

# An overview and analysis of Apple's AirTag technology and FindMy service

Zanolin Lorenzo

June, 2024

## Contents

<b>1</b>	<b>Introduction</b>	<b>3</b>
<b>2</b>	<b>AirTag</b>	<b>3</b>
2.1	Overview	4
2.2	History	4
2.3	Protocols	4
2.3.1	Bluetooth	4
2.3.1.1	Overview	4
2.3.1.2	Security Analysis	5
2.3.2	UWB	7
2.3.2.1	Overview	7
2.3.2.2	Security Analysis	8
2.4	Hardware Analysis	9
2.5	Software Analysis	9
2.6	Security Analysis	11
2.6.1	Vulnerabilities	12
2.6.2	Anti-stalking countermeasures	13
2.7	Patents	14
<b>3</b>	<b>FindMy Network</b>	<b>17</b>
3.1	Overview	17
3.2	Functioning	18
3.3	Security Analysis	19
3.3.1	Preliminary definitions	19
3.3.2	Workflow	20
3.3.3	Cryptography	21
3.4	Support for non-Apple accessories	23
<b>4</b>	<b>Useful applications</b>	<b>23</b>
4.1	Mods	26



## Abstract

The main goal of this project is to dig into how Apple AirTags work, including their setup, security measures, and uses; since everything is tied to the FindMy network, the UWB technology and Bluetooth, we will also look into the security methods used in all of them. The idea is to get a clear picture of how Apple AirTags are put together, how secure they are, and the different ways they're used in the FindMy network.

## 1 Introduction

In the rapidly evolving landscape of technological advancements, Apple's AirTags have emerged as an innovation, offering a solution to tracking and locating personal belongings. We will begin with the history of these devices, then delve into the architecture and security of AirTags, with a particular emphasis on the UWB and Bluetooth standards that underlie their functionality. Finally, several patents related to this technology will be discussed.

Moreover, as AirTags operate within the framework of the FindMy network, this exploration extends to an overview of the security measures embedded in both the device and the overarching network. Through the examination of the relationship between AirTags, UWB, Bluetooth, and FindMy security, this paper seeks to provide insights into the working principles of the ecosystem that enables accurate location tracking, while also addressing concerns related to privacy and data security.

Additionally, practical applications of using AirTags to track objects or leverage their location-tracking abilities will be presented; this includes a quick overview of non-Apple devices that can also be detected within the FindMy network.

More specifically, we will begin with a comprehensive analysis of AirTags in Section 2.6, including the history of the devices, an analysis of the protocols used within them, and an examination of their hardware and software components. This section will also focus on security aspects and existing patents. Subsequently, we will discuss the FindMy network in Section 2.6, starting with a general overview and an analysis of how the service operates. Following this, we will perform a security analysis of the protocol from a cryptographic perspective, detailing the mathematical processes involved in the communication between devices. Finally, practical applications of this service will be presented in Section 4.

## 2 AirTag

An AirTag is a small device from Apple that is intended to assist users in finding and monitoring objects that are easily misplaced or lost, such as wallets, bags, and keys.

## 2.1 Overview

By connecting to compatible Apple devices (iPhones, iPads, and Macs) through Bluetooth, the AirTag enables users to locate the linked object and, subsequently, the AirTag itself using the Find My app. In order to help with lost item recovery, the gadget has capabilities including accurate location tracking, proximity notifications and a Lost Mode. Its design prioritizes privacy and security, safeguarding user data through the use of encryption and anonymization. With the introduction of iOS 14.5 and iPadOS, Apple has introduced the support for AirTags.

## 2.2 History

The first news regarding AirTag dates back to April 19, 2019, when, according to [48], some individuals working on the project confidentially disclosed its existence to the editorial team at 9to5Mac, revealing that a new hardware product was being tested. Initially, Apple referred to this device as B389, which was later revealed to be AirTag. Subsequently, as reported by [9], in April 2020, Apple released a video on YouTube explaining how to reset the phone to its initial settings; the issue was that during the short film, a part showing the deactivation of FindMy (from the settings) displayed the option for detection by AirTag. Later, in March 2021, the site MacWorld [55] discovered that in the iOS 14.5 (beta) version, a new section called Items was present in the Find My application. Finally, the product was officially presented by Apple in April 2021.

Currently, according to [33], Apple has generated over 1 billion dollars in revenue from the sale of this device (about 55 million units sold) and right now Apple is preparing a new generation of AirTag with the codename B589, expected to be released in 2025 (from [2]).

## 2.3 Protocols

First of all, these devices utilize two technologies: Bluetooth and UWB; we will briefly look at both of them.

### 2.3.1 Bluetooth

#### 2.3.1.1 Overview

Bluetooth is situated in the realm of short-range communications. It offers a more convenient alternative to wired connections between two devices. In such applications, having a large available bandwidth is not necessary; this means that Bluetooth radio transmitters can use relatively low transmission power. Bluetooth operates in the 2.45 GHz band, which does not require concessions or licenses.

According to [1], there are various versions of this protocol. In the first one (1.1), transfer speeds were in the order of 700 Kb/s; currently, with versions

5.x, transfer rates can reach around 50 Mb/s. With version 4.x, Bluetooth Low Energy (BLE) technology was introduced, which allows for optimal implementation of IoT applications with very low power consumption. In the 5.x version, BLE has a speed of 2 Mb/s. The frequency band used is the same but the number of channels is different. According to [10], Bluetooth uses 79 channels with 1 MHz bandwidth, while BLE uses 40 channels (37 for data and 3 for advertisement) with 2 MHz bandwidth. The reliable range covered by the two technologies also varies: under 30 meters for the former, while the latter can cover up to 150 meters in unobstructed spaces. The two technologies are intended to serve different purposes. Bluetooth is primarily used for audio and video streaming, as well as data transfer, all of which require high throughput at the expense of energy consumption (1 W). In contrast, BLE is primarily used in healthcare, smart devices and sensors in IoT devices, where efficiency (0.01 - 0.5 W) and low latency are critical.

We will present a brief summary of the differences between the various versions in Table 1. The data is taken from [20, 15].

Table 1: Bluetooth versions comparison.

	Transfer speed - Bluetooth	Transfer speed - BLE	Range (theoretical)	Power consumption
1.x	732 Kb/s (v1.1) - 1 Mb/s (v1.2)	-	10 meters	1W
2.x	2.1 Mb/s	-	30 meters	1 W
3.x	800 Kb/s - 24 Mb/s (if Wi-Fi is present)	-	30 meters	1 W
4.x	25 Mb/s	1 Mb/s	60 meters	0.01 W - 0.5 W
5.x	50 Mb/s	2 Mb/s	240 meters	0.01 W - 0.5 W

### 2.3.1.2 Security Analysis

Firstly, we will analyze the security measures implemented in the basic version of Bluetooth. This technology ensures Authentication and Encryption at layer 2 of the ISO-OSI stack; to achieve this, secret links are created and shared among participants during the initial pairing phase. Typically, each device is identified by its Bluetooth address and a PIN is subsequently required to authenticate the other party (it may happen that the PIN is stored in the device's long-term memory, thus not requiring user input). According to [23], Encryption is performed using the E0 stream cipher, composed of four linear feedback shift registers (LSFRs). The output of these registers is summed, and the result is XORed with the status register value.

For authentication, a challenge and response technique is used to verify one of the parties; both participants possess an E1 authentication function and a pre-shared key that acts as the authenticator. The verifier sends a random number to the claimant, who then uses the E1 function along with the pre-shared key to generate an output that is sent back to the verifier. If the value obtained from the verifier's E1 function matches the one sent by the claimant, then the claimant is authenticated.

Figure 1 visually illustrates the encryption and authentication processes, with further details available in [23].

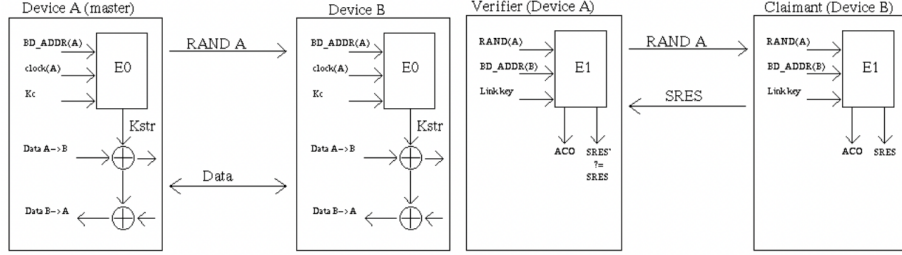


Figure 1: (a) Encryption process (b) Authentication process (images from [57]).

