

Air tag → Stranger's iPhone → Find My Network → Your iPhone

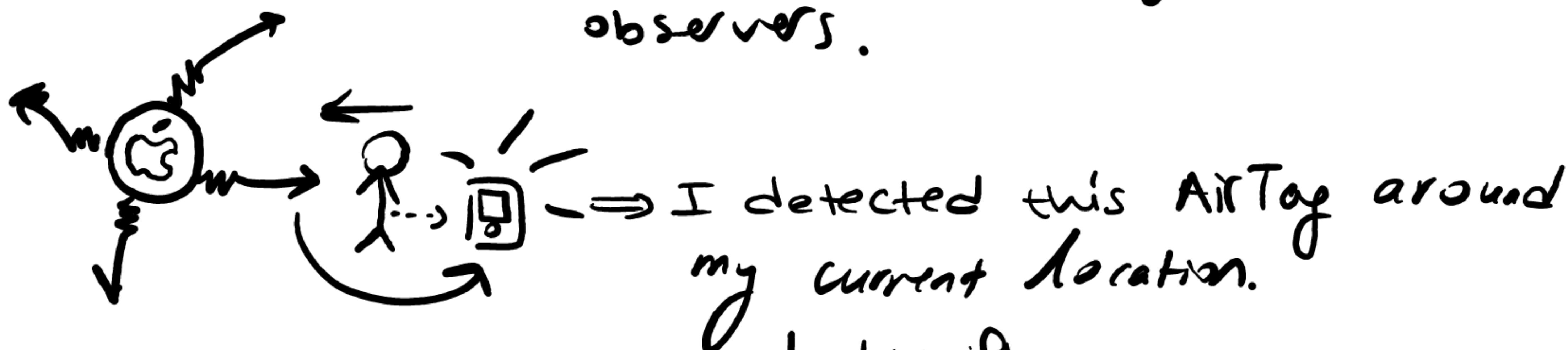
It isn't a GPS device.

It uses surrounding Apple devices GPS to detect location.

#1 Periodic Bluetooth Whispering

When you leave an item forgotten, AirTag periodically whispers this over Bluetooth "A missing item with temporary identity X is nearby"

↳ This changes over time so that it cannot be easily traced by observers.



↓ This iPhone
Sends an encrypted location report.



my iPhone opens
the encrypted report
and now I can see
the approximate location

#2 How Precision Finding Works

Airtag → Bluetooth Nearby iPhone → location
 → interact connection
 → upload it to Find My network

