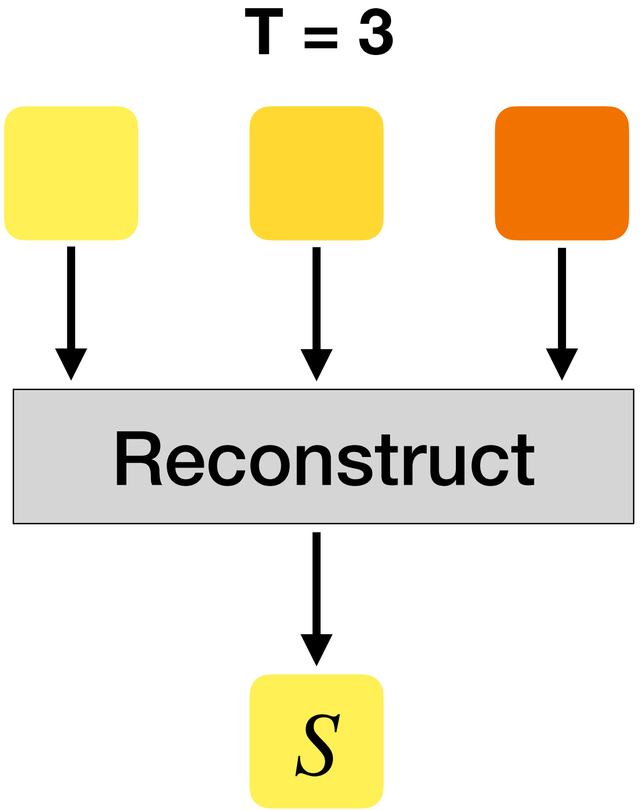
Secret Sharing



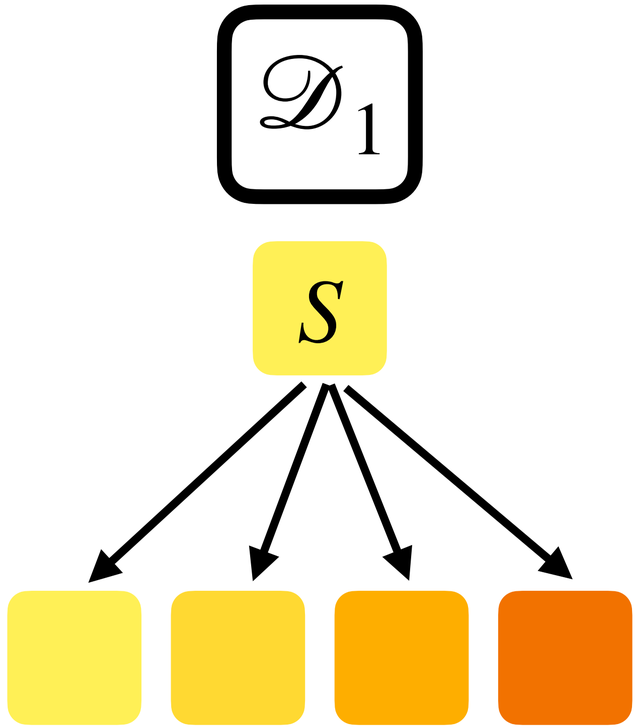


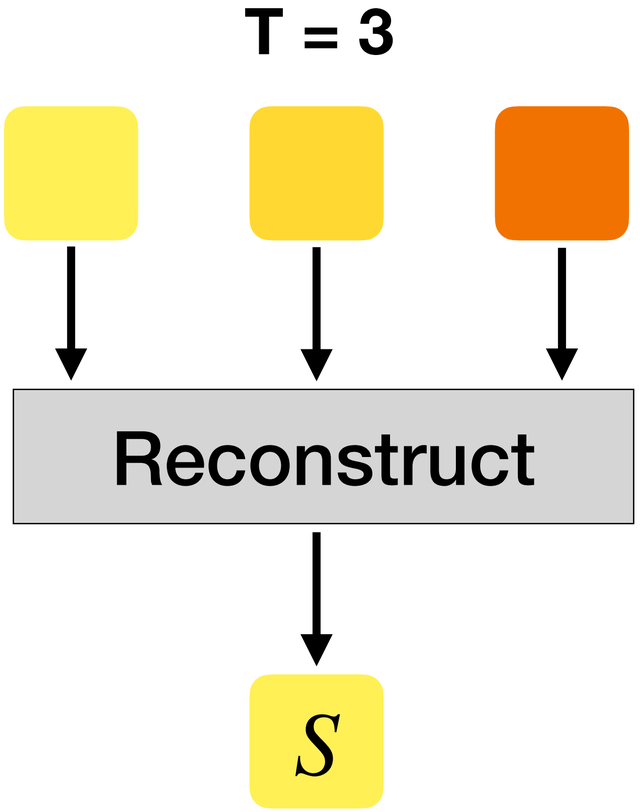
Secret Sharing





Secret Sharing

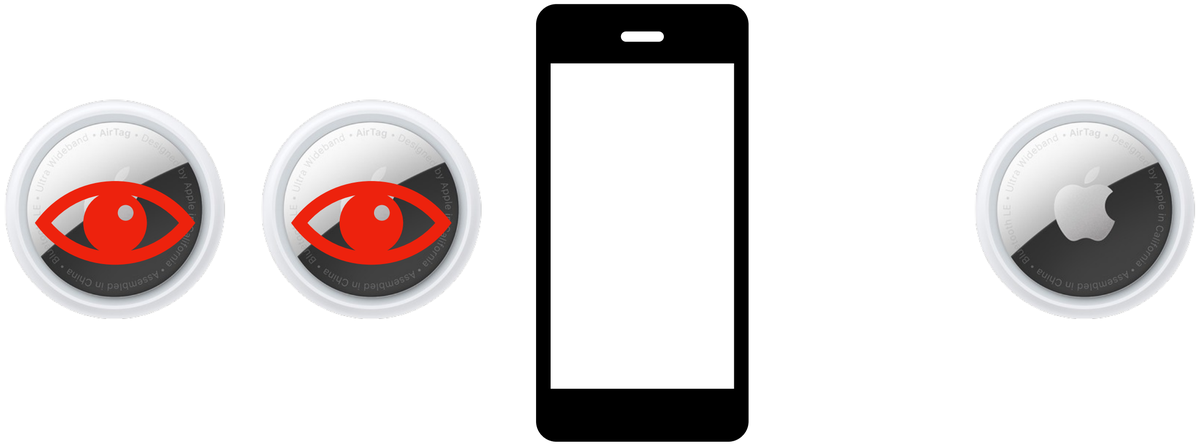




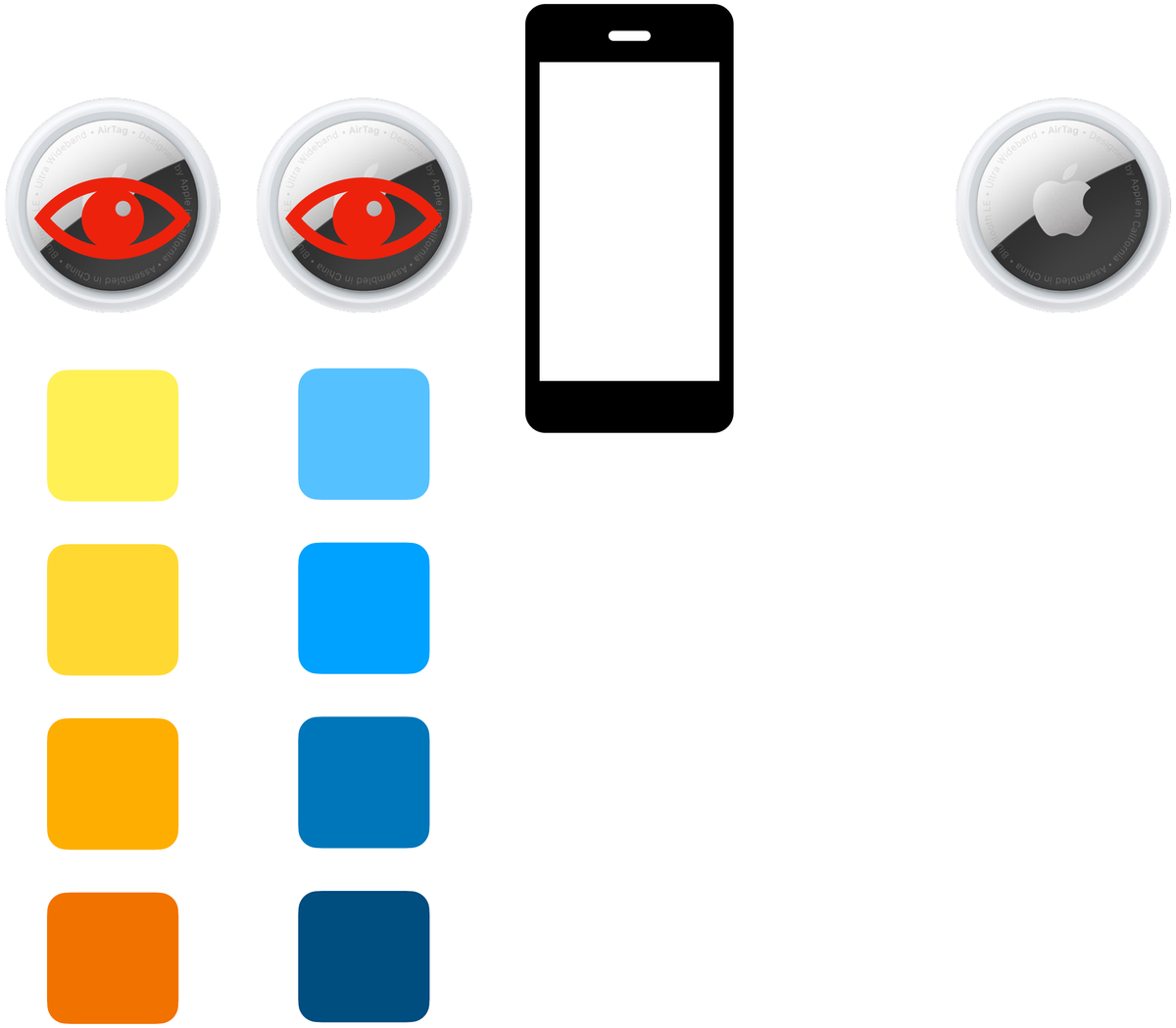
Privacy:  ????

