E-GUIDE

Ultra-Wideband & CCC® Digital Key:

Automobile Security & Convenience

What's Inside

- Ultra-Wideband (UWB) technology overview
- How UWB improves vehicle and pedestrian safety
- Vehicle and user security when using UWB
- Emerging applications of UWB in automotive

Written By:

Kerry Glover

Systems Architect

Introduction

Technology is continually being used to improve our daily lives. For a technology to be truly beneficial, it must be simple, secure, reliable and trustworthy. RF technology is one area where all of these benefits have been achieved.

For example, Wi-Fi has become ubiquitous in every household and every business. Cellular has produced a plethora of new capabilities making the mobile smartphone an indispensable device globally. Bluetooth® is making wireless connectivity for devices such as digital speakers and headphones simple to use on the Internet of Things (IoT) ecosystem.

UWB is another new RF technology that can add benefit to our daily lives. It has one feature not found in any other RF technology: the ability to measure distance between two points with pin-point accuracy. This point-to-point ranging technology can be used in many ways to improve our daily lives. This guide explores how UWB can make interactions with an automobile more convenient, safe and trustworthy.

DOWNLOAD

Our UWB For Dummies eBook

The CCC and Digital Key

Did you know that your car's key-fob can be spoofed? Luckily, there are technical leaders working to prevent this from happening. Digital Key is a new specification by the **Car Connectivity Consortium (CCC)** to standardize how a vehicle can be automatically unlocked as the driver approaches. To prevent illegal access to the vehicle the identity and proximity of the user must be verified. The Digital Key standard calculates the distance to the driver using UWB to ensure that the user is within a few meters of the car. By including a secure distance measurement, the unlock procedure is much more secure and can occur without the user removing their smartphone from their pocket. The reverse would also be true as the person exits the vehicle; the vehicle would automatically lock. The same procedure is also used to secure engine start.

In Digital Key, Bluetooth Low Energy is used for the high-level communication protocol between the vehicle and the driver's smartphone. The process starts as soon as Bluetooth Low Energy is linked with the vehicle. Bluetooth Low Energy will then start to execute the Digital Key messaging. These stacks will then exchange the Digital Key ID using public keys and verify the user has a valid ID. Next, the system will initialize the UWB transceivers, telling each the assigned time to transmit their Scrambled Timestamp Sequence (STS) signal. After all transmissions are complete, the distance will be calculated. This process will be repeated until the user enters or leaves the vehicle.

Car Connectivity Consortium® (CCC)

The CCC is a cross-industry standards organization with a mission to create sustainable and flexible ecosystems that standardize interface technologies to provide consistently great user experiences across all vehicles and mobile devices.

The CCC member companies consist of smartphone and vehicle manufacturers, automotive Tier 1s, integrated circuit vendors, security product suppliers, and more.

