Application Note

Application of CC2755-Based Bluetooth Channel Sounding Technology in Smart Door Lock Keyless Entry Systems

Albin Zhang
Winnie Lee

Connectivity solution

ABSTRACT

This document was translated from a simplified Chinese source. (ZHCAG87)

This application note introduces how to implement a high-precision keyless entry system for smart door locks based on the TI SimpleLink™ CC2755 series wireless MCUs, utilizing the Channel Sounding feature in the Bluetooth 6.0 Core Specification. By combining Phase-Based Ranging (PBR) and Round-Trip Time (RTT) measurements, Channel Sounding technology can achieve centimeter-level distance measurement accuracy, offering a qualitative leap in precision, stability, and security compared to traditional RSSI ranging solutions. Compared to other unlocking methods, it significantly improves user experience and enables seamless, frictionless entry.

This paper articulates the key points, including application principles, implementation methods, and test results, of Channel Sounding technology in smart door locks. It also combines relevant TI products to provide users with system-level solutions and design guidance.

Table of Contents

List of Figures

List of Tables

1 Introduction

Throughout the evolution of the smart door lock industry, a "safer, more reliable, and more frictionless" unlocking experience has always been the core objective of technological advancement. The frictionless unlocking feature of traditional Bluetooth smart door locks typically uses the Received Signal Strength Indicator (RSSI) as the distance criterion, triggering the unlock logic via path loss calculations. However, RSSI signals fluctuate drastically due to factors such as walls, human body obstruction, and metallic reflections; its accuracy is usually on the order of several meters, making it difficult to accurately determine whether a user is truly approaching the door lock, and it carries security risks such as relay attacks.

The Channel Sounding feature introduced in the Bluetooth 6.0 specification fundamentally resolves this issue. No longer relying on signal strength, this feature calculates the physical distance between devices through precise measurements of phase changes and round-trip times of wireless signals, achieving centimeter-level ranging accuracy while integrating security mechanisms against relay attacks.

The TI SimpleLink™ CC2755 series devices are the industry's first wireless MCU product line to receive Bluetooth Channel Sounding certification and enter mass production; they support the Bluetooth® 6.0 specification and integrate an Algorithm Processing Unit (APU) and a Neural Processing Unit (NPU-CDE) dedicated to Channel Sounding post-processing, capable of running high-resolution ranging algorithms such as MUSIC and network models to handle post-processing in complex application scenarios like Line of Sight (LOS) and Non-Line of Sight (NLOS). Taking the smart door lock keyless entry application as the scenario, this paper introduces the system implementation solution based on the CC2755.

2 Profile of CC2755

The CC2755 series devices are an important component of the SimpleLink™ MCU platform; the series is divided into R/P versions based on different transmit powers and includes multiple package and memory configurations. This paper elaborates based on the CC2755R10, as shown in Figure 2-1. For details, please refer to Reference [1].