Secret Sharing Alone Isn’t Enough

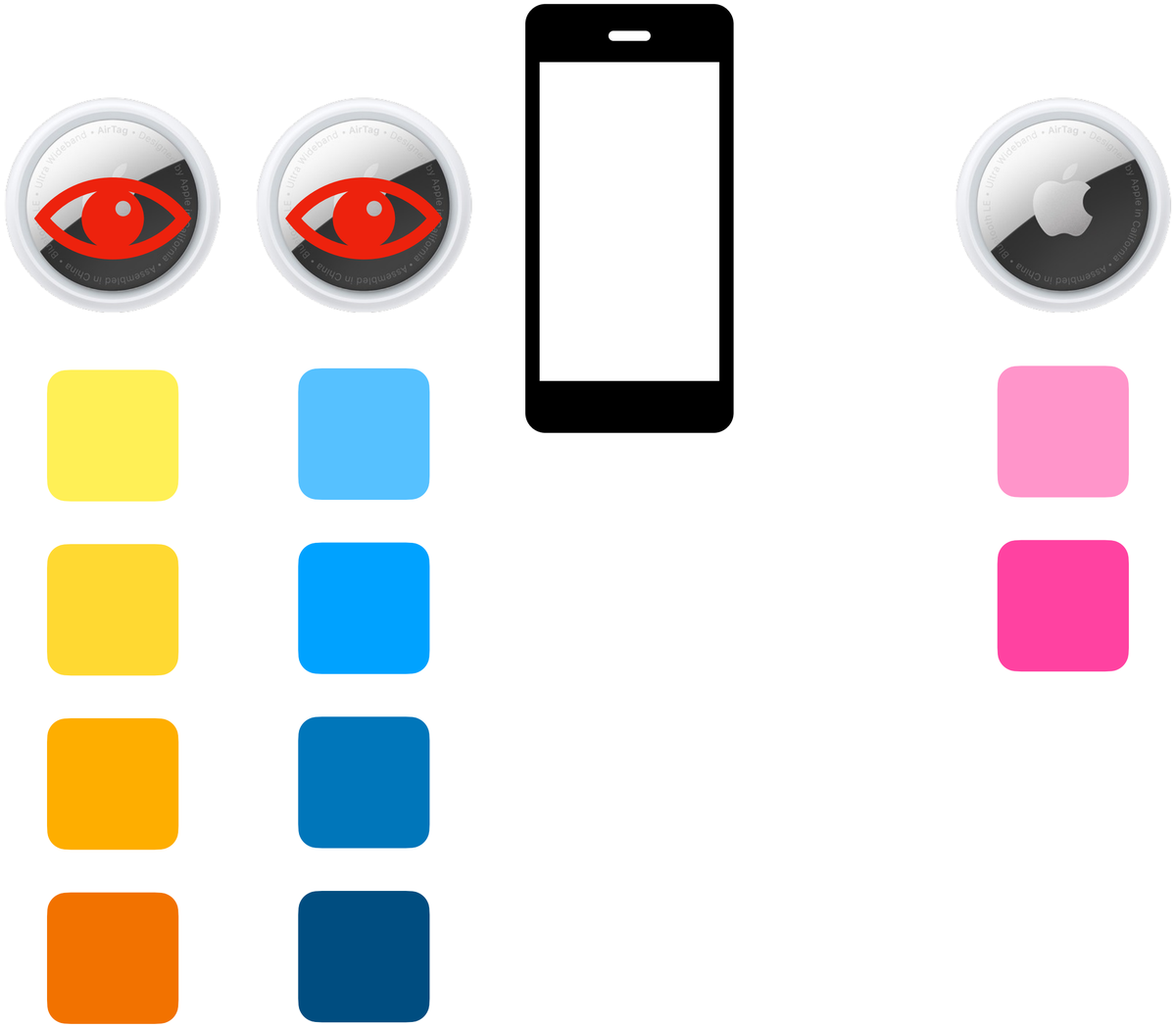
Secret Sharing Alone Isn’t Enough



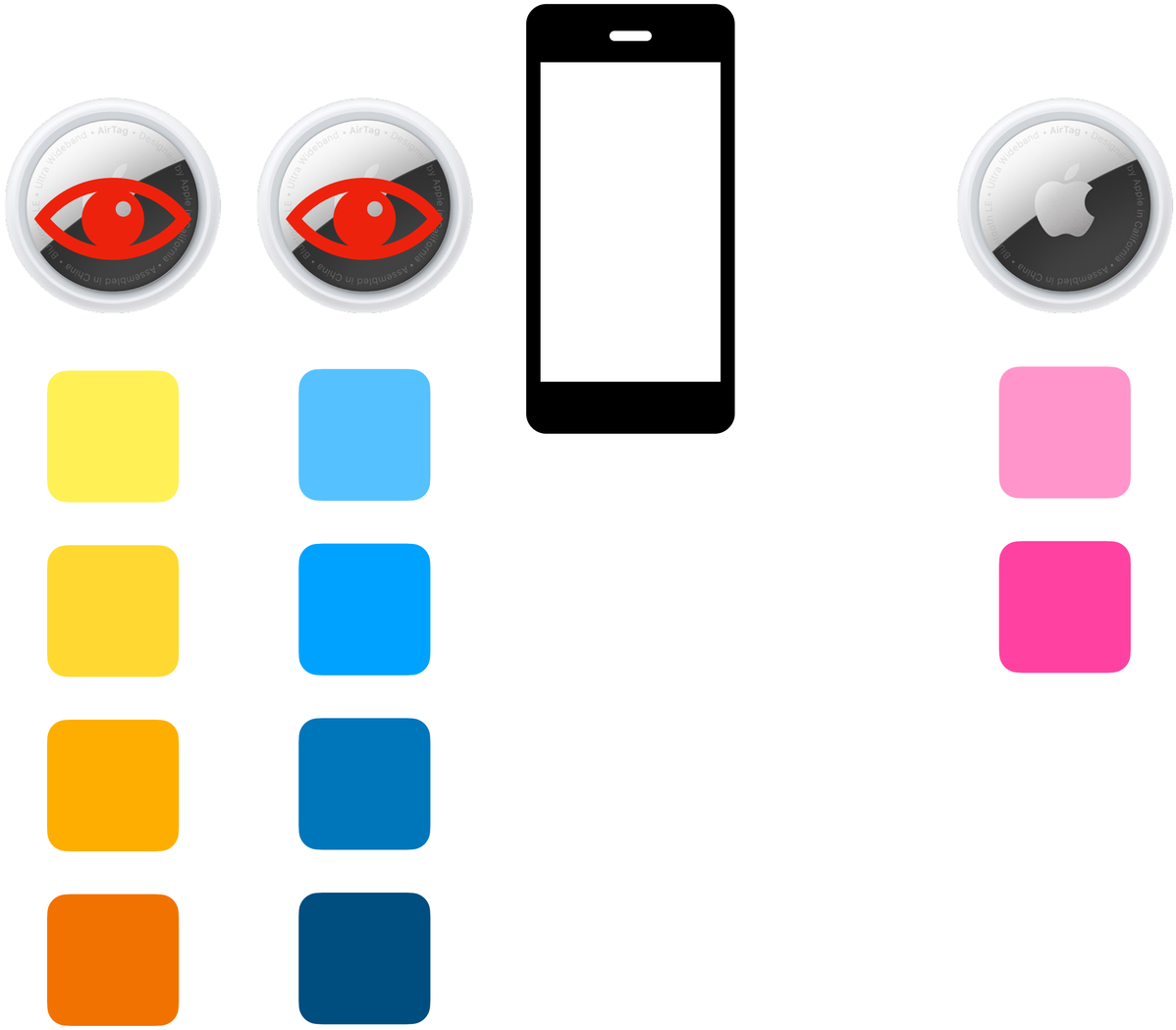
Secret Sharing Alone Isn’t Enough



Secret Sharing Alone Isn’t Enough

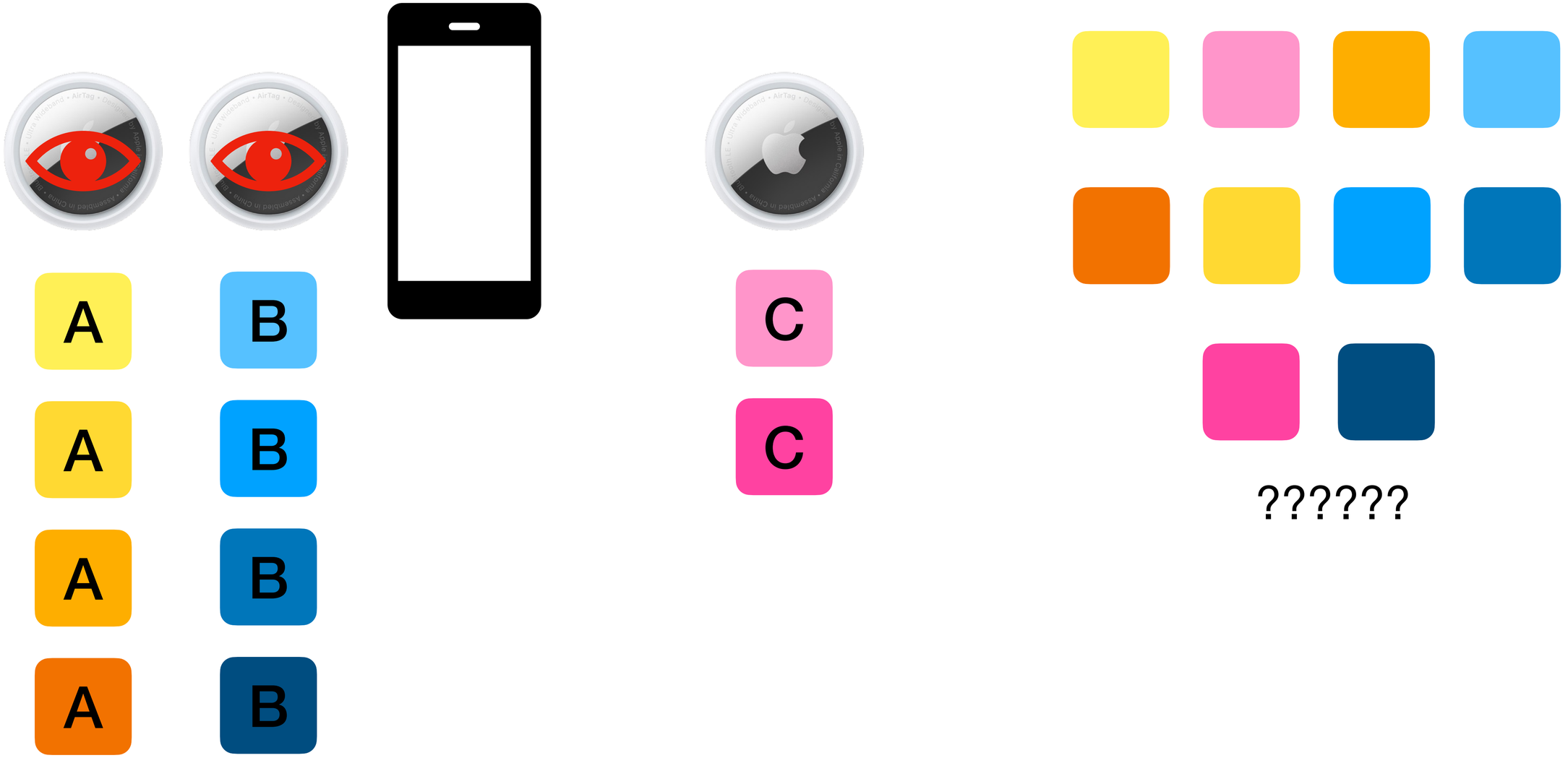


Secret Sharing Alone Isn’t Enough

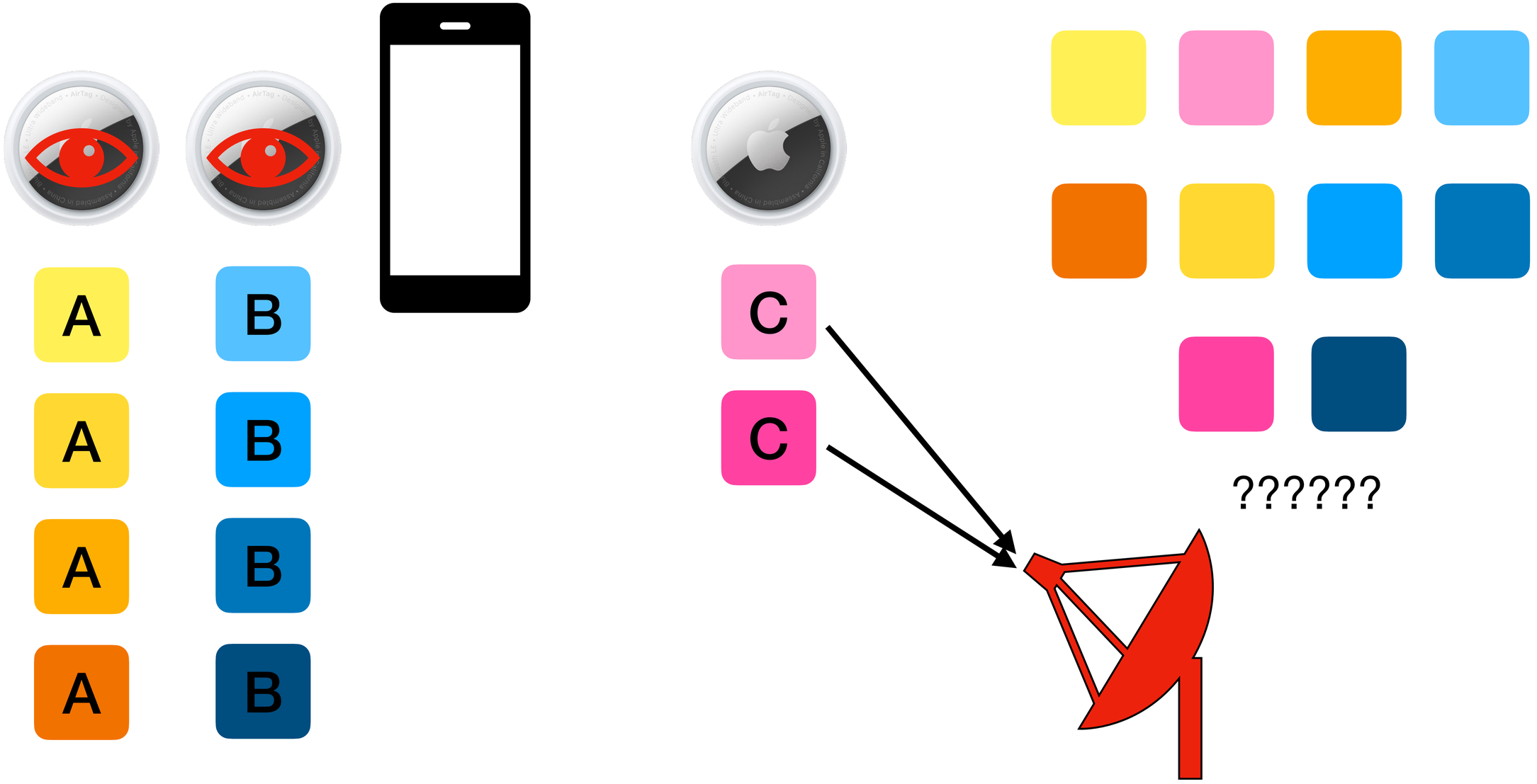


??????