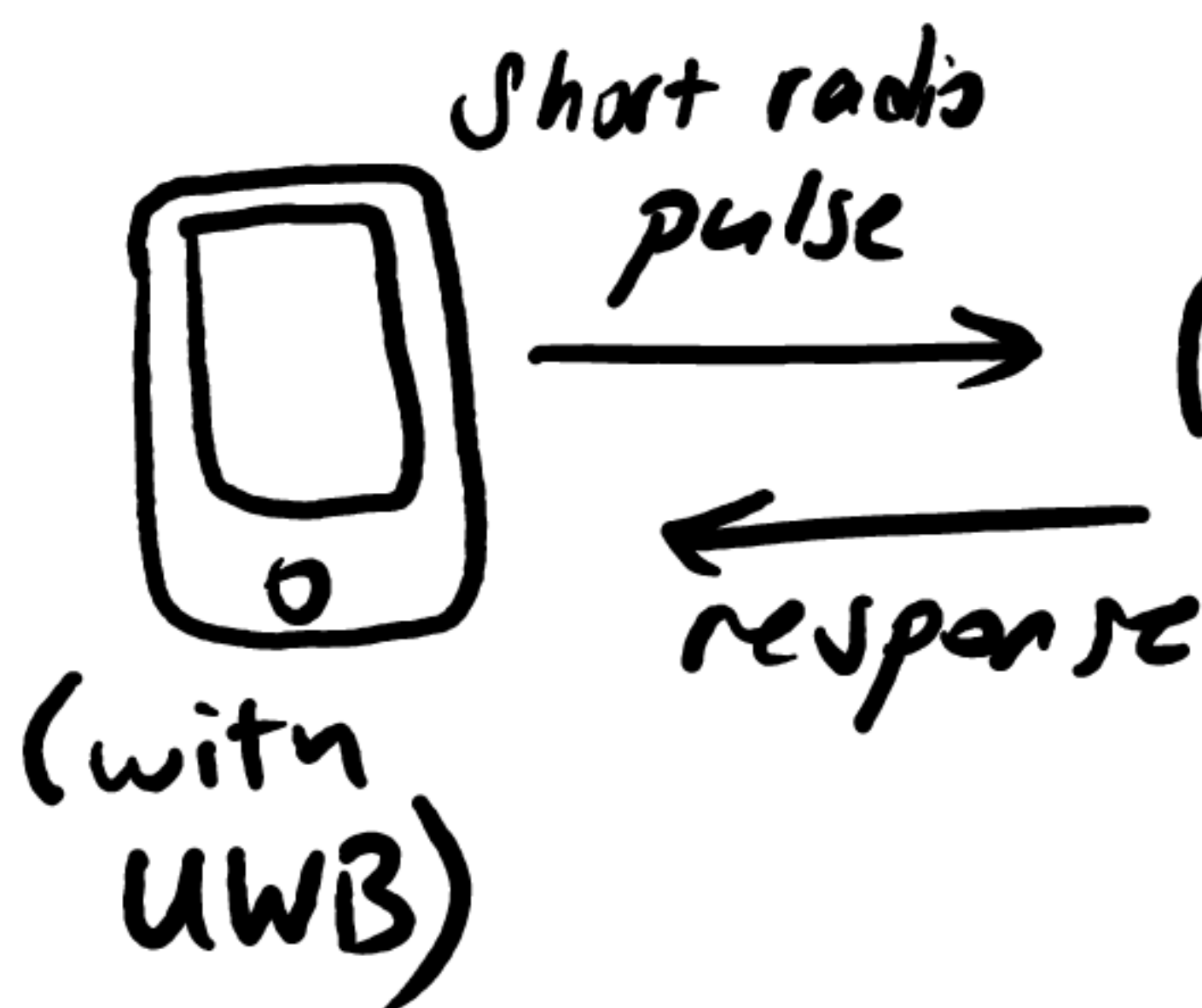
Bluetooth vs (UWB) Ultra Wideband

Is it somewhere nearby?

It is appr. 3 m away, in north direction.

→ if your iPhone has it you can locate it detailly

Distance



$$d \approx \frac{(t_{\text{pulse}} + t_{\text{response}}) \times c}{2}$$

speed of light

$$x = v \cdot t$$

Radio waves move close to speed of light

Direction

Modern iPhones have multiple antennas



Airtag

→ one signal reaches slightly faster than the other so by this iPhone understand what should be the direction

UWB distance measurement

iPhone

Compass

Motion sensor

Camera-based understanding of movement

#3 How AirTag protects location privacy

↳ Stranger's iPhone reports that location without knowing it is yours + Apple cannot read that location

⇒ Goldenit's AirTag, serial # 1234 ⇒ they don't do it like this

Instead

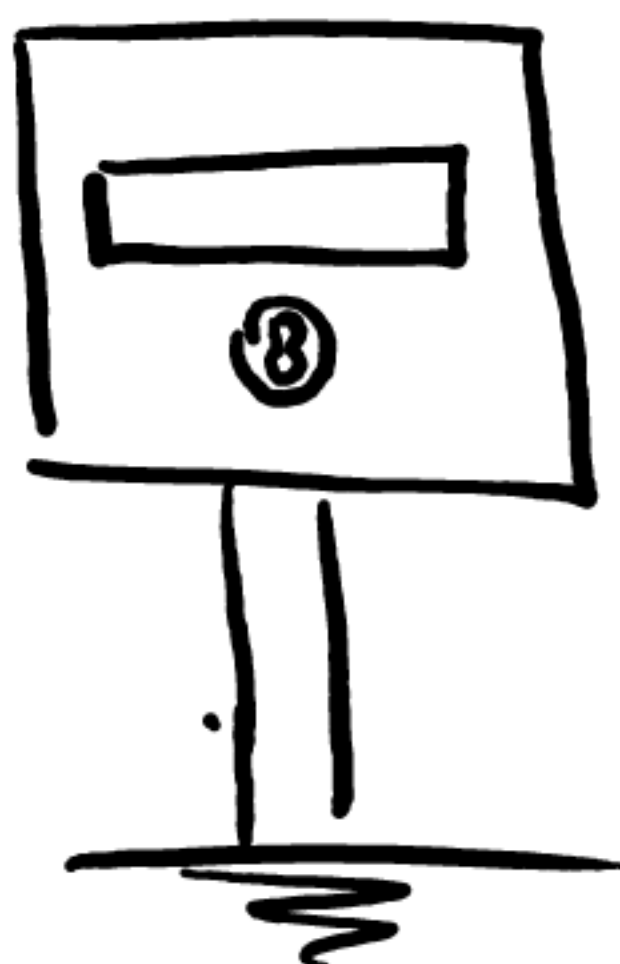
10.00 : ID X74
10.15 : ID P4B
10.20 : ID Mac } constantly changing Bluetooth identifiers