Secondly, Apple, in [7], defines the enhancements made to provide greater security to Bluetooth and BLE; from [7] on page 172: “The Bluetooth security model for both versions includes the following distinct security features:

- Pairing: The process for creating one or more shared secret keys.
- Bonding: The act of storing the keys created during pairing for use in subsequent connections to form a trusted device pair.
- Authentication: Verifying that the two devices have the same keys.
- Encryption: Message confidentiality.
- Message integrity: Protection against message forgeries.
- Secure Simple Pairing: Protection against passive eavesdropping and protection against man-in-the-middle attacks.”

Additionally, Apple has added two features for BLE: Address Randomisation and Cross-Transport Key Derivation.

**Address Randomisation.** According to [7], to ensure that an Apple device is not trackable, its BLE address is frequently changed to prevent traffic analysis. This is achieved through a technique called *Address Randomisation*, which allows the device to frequently change its *public* BLE address. Only known devices can resolve the *private* BLE address, as it requires possession of the resolving key, which is exchanged between the two devices during the pairing phase.

**Cross-Transport Key Derivation.** Initially, the link keys of BLE and Bluetooth were independent of each other; with this functionality (introduced in the Bluetooth standard), it is possible to derive a BLE link key from a Bluetooth link key and vice versa. This reduces the number of pairings required between two devices, thereby enhancing convenience and security, according to [6].

## 2.3.2 UWB

### 2.3.2.1 Overview

Within the domain of wireless communication technologies, UWB operates by employing extremely low-power, short-duration pulses that span a broad spectrum and result in increased distance measuring precision, allowing for high data transfer rates and precise positioning capabilities over a wide frequency range, typically several gigahertz. Originally conceived for military and radar applications, it has gradually invaded diverse sectors, finding particular prominence in consumer electronics, healthcare, automotive systems and the Internet of Things (IoT).

An advantage of UWB technology is its ability to provide accurate and real-time tracking, thanks to techniques such as Time-of-Flight (ToF)<sup>1</sup>, Time Difference of Arrival (TDoA)<sup>2</sup> and Two-Way Ranging (TWR)<sup>3</sup>. According to [18], the ranging error can be as low as 58 mm.

Because of its wide spectrum utilization, UWB can coexist peacefully with other wireless technologies and send out massive volumes of data quickly; also, it has a reduced range of operation due to the wide radio bandwidth it uses (according to [58], “U1 chip can emit data using two frequencies: 6.24 GHz and 8.2368 GHz. The FCC has allocated ultrawideband a spectrum starting from 3.1 GHz to 10.6 GHz.”). To overcome this problem, we can use an antenna of type *MIMO* (multiple-input and multiple-output) to enhance UWB’s range; this kind of device can be embedded into our everyday devices due to their reduced size.

According to [7], “Apple-designed U1 chip uses UWB technology for spatial awareness, allowing iPhone 11, iPhone 11 Pro and iPhone 11 Pro Max or later iPhone models to precisely locate other U1-equipped Apple devices”. This means that when two U1 devices come close to each other, the two start measuring their exact distance using ToF. According to IEEE 802.15.4a [29], the range of visibility for UWB is approximately 200 meters., which means that we can leverage this technology to track items that are very close to us and those that are relatively distant.

It is important to distinguish the differences between BLE and UWB. The former allows for detecting a device but cannot accurately measure its position, as it relies on the device’s range. UWB, on the other hand, enables precise localization of the device by measuring the position based on the time interval between when the signal leaves point A and when it arrives at point B. Table 2 represents the principal differences between the two technologies, data is taken

---

<sup>1</sup>From [4], “Time of flight is the measurement of time taken to travel a distance in order to determine distance, speed, or properties of the medium”.

<sup>2</sup>From [27], “TDoA is a positioning methodology that determines the difference between the time-of-arrival (ToA) of radio signals. TDoA is used in a real-time location system (RTLS) to accurately calculate the location”

<sup>3</sup>From [53], “The Two Way Ranging method determines the Time of Flight of the UWB RF signal and then calculates the distance between the nodes by multiplying the time by the speed of light.”

from [16]:

Table 2: BLE-UWB comparison.

	UWB	Bluetooth (BLE Beacons)
<b>Battery</b>	Low consumption	Low consumption
<b>Data Rate</b>	1 Gbps	2 Mbps
<b>Range</b>	up to 200 meters	up to 100 meters
<b>Accuracy</b>	10 centimeters	up to a meter
<b>Cost</b>	Low	Depend on the context

### 2.3.2.2 Security Analysis

The fact that UWB pulses are resistant to the multipath effect<sup>4</sup> is one of its key characteristics. This occurs when radio waves are reflected or refracted by artificial or natural objects near the primary signal channel, causing the signal to reach the receiver via many paths. Positioning accuracy is improved by immunity to the multipath effect, particularly when compared to other technologies that are more vulnerable. Moreover, UWB’s resilience to jamming and narrowband fading makes it a particularly reliable technology choice, even when several UWB systems are being used at once.

Another important aspect to consider is the resistance to Relay Attacks, which is a vulnerability of the majority of signal-based architectures; we will present a concrete example taken from [22]. In this attack, the goal is to trick a car into thinking the key and owner are close by using two people with hacking devices. The first relays signals from the car to the second thief, who transmits the signal to the house. The key responds, allowing entry into the car. The relay attack intercepts and amplifies wireless signals used to unlock the door and start the car, despite the key’s distance. With UWB, that would not be possible due to its working scheme: to ensure the car doesn’t have to make assumptions, rapid measurements are utilized to establish distance very precisely. Any attempt to relay attack or intercept the UWB signal will merely cause the answering device’s acknowledgement signals to arrive later, indicating to the car that the real key is actually farther away. The car’s presumption is replaced with assurance when using UWB, which greatly increases the security of the passive keyless entry system.

The implemented security measures, taken by Apple, are the following: MAC address randomisation and frame sequence number randomisation [7].

**MAC address randomisation.** This functionality is very similar to that discussed in 2.3.1.2, with the objective of concealing the MAC address of the device. In [7], it is explained that the randomization procedure used for UWB

<sup>4</sup>From [17]: “Multipath interference occurs when a signal from a transmitter arrives at a receiver via two or more routes; typically there is a direct path plus a number of indirect paths caused by reflections”.



is the same as that used for Wi-Fi. During a scanning procedure, the device randomizes its MAC address to prevent situations where someone might sniff the traffic to analyze the device’s behavior. Once connected to a network, it will consistently show the same (randomized) MAC address, which will change once the session ends. This provides protection against visibility from malicious individuals attempting to sniff the traffic for malicious purposes.

**Frame sequence number randomisation.** This functionality stipulates that each time the device randomizes its MAC address (following a scan or disconnection), the sequence number of its packets is also randomized; as before, this addition increases privacy and also avoids the possibility of replay attacks.

Now, we will analyze the architecture of this product; the information has been reverse engineered by Adam Catley in [12]. We will cover both the hardware and software aspects of this kind of device.

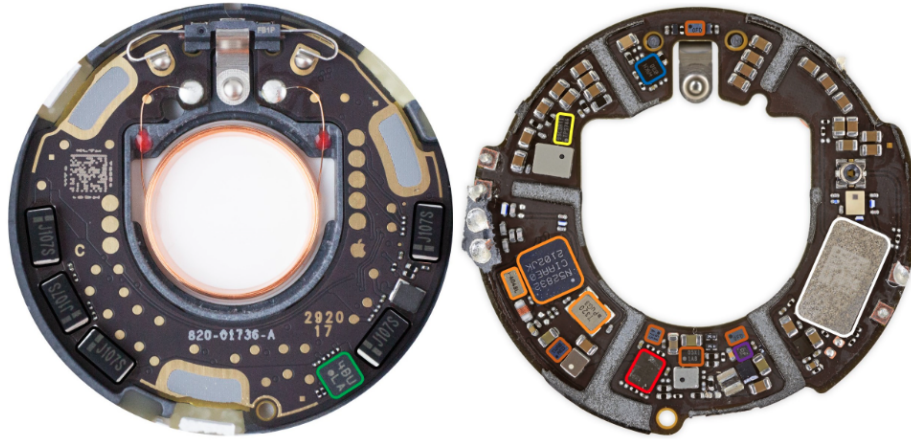
## 2.4 Hardware Analysis

As for the hardware part, an important aspect comes to light: all of the used components, aside from Apple’s U1 UWB chip, are off the shelf, as we can see in Figure 2. Each AirTag has three antennas: one for BLE that works at 2.4 GHz, one for NFC at 13.56 MHz and one for UWB one at 6.5-8 GHz. We have a plastic case that works as a diaphragm and it is adhered to the voice coil. When the coil is energized, the fixed magnet causes it to move back and forth, creating sound and serving as the speaker. If motion is detected, the speaker will loudly beep for up to 20 seconds after being away from its owner for three days. After that, it will be silent for the following six hours before watching for movement once more.