Secret Sharing Alone Isn’t Enough

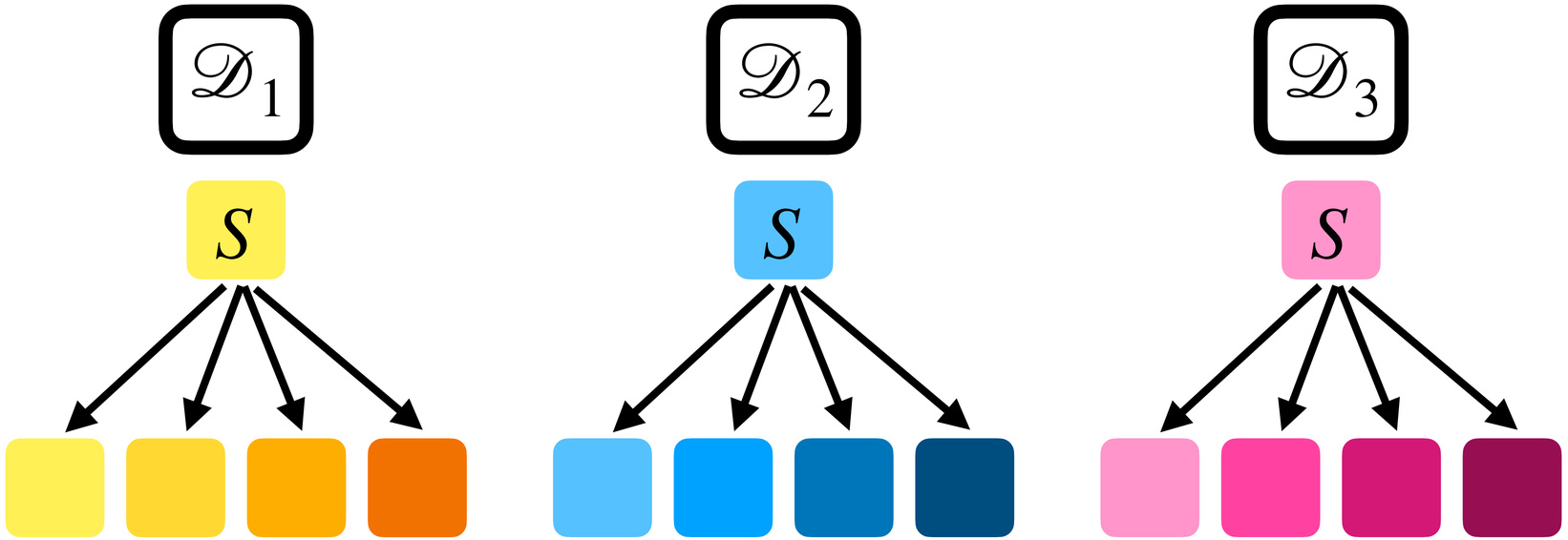


Secret Sharing Alone Isn’t Enough

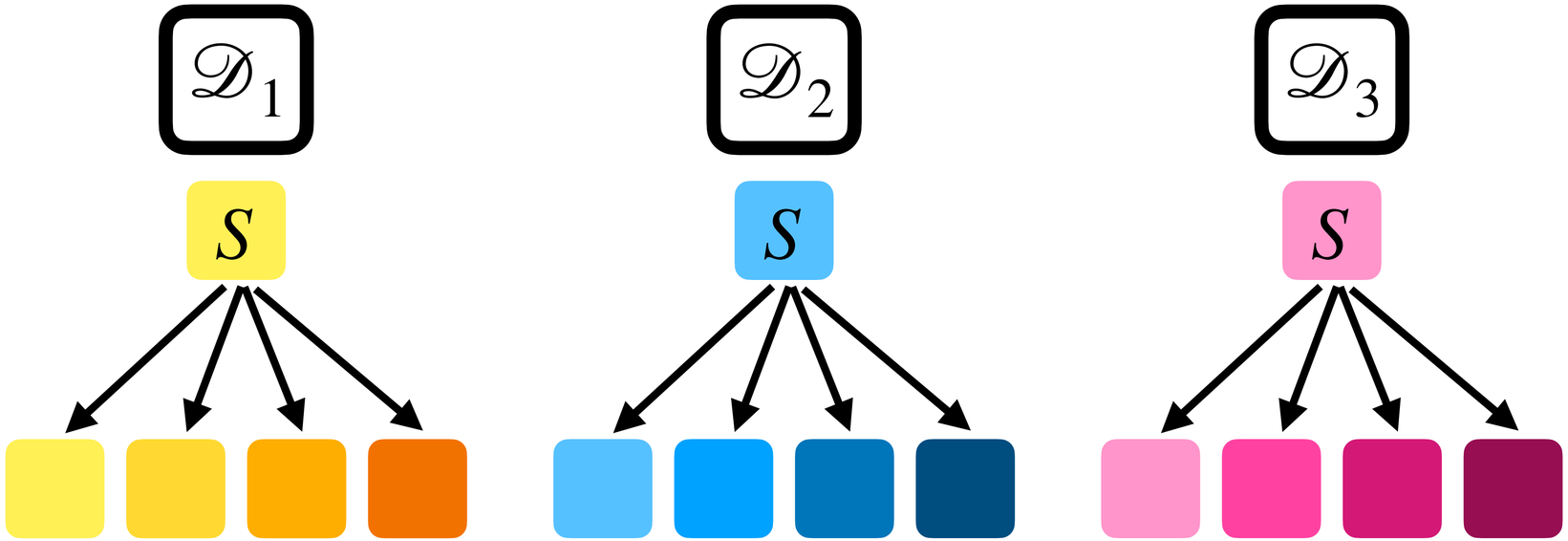


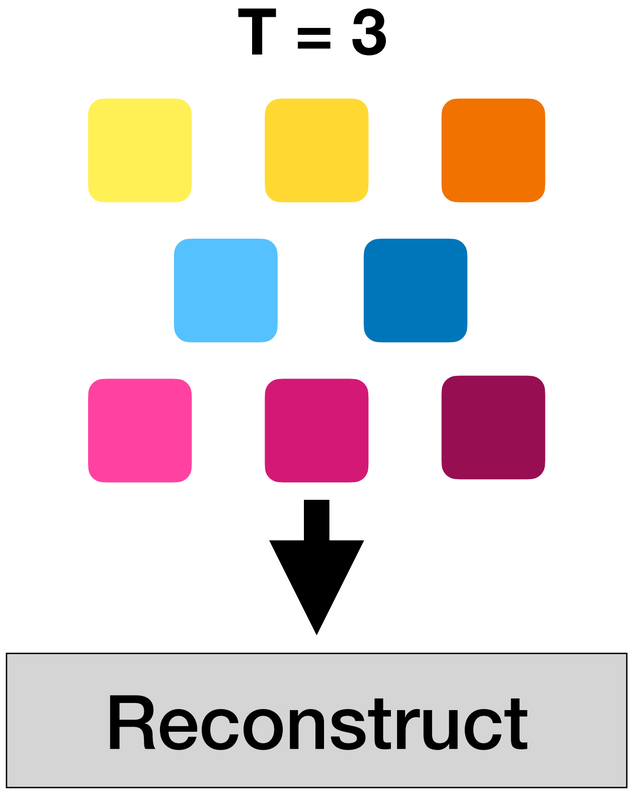
Multi-Dealer Secret Sharing

Multi-Dealer Secret Sharing

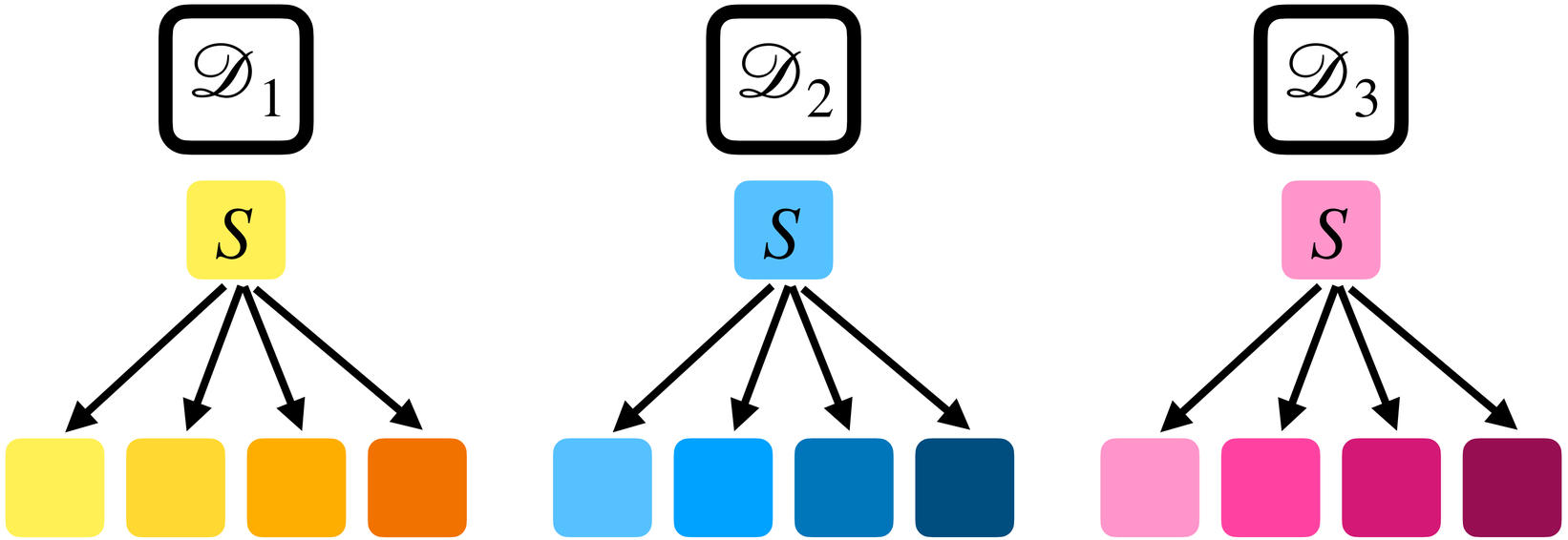


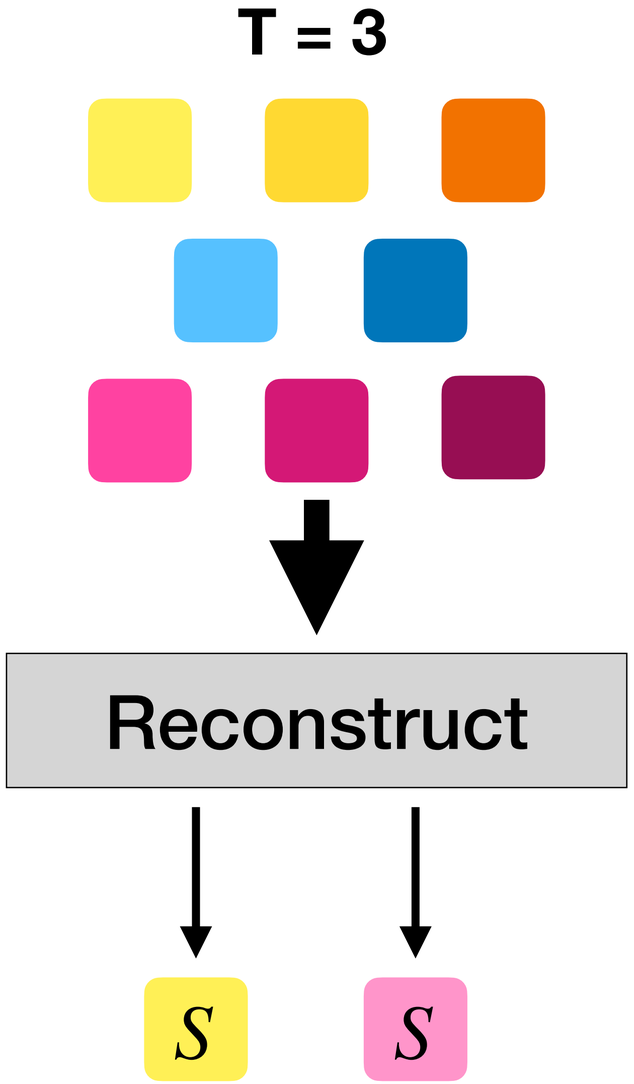
Multi-Dealer Secret Sharing



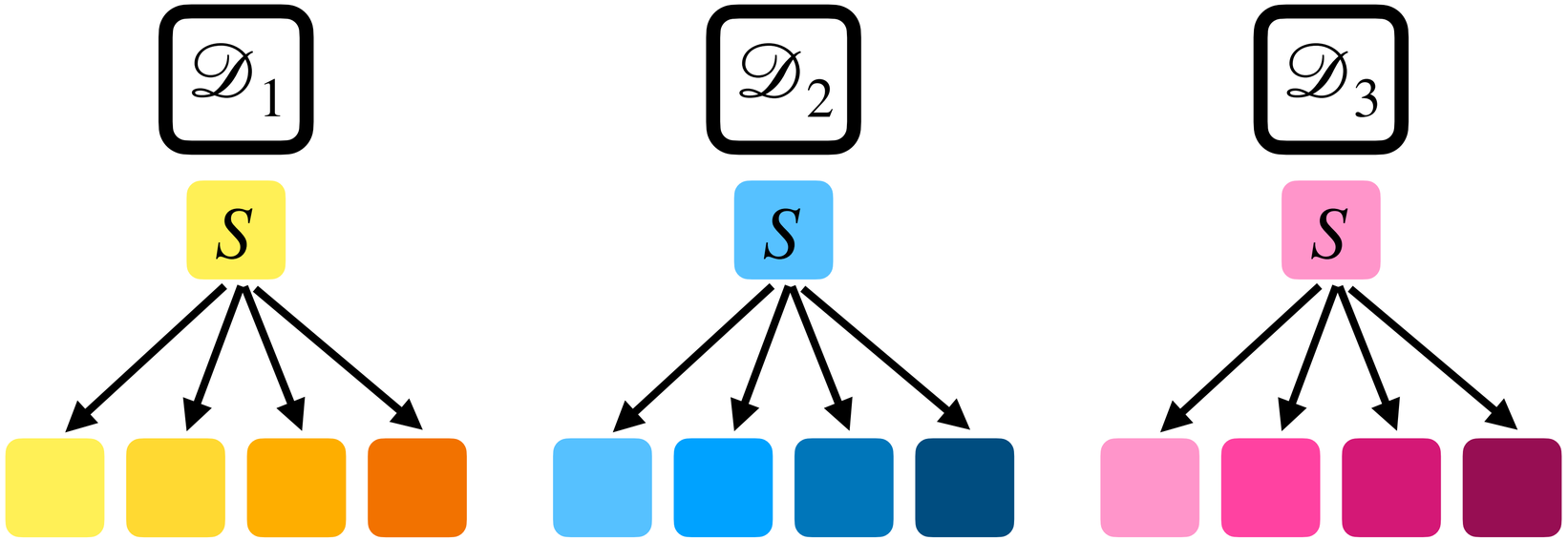


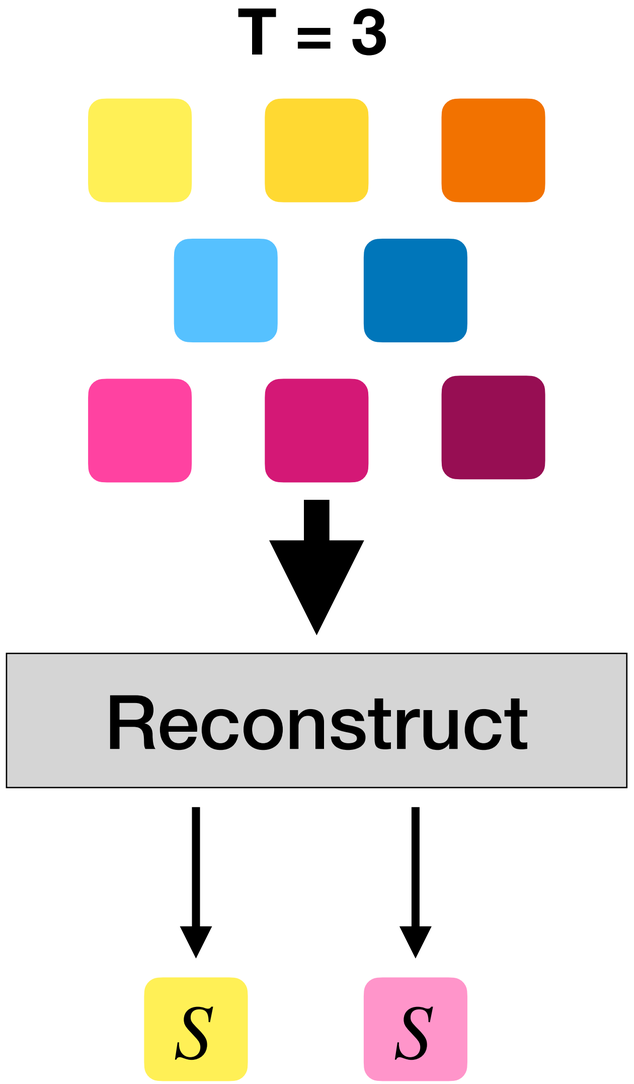
Multi-Dealer Secret Sharing





Multi-Dealer Secret Sharing

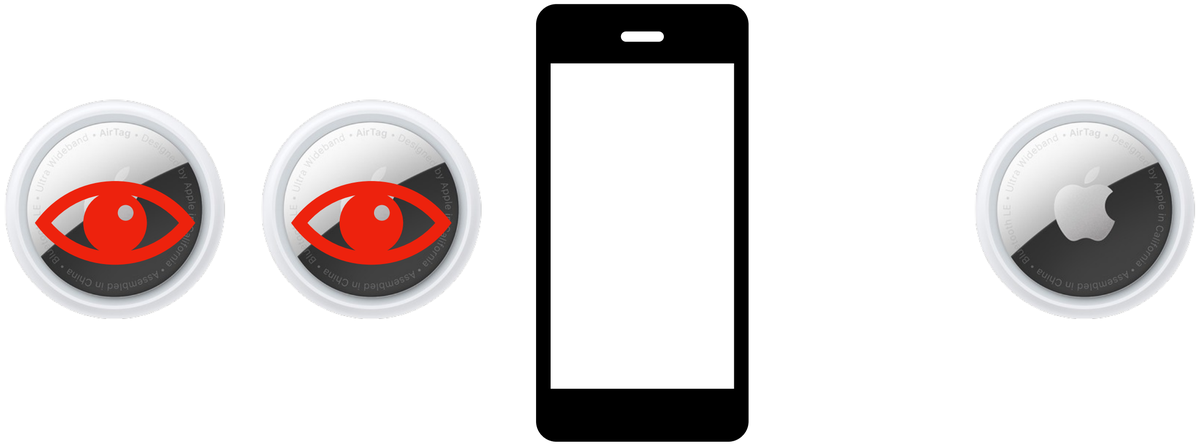




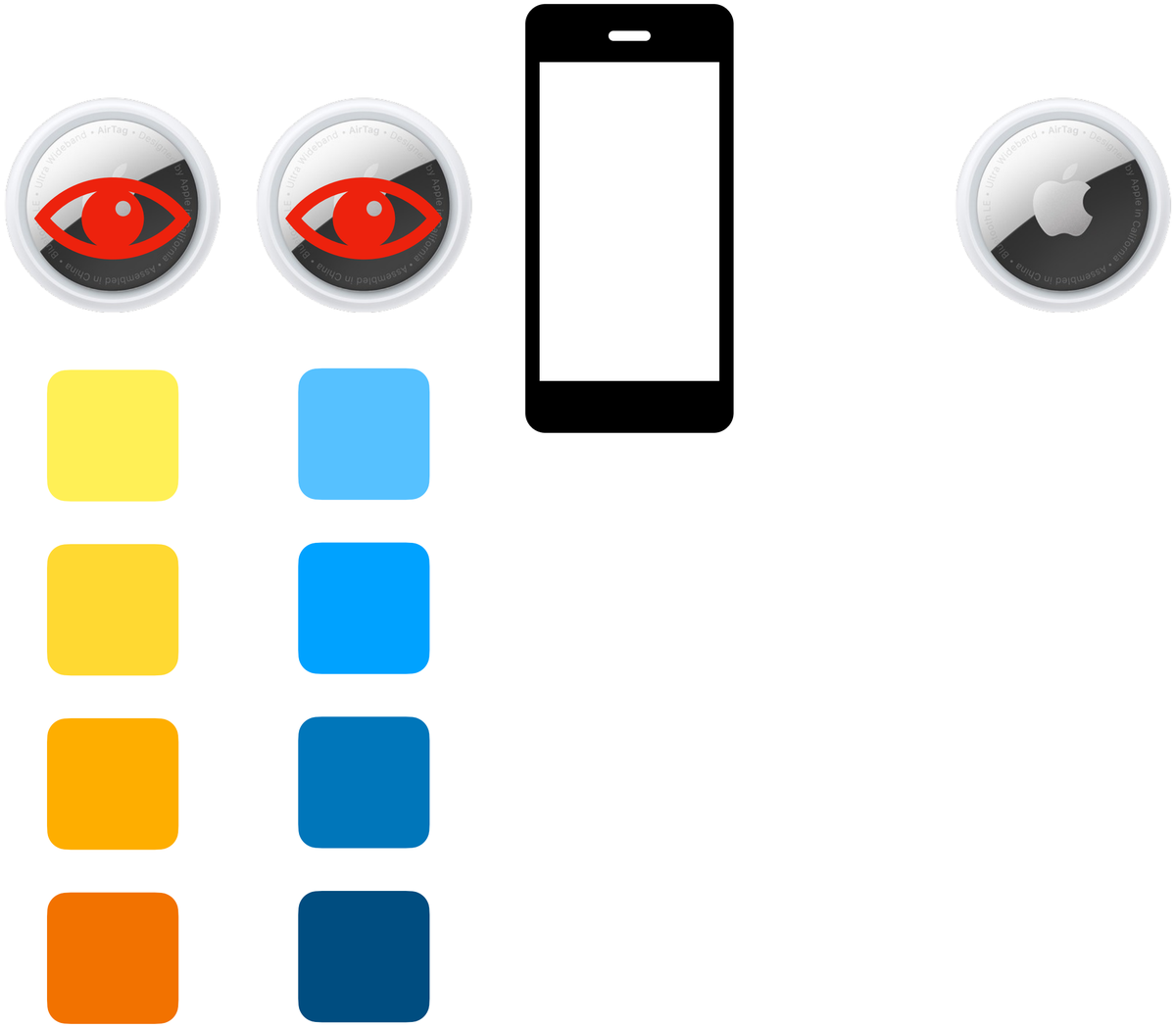
Unlinkability (**K = 2**):

How Can MDSS Help?

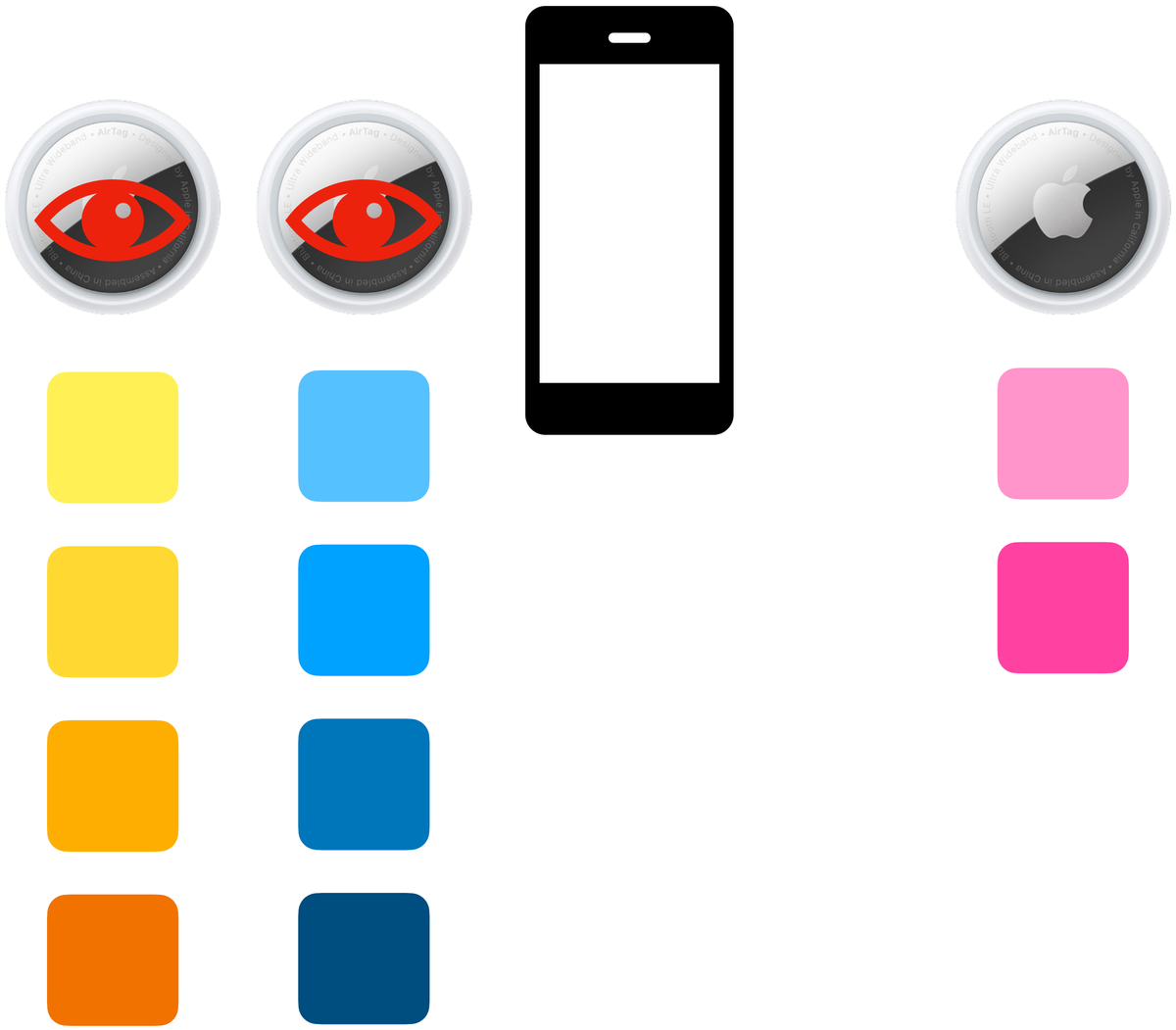
How Can MDSS Help?