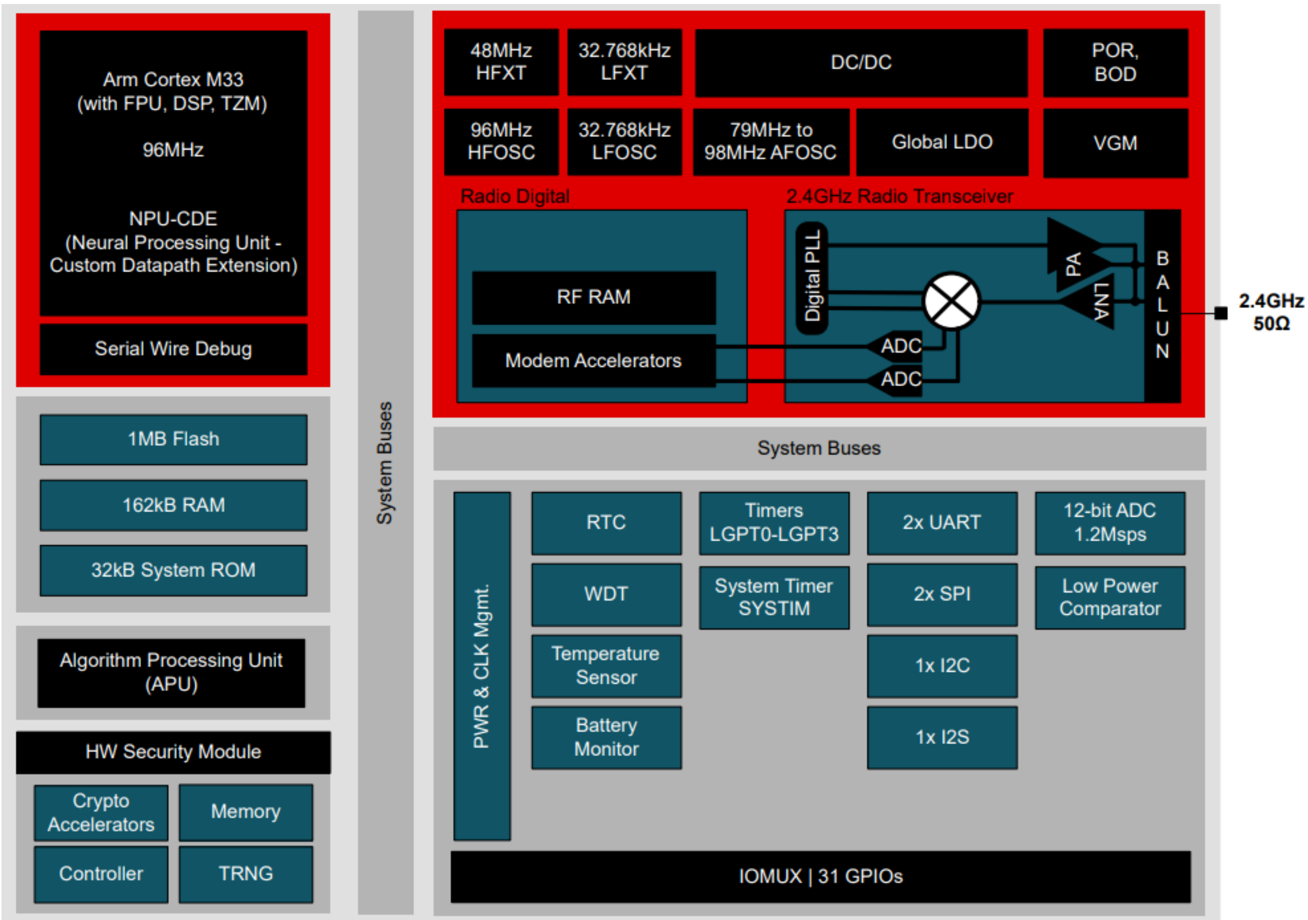


Figure 2-1. CC2755 Functional Block Diagram

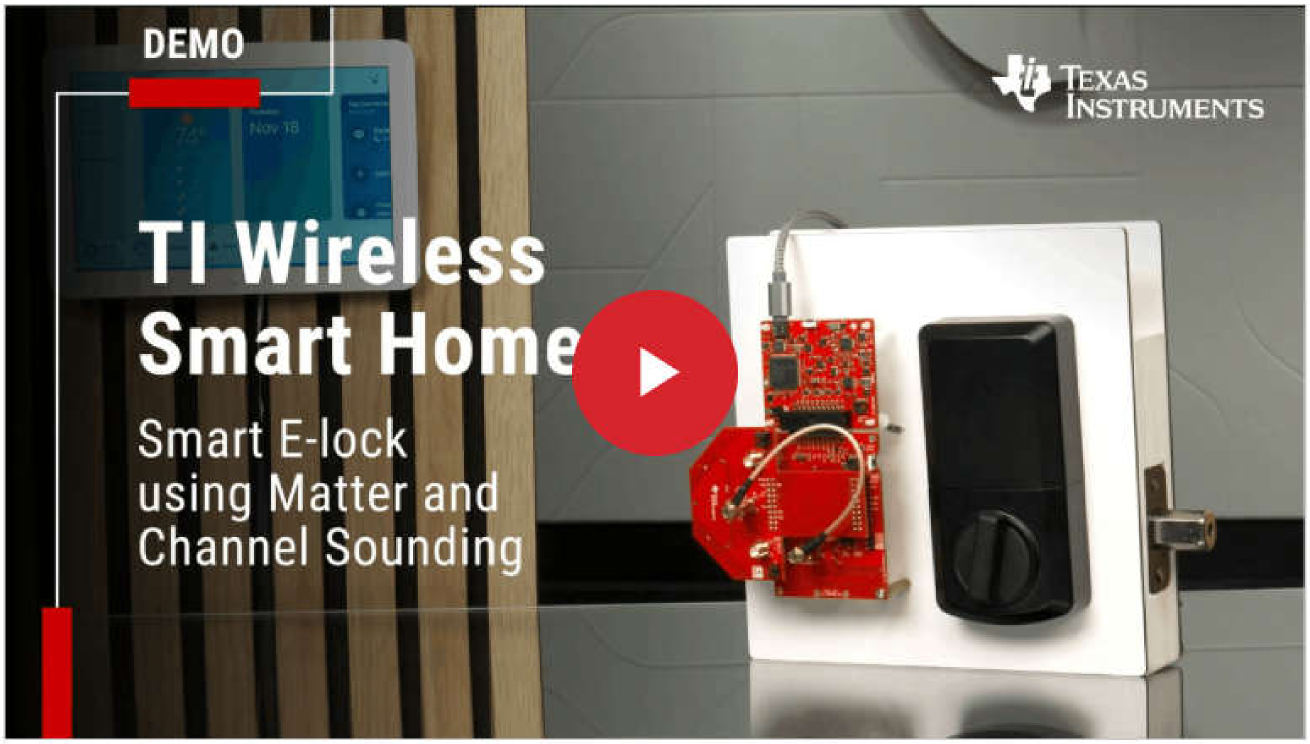
Its core features are as follows. In particular, it is equipped with a processor core that supports NPU-CDE and an Algorithm Processing Unit, which significantly accelerates the post-processing time of Channel Sounding and further reduces processing power consumption. Simultaneously, it can also support Edge AI operations; for details, refer to Reference [2].

- Processing Core: ARM® Cortex®-M33 processor supporting TrustZone®-M, FPU, and NPU-CDE for machine learning acceleration.
- Algorithm Processing Unit (APU): Dedicated mathematical accelerator (96MHz) supporting efficient vector and matrix operations, acting as the post-processor for Channel Sounding to run high-resolution ranging algorithms such as IFFT and MUSIC.
- Memory Resources: The CC2755R10 features 1MB of system programmable Flash, 162KB SRAM, and 32KB system ROM (including secure boot root of trust and serial bootloader).
- RF Performance: Integrated BALUN and RF switch, with a receiver sensitivity of -97dBm in 1Mbps mode and -103.5dBm in 125kbps Coded PHY mode. The R version provides an output power of up to +10dBm, and the P version provides an output power of up to +20dBm.
- Low Power Consumption: RX current of 6.1mA, TX current (at 0dBm) of 7.7mA, standby mode of 0.9μA (with RTC on and full SRAM retention), and shutdown mode of only 160nA.
- Security: Integrated HSM hardware security module, supporting AES-256, ECC-521, RSA-3072, and SHA-512 acceleration, true random number generator, etc.

- Peripherals: 23 GPIOs, 12-bit ADC, low-power comparator, 2×UART, 2×SPI, 1×I2C, 1×I2S, etc.