## 2.5 Software Analysis

As for the software part, we will present information taken from [12]: “There are various states in which AirTag can be; we will now quickly present all of them.

- *Not registered:* When the AirTag is brand new, has been reset, or has been removed from the FindMy network. Waits to be connected to while advertising itself every 33ms.
- *Initialisation:* The AirTag is being registered to an Apple ID and a public/private key pair is generated and shared between the AirTag and the connected iOS device.
- *Connected:* The owner’s device is in range. No broadcasts occur.
- *Disconnected:* The owner’s device is out of range. Broadcasts identity every 2000 ms.



- Nordic nRF52832 SoC with BLE and NFC, plus 32MHz and 32.768kHz crystals
- Apple U1 UWB Transceiver
- GigaDevice GD25LE32D 32Mbit NOR flash
- Bosch BMA280 accelerometer
- Maxim MAX98357AEWL audio amplifier
- TI TPS62746 DC-DC buck converter
- TI TLV9001IDPWR opamp
- 100uF Electrolytic Capacitors (5x)
- Unknown. Unable to decode markings

Figure 2: PCB overview (image from [12]).

- *Out of sync*: Happens when an AirTag reboots while separated from its owner’s device. Acts like Disconnected but absolute time is lost so events are relative to time since power-up. Identity resets to initial value.
- *Lost*: Occurs 3 days after Disconnected or Out of sync begin. Moves to Waiting for motion every 6 hours.
- *Waiting for motion*: Samples the accelerometer every 10 seconds until motion is detected.
- *Sound alert*: A command to play a noise is received from either a connected device or by detecting motion. Lasts a maximum of 20 seconds.
- *Precision finding*: Triggered by the owner’s device while in Connected. Is overridden by Sound alert.”

As we will see in Section 2.4, even if the finder has an Android device, they may be able to identify the owner of an AirTag thanks to its NFC antenna. Depending on its current status, the tag carries a URL that uniquely identifies the AirTag. It can only be read when the AirTag is turned on (meaning that the battery within it is sufficiently charged). There are some parameters that are attached to the URL, used to identify the device; we will briefly present

them. All of the following parameters are fixed for a single unit, even after power cycles, long runtime, resets and modes. From [12], “

- *pid*: product ID for AirTag.
- *b*: something related to the battery.
- *pt*: UWB Precision Tracking version.
- *fv*: firmware version.
- *dg*: something related to diagnostic.
- *z*: unknown.
- *bt*: Bluetooth address; will be present only when Unregistered.
- *st*: serial number of the tag (the one printed on the device under the battery); will be present only when Unregistered.
- *bp*: Bluetooth protocol version; will be present only when Unregistered.”

In the **Unregistered** state, the stored URL has the following format: <https://found.apple.com/airtag?pid=5500&b=00&pt=004c&fv=00100e10&dg=00&z=00&bt=A0B1C2D3E4F5&sr=ABCDEF123456&bp=0015>

According to [12], once the device is registered, “The parameters *bt*, *sr*, *bp* will be removed and replaced with a single anonymous identifier *pi*, which is the only parameter that changes at least every 15 minutes when the Bluetooth address and/or the advertising data change”. Probably, it is the P-224  $p_i$  presented in 3.3.3 or the SHA-224 of it.

The device operates on a schedule designed to optimize its functionality: at 4:00 am every day, it updates its BLE address and public key, ensuring secure communication channels. Advertisement data is refreshed every 15 minutes, guaranteeing that nearby devices receive the most current information. Should it become separated from its owner’s device for three days, the device enters a lost mode, activating specific features to aid in recovery efforts. While in this lost mode and detecting movement, the device emits a noise every 6 hours to alert nearby individuals. To conserve energy while remaining responsive, the accelerometer is sampled every 10 seconds while waiting for motion; upon detecting movement, its sampling frequency increases to every 0.5 seconds for 20 seconds, providing detailed tracking data. When it’s away from the owner, the device transmits BLE advertisement signals every 2 seconds, enhancing its detectability. Finally, in close proximity to its proprietor’s device, the tag establishes a BLE connection interval of 1 second, ensuring efficient communication and responsiveness.

## 2.6 Security Analysis

Security-wise, from [12] it has emerged that no security checks are performed on the device during its operations; in fact, none of the data in the AirTag is protected from tampering or disclosure.

### 2.6.1 Vulnerabilities

We will present some vulnerabilities that have been found by Adam Catley in [12]; Table 3 resumes them.

**Exploitable voltage levels.** The Nordic nRF52832 has the function Access Port Protection [51] that is used to prevent external parties from reading the internal memory and to limit access to the Debug Port via SWD<sup>5</sup>; however, according to [50], side channel attacks are effective against this mechanism, more specifically voltage glitching. Consequentially, “It would be possible to disable other privacy features that Apple advertises, extract Bluetooth pairing keys to connect to the owner’s phone, or run completely custom firmware”, from [12]. In this case, if an attacker is able to use voltage glitching to inject a modified firmware, maybe he can use it to track the owner and it will not be discovered since the anti-stalking countermeasures presented in 2.6.2 do not work with personal objects. To ensure protection against voltage glitching attacks, it is necessary to implement a detector directly on the circuit that can detect when voltage levels are being tampered with. The Voltage Glitch Detector IP from INVIA “Detects positive and negative supply voltage glitches, and has a slope detection range between 100 MV/s and 2 GV/s”, according to [26].

**Insecure Storage.** All the information saved into the GD25LE32D 32Mbit NOR flash is clear, as we can see in [39]; also, the nRF52832 does not have any encryption functionality. In this case, we don’t know if this is a real vulnerability since we do not know whether the FindMy private key-pair is stored inside the AirTag. However, an attacker can read without problems all the information that is stored within the device and, in general, this behavior can be exploited (maybe in the future) to inject malicious data into the AirTag or to read sensible information. To prevent this, we can implement encryption via software or hardware; typically, on small devices, it is better to use dedicated hardware circuitry to encrypt data.

**Unauthenticated transmission.** The only way to identify an AirTag is to use its public key, which is transmitted via BLE advertising packets; this identification does not require authentication. These IDs can be recorded and replayed by any nearby BLE device to mimic the appearance of the real AirTag. Supposing a malicious actor obtains a BLE device and registers the public key of the sender; once power is removed from the AirTag, the attacker can send BLE packets containing the AirTag’s public key, thereby falsifying the location of the AirTag without a battery. In this case, the AirTag is exploited to steal personal belongings from the owner (example taken from [12]). To avoid this, Apple can use authenticated encryption; for example, we can use GCM, which offers the ability to verify the authenticity and integrity of extra authenticated data

---

<sup>5</sup>From [41], “SWD is a standard for debugging and accessing microprocessor registers. This protocol has been in use for many years and is still in use today.”

(AAD) that is provided in clear text in addition to authenticated encryption (confidentiality and authentication). More details can be found in [30].

Table 3: Vulnerabilities.

Vulnerability	Possible attack	Countermeasure
Exploitable voltage levels	Side-channel attack	Use detector
Insecure storage	Memory-reading attack	Implement hardware encryption
Unauthenticated transmission	Replay attack	Implement authenticated encryption

### 2.6.2 Anti-stalking countermeasures

An important aspect that has emerged with the AirTags is the stalking problem. Stalking using AirTags refers to the potential misuse of Apple’s AirTag tracking devices to monitor and track individuals without their consent; these small devices are designed to help users locate misplaced items. However, due to their small size and long battery life, AirTags could potentially be used for nefarious purposes, such as stalking. An individual could secretly place an AirTag in someone’s belongings and then use the Find My app to monitor their movements in real-time. Since AirTags are designed to be difficult to detect, the victim may not realize they are being tracked for an extended period of time.