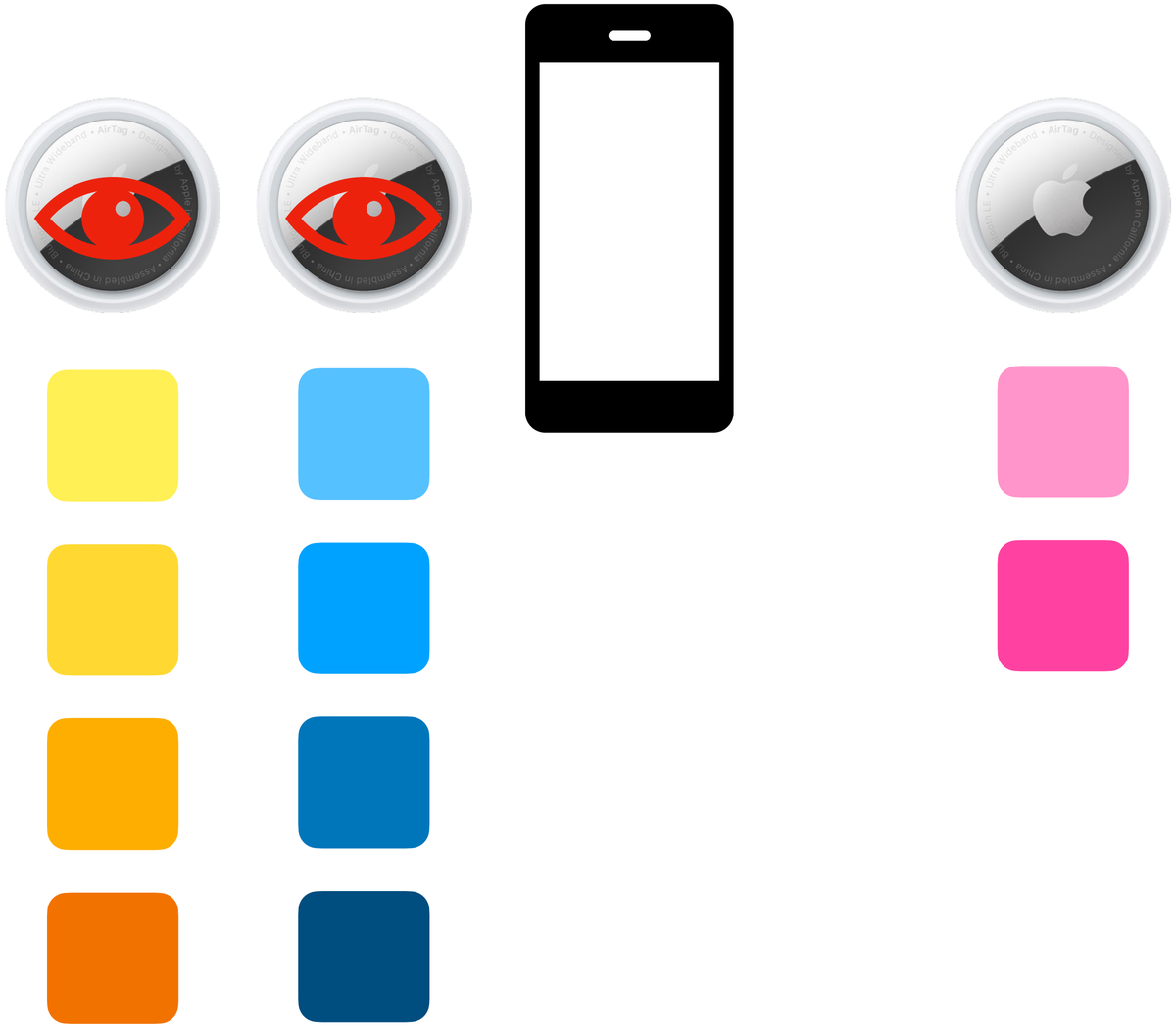
How Can MDSS Help?

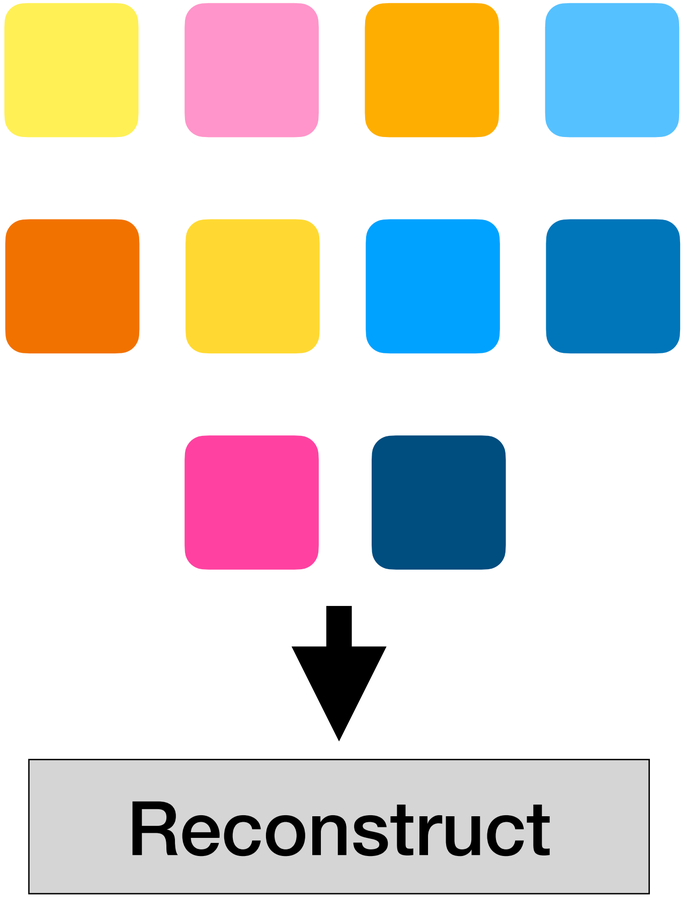


How Can MDSS Help?

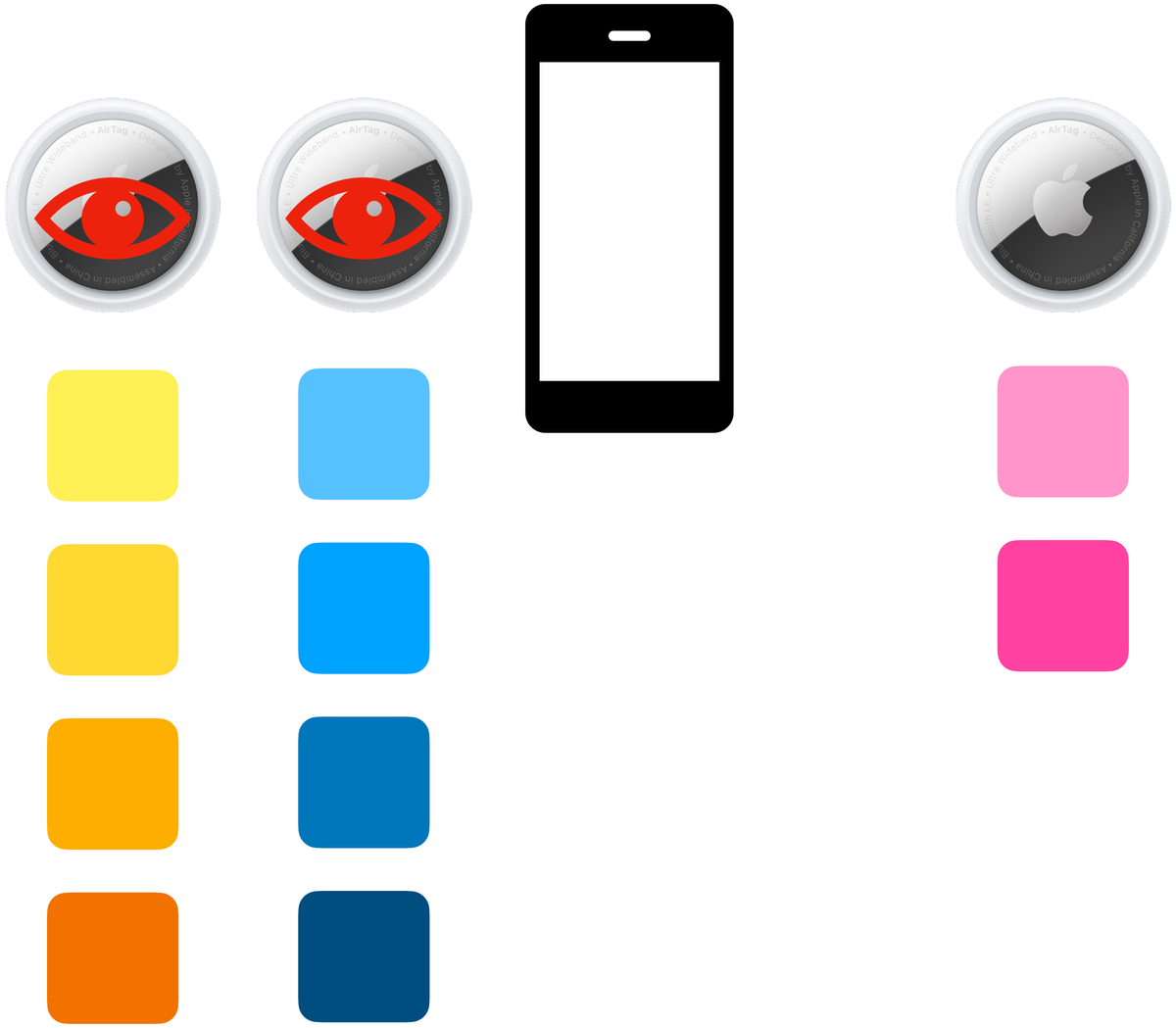


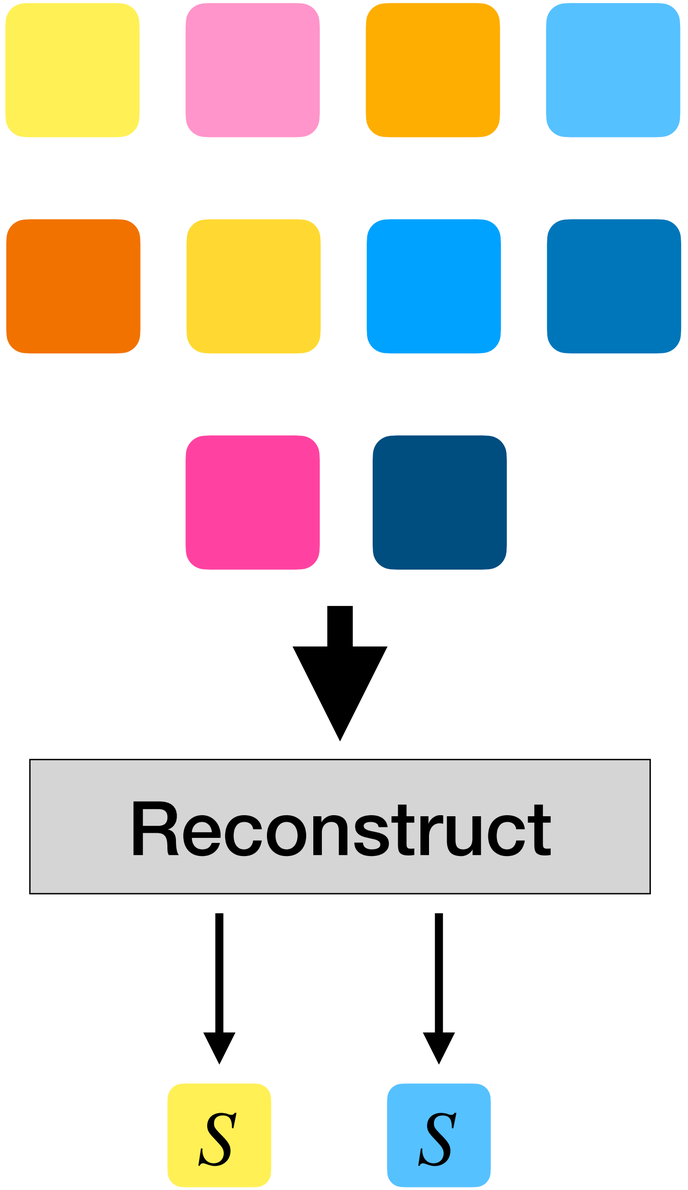
How Can MDSS Help?





How Can MDSS Help?

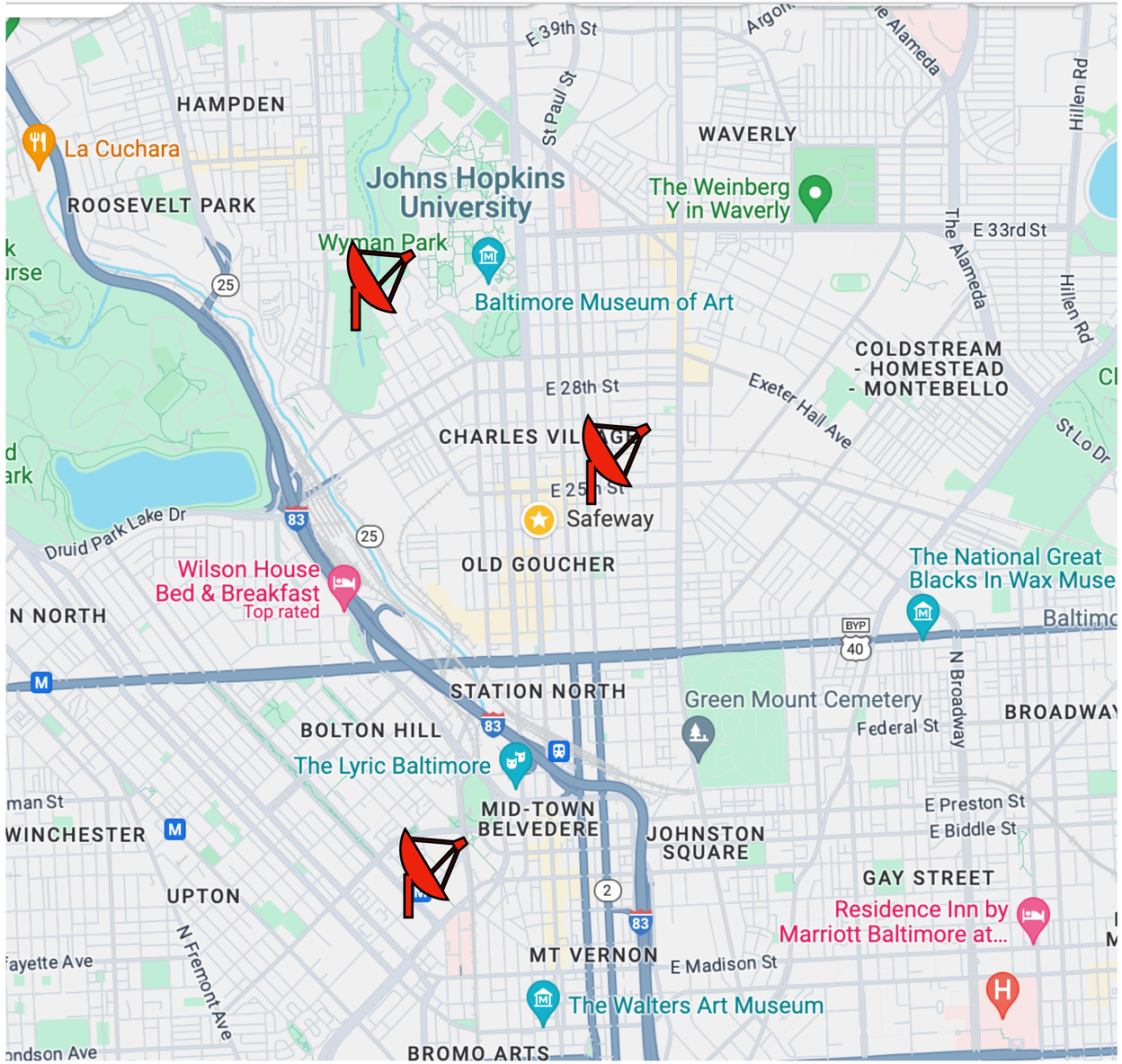




How Can MDSS Help?