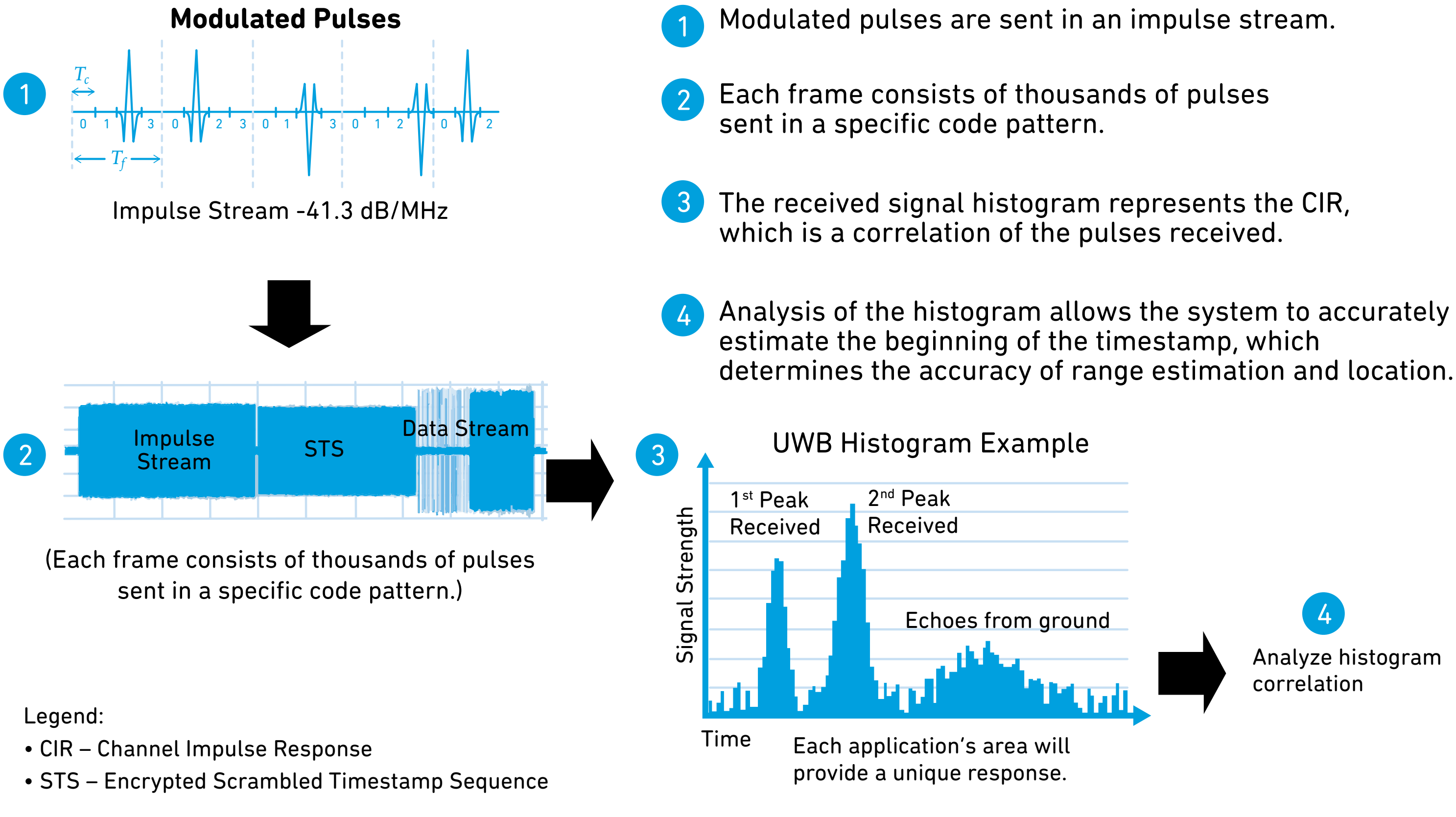
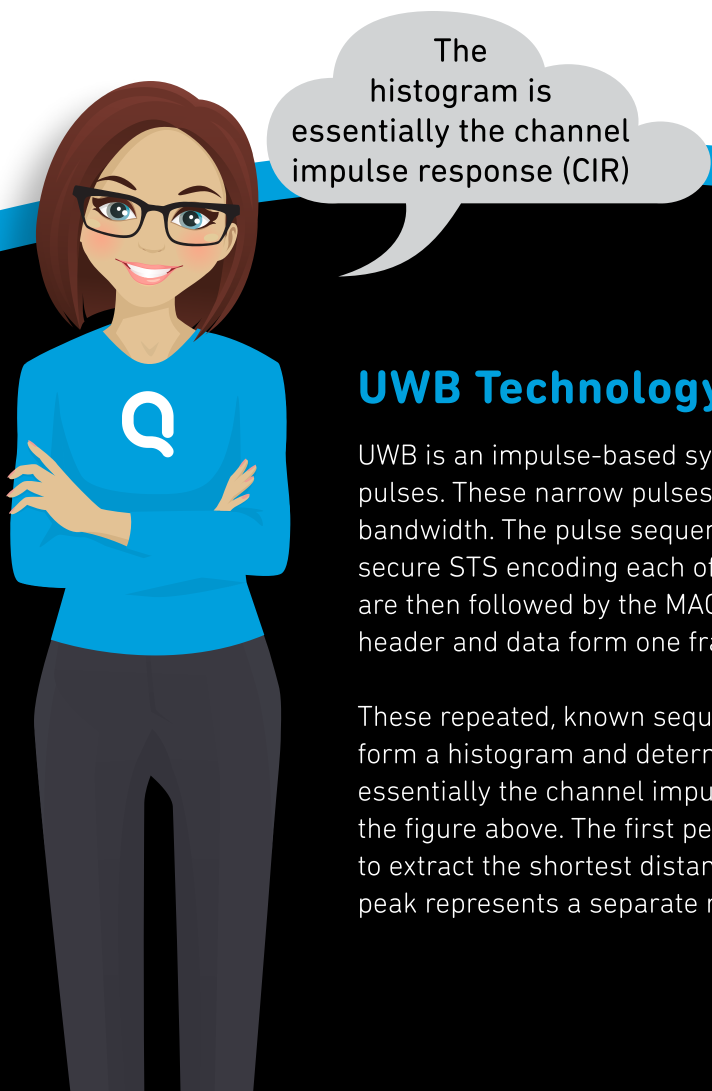


Figure 1. UWB pulsed radio system response.