3 Demonstration of the TI Door Lock Solution

In the CC2755-based smart lock demonstration system showcased by TI at Embedded World 2025, the Channel Sounding technology achieved sub-50cm ranging accuracy, and the system maintained stable and reliable operation within a range of 30 to 40m. The multi-antenna design solution can achieve an accuracy of approximately 0.3m within 5m, and approximately 0.5m beyond 5m. Meanwhile, it also demonstrated the Matter over Thread solution, as well as the technology for keyword recognition utilizing Edge AI. This paper focuses on Channel Sounding technology. For Matter and Edge AI, please consult other relevant TI documentation.



Smart e-Lock with Matter over Thread and Channel Sounding support

Figure 3-1. CC2755-Based Smart Lock System

4 Overview of Channel Sounding Technology

4.1 Basic Principles

Channel Sounding is a method for estimating the distance between two devices connected via BLE. The two devices participating in ranging are referred to as the Initiator and the Reflector, respectively. The two devices complete distance measurement by exchanging synchronization information, ranging packets, and tone signals. This process defines multiple steps in the Bluetooth 6.0 specification:

- Mode 0 is used to exchange synchronization information
- Mode 1 is used for RTT packet exchange to enhance security
- Mode 2 is used to exchange unmodulated tones for PBR measurement
- Mode 3 is an optional step that combines RTT and PBR operations

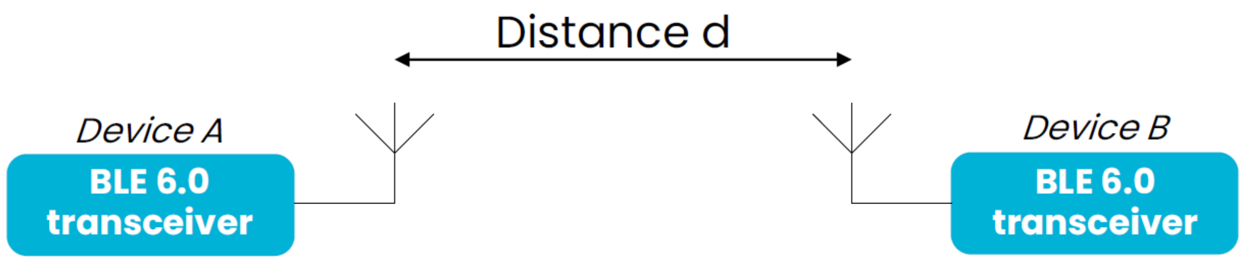


Figure 4-1. Schematic Diagram of Channel Sounding Principles

4.2 Ranging method

Channel Sounding uses two complementary ranging methods to determine the distance between two devices.

Phase-Based Ranging (PBR): The initiator transmits a signal with specific frequency and amplitude information, and the reflector measures the phase of the received signal and returns a response; the relative distance is calculated by comparing the phase difference between the signals of the two devices (as shown in Figure 4-2). PBR can provide extremely high ranging accuracy, reaching up to ±10cm at close range.

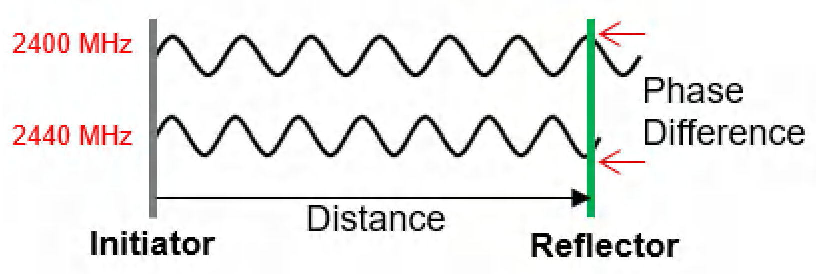


Figure 4-2. Schematic Diagram of PBR Principles

The measurement flow of PBR is shown in Figure 4-3:

1. The initiator transmits an unmodulated tone signal at F1.
2. The reflector performs a phase measurement on the incoming tone F1.
3. The reflector transmits an unmodulated tone at F1.
4. The initiator performs a phase measurement on the incoming tone.
5. The reflector transmits the phase measurement to the initiator to subtract the relative phase of the initiator/reflector local oscillators.

The above steps (1)-(4) are executed across multiple tone frequencies (typically 72 steps).

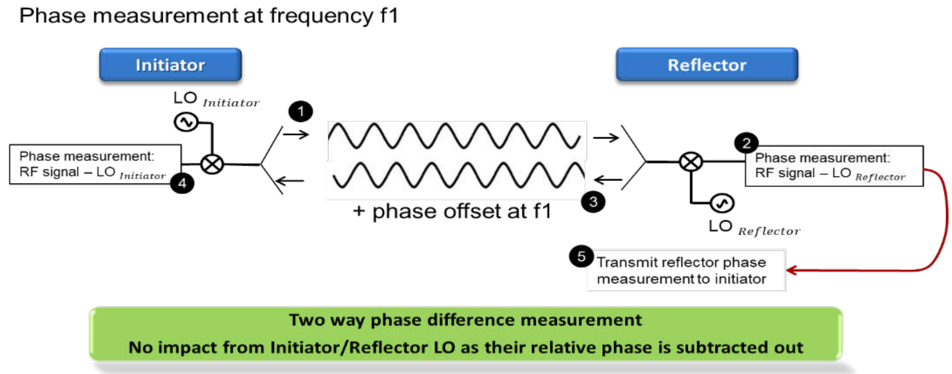


Figure 4-3. PBR Measurement Flow

Round-Trip Time Measurement (RTT): Estimates distance by measuring the Time of Flight (ToF) of a signal traveling back and forth between the initiator and the reflector. The two devices record the Time of Arrival (ToA) and Time of Departure (ToD) of the signal respectively, and the distance data is obtained by analyzing the difference between the two.