- Privacy against trackers follows from **unlinkability**

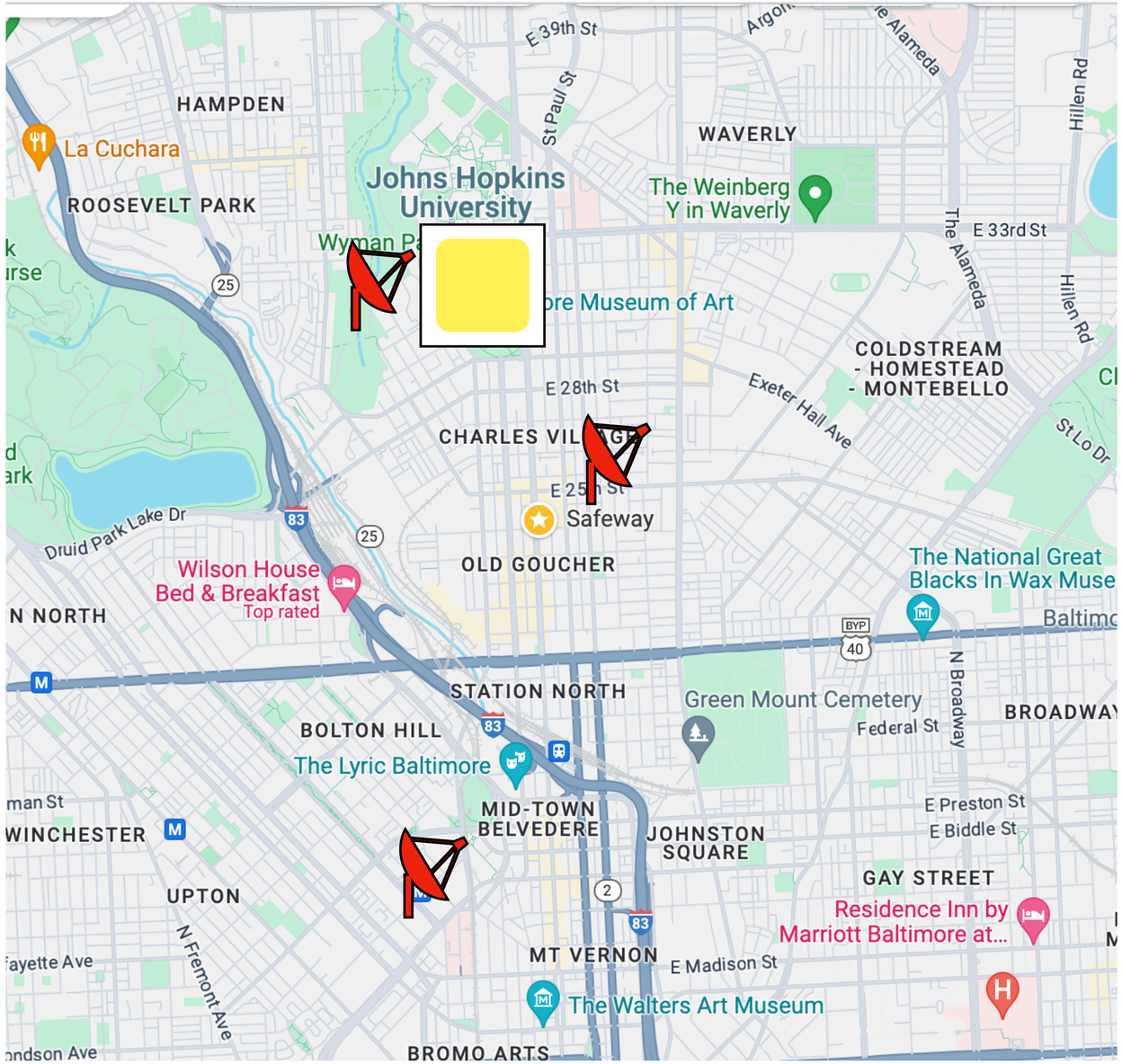
K = 3



How Can MDSS Help?

- Privacy against trackers follows from **unlinkability**

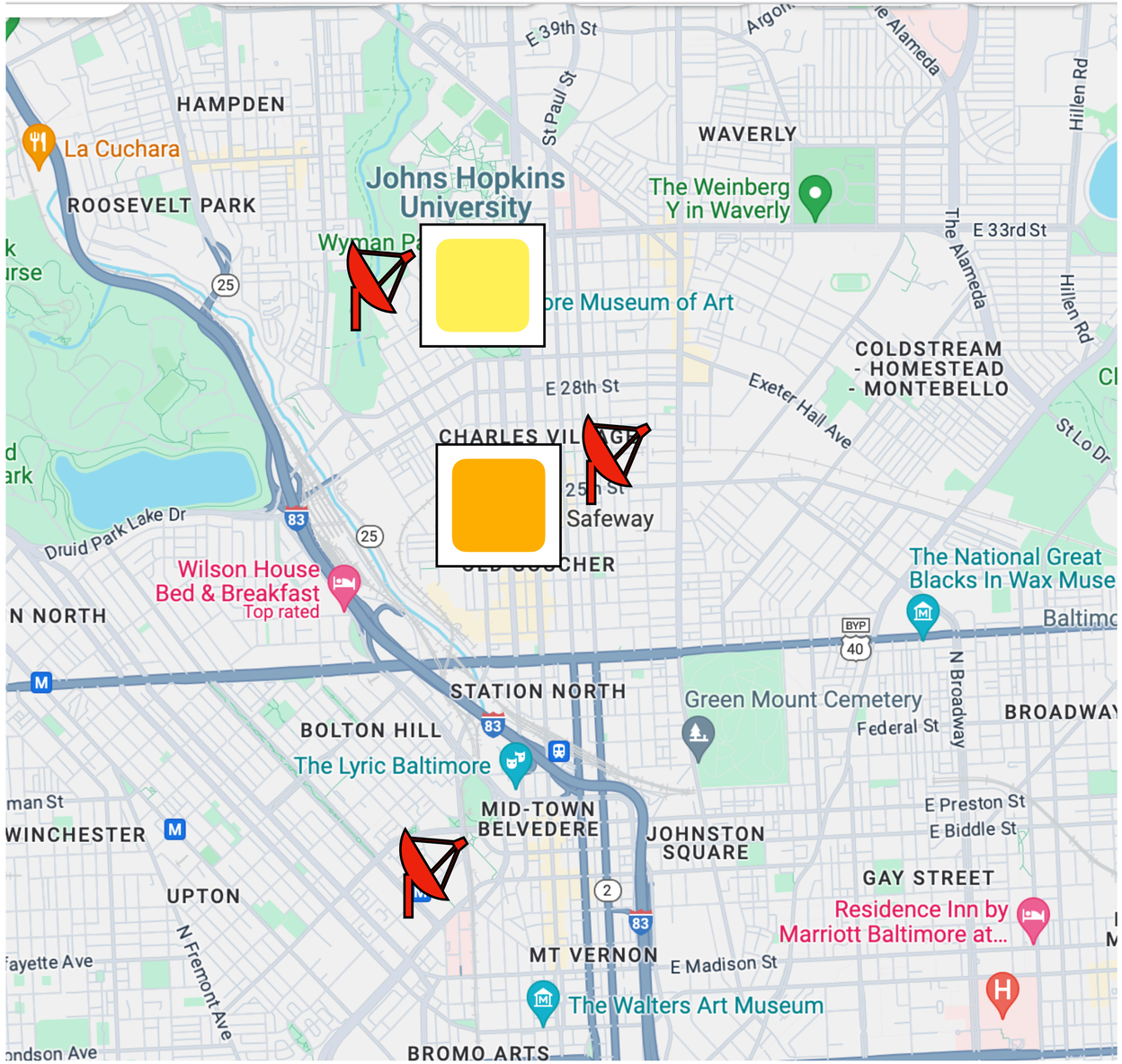
K = 3



How Can MDSS Help?

- Privacy against trackers follows from **unlinkability**

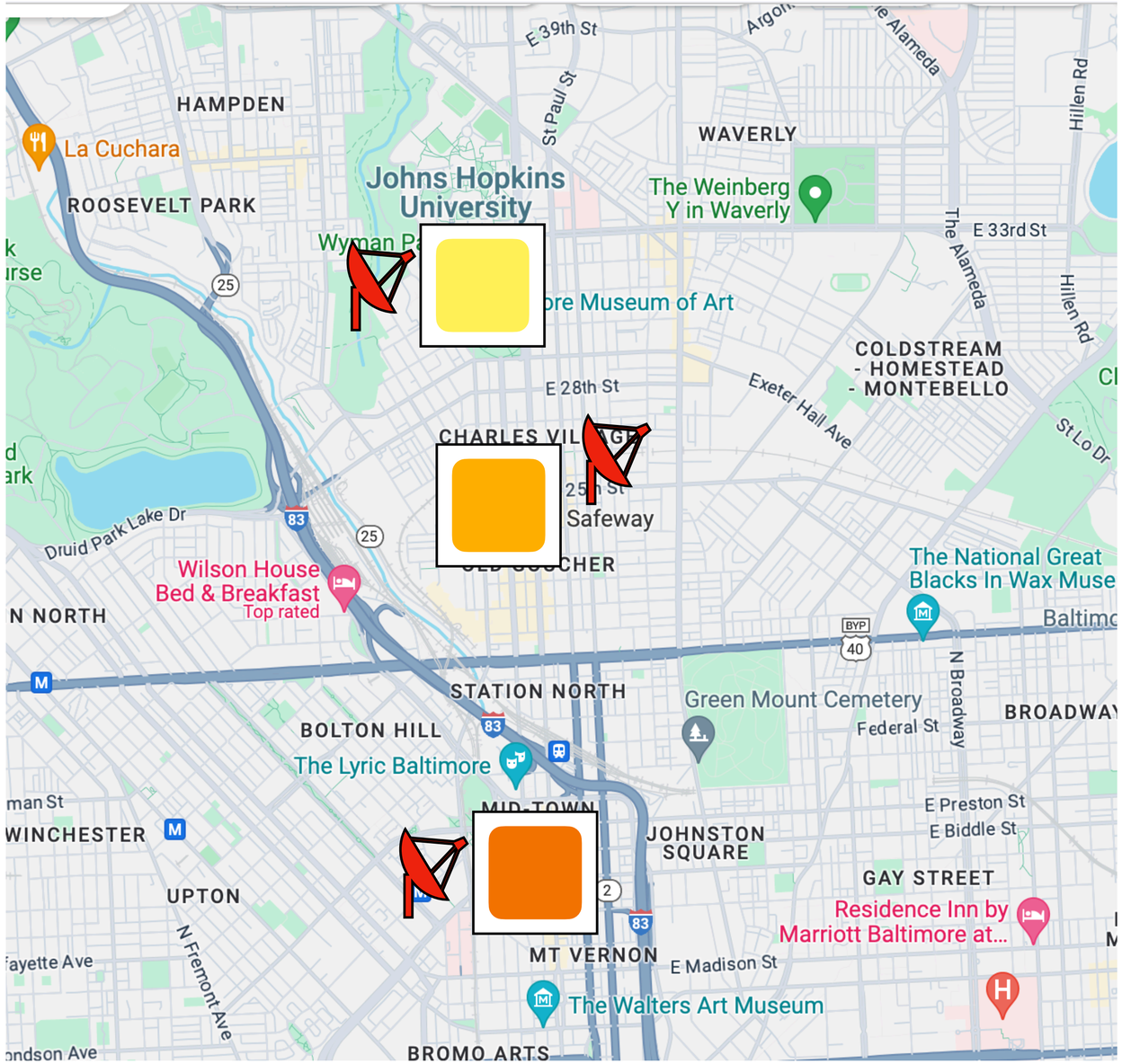
K = 3



How Can MDSS Help?

- Privacy against trackers follows from **unlinkability**

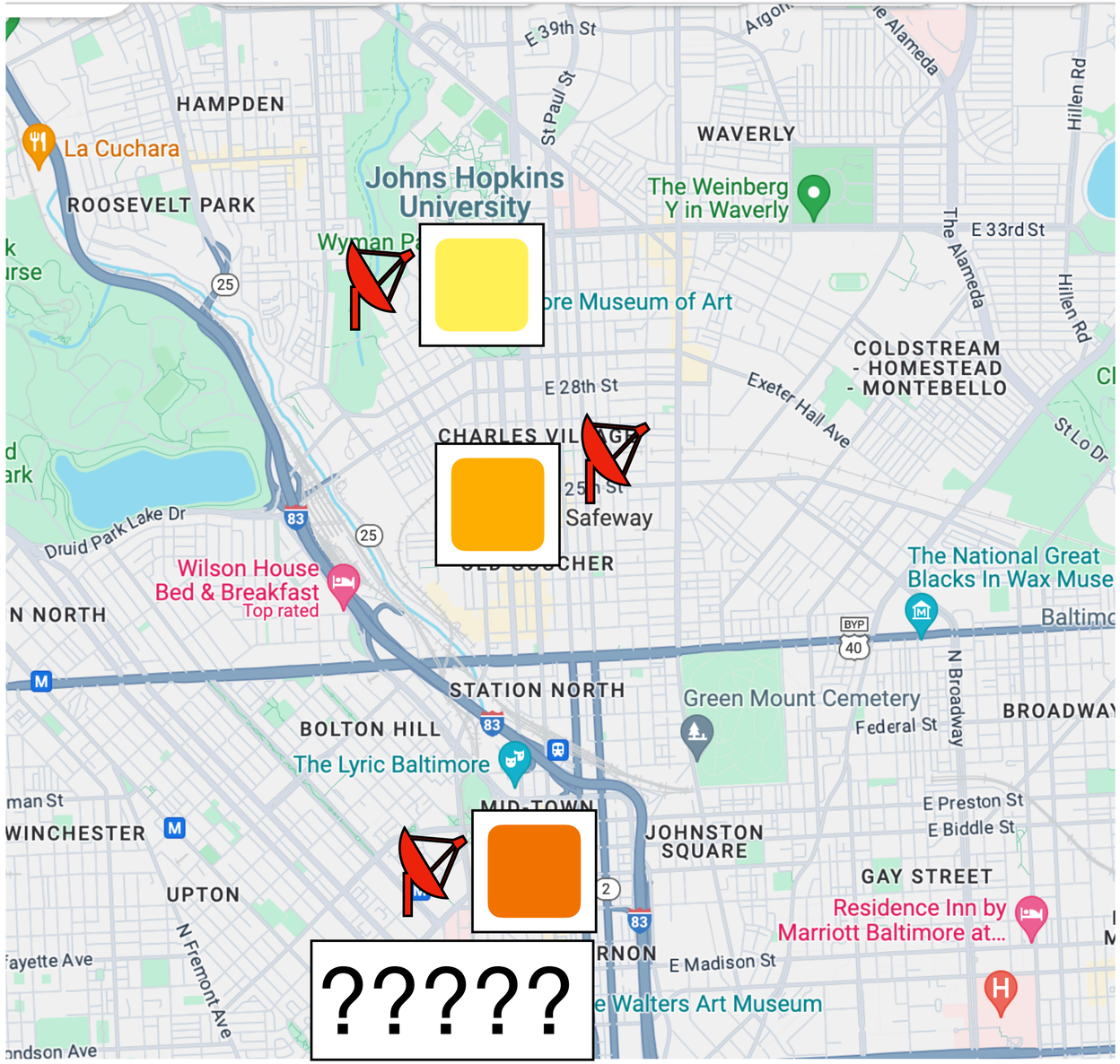
K = 3



How Can MDSS Help?

- Privacy against trackers follows from **unlinkability**

K = 3



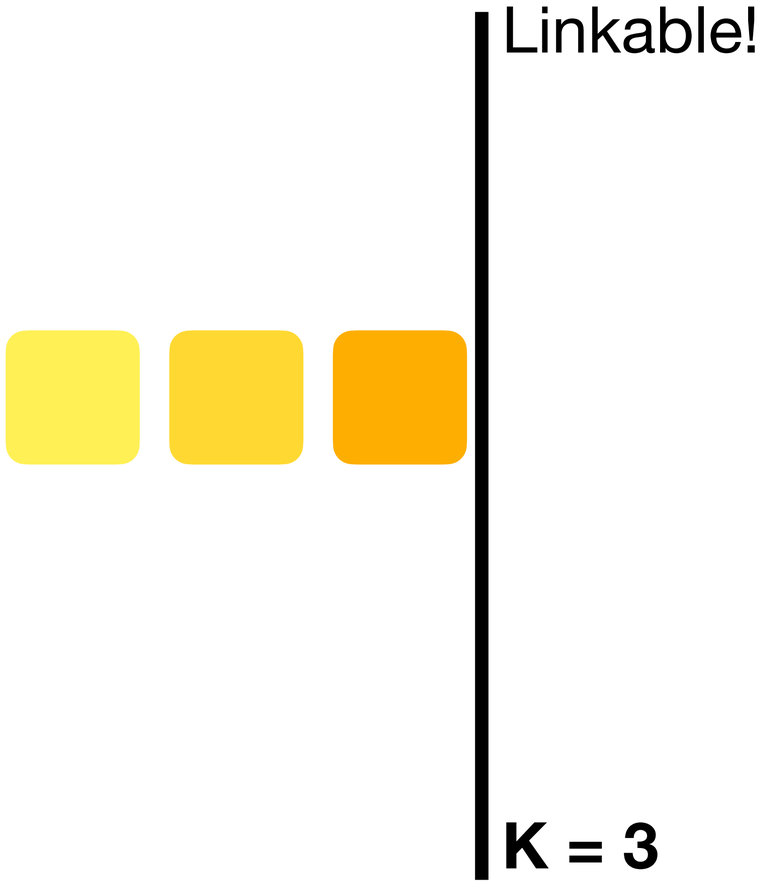
What Makes a Good MDSS?

What Makes a Good MDSS?