AirTag → Stranger's iPhone

Temp id: P4B
Location: new cafe
Time: 14:32

⇒ But in an encrypted way

mailbox



→ everyone can put letters in it

→ but only you have the key to open and read the letters

↗ used for encryption of the message

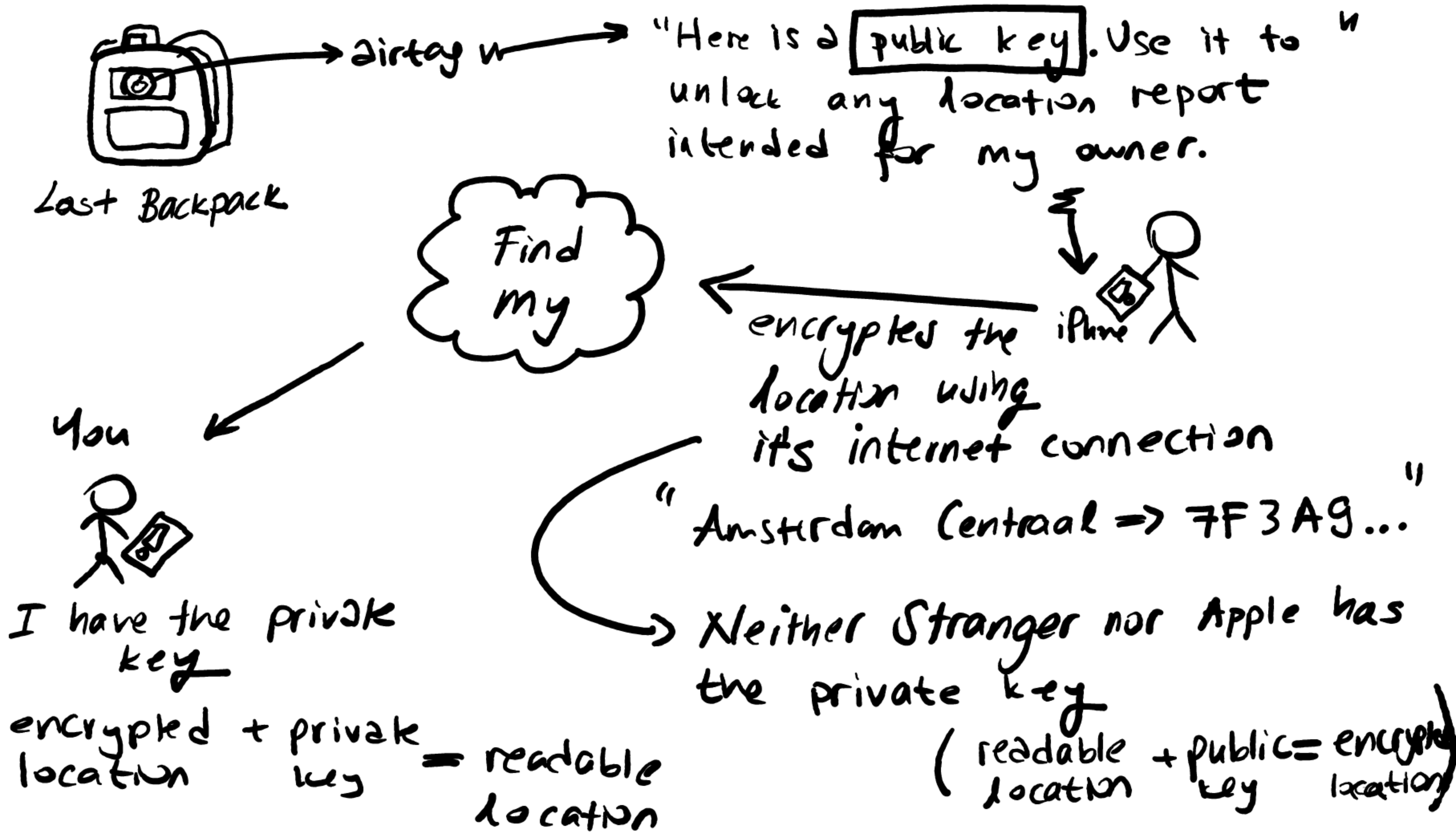
→ public key

→ private key

↳ used for decrypting the message



Quick Scenario, on the next page...



Analogy

private key $\rightarrow$ public key (easy) $\rightarrow$ but not impossible

public key $\rightarrow$ private key (computationally impractical)

Blue + Yellow $\rightarrow$ Green (easy)

green $\rightarrow$ blue + yellow (impractical on molecular level)

$\rightarrow$ It's mathematical logic is at the end of this article in a PDF format.