Apple has implemented measures to prevent the misuse of AirTags, including alerts and notifications for when an unknown AirTag is detected near a user’s device, as well as features like Precision Finding, which can help users locate unwanted AirTags. The first line of defense in the event that someone plants an AirTag on a victim’s belongings might be an alert to his iPhone indicating the presence of a foreign AirTag. Apple built the iPhone-AirTag connection to do this in two ways: either when you get to the place that your iPhone’s machine learning intelligence has detected as home (or when you manually record it as home) or after the AirTag has stuck with you for a certain “continuous” period of time that Apple deems sufficient to be considered abnormal. This seems perfect; however, if the victim has a non Apple device, such as an Android phone, this could be a problem. To prevent this, Google and Apple collaborated to develop Unknow Tracker Alerts, which is a feature that was announced during the Google I/O 2023 opening presentation.

In the paper [52], an experiment was conducted in which the payload of the beacon transmitted by the AirTag was successfully modified to appear as an iPhone, rendering it undetectable as a tracking device. As a direct consequence, tracking notifications were not triggered.

An important factor is that AirTags can emit sounds when they are separated from the owner’s devices for an extended period of time. This way, a victim of a stalking attempt can hear the noise emitted by the device and realize they are

being tracked. More precisely, three days following separation is when sound alerts begin; even in that case, once the tag detects movement, it will emit a sound for about 20 seconds, followed by at least 6 hours of silence (even if further movements are detected). The issue with this feature is that 20 seconds of sound followed by silence for 6 hours can be ineffective if the victim is in a noisy environment and unable to hear the emitted sounds from the device. Moreover, during the initial three days of silence, the attacker can study the victim’s movements undisturbed without him being aware of it. According to [38], “The frequency and duration of sounds can be adjusted from the Apple server side”, meaning that Apple can increase both of them to avoid situations in which the victim is unable to hear the sounds.

However, despite these safeguards, the potential for AirTags to be used for stalking remains a concern; in fact, a problem is that the voice coil can be disconnected without disassembly. The resulting problem is that an AirTag can function normally without the voice coil, and therefore, if used for stalking, it will be difficult for a user without an Apple device to detect its presence if it is well hidden.

## 2.7 Patents

There are various patents related to AirTags; illustrations and information from these patents will be presented below. In the patent US2020028424 (Wirelessly locatable tag) [45], the structure of the tag is first described, as shown in Figures 3,4; subsequently, the abstract requirements for the components that this device must include are outlined.

Other patents similar to the one just mentioned include:

- US20220004834A1 (Antenna assembly for a wirelessly locatable tag) [44], which provides information on the arrangement of the antenna.
- US11659916B2 (Mounting base for a wirelessly locatable tag) [43], which outlines the construction of the mounting base for the tag.
- US20200333421A1 (Fastener with a constrained retention ring) [42], which describes the design of a generic holder for the tag.
- US20200272221A1 (Multi-Interface transponder device - power management) [19], which describes the various states in which a positioning tag can be; they are represented in Figure 5.
- US20240073648A1 (Tracking Systems with Electronic Devices and Tags) [47], which describes the need for communication circuitry to permit communication between tags and devices.

Many figures are shared among all the previous patents.

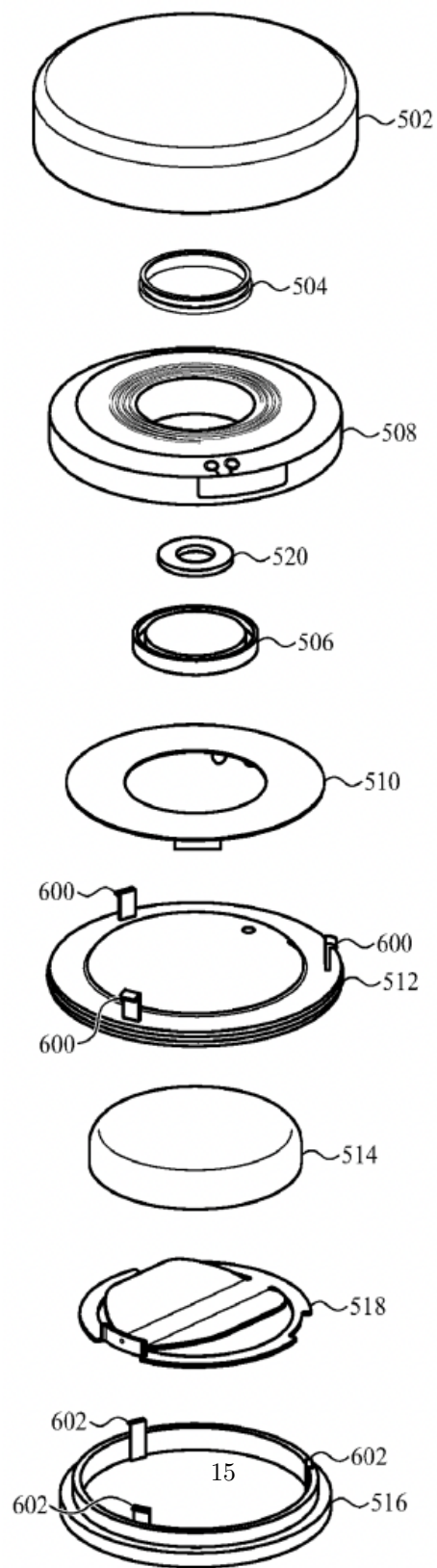
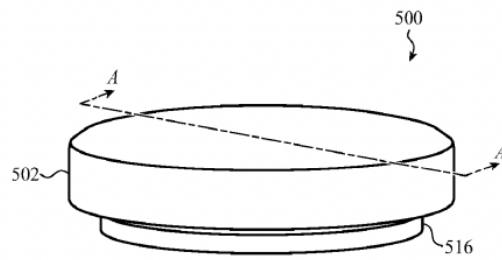


Figure 3: Tag composition (image from [45]).



**FIG. 5A**

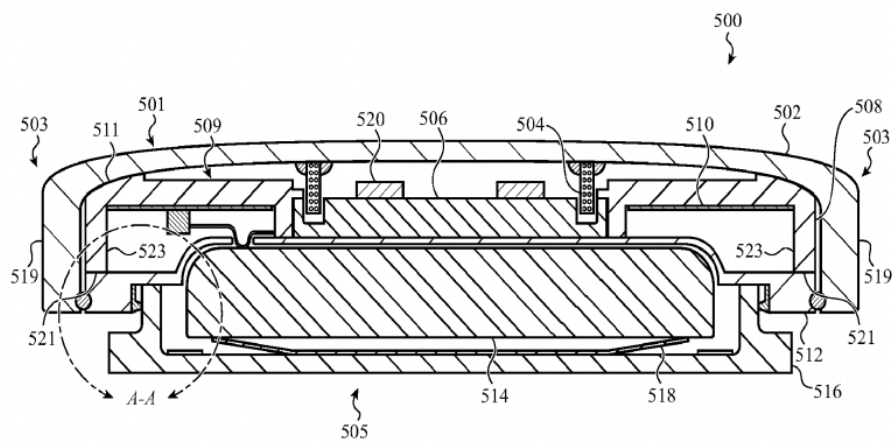


Figure 4: Tag sectional drawing (image from [45]).



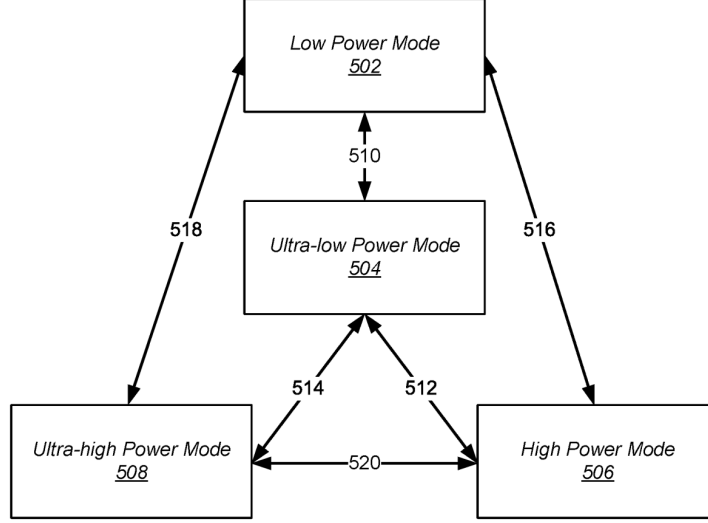


Figure 5: State diagram that represents power modes of a tag (image from [19]).