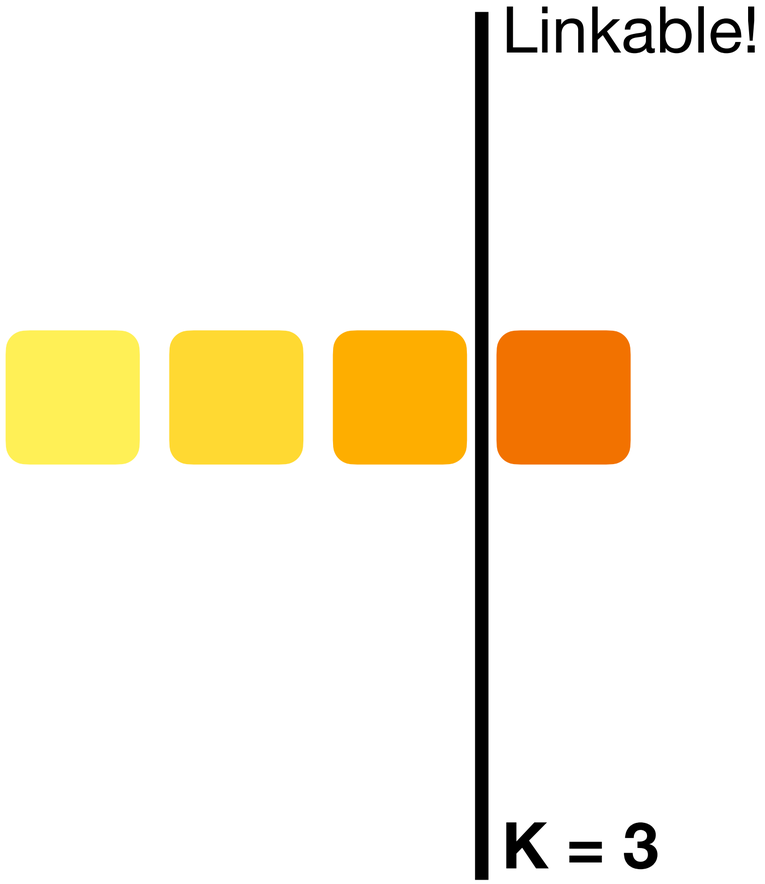
What Makes a Good MDSS?

What Makes a Good MDSS?

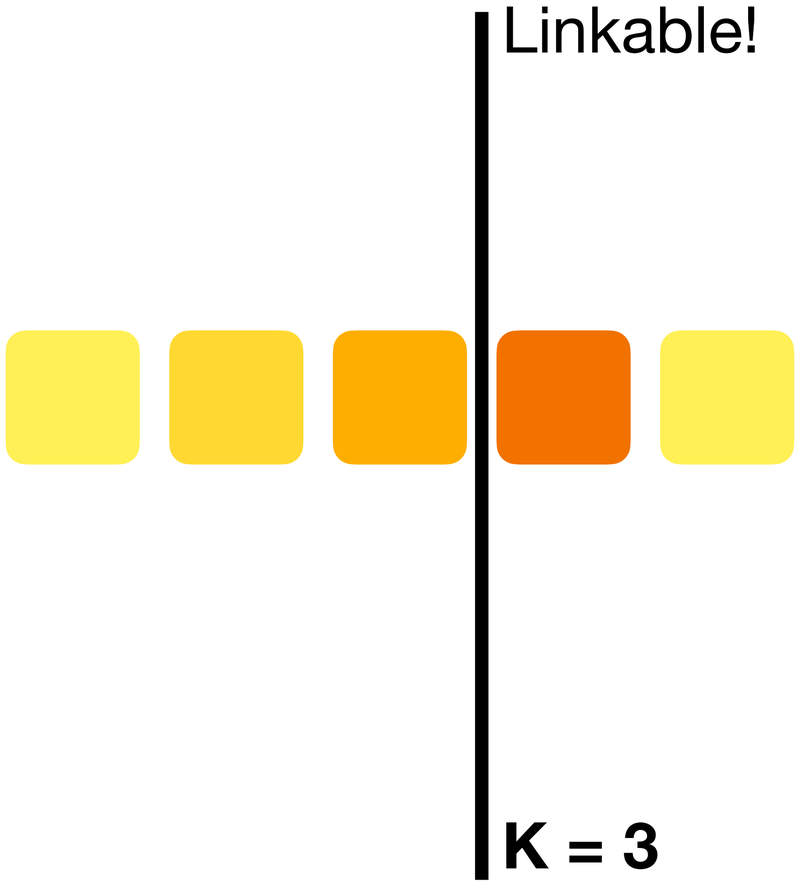
What Makes a Good MDSS?



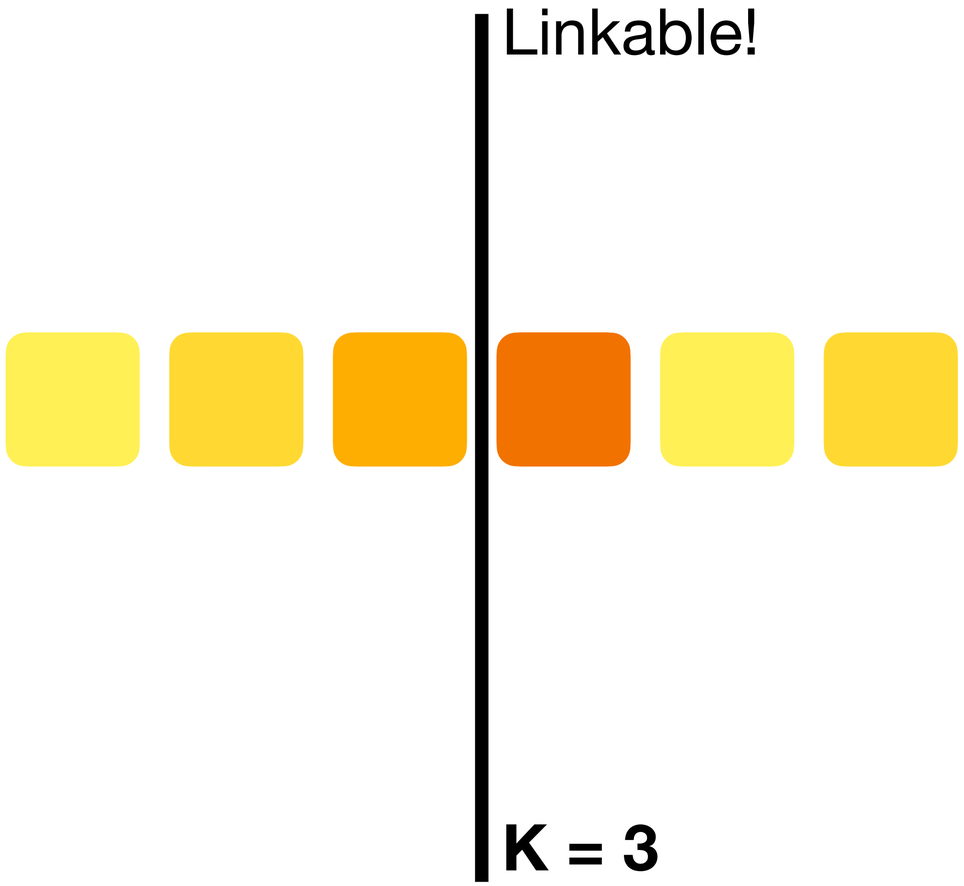
What Makes a Good MDSS?



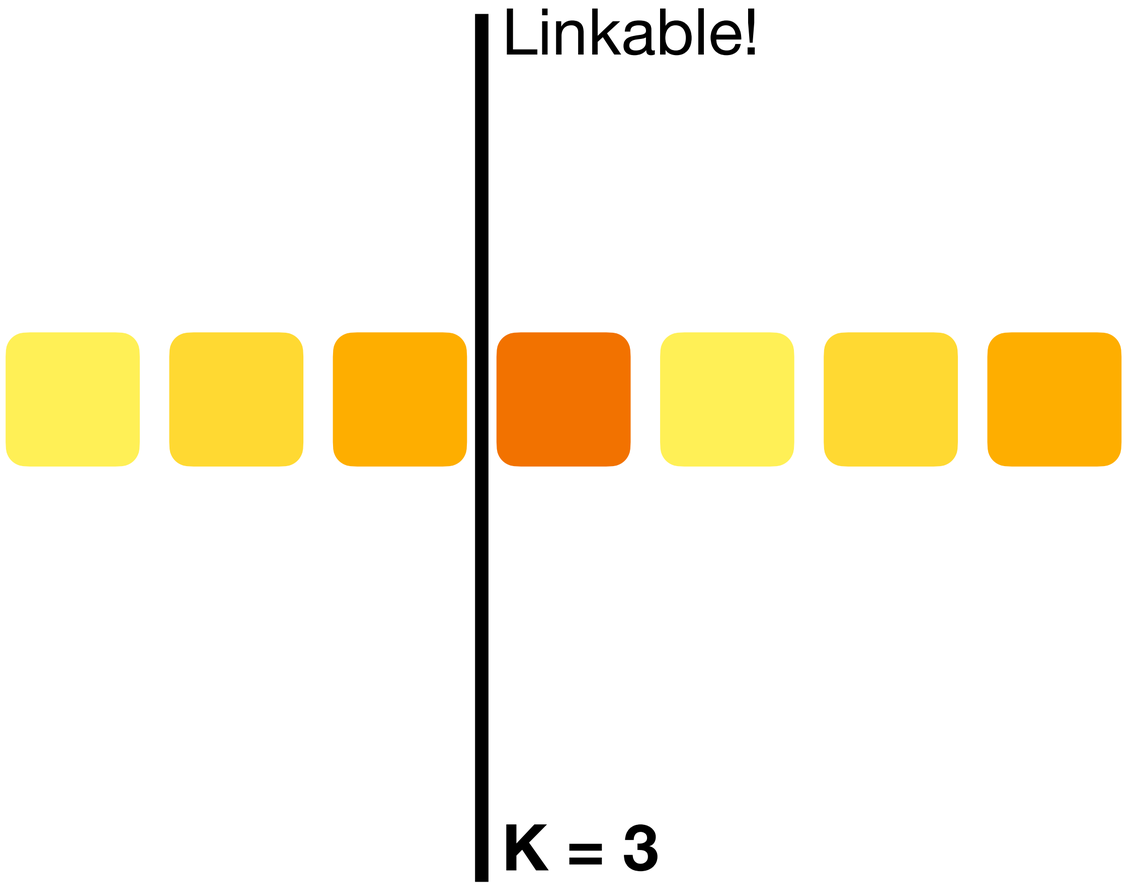
What Makes a Good MDSS?



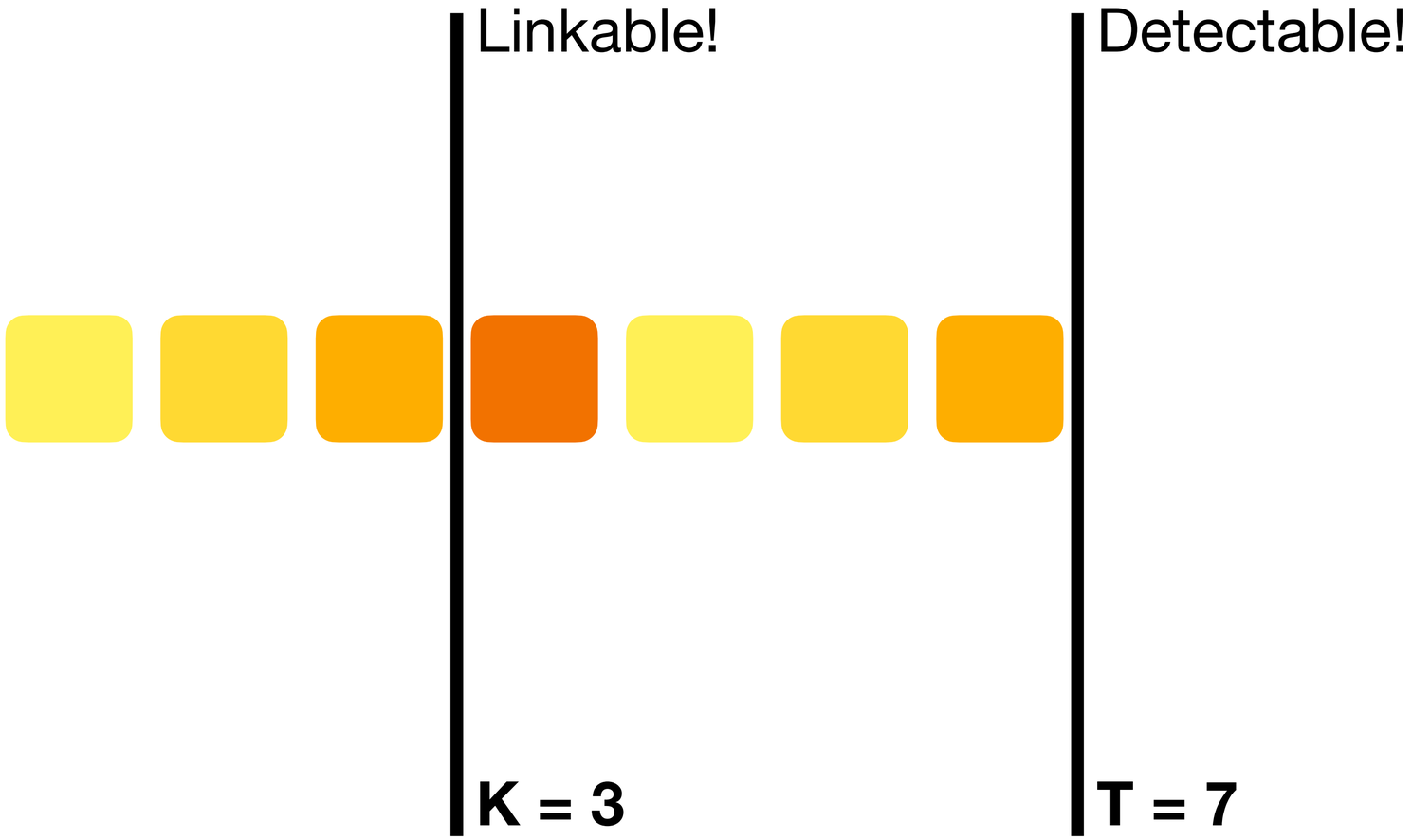
What Makes a Good MDSS?



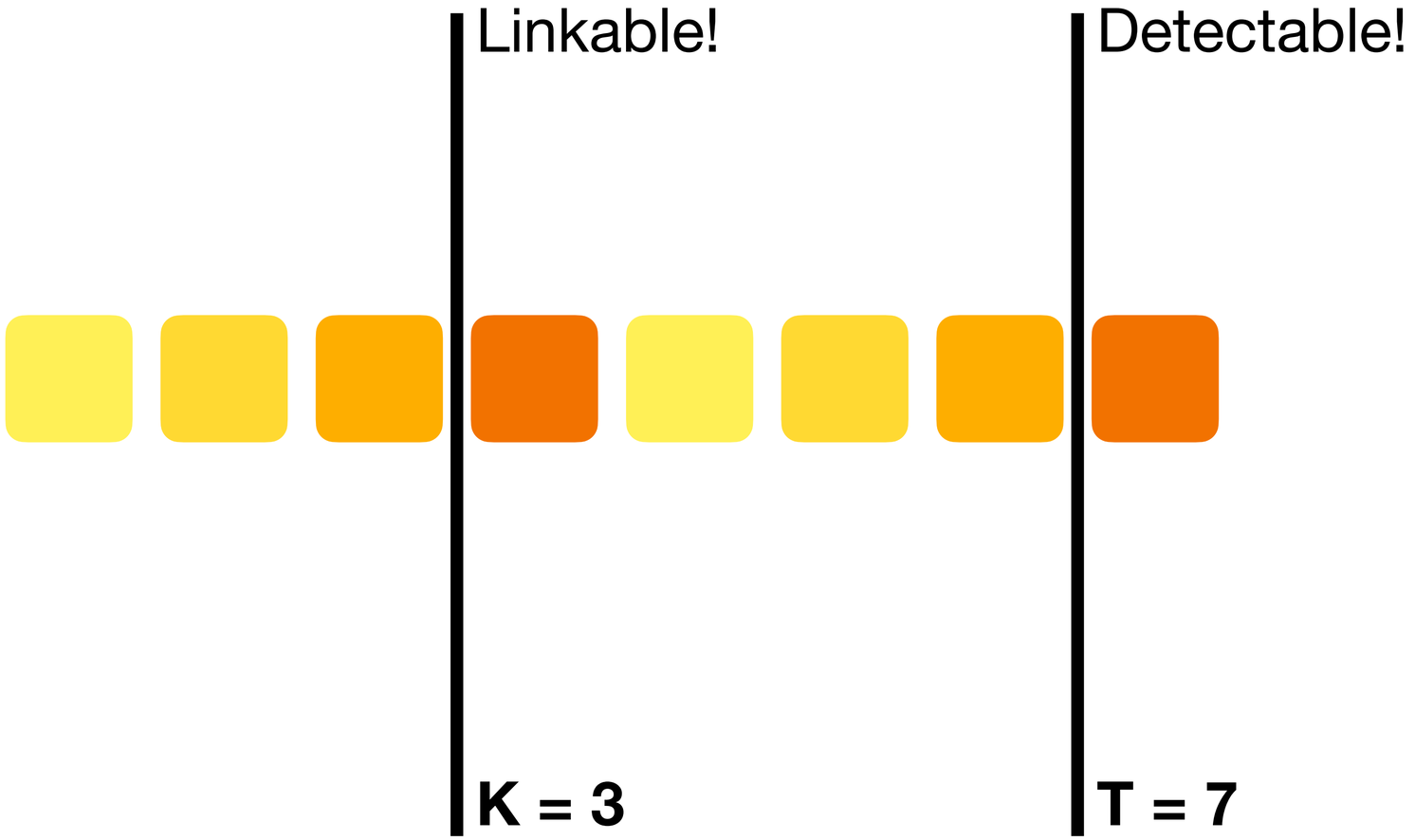
What Makes a Good MDSS?