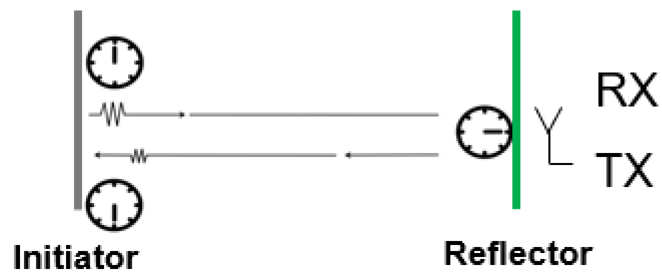


Figure 4-4. Schematic Diagram of RTT

The collaborative operation of PBR and RTT offers multiple advantages: RTT resolves the distance ambiguity issue in phase measurements and extends the effective ranging scope; concurrently, the timestamp mechanism attached to RTT effectively prevents relay attacks; the cross-verification of PBR and RTT further enhances the anti-attack capability of the system.

For door lock applications, the basic flow and roles are as follows:

- **Connection Establishment and Capability Negotiation**: The door lock side (Initiator) establishes a BLE connection with the key side (Reflector) to exchange Channel Sounding capability information (including the number of supported antennas, antenna switching modes, etc.).
- **Synchronization (Mode 0)**: Exchange synchronization information to ensure timing alignment between both sides.
- **RTT Measurement (Mode 1)**: Perform RTT packet exchange to obtain round-trip time data while enhancing security.
- **PBR Measurement (Mode 2)**: Exchange unmodulated tones across multiple channels to obtain phase difference information.
- **Post-processing using NPU-CDE and APU**: The internal APU of the CC2755 processes the collected IQ data, running high-resolution algorithms such as IFFT and MUSIC to calculate the precise distance.
- **Distance Output**: The APU passes the calculated distance value to the application layer for decision-making.

4.3 Accuracy and Reliability

The Channel Sounding technology of the CC2755 has been widely applied in automotive Passive Entry Passive Start (PEPS) systems. It achieves sub-50cm ranging accuracy, and the system maintains stable and reliable operation within a range of 30 to 40m. The dual-antenna design solution can achieve an accuracy of approximately 0.3m within 5m, and approximately 0.5m beyond 5m.

Channel Sounding supports up to 4 antenna paths and 8 antenna combinations, effectively mitigating the impact of multipath reflections on ranging accuracy in complex environments, which presents significant advantages in stability and reliability over RSSI solutions.

Based on smart door lock applications, this paper also provides a detailed test report on accuracy within a close range of 2m. See Section Test results.

5 Overall System Design

5.1 Overall System Architecture

Electronic smart locks (electronic locks) are typically composed of the following key functional modules:

- Human-Machine Interface (HMI): The HMI provides users with a method to interact with the system or view electronic lock responses. The HMI may include backlighting, LEDs, screens, speakers, keypads, and even microphones. Some electronic lock designs implement the HMI on a PCB that is physically isolated from the rest of the system. The HMI can implement a low-power mode (such as retaining only a small number of LEDs or buzzers during standby), and some electronic lock designs activate the HMI when a user approaches (awakened via capacitive touch or sensors). Meanwhile, wireless connectivity supports operating certain HMI functions, such as the keypad, on remote devices (such as smartphones or tablets).
- Wireless Connectivity and Host Controller: Wireless connectivity (such as Bluetooth Low Energy, Wi-Fi, Sub-1GHz, or RFID) adds an additional data interface to the lock. This interface can be used for various purposes, including wireless user authentication, remote control and monitoring, over-the-air (OTA) software updates, or communication with IoT sensors. In some cases, by adding a wireless interface, parts of the HMI functionality can be operated via remote devices (such as smartphones or tablets). The host controller is responsible for processing sensor inputs from the user, and it also generates responses by driving the physical locking mechanism or providing feedback through the HMI. By using the CC2755 wireless MCU, the host controller and Bluetooth Low Energy can be integrated into a single chip.
- Motor Subsystem: The motor subsystem includes the motor driver and the motor used to drive the locking mechanism. Electronic locks typically use brushed DC motors or stepper motors to operate the locking mechanism. Low-voltage single H-bridge or dual H-bridge motor drivers can be utilized.
- Sensors: Various sensors can be used in electronic locks to detect the status of the lock and the door (for example, using accelerometers or Inertial Measurement Units (IMUs) to detect the door's open/closed state) or whether a user is present or approaching (for example, using Passive Infrared (PIR) sensors or millimeter-wave radar for proximity detection).
- Power Management: There are primarily three power topologies applicable to such smart lock applications —Low Dropout Regulators (LDOs), buck DC-DC converters, and boost DC-DC converters. LDO and buck converter solutions are time-independent, meaning that regardless of how many locking and unlocking events occur in a day, both topologies consume the same amount of energy. LDOs and buck converters step down the voltage to generate lower-voltage supply rails to run the MCU, while the higher-voltage needs are powered by the higher-voltage battery. The boost converter solution is event-dependent because each locking and unlocking event must step up the voltage from 3V to 5V to ensure the operation of the motor and LEDs. This design selects the buck converter solution because LDOs exhibit ground leakage current, whereas buck converters feature zero ground leakage current, thereby yielding higher overall efficiency.

Figure 5-1 shows a typical block diagram of an electronic lock system supporting Bluetooth Channel Sounding.