## 3 FindMy Network

### 3.1 Overview

Apple created the technology, known as the FindMy network, which is intended to assist consumers in finding compatible third-party accessories, such as Apple AirTags, as well as their Apple devices, including iPhones, iPads, Macs, and AirPods. By utilizing UWB and BLE technologies, the FindMy network facilitates accurate and instantaneous location tracking.

Apple merged the applications Find My Friends and Find My iPhone together into a single one called *Find My*, allowing users to locate everything they need in one place. Subsequently, Apple has enhanced the Find My app, incorporating functionalities such as monitoring when an iPhone is disconnected, when it is turned off and when it has been wiped.

Sections of the app are located at the bottom. *People* is located on the left and represents friends location (they have to share it in order to be visible), while personal belongings, including Bluetooth goods with Find My functionality and AirTags, are located in the center; finally, on the right, there's a *Me* tab with all of the owner's settings and info, as we can see in Figure 6.

There are several useful features within this app, we will present some examples taken from [14]:

- *Separation alerts*: you will get notified if you unintentionally leave behind an Apple device, an AirTag-tagged item or a third-party device that has enabled Find My features.

- *Locating friends and sharing location*: this feature allows you to share your location with friends or family so they can view it when needed. One useful aspect of this function is that it also enables you to monitor your children or individuals with certain orientation problems, helping them if they get lost.
- *Locating devices without connection*: this feature is very useful as it allows offline devices to be tracked using the FindMy network. Essentially, a lost device uses BLE to send beacon packets to nearby Apple devices, which then send the encrypted location to the owner’s iCloud account. As we will see later, it will also be possible for some devices to be located even without battery charge, meaning when the device is turned off.
- *Anti-stalking measures*: this feature helps prevent situations where a malicious individual secretly places a device belonging to a FindMy network in your belongings to track your location in real time, using your device to upload its position. When your device receives multiple BLE beacons from a nearby device, it will notify you that you might be tracked by a device and ask if you want to disable its location sharing. We will also come back on this following the studies done in [24].
- *Precision finding*: this feature requires the presence of the U1 chip, which uses UWB technology to locate another device equipped with the same chip. It is very useful for precisely locating AirTags, which are often attached to items that we tend to lose frequently. The range of this technology is limited to that of UWB, as we previously discussed.

### 3.2 Functioning

Now, we will describe the entire functioning process. First of all, products have to be registered within the application; in the case of a non-accessory item, it will automatically be inserted in the *Devices* section. In the case of accessories, like AirTag, they will be added within the *Items* section.

Now devices should be localizable from the map; in the case of a close AirTag it is also possible to use the *Precision finding* to locate the object using U1 chip, as represented in Figure 7. As always, Apple creates an excellent graphical interface for its features; for instance, Precision Finding utilizes multiple components. From [40]: “The technology fuses input from the iPhone’s camera, ARKit, accelerometer and gyroscope in order to guide the user to their AirTag using a combination of sound, haptics, and visual feedback.”

In case of a stolen device, it is always possible to activate *Lost Mode*; a notification will be sent as soon as the iPhone is detected, which means that if the phone is connected to a network or via BLE to other Apple devices, the owner will receive a message from FindMy containing the position of the device. Also, in this modality, all the registered cards in Apple Pay will be temporarily disabled.

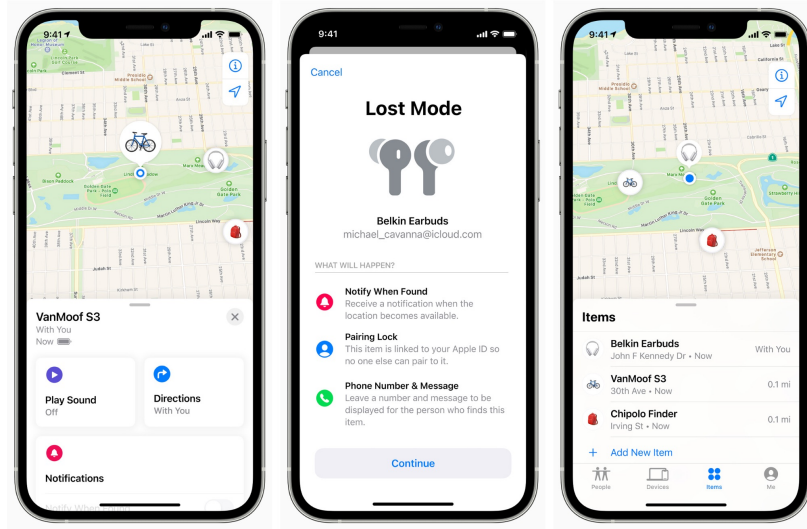


Figure 6: FindMy screenshots (images from [59]).

This technology seems pretty useful already, but if a device is powered off, how can it be localized? If it is U1-equipped, its Bluetooth is enabled and its iOS version is at least 15, then it can be localized even if turned off, since it works like an AirTag. This seems very useful; what about other devices, like Macbooks? Since Apple has not commented on the matter, the author conducted some tests and discovered that even machines with high specifications lack the U1 chip and are therefore not localizable when turned off.

Like other devices registered on FindMy, AirTags can also be located by other Apple devices in the same manner as written before. Specifically, as we will see in Section 2.5, once an AirTag moves out of the proximity range of the owner’s other devices, it begins to send BLE beacons to be identified and detected on FindMy. The only way to stop an AirTag from being fully detectable is to remove the CR2032 coin battery (or when it fully discharges).

### 3.3 Security Analysis

In this section, we will analyze the security measures implemented in FindMy to increase the safety of the architecture.

#### 3.3.1 Preliminary definitions

We will first define a few terms taken from [25]:

- *Owner Devices*: Apple devices owned by the user that can be located; the complete list of detectable devices is available in [8]. Within the FindMy



Figure 7: Precision Finding.

section of your iCloud account, you can view the location of all your devices.

- *Lost Devices*: There are two types of Apple devices that can exist: devices and accessories (according to [25]). The former (appearing in the Devices section of FindMy) are marked as lost when they lose their internet connection, whereas the latter (appearing in the Items section) are marked as missing when they lose connection with all of the owner's Apple devices. As we will see in Section 3.3.3, these devices start sending BLE beacons to be detectable by other Apple devices.
- *Finder Devices*: Apple devices that are capable of localizing lost devices; a GPS module is needed to be a finder.
- *Apple's Servers*: They are used to store all location reports sent by the various finder devices, and only the respective parties can access and download them locally. All information is encrypted, and only those with the private key can access it, namely the owners of the involved devices.

### 3.3.2 Workflow

An Apple device or accessory that enters the Lost state begins emitting BLE beacons that can be detected by nearby Apple finder devices. Once a beacon is detected, the Finder device creates a packet containing information about the lost device and uploads it to iCloud. An example of the previous workflow is represented in Figure 8.

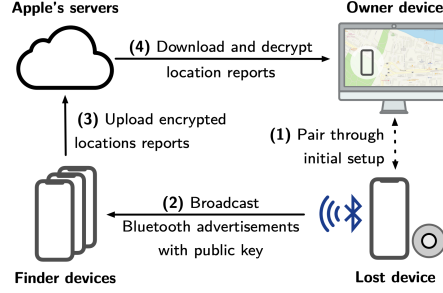


Figure 8: FindMy workflow (image from [25]).

All Finders scan for FindMy beacons (if the option is enabled in Settings). More specifically, this kind of device creates and uploads an encrypted position report to Apple’s servers whenever they receive a beacon in the FindMy advertising format; they are likely to use less energy and bandwidth because they gather reports over time and transfer them in batches on a regular basis. The evaluation done in [25] discovered that “The median time from generating to uploading a location report is 26 minutes. The delay can increase to several hours if the finder device is in low power mode”.

### 3.3.3 Cryptography

We will now delve more into the Cryptography protocols used.

**Advertisement keys.** FindMy utilizes Elliptic Curves [37]; according to [7, 25], “The process to generate *advertisement keys* is the following:

1. Each owner device generates a private/public key pair  $(d_0, p_0)$  on the NIST  $P - 224$  curve and a 32-byte symmetric key  $SK_0$  that together form the master beacon key. Those keys are never sent out via BLE and are used to derive the rolling advertisement keys included in the BLE advertisements. Note that device tracking is hard since rolling keys can be deterministically derived if and only if one knows the initial input keys  $(d_0, p_0)$  and  $SK_0$ .
2. OF iteratively calculates the advertisement keys  $(d_i, p_i)$  for  $i > 0$  as follows using the ANSI X.963 key derivation function  $KDF$  [3] with  $SHA - 256$  [21] and a generator  $G$  of the NIST P-224 curve:

$$SK_i = KDF(SK_{i-1}, 'update', 32) \quad (1)$$

$$(u_i, v_i) = KDF(SK_i, 'diversify', 72) \quad (2)$$

$$d_i = (d_0 * u_i) + v_i \quad (3)$$

$$p_i = d_i * G \quad (4)$$

where Equation (1) derives a new symmetric key from the last used symmetric key with 32 bytes length. Equation (2) derives the so-called “anti-tracking” keys  $u_i$  and  $v_i$  from the new symmetric key with a length of 36 bytes each. Finally, Eqs. (3) and (4) create the advertisement key pair via EC point multiplication using the anti-tracking keys and the master beacon key  $d_0$ .