UWB Technology Overview

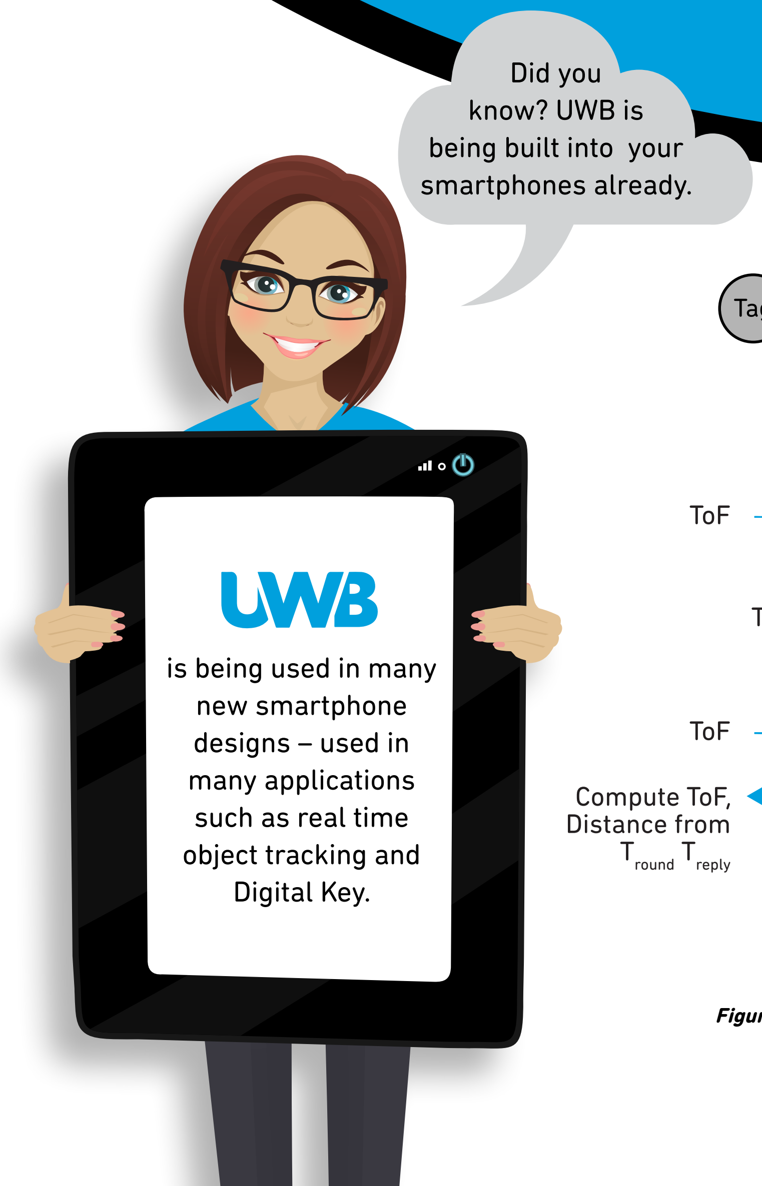
UWB is an impulse-based system that uses a series of very narrow 2 nanosecond pulses. These narrow pulses are encoded and spread so they occupy a 500 MHz bandwidth. The pulse sequences are encoded using IPATOV and pseudo-random secure STS encoding each of which are repeated many times. The header and STS are then followed by the MAC header and data. This sequence of header, STS, MAC header and data form one frame.

These repeated, known sequences allows the receiver to use auto-correlation to form a histogram and determine the exact time of reception. The histogram is essentially the channel impulse response (CIR) of the received signal as shown in the figure above. The first peak represents the line-of-sight path and can be used to extract the shortest distance between transmitter and receiver. Each subsequent peak represents a separate reflection from a surface in the environment.

UWB Two-Way Ranging

Two-way ranging (TWR) is the method to determine the distance between two UWB transceivers. With TWR, each transceiver takes a turn in transmitting the STS. In addition to the STS information, the exact time of transmission and the exact time of reception can be communicated over the data link, which are encrypted with evolving secure keys derived from the initial session key. After this information is received twice, the time of flight can be calculated and translated into distance. In addition, having received the information from two measurements, any error caused by clock mis-synchronization and variation can be removed.

In Digital Key, two-way ranging is a one-to-many protocol, meaning the transceiver in the UWB enabled smartphone or key-fob transmits a signal which is received by many receivers referred to as UWB anchors. During the reply portion of the protocol, each of the UWB anchors on the vehicle will take turns in replying. As a final step, the smartphone or key-fob transmits back the time the STS arrived from each sensor on the vehicle. The UWB sensors in the vehicle can then calculate that exact distance to the smartphone or key-fob. Ultimately the more sensors in and around the vehicle, the more accurate the location measurement.