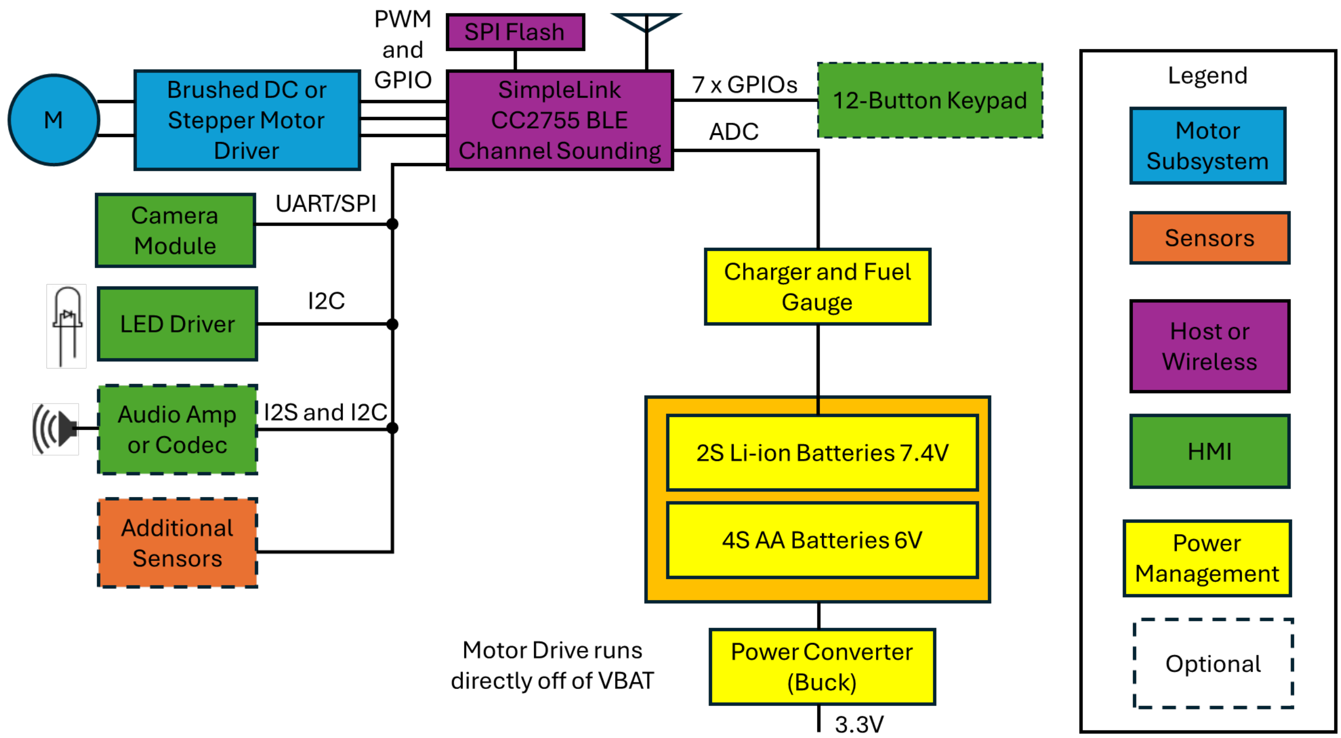


Figure 5-1. Example Block Diagram of an Electronic Lock System Supporting Bluetooth Channel Sounding

5.1.1 Power Design Guidance

The power management module must be powered by user-installed batteries. The choice of battery type, quantity, and voltage is closely related to the system's power architecture and power management choices:

- AA-sized alkaline batteries: Most electronic locks are powered by 4 or 8 batteries, with a single-cell voltage of 1.5V, providing an overall battery life of approximately 6–12 months. They are widely used in smart locks due to their widespread availability among consumers and low cost.
- Lithium batteries: High-end models are equipped with rechargeable lithium batteries, supporting USB-C charging, with a lifespan of 2–3 years.

5.1.1.1 Linear Regulator Architecture

Taking a connection of four AA batteries in series and one in parallel as an example, a 6V supply voltage is generated to power the motor. Therefore, only a simple motor driver is required to turn the motor on or off, without the need for any additional power management. Consequently, the motor subsystem operates at an efficiency close to 100%. The LDO steps down the higher battery voltage to a lower voltage, for example, using an LDO to convert the 6V battery voltage to the 3.3V required by the wireless microcontroller. Any LDO converting 6V to 3.3V achieves a maximum efficiency of 55%, and in standby mode, its efficiency will be much lower due to the high quiescent current of the LDO. For example, the TPS76633 is suitable for converting four AA batteries to 3.3V. The device achieves 55% efficiency under higher loads, but under a standby load of 1.2μA, its efficiency drops to only 1.2% due to its 55μA quiescent current. This extremely low efficiency causes the smart electronic lock to have relatively high power consumption during standby, thereby shortening battery life.

5.1.1.2 Buck Converter Architecture

Adopting the same power architecture as the LDO system but replacing the LDO with a buck converter can significantly improve efficiency. At the full load of the wireless microcontroller, the efficiency of the buck converter (such as the TPS62745) is 90%. The motor subsystem still maintains an efficiency close to 100% because it is directly connected to the battery pack.

Standard buck converters possess a relatively large quiescent current, and the presence of high quiescent current will drastically reduce efficiency in standby mode, just as it does in an LDO. However, the ultra-low-power buck converter used in this example features an ultra-low quiescent current specifically designed for IoT applications, which are characterized by high peak currents and long system standby times. When outputting a 3.3V voltage, the ultra-low quiescent current enables the efficiency to still exceed 67% under typical standby mode load currents.

Table 5-1 lists the recommended buck converter products for use in electronic lock systems.