**Key synchronization.** To download and decode location information, the advertisement keys must be accessed by all owner devices. In order to synchronize the master beacon keys, FindMy uses iCloud to encrypt a property list file in the Galois/Counter mode of the Advanced Encryption Standard (AES-GCM) [30]. The file’s decryption key is kept in the iCloud keychain underneath the label “Beacon Store”.

**Encryption.** Each BLE beacon contains an Elliptic Curve public key  $p_i$ . When a finder device intercepts a beacon, it saves its location and encrypts it using the  $p_i$  key; subsequently, it uploads the packet to Apple’s servers. OF uses the Elliptic Curve Integrated Encryption Scheme (ECIES), which generates a shared secret that is utilized to encrypt the report through an ephemeral key exchange (Elliptic Curve Diffie-Hellmann (ECDH)). According to [25], “The finder’s encryption algorithm works as follows:

1. Generate a new ephemeral key  $(d', p')$  on the NIST P-224 curve for a received FindMy lost advertisement.
2. Perform ECDH using the ephemeral private key  $d'$  and the advertised public key  $p_i$  to generate a shared secret.
3. Derive a symmetric key with ANSI X.963  $KDF$  on the shared secret with the advertised public key as entropy and SHA-256 as the hash function.
4. Use the first 16 bytes as the encryption key  $e'$ .
5. Use the last 16 bytes as an initialization vector  $IV$ .
6. Encrypt the location report under  $e'$  and the  $IV$  with AES-GCM.

The ephemeral public key  $p'$  and the authentication tag of AES-GCM are part of the uploaded message. All location reports are identified by an id, which is a SHA-256 hash of  $p_i$ ,” as we can see in Figure 9.

**Decryption.** For decryption, the procedure implemented is the reverse of the encryption process. From [25], “An owner device that downloads encrypted location reports follows the inverse of the encryption procedure:

1. The owner device selects the proper advertisement keys  $(d_i, p_i)$  based on the hashed  $p_i$  of the location report.

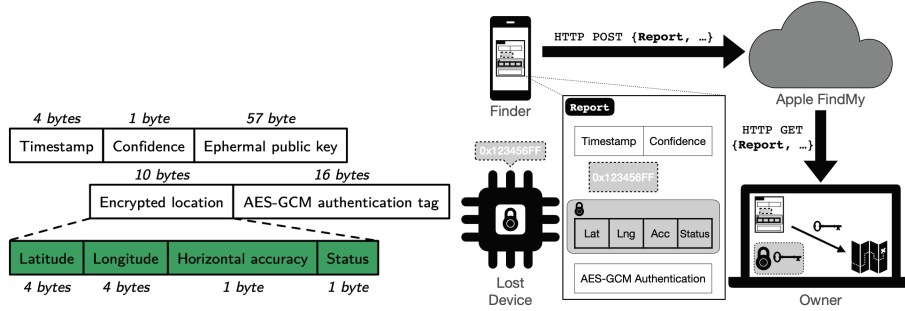


Figure 9: (a) Binary format of a location report (b) Example of sent payload (images from [25],[24]).

2. It performs the ECDH key exchange with the finder’s ephemeral public key  $p'$  and the lost device’s private key  $d_i$  to compute the symmetric key  $e'$  and the  $IV$ .
3. Now, the owner can use  $e'$  and  $IV$  to decrypt the location report.”

### 3.4 Support for non-Apple accessories

Following WWDC 2020, support for third-party accessories within the FindMy network was announced. Subsequently, Apple released the Find My Certification Assistant app on the App Store, enabling developers to test the FindMy network functionalities on accessories developed by external companies. According to [11], several companies have already signed agreements with Apple to be integrated into this service; these include Belkin (with the SoundForm Freedom), Chipolo (with the One Spot tag) and VanMoof (with the X3 and S3 bicycles). Additionally, Beats (owned by Apple) also supports the FindMy network with its latest products.

To verify if your product under development is compatible with the FindMy network, it is necessary to be enrolled in the Made for iPhone (MFi) program [5], which provides guidelines for creating electronic tools that can interface with Apple devices.

## 4 Useful applications

Some useful applications include the following:

- *Travel*: AirTags can be beneficial for travelers. They can attach AirTags to their luggage, making it easier to identify and track their bags during travel. As an example, for a tourist who has just landed from a trip and is eager to grab his bags, waiting at the carousel can be frustrating.

If his bags contain an AirTag inside, the owner can quickly check if the belongings are at the airport or somewhere else.

- *Pet Tracking:* While not explicitly designed for pets, some users have found AirTags useful for tracking their pets; by attaching an AirTag to a pet’s collar, owners can monitor their pet’s location and quickly locate them if they wander off. Some tests were conducted in [32] and, as we could expect, it seems that the AirTag doesn’t work quite well when in motion, for example, on a moving cat. In [54], they conducted a test trying to track a dog. As before, the experiment was delusional; they tried to simulate the dog using a plastic box that contained the AirTag and was dropped near a spot where dog walkers regularly walk past it every day. The test results were unsatisfactory because several hours passed before the AirTag’s location was updated; furthermore, there were no more updates after the initial alert.
- *Child Safety:* Similarly to pets, AirTags can provide an extra degree of protection for monitoring kids in busy or strange places. Parents can hide or attach an AirTag to their child’s clothing or belongings to track their real-time location and ensure there are no dangerous situations where the child gets lost or kidnapped. From [31]: “Ethical debates can arise regarding this issue, as experts have long been worried about the impact of more restrictive parenting on children’s mental health and development”. We will not go any deeper on this question since it is a technical report.
- *Vehicle Tracking:* AirTags can also be used to track vehicles, such as bicycles, motorcycles or cars, in the same way as the two above. An experiment was done in [35], comparing the following devices: Apple AirTag, Samsung SmartTag+, a GPS device with 4G compatibility, and BMW’s ConnectedDrive system. The aim was to determine the most cost-effective technology for object tracking. Table 4 compares the cost of the used options, data is taken from [35]. The testing route consists of a 45 km drive and includes four checkpoints; there is no LTE or cell service in close proximity of the last checkpoint. After going back to the starting point, the test ends by evaluating how well each gadget finds the parked automobile once it is in range and idly. The results were as assumed: both aftermarket and built-in GPS units were expected to function properly, transmitting accurate locations via cellular networks, facilitating easy vehicle tracking; however, their main drawback is their cost and the need for ongoing battery monitoring or charging to ensure continuous functionality. In terms of UWB, the AirTag has proven to be a cost-effective solution for vehicle tracking, although it does not have the same update frequency as GPS devices. Interestingly, it was found that the SmartTag+ has a higher update frequency compared to the AirTag.
- *People with Dementia Tracking:* Alzheimer’s patients and those suffering from other types of dementia may notice a reduction in their memory for



Table 4: Solutions cost comparison.

Device	Cost (\$AUD)
Apple AirTag	\$45
Samsung SmartTag+	\$60
GPS tracker with SIM card	\$147 + \$7 per month
BMW ConnectedDrive	From \$119 per year



Figure 10: Unremovable bracelet (image from [56]).

recognizing where they are, which can result in wandering and feelings of being lost or confused. AirTags can offer comfort in these situations and assist caretakers in making sure the person’s whereabouts are known; some bracelets have been developed to facilitate the use of them in this context. As we can see in Figure 10, the Unremovable Bracelet is used to track every movement and it takes two hands to open it, thus making it impossible for your loved ones to take it off.