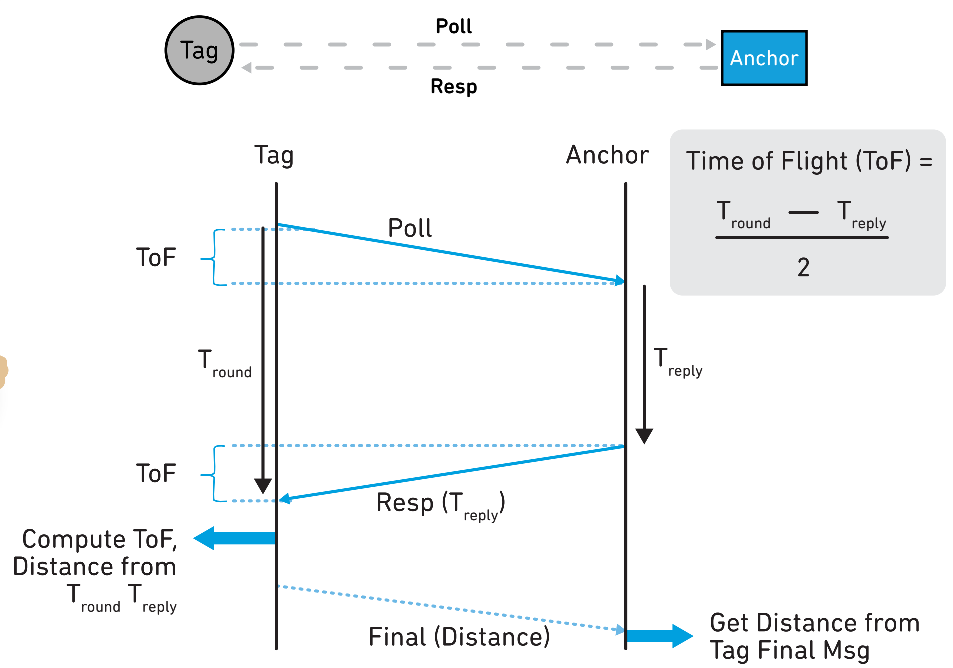


Figure 2. *Secure two-way ranging between UWB tag and anchor.*

Secure Distance Measurement

UWB ranging includes a security feature designed to ensure that no third party can spoof the transmission and create an incorrect distance measurement. The message format includes an STS, which employs pseudo-random sequences and cryptographic techniques to protect the integrity of the timestamp data generated within each frame. This generation process relies upon the secure Advanced Encryption Standard (AES) protocol. AES is a symmetric block cipher or deterministic algorithm chosen to protect information. The initial timestamp data packets for the STS are generated using a secure element and derived from secure sources. During the initialization process, both ends of the link securely exchange these codes. This can be performed utilizing private and public keys from each end of the link to encrypt and exchange the initial STS key. After initialization, a complex algorithm is used to change this STS code after every transmission. For more details see the **IEEE 802.15.4z-2020 specification**.

Additionally, this session key can be shared with several UWB transceivers, encrypted of course, and allows those devices and only those devices to correctly receive the transmission.

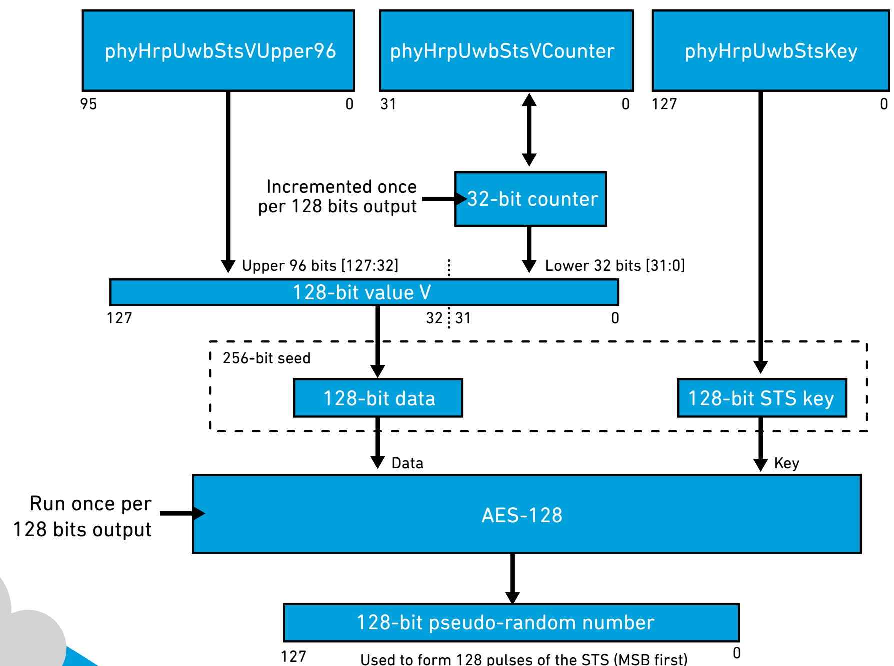


Figure 3. *Deterministic random bit generator (DRBG) for STS.*

Vehicle security and safety are always top-of-mind for automotive manufacturers, sellers and customers. Safety and security save lives! Implementing UWB technology in vehicles can achieve these goals while adding convenience and efficiency.

Digital Key Security and Exchange

The Digital Key specification provides the methodology for private and public key management. OEMs manage the Digital Key root certification while local dealerships provide Digital Key intermediate certification and issue the Digital Key product certification. Digital Key also allows for several additional mechanisms in situations such as a lost key, the sale of a vehicle, valet parking, key sharing, etc. With key sharing, you can issue a secondary key which will allow limited access to your vehicle. These limitations can include time limits for when the vehicle can be operated.

Digital Key uses Bluetooth as the primary data communications system to exchange information between the vehicle and the smartphone or key-fob. As a part of this process, the Bluetooth exchange must communicate the initial UWB STS seed. This is done using private and public key cybersecurity protocols. The public key is shared between both ends of the link and used to encode information. This can also be used to encode the data in the UWB payload. After the information is exchanged, the system can decode the digital key using the private key. In addition, the private key could be used to digitally sign a message to ensure no one has attempted to modify the data.