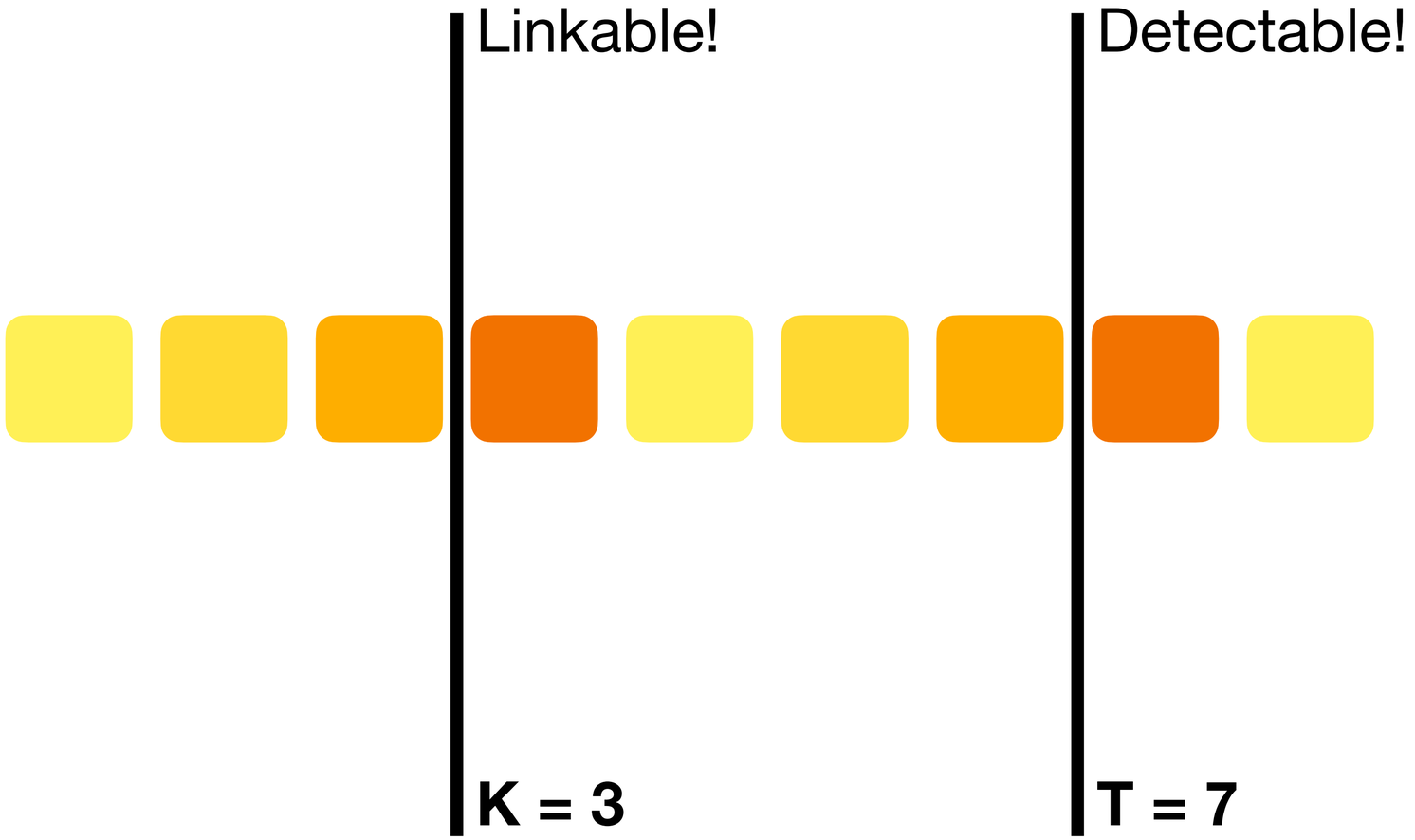
What Makes a Good MDSS?



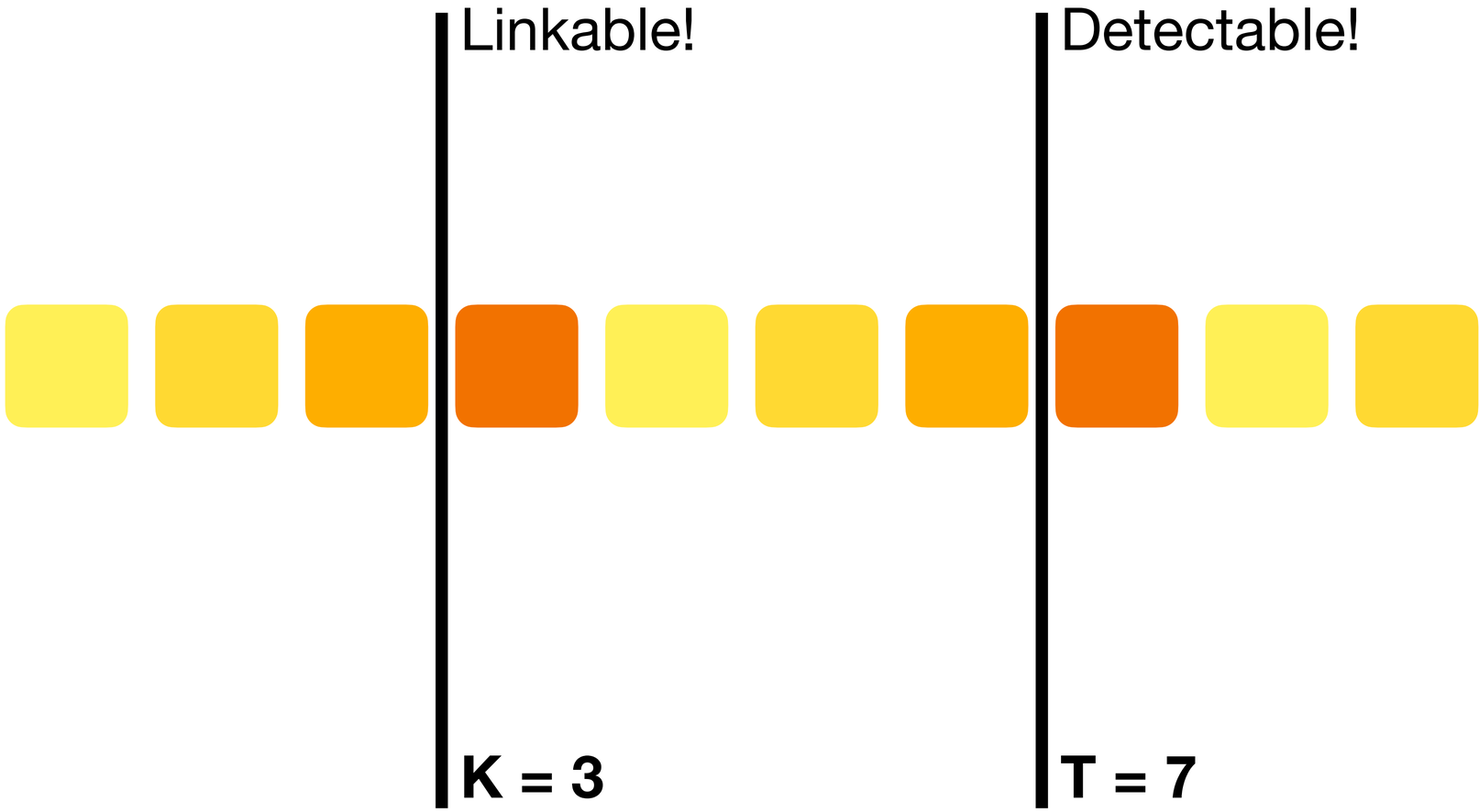
What Makes a Good MDSS?



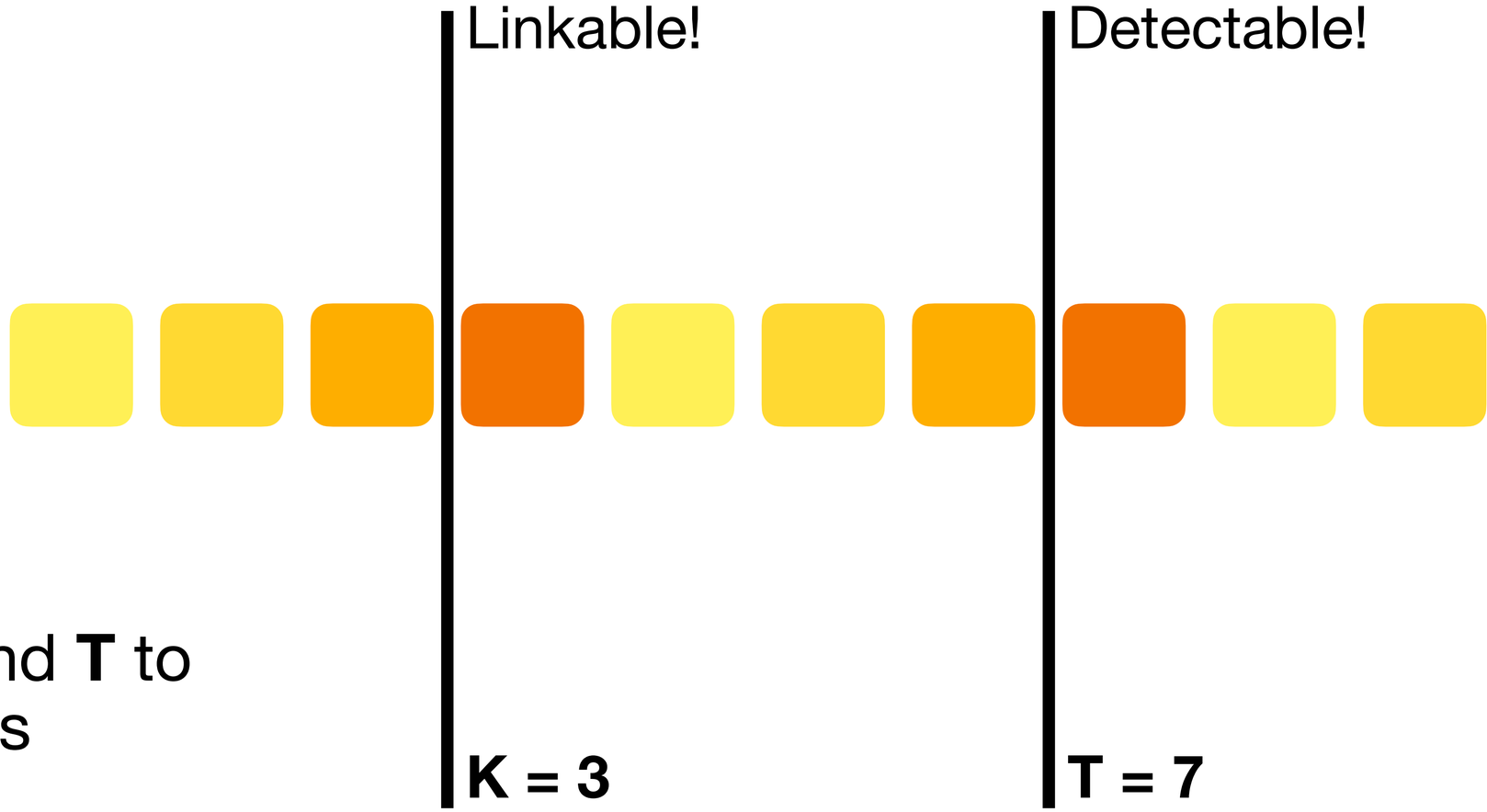
What Makes a Good MDSS?



What Makes a Good MDSS?



What Makes a Good MDSS?



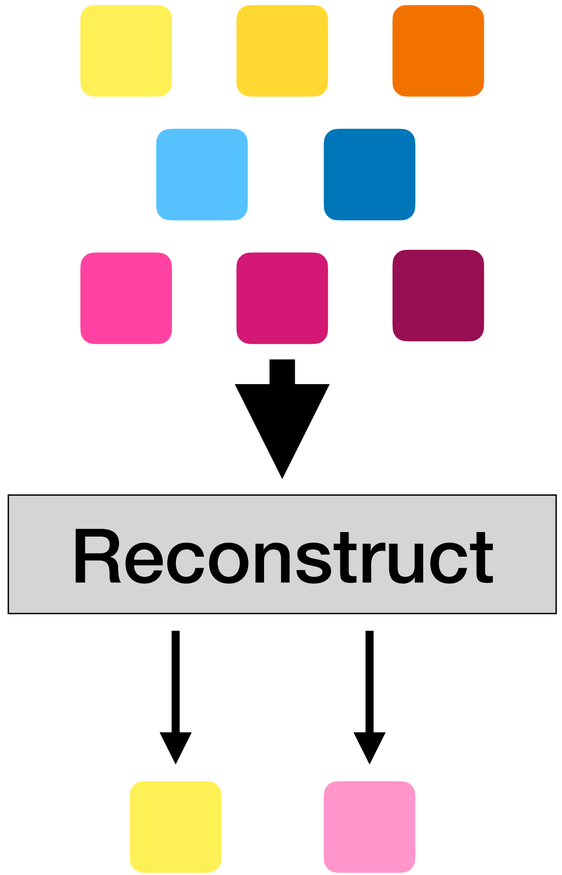
We want **K** and **T** to be as close as possible!

What Makes a Good MDSS?

$$D = 2$$

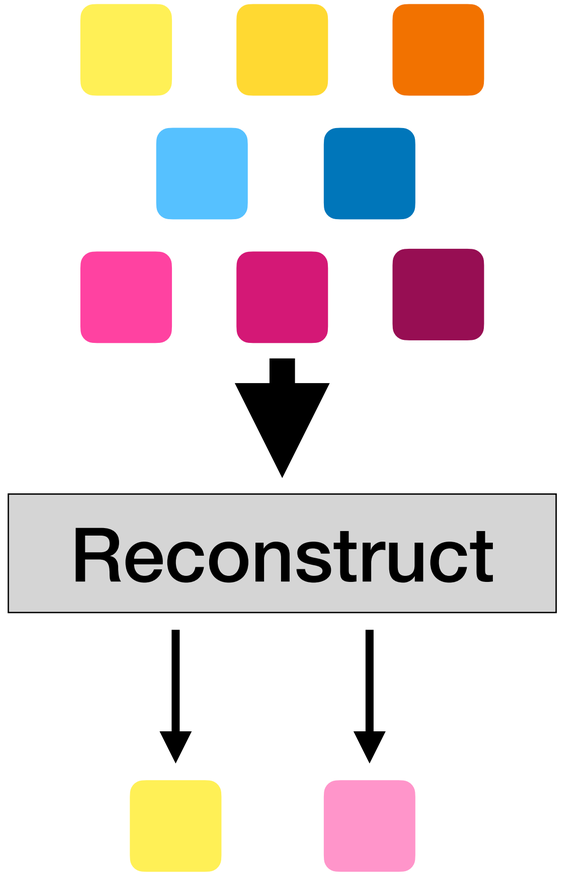
What Makes a Good MDSS?

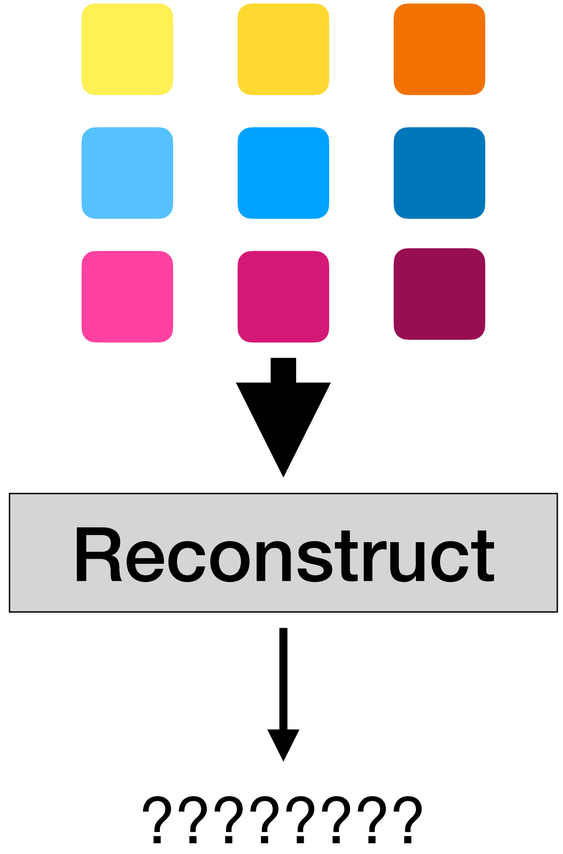
D = 2



What Makes a Good MDSS?