- *Intrusion detector*: An innovative usage can be as an intrusion detector. In a scenario where it is needed to check whether anyone is near a specific remote cabin; if an AirTag is hidden somewhere near it and someone with an iPhone passes nearby, then a notification will be sent in minutes since the intruder’s device will forward to iCloud the AirTag position.
- *Wallet tracker*: This can be the most obvious application of this kind of device. A lot of wallets with built-in space for the AirTag were created, making it easier for the user to track their wallets.
- *Supermarket shelf localizer*: An interesting usage can be to act as a localizer inside a supermarket. In a scenario where an elderly person goes grocery shopping in a very large supermarket and gets lost inside, an application could be developed using Apple’s APIs to help locate all the shelves for the user, utilizing the precision finding offered by UWB. In the future, integrated tablets could be available on shopping carts, allowing users to locate shelves using navigation (Precision Finding) provided in FindMy.

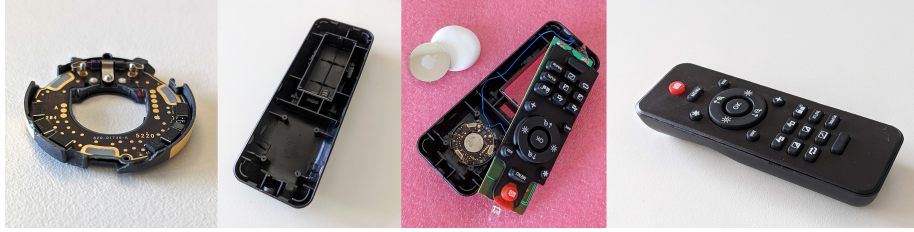


Figure 11: AirTag inside a remote control (images from [12]).

#### 4.1 Mods

After some Internet research, the author discovered that the AirTag has been modified in certain ways. For instance, in [13] A. Catley has attached the AirTag to a remote controller and is powering the AirTag components using the host's battery. This could be very useful in situations in which the remote controller gets lost in the house; thanks to Precision Finding, the owner can find it easily. Figure 11 shows the final result.

### 5 Conclusion

In conclusion, the paper provided a comprehensive exploration of various technological aspects. The AirTag technology and FindMy architecture offer a smart solution to address the tracking issue by intelligently utilizing the network of Apple devices worldwide, all at a much lower price compared to competitors. Other technologies also utilize the same principle, but AirTag's strength lies in the Apple device network present worldwide. Currently, according to [34], Apple holds 29.27% of the smartphone market share; this explains why the service performs so well. There are numerous possibilities for the future, some of which have been discussed in Section 4. One potential future development of this technology could involve integrating it into everyday tools to add precision tracking capabilities; for instance, integrating FindMy into shopping carts in supermarkets to locate shelves. In the future, this technology can only improve as the network of Apple devices supporting both FindMy and Precision Finding continues to grow with the purchase of new iPhones (which now integrate the UWB chip). Security-wise, vulnerabilities highlighted in Section 2.6.1 need to be addressed, as user privacy is paramount and a company like Apple cannot afford to ignore the issue.

### References

- [1] en-US. Sept. 2022. URL: <https://resources.pcb.cadence.com/blog/2022-transmission-rate-vs-bandwidth-in-bluetooth-technology>.

- [2] en. May 2024. URL: <https://www.bloomberg.com/news/newsletters/2024-05-19/what-is-apple-doing-in-ai-summaries-cloud-and-on-device-llms-openai-deal-lwdj5pkz>.
- [3] en. URL: [https://csrc.nist.gov/CSRC/media/Events/Key-Management-Workshop-2000/documents/x963\\_overview.pdf](https://csrc.nist.gov/CSRC/media/Events/Key-Management-Workshop-2000/documents/x963_overview.pdf).
- [4] en. URL: <https://www.analog.com/en/resources/glossary/time-of-flight.html>.
- [5] en-US. URL: <https://mfi.apple.com/>.
- [6] Daniele Antonioli et al. “Bluetooth: Exploiting cross-transport key derivation in bluetooth classic and bluetooth low energy”. In: *Proceedings of the 2022 ACM on Asia conference on computer and communications security*. 2022, pp. 196–207.
- [7] Apple. *Apple Platform Security*. en. May 2022. URL: <https://support.apple.com/en-gb/guide/security/welcome/web>.
- [8] Apple. *iCloud+ - Find my*. en-US. URL: <https://www.apple.com/icloud/find-my/>.
- [9] *Apple accidentally confirms the existence of an unreleased product, AirTags*. Apr. 2020. URL: [https://techcrunch.com/2020/04/02/apple-accidentally-confirms-the-existence-of-an-unreleased-product-airtags/?guccounter=1&guce\\_referrer=aHR0cHM6Ly91bi53aWtpcGVkaWEub3JnLw&guce\\_referrer\\_sig=AQAAAFwBYOWxztTVLDOZqfDxI7FEfhMGWanPQAJHHzQDGUmDVInr-WTC670Gr5Q7TJ56qCGlfDdFY52gyoFpCgnF6-91AuKJxdf9uj0hjEl1mmsdH6WhFdKMCr\\_8WEguBRSNHKV3tDMYbJa9gxPiZ3pTW21wTCFf4rfQHRQXhHCCiQg](https://techcrunch.com/2020/04/02/apple-accidentally-confirms-the-existence-of-an-unreleased-product-airtags/?guccounter=1&guce_referrer=aHR0cHM6Ly91bi53aWtpcGVkaWEub3JnLw&guce_referrer_sig=AQAAAFwBYOWxztTVLDOZqfDxI7FEfhMGWanPQAJHHzQDGUmDVInr-WTC670Gr5Q7TJ56qCGlfDdFY52gyoFpCgnF6-91AuKJxdf9uj0hjEl1mmsdH6WhFdKMCr_8WEguBRSNHKV3tDMYbJa9gxPiZ3pTW21wTCFf4rfQHRQXhHCCiQg).
- [10] *Bluetooth VS Bluetooth Low Energy: A Detailed Comparison*. en. URL: <https://www.mokosmart.com/bluetooth-vs-bluetooth-low-energy-a-detailed-comparison/>.
- [11] Tucker Bowe. *All the Non-Apple Gadgets the “Find My” App Can Find*. en-US. Aug. 2022. URL: <https://www.gearpatrol.com/tech/g36063168/apple-find-my-compatible-gadgets/#:~:text=Your%20iPhone's%20Find%20My%20now,Check%20'em%20out%20here.&text=In%20April%202021%2C%20Apple%20officially,Apple%20devices%20%E2%80%94%20no%20AirTag%20required..>
- [12] Adam Catley. *Apple AirTag Reverse Engineering - Adam Catley*. en. URL: <https://adamcatley.com/AirTag.html#pcb-overview>.
- [13] Adam Catley. *Tweet by Adam Catley*. May 2021. URL: <https://twitter.com/adamcatley/status/1393171134489808896>.
- [14] Juli Clover. “Find my App: Everything to Know”. en-US. In: *MacRumors* (Feb. 2022). URL: <https://www.macrumors.com/guide/find-my/>.
- [15] *Comparison of Bluetooth BR/EDR and Bluetooth LE specifications*. it. URL: <https://it.mathworks.com/help/bluetooth/gs/comparison-of-bluetooth-bredr-and-bluetooth-le.html>.

- [16] Encstore. *BLE vs UWB: What Are the Differences*. s.d. URL: <https://www.encstore.com/blog/5524-ble-vs-uwb-what-are-the-differences>.
- [17] Chad Figueroa. *What does antenna diversity do?* Durrell2012.com. en-US. Sept. 2022. URL: <https://durrell2012.com/what-does-antenna-diversity-do/>.
- [18] Jaron Fontaine et al. “Edge Inference for UWB Ranging Error Correction Using Autoencoders”. In: *IEEE Access* 8 (Jan. 2020), pp. 1–1. DOI: [10.1109/ACCESS.2020.3012822](https://doi.org/10.1109/ACCESS.2020.3012822).
- [19] James H. Foster, Marlene Nilsen, and Paul G. Puskarich. *Multi-Interface Transponder Device - Power Management*. Aug. 2020.
- [20] Andy G. *Different Bluetooth versions: what you need to know*. en-US. May 2023. URL: <https://www.headphonesty.com/2021/01/bluetooth-versions/>.
- [21] Henri Gilbert and Helena Handschuh. “Security analysis of SHA-256 and sisters”. In: *International workshop on selected areas in cryptography*. Springer. 2003, pp. 175–193.
- [22] Deb Spitler Hid Global. *Applying Ultra-Wideband wireless technology for security and automation*. en-US. Nov. 2020. URL: <https://www.securityindustry.org/2020/11/17/applying-ultra-wideband-wireless-technology-for-security-and-automation/>.
- [23] C.T. Hager and S.F. Midkiff. “An analysis of Bluetooth security vulnerabilities”. In: *2003 IEEE Wireless Communications and Networking, 2003. WCNC 2003*. Vol. 3. 2003, 1825–1831 vol.3. DOI: [10.1109/WCNC.2003.1200664](https://doi.org/10.1109/WCNC.2003.1200664).
- [24] Alexander Heinrich, Niklas Bittner, and Matthias Hollick. “AirGuard-protecting android users from stalking attacks by apple find my devices”. In: *Proceedings of the 15th ACM Conference on Security and Privacy in Wireless and Mobile Networks*. 2022, pp. 26–38.
- [25] Alexander Heinrich et al. “Who Can Find My Devices? Security and Privacy of Apple’s Crowd-Sourced Bluetooth Location Tracking System”. In: *CoRR* abs/2103.02282 (2021). arXiv: [2103.02282](https://arxiv.org/abs/2103.02282). URL: <https://arxiv.org/abs/2103.02282>.
- [26] *How a voltage glitch attack could cripple your SoC or MCU - and how to securely protect it*. en. URL: <https://www.design-reuse.com/articles/48553/how-a-voltage-glitch-attack-could-cripple-your-soc-or-mcu.html>.
- [27] Inpixon. *Time Difference of Arrival (TDOA) multilateration — INPIXON*. en. URL: <https://www.inpixon.com/technology/standards/time-difference-of-arrival>.