Digital Key Security Exchange Overview

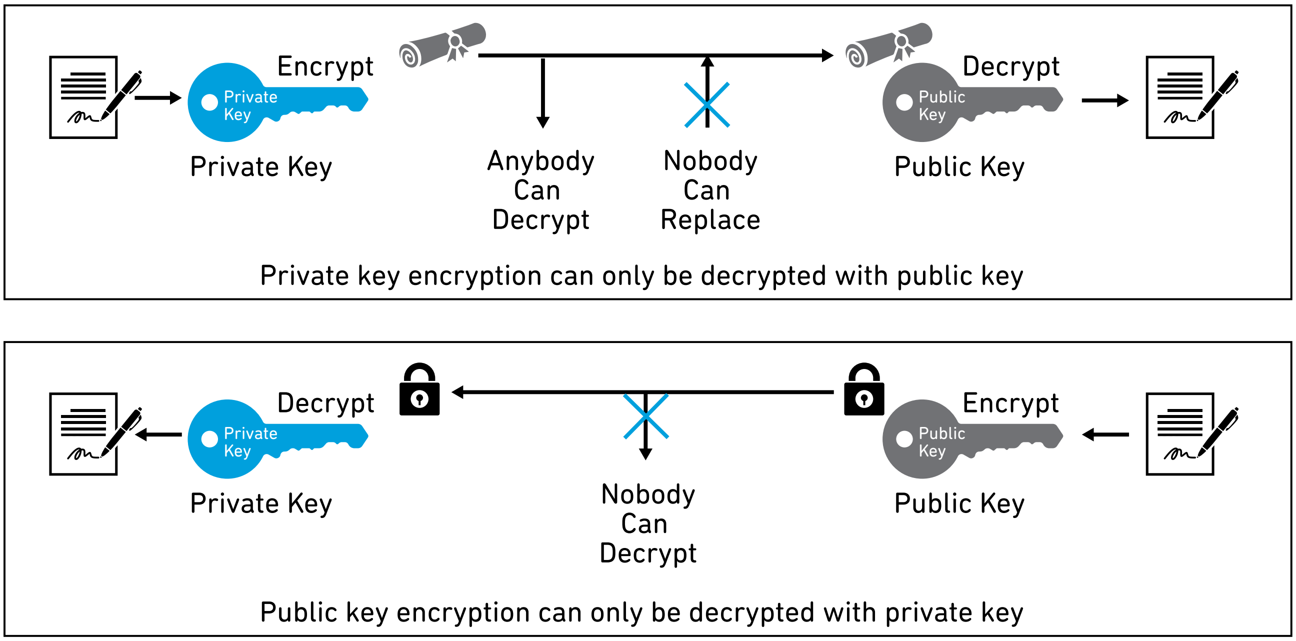


Figure 4. *Digital Key security and exchange process.*

Digital Key Physical Layout – Simple Scenario

Initially, Digital Key was a simple method of using a person's smartphone to create a link, using Bluetooth, between the smartphone and the Bluetooth located on or inside the user vehicle. This approach provided the needed functionality and convenience to allow a person to unlock a vehicle as they approached. However, it was soon found this method had several shortcomings such as the relay attack where a person's information could be snooped and relayed to the vehicle over a remote RF link.

This problem was solved by adding a UWB element into the mix with its secure distance measurement. Now, in addition to the Bluetooth exchanging Digital Key information, it also provided for a secure UWB distance measurement to ensure the person was at an expected distance from the vehicle before unlocking. The UWB secure ranging provides the added protection to ensure a thief cannot spoof, relay attack or otherwise fool the Digital Key signal.

This UWB distance measurement forms a "security bubble" around the vehicle, which allows the vehicle to unlock only if the smartphone is within that bubble. The level of security used is like a credit card used in secure financial transactions, meaning it must be physically present for the transaction to occur.

The simplest implementation would have a single UWB device on the vehicle measuring the distance to the cell phone. Although the distance measurement is highly accurate in this scenario, the direction is unknown. Therefore, the vehicle does not know if the smartphone is approaching from the driver side, passenger side, in front or behind the vehicle. Having only one transceiver sensor on the vehicle limits the ability of accurately showing what direction the drivers smartphone is from the vehicle. We address how to resolve this limitation in the next section.