D = 2



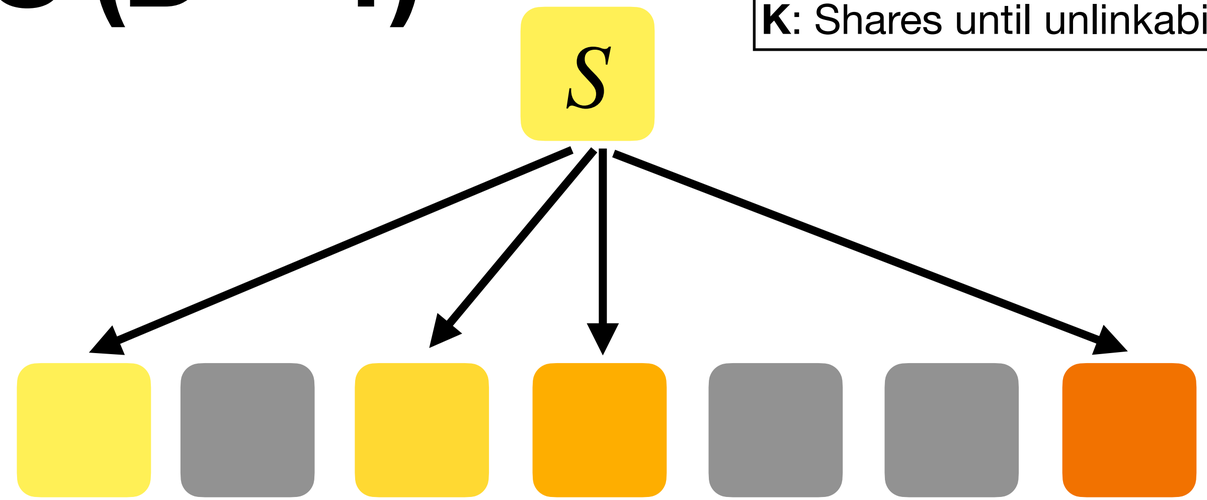


How To Build MDSS (D = 1)

D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken

How To Build MDSS (D = 1)

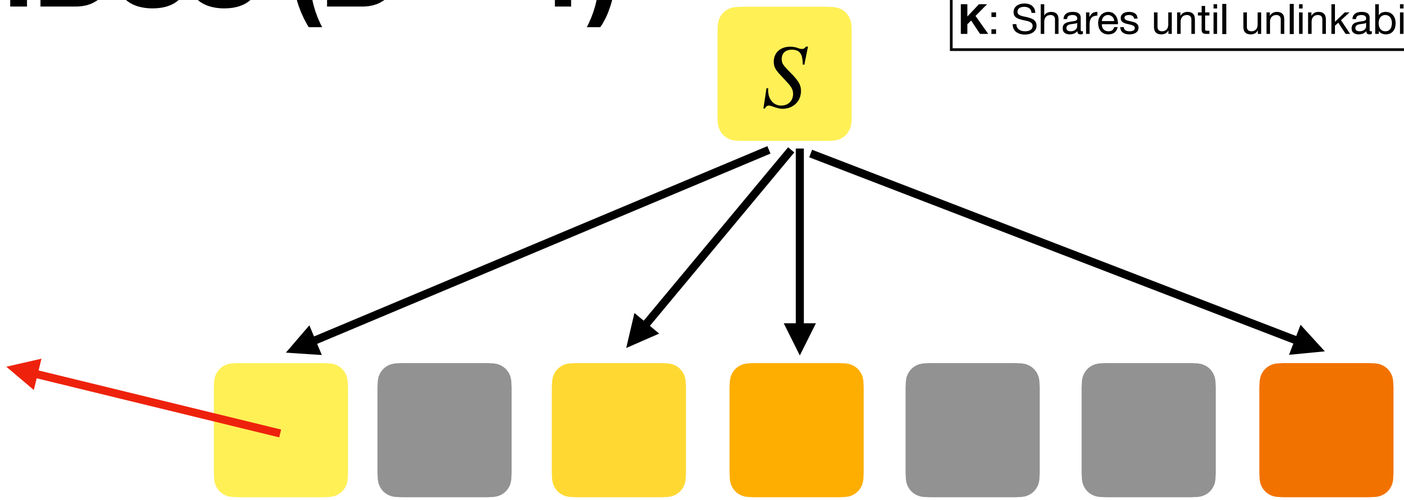
D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken



How To Build MDSS (D = 1)

D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken

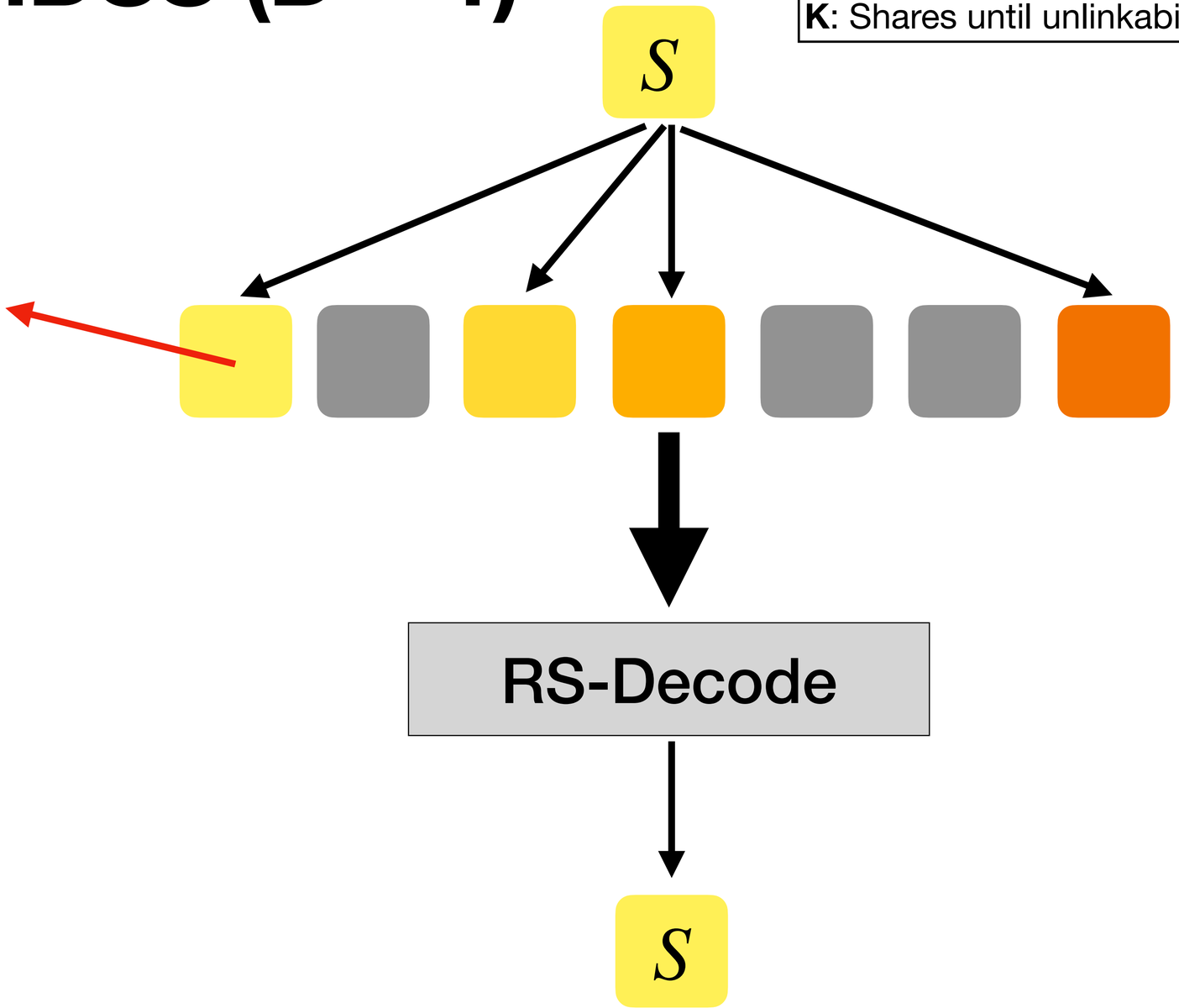
$$sh_i = (a_i, p(a_i))$$



How To Build MDSS (D = 1)

D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken

$$sh_i = (a_i, p(a_i))$$



How To Build MDSS (D = 3)

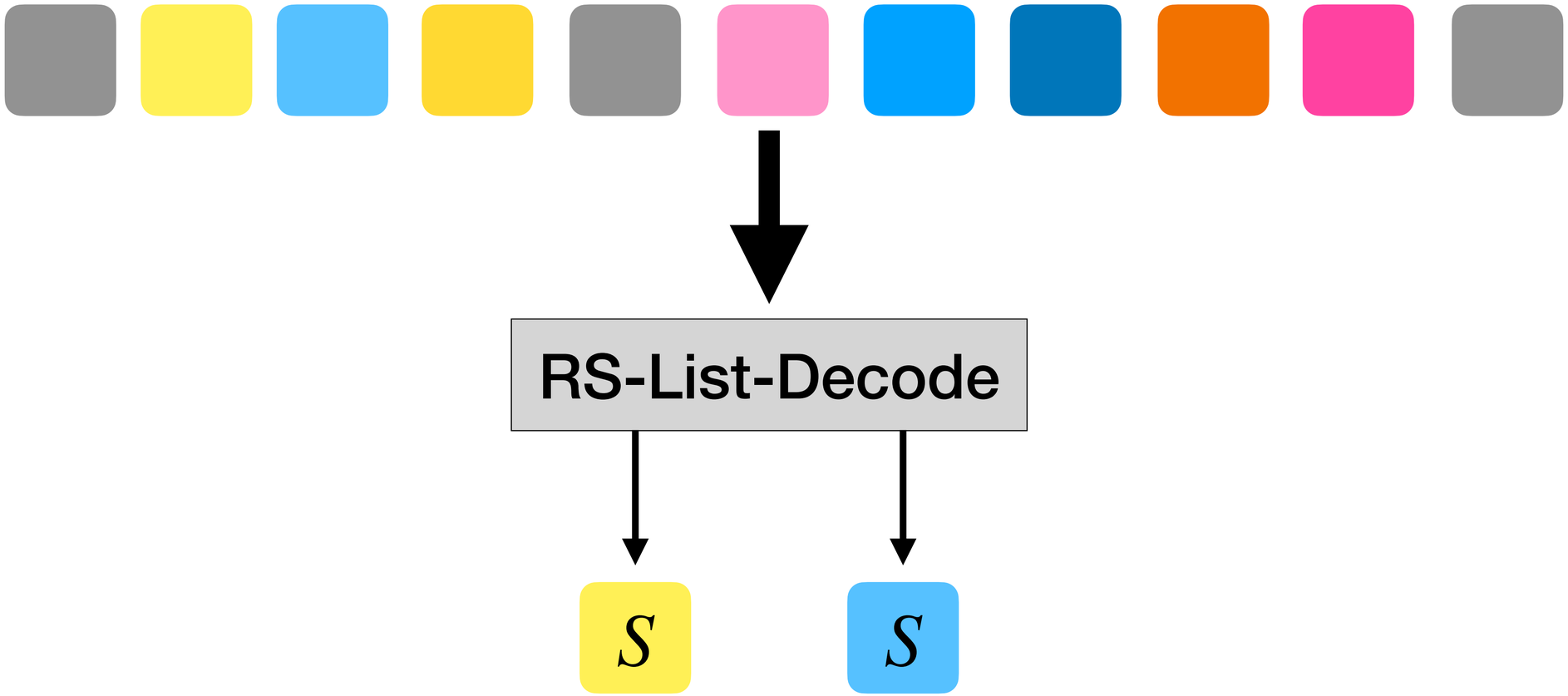
D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken

How To Build MDSS (D = 3)

D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken

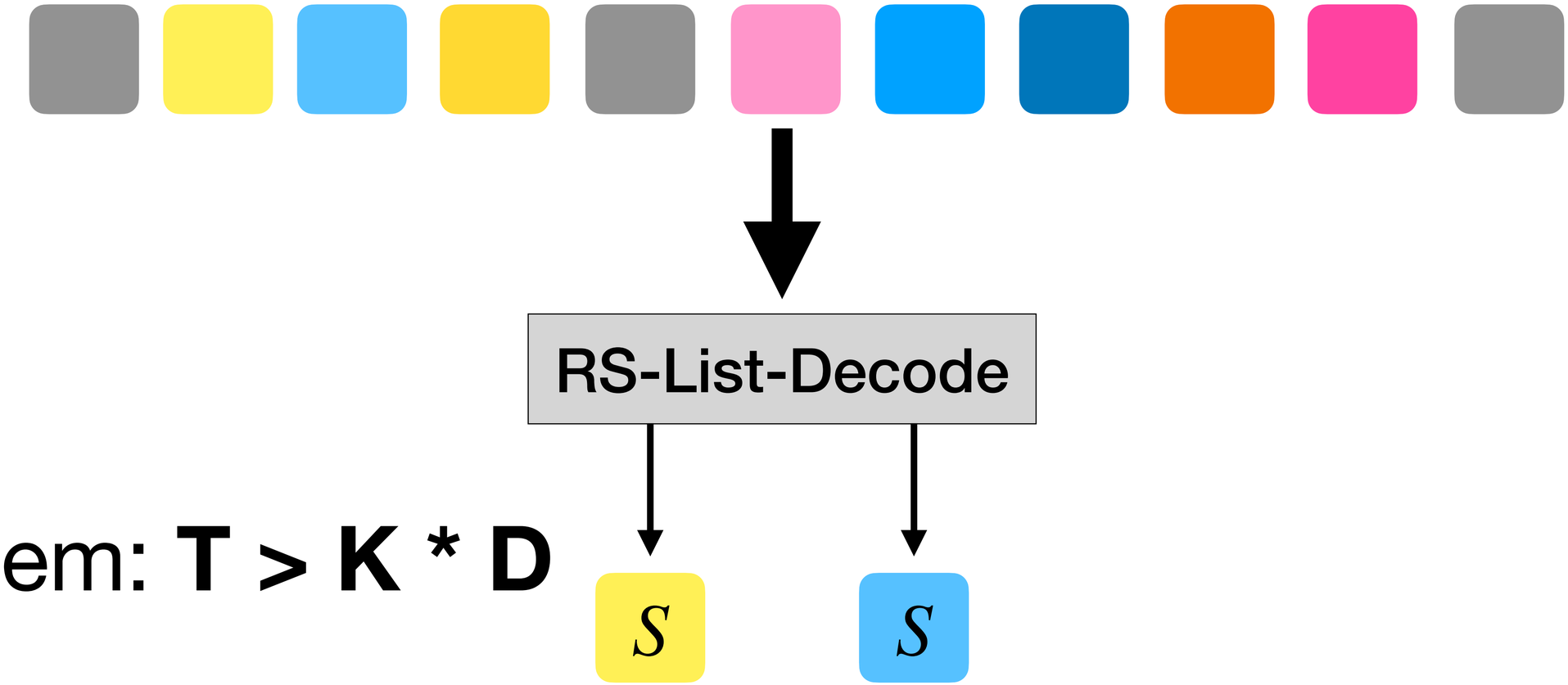
How To Build MDSS (D = 3)

D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken



How To Build MDSS (D = 3)

D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken



Problem: **T > K * D**

Better MDSS

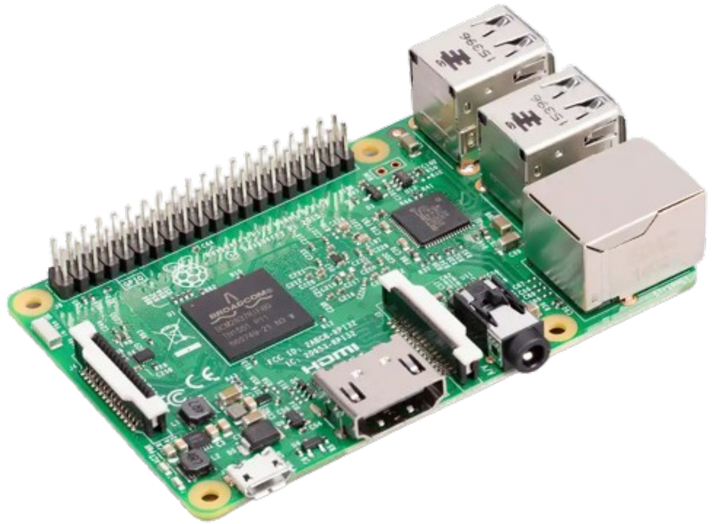
D: Number of Dealers
T: Shares until stalker is detected
K: Shares until unlinkability is broken

- Problem: **T > D * K**
- Solution: Use a different type of code
  - $sh_i = (a_i, p_1(a_i), p_2(a_i), \ldots, p_c(a_i))$
  - [BKY04, CS03, CH11] too inefficient and only work for **random** errors. We modify [CH11] to **heuristically** recover dealer secrets
- Better Bound (approximate): $\mathrm{T} > \frac{1}{c+1}(\mathrm{D} + c \cdot \mathrm{K})$

Implementation Stats

- Allow up to **3 simultaneous stalkers**
- New Share every **60 seconds**
- Detect stalkers in **1 hour**
- Stay unlinkable for **41 minutes**

Implementation Runtime



Generates shares in **0.05** seconds

Decodes in **1.27** seconds

Conclusion

Balancing stalker detection and tracker privacy is possible!

Conclusion

Balancing stalker detection and tracker privacy is possible!

Thank you!

Image Attributions

- AirTag: https://www.apple.com/shop/buy-airtag/airtag/1-pack
- Puck.js: https://shop.espruino.com/puckjs
- Raspberry Pi 3B: https://www.raspberrypi.com/products/raspberry-pi-3-model-b/