Table 5-1. Recommended Buck Converter Products in Electronic Lock Systems

High Performance / Cost-Effective / New Product	Part Number	Brief Description	Package Size	Key Specifications	Positioning (Compared with Competitors & Suitability)	Supporting Materials
High Performance	TPS62745	10V, 300mA Buck	WSON	Ultra-low quiescent current 400nA; efficiency up to 90%; compatible with small 3.3µH or 4.7µH inductors	Ultra-low Iq extends battery life; easy to use small inductors; high efficiency;	TIDA-00757 TPS62745EVM-622
Cost-Effective / New Product	TPS562202 TPS563202	17V, 2A/3A Synchronous Buck	SOT563	High cost-effectiveness; small package; DCA2P control topology	Small size and easy to use; fast transient response; low standby current;	TPS562202EVM TPS563202EVM TIDA-010231
High Performance / New Product	TPS62901 TPS62902 TPS62903	17V, 1A/2A/3A Synchronous Buck	QFN	Low Iq (4µA); small package; single-layer routing; high precision, fast transient response	Low Iq extends battery life; saves PCB area, supports small-size design; supports high-performance design;	TPS62901EVM-069 TPS62902EVM-069 TPS62903EVM-069 TIDA-050052
Cost-Effective / New Product	TPS562211 TPS563211	17V, 2A/3A Synchronous Buck	SOT583	High cost-effectiveness; small package; optional PG/SS, FCCM/ECO	More flexible customer design, reduced certification workload; minimal external components, optimized board space; fast transient response at fixed frequency;	TPS562211EVM TPS563211EVM
High Performance / New Product	TPS629203 TPS629206 TPS629210	17V, 0.3/0.6/1A Synchronous Buck	SOT583	Low Iq (<4µA); small pin package; high precision, fast transient response	Low Iq extends battery life; saves PCB area, supports small-size design; supports high-performance design;	TPS629203EVM PMP23331 TPS629206EVM TPS629210EVM

5.1.2 Motor Driver Design Guidance

- Low-feature smart locks (almost no wireless connectivity, basic locks): Require small size and simple design; motor current chopping/feedback typically does not use current regulation—no inrush current limitation for brushed DC motors; lock position can be determined via Hall or magnetic sensors.
- High-end smart locks: Require small size, protection features, and position/speed control; utilize current regulation (low-side sensing resistor)—limits inrush current when the motor starts, protecting the battery system and extending battery life.

Table 5-2 lists the recommended motor driver products for use in electronic lock systems.

Table 5-2. Recommended Motor Driver Products in Electronic Lock Systems

High Performance / Cost-Effective / New Product	Part Number	Brief Description	Package Siz	Key Specifications	Positioning (Compared with Competitors & Suitability)	Supporting Materials
Cost-Effective / New Product	DRV8210/P DRV8212/P	12V, 1.76A H-bridge driver; 12V, 4A H-bridge driver;	SOT563 WSON	High integration, simple design; small size; DRV8210P/DRV8212P are pin-to-pin compatible with DRV8837C / DRV8837	Basic locks, no wireless connectivity; small size + low cost, suitable for entry-level smart locks;	DRV8210EVM TIDA-010266 DRV8212EVM DRV82xxEVM Hardware Files
High Performance	DRV8847 DRV8832 DRV8833C	18V, 2A H-bridge driver; 7V, 1A H-bridge driver; 10.8V, 1A H-bridge driver;	HTSSOP, TSSOP, WQFN; HVSSOP, VSON; HTSSOP, WQFN;	Features current regulation and independent half-bridge control; Features voltage regulation (constant speed control);	High-end locks; requires precise control; inrush limitation extends battery life;	DRV8847EVM TIDA-010072 DRV8832EVM Board Files: DRV8830 EVM and DRV8832 EVM
High Performance	DRV8876	40V, 3.5A H-bridge driver;	HTSSOP, VQFN;	Integrated current sensing and current sensing feedback	Small volume, high power, sensorless detection; suitable for high-end locks with compact designs;	DRV8876EVM slvae68b TIDA-010073
High Performance / New Product	DRV8213 DRV8214	11V, 4A Brushed DC driver; 11V, 4A H-bridge driver	WSON, WQFN; WQFN	Integrated current sensing, current regulation, and stall detection; Ripple counting and I2C interface;	Small volume, sensorless detection; suitable for high-end locks with compact designs;	DRV8213EVM DRV8214EVM

6 CC2755-Based Ranging Implementation

6.1 Keyless Entry Logic

To achieve frictionless proximity unlocking between the smartphone and the door lock, the core lies in utilizing Channel Sounding to obtain centimeter-level distances, combined with safety logic to prevent accidental unlocking or relay attacks. The following is a feasible logical framework:

6.1.1 Basic Configuration and Calibration

- **Hardware Requirements**: Both the smartphone (or other physical key devices) and the door lock must support Bluetooth CS and complete pairing and binding.

Note

Note: Among these, the smartphone side requires deep cooperation with the mobile device manufacturer to run in the background. Otherwise, a responsive APP activation process needs to be initiated.

- **Environmental Calibration**: During initial use, guide the user to pause briefly at typical positions outside the door such as 0.5m, 1m, and 2m, allowing the door lock to record the RSSI and channel impulse response characteristics under that environment to establish a distance calibration mapping.

6.1.2 Real-Time Ranging Process

- **Trigger Wake-up**: The door lock integrates a low-power accelerometer or proximity sensor; when it detects a person staying in front of the door for ≥1 second, it initiates a CS ranging request.
- **Bidirectional Ranging**: The smartphone background responds to the request, and both sides execute multiple Channel Sounding measurements.
- **Anti-Relay/Replay**: Each ranging data packet is appended with a rolling timestamp and a session random number; the door lock verifies the freshness to prevent remote hijacking via Bluetooth amplifiers.

6.1.3 Frictionless Unlocking Decision Logic

Three-Level Distance Thresholds (with the door lock as the origin):

- Far Zone (>2.5m): No action, remain in sleep mode.
- Proximity Zone (1.2m-2.5m): Marked as "Approaching".
- Action Zone (<1.2m): Initiate continuous distance sequence analysis.