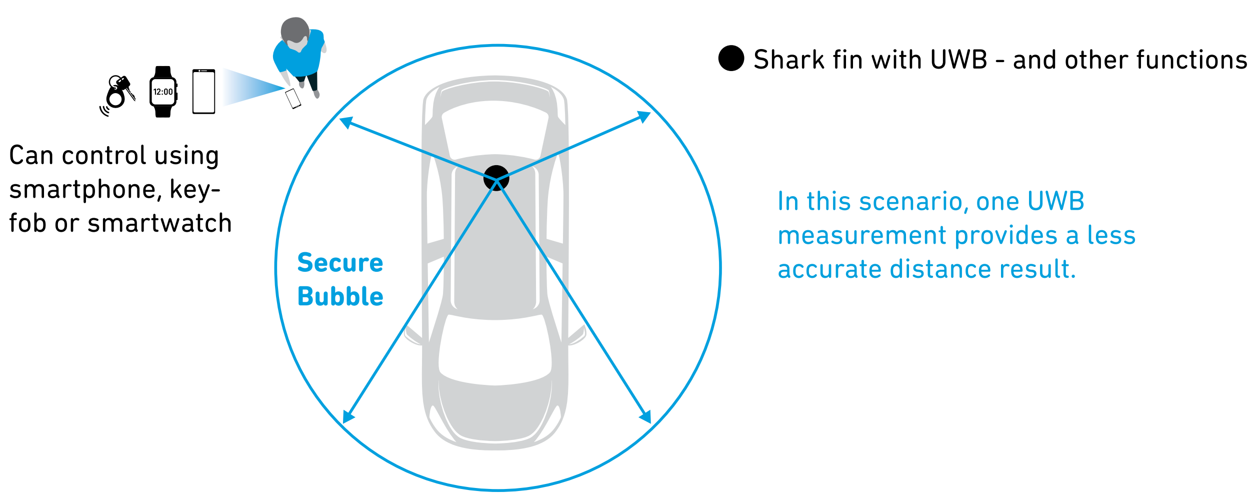


Figure 5. *Digital Key with single UWB sensor in shark fin calculating distance only.*

Digital Key Physical Layout – Robust Scenario

The previous example used a single UWB sensor to sense the distance to the vehicle owner/operator. This provides a low-cost solution. A more robust implementation would use several UWB sensors on the outside of the vehicle to accurately measure the distance to the driver's smartphone. Because the sensors are located in the outer body of the vehicle in several locations, the path loss is lower, allowing UWB to measure longer distances. In addition, the use of multiple external sensors makes it possible to accurately determine the driver's location relative to the vehicle.

In this application, the vehicle is responsible for locking/unlocking the vehicle and therefore calculates the distance. As the driver approaches, the vehicle will unlock the passenger's door, driver's door or trunk depending on the driver's distance and direction.

Another UWB sensor is needed inside the vehicle to determine if the Digital Key (smartphone) is inside the vehicle. If no key is detected inside the vehicle, the vehicle would not be started. The UWB sensor inside the vehicle also leads to other possible used cases for this sensor such as occupancy detection.

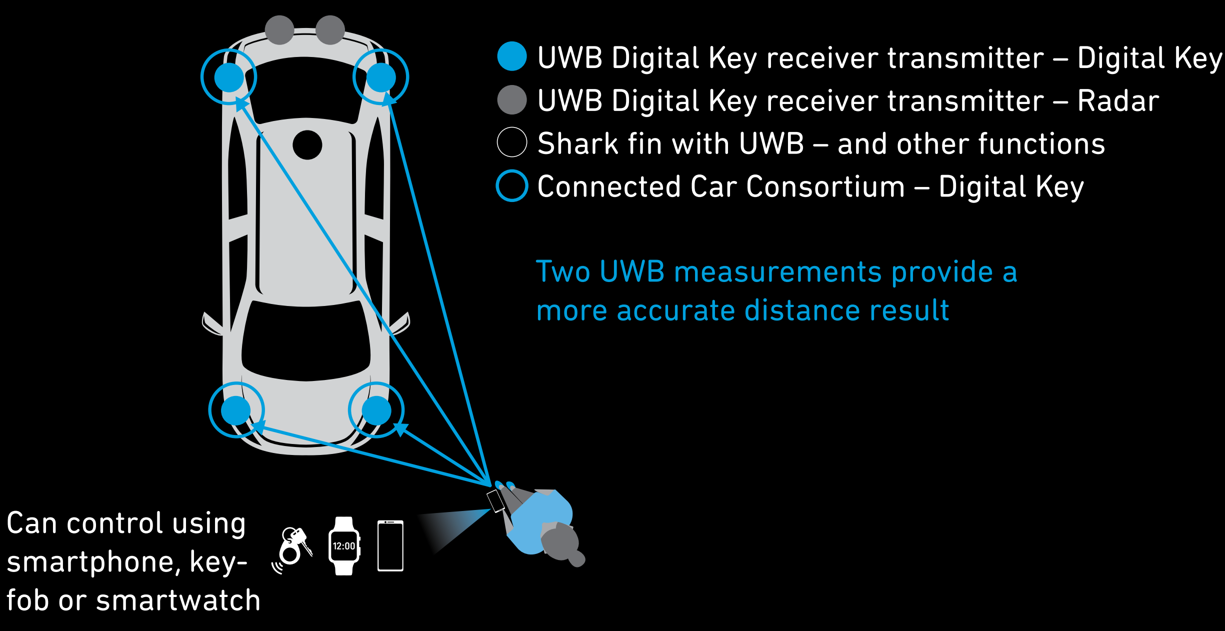


Figure 6. *Multiple UWB sensors with Digital Key – distance and direction.*

Future – UWB, Location and Distance Measurement

At first, the ability to accurately measure distance may not seem very important. However, upon deeper inspection, this is a fundamental need to enable many new automobile safety, security and convenience applications. One of the uses for low-cost, RF distance measurement is with security of physical assets. For these applications, a UWB transceiver can be installed in each device: the key and the asset.