- [28] Mahmoud Itani. *How are iPhones still findable even when turned off*. en. Oct. 2021. URL: <https://www.xda-developers.com/iphone-findable-turned-off/#:~:text=Most%20time%2C%20U1%20is%20on,the%20connected%20device%20via%20Bluetooth..>
- [29] Eirini Karapistoli et al. “An overview of the IEEE 802.15.4a Standard”. In: *IEEE Communications Magazine* 48.1 (2010), pp. 47–53. DOI: [10.1109/MCOM.2010.5394030](https://doi.org/10.1109/MCOM.2010.5394030).
- [30] Emilia Käsper and Peter Schwabe. “Faster and timing-attack resistant AES-GCM”. In: *International Workshop on Cryptographic Hardware and Embedded Systems*. Springer. 2009, pp. 1–17.
- [31] Heather Kelly. “Parents are using AirTags to track kids and give them freedom”. en. In: *Washington Post* (Aug. 2023). URL: <https://www.washingtonpost.com/technology/2023/07/26/tracking-kids-airtags/>.
- [32] Emily - KittyCatGO. *The Apple AirTag for Cats: A pet tracking review*. en-US. Mar. 2024. URL: <https://kittycatgo.com/the-apple-airtag-for-cats-a-pet-tracking-review/>.
- [33] Anurag Kumar. “Apple AirTags made \$1 Billion revenue - Medium”. en. In: *Medium* (June 2023). URL: <https://anurag-iim.medium.com/2022-apple-airtags-made-1-billion-revenue-88880a31b752>.
- [34] Ying Lin. *Smartphone Market Share Worldwide [Feb 2024 Update]*. en-US. URL: <https://www.oberlo.com/statistics/smartphone-market-share>.
- [35] Paul Maric. “How to keep track of your car with these cheap devices: AirTag v SmartTag+ v GPS — CarExpert”. enAU. In: *CarExpert* (Mar. 2023). URL: <https://www.carexpert.com.au/car-comparisons/stolen-car-these-cheap-devices-will-track-it-airtag-smarttag-and-gps-tracker>.
- [36] Benjamin Mayo. *iOS 15: Find My network can still find your iPhone when it is powered off, or factory reset - 9to5Mac*. en-US. June 2021. URL: <https://9to5mac.com/2021/06/07/ios-15-find-my-network-can-find-your-iphone-when-it-is-powered-off/>.
- [37] Victor S Miller. “Use of elliptic curves in cryptography”. In: *Conference on the theory and application of cryptographic techniques*. Springer. 1985, pp. 417–426.
- [38] Dan Moren. *The Fine Print on Apple’s AirTags*. Apr. 2021. URL: <https://daringfireball.net/linked/2021/04/20/moren-fine-print>.
- [39] Ghidra Ninja. *Tweet by Ghidra Ninja*. May 2021. URL: <https://twitter.com/ghidraninja/status/1390619216823390208>.
- [40] Britta O’Boyle. *What is Precision Finding on AirTags and how does it work?* en. Nov. 2021. URL: <https://www.pocket-lint.com/phones/news/apple/156605-what-is-precision-finding-on-apple-airtags-and-how-does-it-work/>.

- [41] Nicolas Oberli. *SWD - ARM's alternative to JTAG*. en. May 2019. URL: <https://research.kudelskisecurity.com/2019/05/16/swd-arms-alternative-to-jtag/>.
- [42] Ryan C. Perkins, Jong Erik G. De, and Tirshathah A. Hunter. *FAS-TENER WITH A CONSTRAINED RETENTION RING*. Oct. 2020.
- [43] Ryan C. Perkins and Paul J. Thompson. *Mounting base for a wirelessly locatable tag*. May 2023.
- [44] Ryan C. Perkins et al. *ANTENNA ASSEMBLY FOR A WIRELESSLY LOCATABLE TAG*. Jan. 2022.
- [45] Ryan C. Perkins et al. *WIRELESSLY LOCATABLE TAG*. Mar. 2022.
- [46] Jake Peterson. *20 surprisingly practical uses for Apple AirTags*. en. Dec. 2022. URL: <https://ios.gadgethacks.com/how-to/20-surprisingly-practical-uses-for-apple-airtags-0384571/>.
- [47] Paul G. Puskarich. *Tracking Systems with Electronic Devices and Tags*. Feb. 2024.
- [48] Guilherme Rambo. *Apple revamping Find My Friends & Find My iPhone in unified app, developing Tile-like personal item tracking - 9to5Mac*. en-US. Aug. 2019. URL: <https://9to5mac.com/2019/04/17/find-my-iphone-revamp/>.
- [49] Apple Inc. All rights reserved. *MFfi Program - create accessories that communicate with Apple devices using MFfi technologies and components*. en. 2023. URL: <https://mfi.apple.com/>.
- [50] Limited Results. *nRF52 Debug Resurrection: Approtect Bypass*. June 2020. URL: <https://limitedresults.com/2020/06/nrf52-debug-resurrection-approtect-bypass/>.
- [51] Nordic Semiconductor. *Nordic Semiconductor Infocenter*. s.d. URL: [https://infocenter.nordicsemi.com/index.jsp?topic=%2Fps\\_nrf52833%2Fdif.html&anchor=concept\\_udr\\_mns\\_1s](https://infocenter.nordicsemi.com/index.jsp?topic=%2Fps_nrf52833%2Fdif.html&anchor=concept_udr_mns_1s).
- [52] Narmeen Shafqat et al. "Track you: A deep dive into safety alerts for apple airtags". In: *Proceedings on Privacy Enhancing Technologies* (2023).
- [53] Milan Simek. *Two Way Ranging (TWR) - SeWiO RTLS*. en-US. Jan. 2024. URL: <https://www.sewio.net/ubw-technology/two-way-ranging/>.
- [54] Src. *Can I use an AirTag to track my dog?* en-GB. Mar. 2024. URL: <https://www.pitpat.com/doggy-products/can-i-use-an-airtag-to-track-my-dog/>.
- [55] Macworld staff. "Apple AirTags rumors: iOS 14.5 can track 'Items' in the Find My app". en. In: *Macworld* (2021). URL: <https://www.macworld.com/article/234037/apple-airtags-bluetooth-track-find-my-ultrawide-band-uf-keychain-locate-lost-items.html>.

- [56] *Unremovable AirTag® bracelets*. en. URL: <https://www.medicalidfashions.com/Unremovable%20AirTag%20Bracelets>.
- [57] Juha T Vainio et al. “Bluetooth security”. In: *Proceedings of Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory, Seminar on Internetworking: Ad Hoc Networking, Spring*. Vol. 5. 2000.
- [58] Ramish Zafar. “iPhone 11’s U1 Chip Uses 6Hz & 8GHz Frequencies In UWB Spectrum”. en-US. In: *Wccftech* (Nov. 2019). URL: <https://wccftech.com/iphone-11-u1-chip-uw/>.
- [59] Christian Zibreg and Christian Zibreg. “How to add third-party accessories to Apple’s Find My app to keep track of them”. en-US. In: *iDownloadBlog.com* (Apr. 2021). URL: <https://www.idownloadblog.com/2021/04/09/add-third-party-find-my-accessories-tutorial/>.