6.1.3.1 Intent Judgement

Unlocking is not executed merely because the distance is <1.2m; the following conditions must be met simultaneously:

- Continuous Approach to the Door: The last 3 ranging values are strictly monotonically decreasing (distance shortening), ruling out wandering or walking past the door.
- Standstill Verification: After entering the action zone, the distance fluctuation is <0.15m and the duration lasts for ≥0.8 seconds (indicating the user actively stopped to prepare to open the door).
- Consistent Phone Attitude: The smartphone gyroscope shows a near-horizontal orientation and the acceleration is stable (ruling out swinging the phone in hand or bumping inside a bag).
- Security Lockout: If the action zone is entered 3 consecutive times without unlocking (the user just walked past), the ranging request will be temporarily blocked for 2 minutes.

6.1.4 Unlock Execution and Feedback

- The door lock verifies that the smartphone remains within the action zone, executes the unlocking, and records this successful distance (used for adaptively fine-tuning the threshold).
- The smartphone end remains seamless (no pop-ups), but the door lock can emit a soft success prompt tone.
- Anti-Repeated Trigger: All ranging results are ignored within 5 seconds after unlocking to avoid repeated locking and unlocking.

6.1.5 Exception Handling

- Low Battery: Frictionless unlocking is disabled when the door lock battery is low, requiring manual authentication.
- Multi-Phone Interference: If two bound smartphones are detected simultaneously, priority is given to the phone that is closer and conforms to the approaching trend.
- Ranging Failure: If 10 consecutive soundings are invalid (signal obstruction), it automatically falls back to rough Bluetooth RSSI measurement or requires manual touch wake-up.

While ensuring convenience, this logic effectively prevents risks such as walking past or accidental unlocking by neighbors through the triple conditions of "distance threshold + trend judgment + brief standstill". During actual deployment, the distance thresholds need to be fine-tuned based on the door lock installation position (attenuation from metal doors).

6.2 RF Hardware Design

6.2.1 Key End Solution Selection

The key end can flexibly choose solutions based on application scenarios:

- Smartphone Solution: Utilizing a smartphone carried by the user that supports BLE 6.0 Channel Sounding as the key end. Major smartphone manufacturers are progressively integrating BLE 6.0 Channel Sounding capabilities into new phone models, enabling keyless entry via a companion App.
- Dedicated Key Solution: Employing the CC2755 or CC2340 to build dedicated key devices (in forms such as key fobs, wristbands, etc.), which can serve as backup keys or be provided to users without BLE 6.0 smartphones.

6.2.2 Door Lock End Solution Selection

Depending on the system features, it can be decided whether to adopt a dual-chip (BLE+MCU) solution or utilize the CC2755 as the main controller.

6.3 Hardware Reference Design

Hardware design guidance documentation: CC234x and CC27xx Hardware Configuration and PCB Design Considerations (Rev. A) as well as CC27xx System Design - Schematic and Layout Guidelines

This paper does not dissect or explain the basic designs.

TI will also release a miniaturized dual-antenna-based reference design, as shown in the figure below.