With a physical asset, the key needs to be in the vicinity of the asset in order to unlock that asset such as a vehicle. UWB measures the physical distance between two points and therefore can ensure the key (user) is within a specific distance to the asset (vehicle) in question before unlocking the asset.

This has other benefits as well. As the user approaches the vehicle, the distance to the user could be divided into zones. When the user is beyond the zones, nothing will happen. As they approach zone 3 (see figure below), the vehicle flashers could blink. As they approach zone 2, the welcome lights could turn on. Finally, as they approach zone 1, the vehicle would unlock and could configure advanced features such as start the vehicle, set climate controls to the driver's desired settings, set infotainment preferences such as music/podcasts and other type of comfort control features.

Distance Measurement Zones

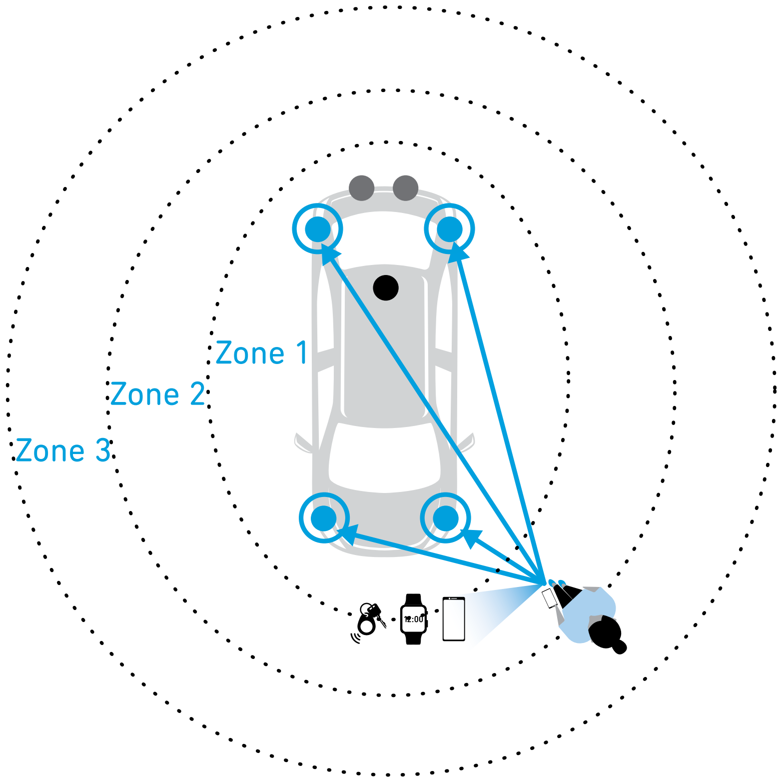


Figure 7. *UWB enabling individual distance measurement zones.*

Future – Passenger Pick-up Identification

Using UWB sensors in the vehicle and the passenger's smartphone, a vehicle can identify and locate the correct passenger to pick up. While Bluetooth Low Energy could be used to start the UWB sessions, another mechanism would be to use vehicle-to-pedestrian (V2P) protocols to set up the UWB link and start the distance measurement process. The vehicle can then determine the distance to the passenger and vice versa. With multiple sensors, the vehicle could pinpoint the passenger's location as well as the distance. For ride sharing services, this would allow a driver to locate a targeted fare in a crowd.

In this case, both the cell phone and the sensor would need to know the distance since both the passenger would need to identify the pickup vehicle and the vehicle would need to identify the passenger.