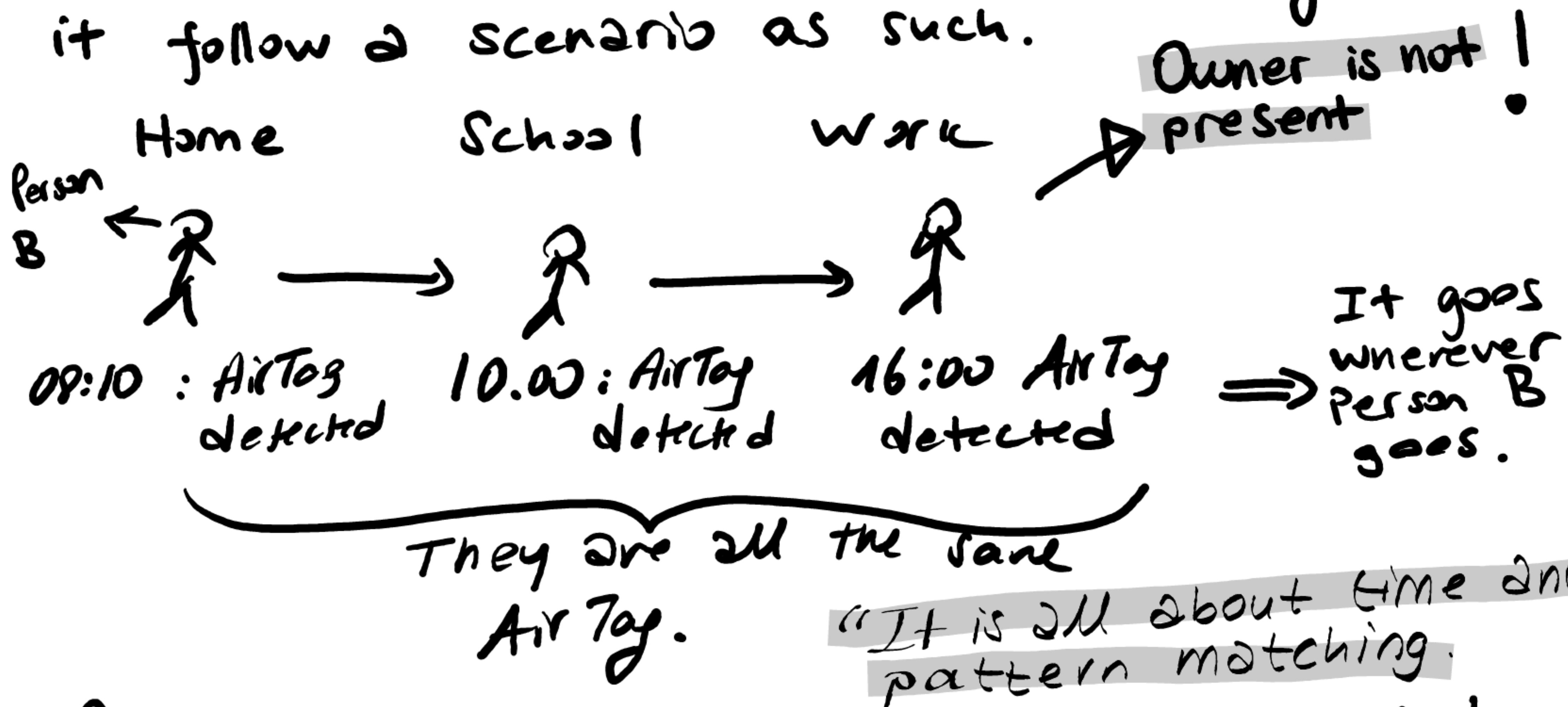
#4 How does AirTag prevent secret tracking

→ When AirTag is registered, it recognises a device as such:
AirTag 83F2 belongs to Gökdeniz's Apple Account

→ Ownership can also be shared which were added in the belongs to list.

But, passing strangers with AirTag doesn't trigger an alert immediately.

For example, take Person A has an AirTag and secretly put it into Person B's bag. In order it to be seen as an unwanted tracking case it follow a scenario as such.



On the other hand, imagine you are in a bus and commuting for 20 minutes with a person who has a bag with an AirTag. This doesn't trigger unwanted trigger action since the owner is present.

Also, there is no precise timing published by Apple, since this could also be used by stalkers.

In a nutshell, if Apple's system gets suspicious, you receive a message as such: Safety Alert: Your current location can be seen by the owner.