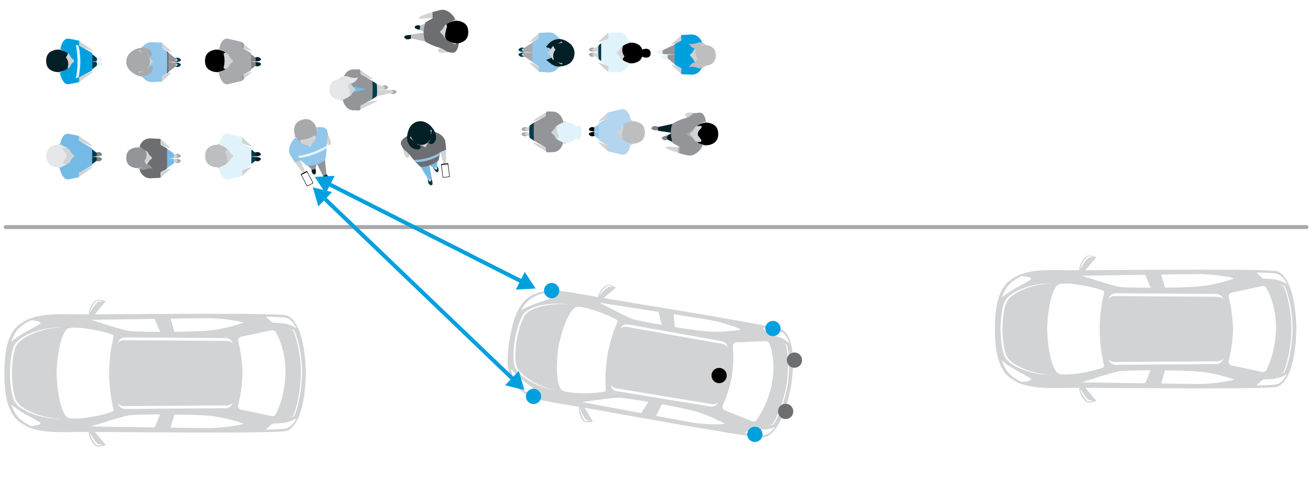


Figure 8. *Using UWB to identify a passenger to pick up.*

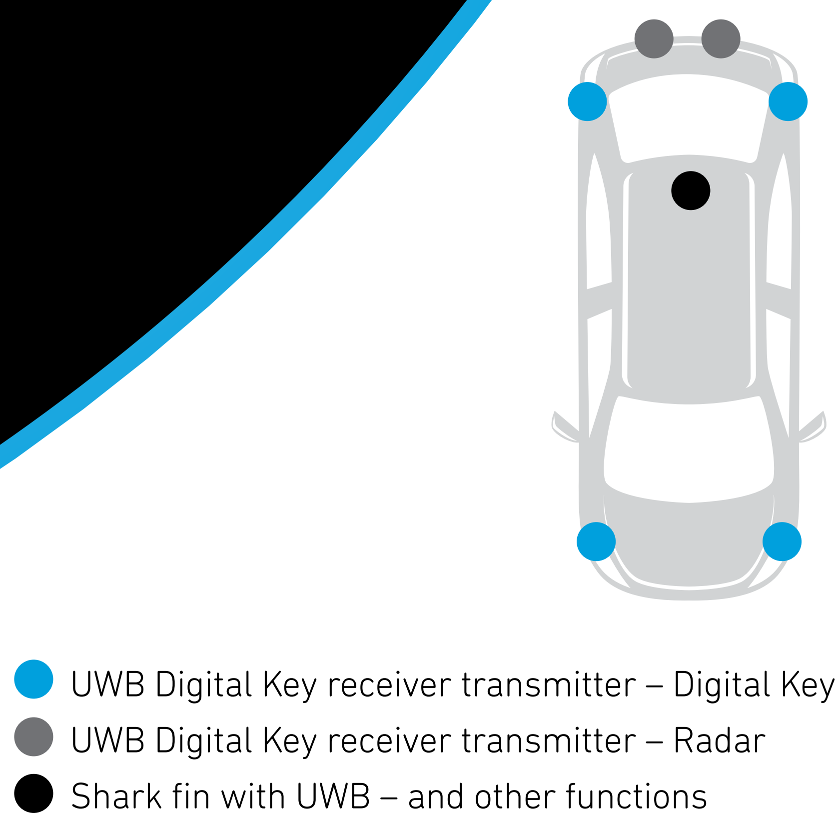
Digital Key provides key sharing where you can send/share your Digital Key information with another user who can then have access to your vehicle. This can be provided for a given time limit. In this scenario UWB can be used by the limited-user to identify the location of the vehicle in a crowded parking lot, as providing access to the vehicle.

Conclusion

UWB is becoming the new groundbreaking go-to technology for many applications like home automation, industrial 4.0, and now the automotive space. With automotive keyless entry and Digital Key as its springboard, it is being looked at for many more use cases and has the potential for enhancing and improving overall vehicle safety.

In this e-Guide we have only touched on emerging applications of UWB in the automotive space. In future papers we will explore new automotive applications for UWB and show how this technology will catapult UWB into many areas of vehicle safety and security as well as being a key enabler for several autonomous driving use cases. One of the great things about UWB is that it provides a low-cost, highly accurate point-to-point ranging sensor solution in automotive areas where important external location information would not be feasible. In addition, the use of UWB in conjunction with other vehicle technologies like vehicle to everything (V2X) can have many benefits such as preventing collisions.

It is predicted that 50% of all new vehicles will include Digital Key with UWB in the next few years, enhancing convenience and theft protection. This will provide a large installed base of UWB sensors in vehicles. It is important to understand the full variety of potential UWB applications in order to make an informed decision about the type of UWB system to implement in vehicles today. Wouldn't it be great if the functionality of the installed base could be extended from basic theft protection to life saving applications!



About Qorvo

Qorvo supplies innovative semiconductor solutions that make a better world possible. We combine product and technology leadership, systems-level expertise and global manufacturing scale to quickly solve our customers' most complex technical challenges. Qorvo serves diverse high-growth segments of large global markets, including consumer electronics, smart home/IoT, automotive, EVs, battery-powered appliances, network infrastructure, healthcare and aerospace/defense. Visit www.qorvo.com to learn how our diverse and innovative team is helping connect, protect and power our planet.

Visit **www.qorvo.com** to learn how Qorvo connects and powers the world.

About the Author

Dr. Kerry Glover is a System Engineer with a broad background in RF, analog and digital systems. Kerry has worked in advanced technologies, systems architectures, product definition, software development, business development and marketing throughout his career and has more than 20 patents. Kerry received his BS, MS and DE degrees in Electrical Engineering from Texas A&M University.