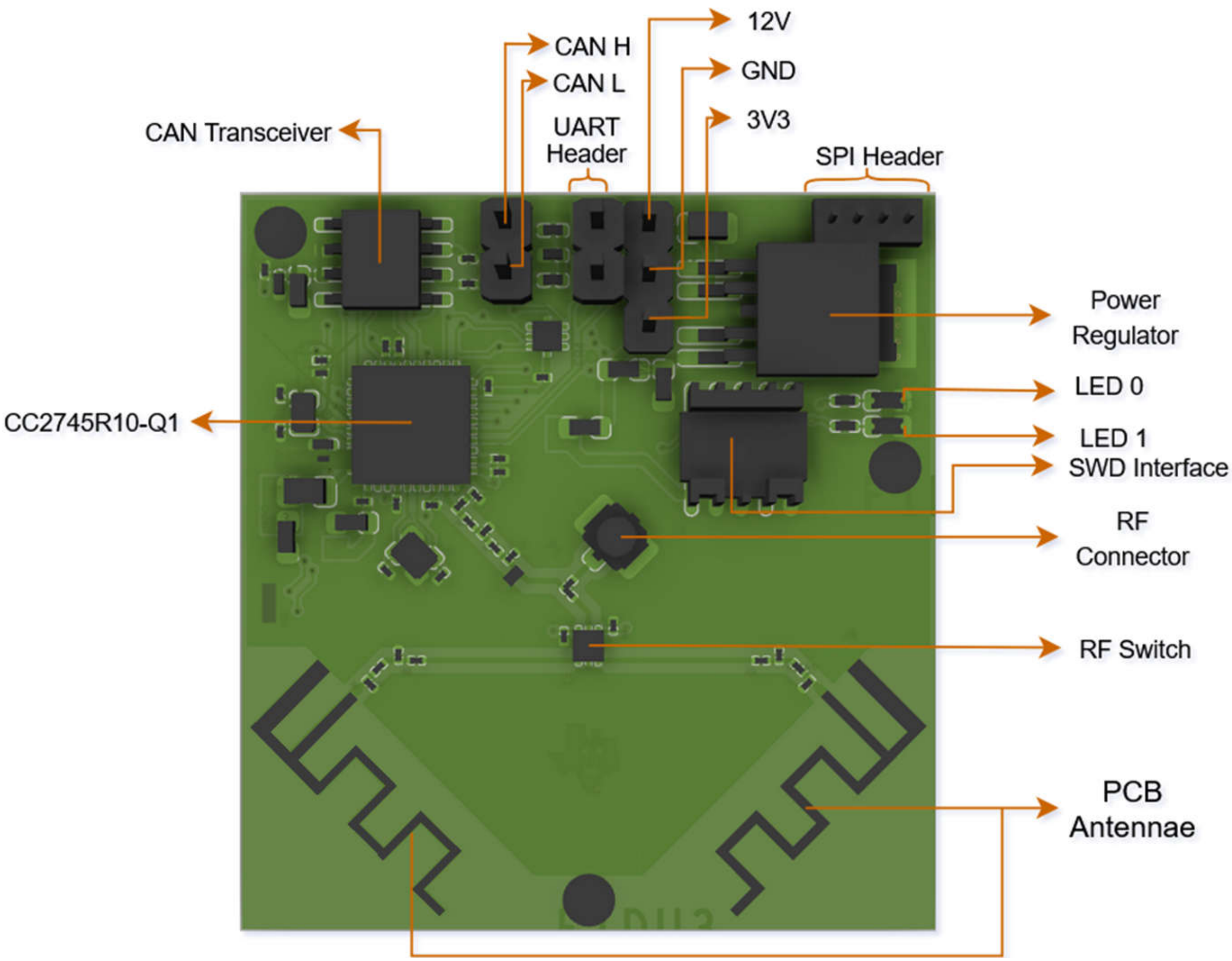


Figure 6-1. CC2755 Reference Dual-Antenna Reference Board

6.4 Single Antenna and Multi-Antenna

6.4.1 Impact of Antenna Quantity on Channel Sounding Ranging Performance

In Bluetooth Channel Sounding (CS), antenna configuration is a critical design factor affecting ranging accuracy and system robustness.

6.4.2 The Role of Antennas in Phase-Based Ranging

Bluetooth Channel Sounding employs two methods for distance estimation: Phase-Based Ranging (PBR) and Round-Trip Time (RTT). Among them, PBR utilizes the phase rotation characteristics of RF signals—a signal traveling a distance D will generate a phase offset, and the relative distance between devices is calculated by measuring the phase difference between signals of different frequencies. This process essentially depends on precise perception of wireless channel transmission characteristics.

Under a single-antenna configuration, the device can only acquire the amplitude and phase information (i.e., IQ data) of the channel from a fixed spatial sampling point. However, real-world wireless channels are not ideal models—factors such as relative orientation changes between devices, human body obstruction, environmental obstacles, and multipath effects will all cause distortion in the phase information of the received signal, thereby introducing errors into the distance estimation algorithm.

The fundamental advantage of multi-antenna configurations lies in the introduction of spatial diversity. By deploying multiple antennas at different spatial locations, the device can sample the same channel from multiple angles, obtaining multiple sets of independent or weakly correlated IQ data. This provides redundant information for subsequent signal processing—such as suppressing environmental interference through multipath identification and optimal path selection—thereby enhancing the reliability and accuracy of ranging. A detailed analysis of this will be unfolded below.

6.4.3 Analysis of Advantages and Disadvantages of Single-Antenna Configuration

6.4.3.1 Advantages: Simplicity and Low Cost

The greatest advantage of the single-antenna configuration lies in the simplicity of its hardware design. It requires only one RF transceiver link and one antenna, eliminating the need for RF switches and multiplexing circuits, which significantly reduces bill of materials (BOM) costs and PCB layout complexity. For ranging applications that do not demand high accuracy or operate in ideal environments, the single-antenna configuration can meet basic needs.

6.4.3.2 Disadvantages: Limited by Multiple Interference Factors

The reliability of single-antenna ranging is limited by various factors. First, the impact of relative antenna orientation is uncontrollable. In mobile device scenarios, the relative direction of the two devices' antennas is unpredictable. Certain specific orientations generate frequency-dependent null points, leading to severe attenuation of signal amplitude. In Bluetooth Channel Sounding, this attenuation causes phase information distortion in the PBR-measured IQ data, thereby introducing errors in distance estimation.

Second, multipath interference is the core challenge faced by single-antenna configurations. In indoor environments, signals reflect off walls, floors, human bodies, and other obstacles to form multiple propagation paths that reach the receiving end. These multipath components possess random phases and amplitudes, and their mutual superposition distorts the true phase measurement results. For a single-antenna device, it cannot differentiate which IQ data originates from the Line-of-Sight (LoS) path and which from reflection paths (multipath), making it impossible to eliminate contaminated measurements. The relative orientation between devices, the human body, obstacles in the environment, and multipath interference act together to limit the reliability of single-antenna ranging.

Finally, the upper limit of accuracy is constrained. When introducing the Channel Sounding feature, the Bluetooth Special Interest Group (SIG) set a requirement to achieve a target ranging accuracy of 0.5m in most scenarios. However, in most practical use scenarios, it is very difficult, or even impossible, to reliably achieve 0.5m accuracy without using multiple antennas. Industry practice indicates that it is difficult for phase-based ranging accuracy under a single-antenna configuration to significantly surpass this level due to specification constraints, the fundamental reason being the inability to effectively combat the aforementioned diverse environmental interferences.

6.4.4 Analysis of Advantages and Disadvantages of Multi-Antenna Configuration

6.4.4.1 Advantage 1: Anti-Multipath Capability Brought by Spatial Diversity

The most core advantage of the multi-antenna configuration is the introduction of spatial diversity to combat multipath effects. When a device is equipped with two or more antennas, the wireless channels experienced by different antennas—including the relative gain and phase of the direct path and various reflection paths—are typically independent or weakly correlated. This means that even if a certain antenna encounters severe frequency-selective fading or sits in a deep null point, other antennas may still receive high-quality signals. By analyzing IQ data from multiple antenna paths, the device can identify and eliminate measurements severely contaminated by multipath, thereby enhancing ranging robustness.

In principle, the reason multi-antenna configurations can effectively combat multipath is that antennas at different spatial locations correspond to different channel impulse responses. When multiple propagation paths exist, certain antenna positions may happen to be at the phase cancellation point between the direct path and a strong reflection path, while an antenna at another position might be in an area where the two add in phase. By synthesizing the measurement results of multiple antennas, the system can obtain more observations of the channel's spatial distribution without increasing bandwidth, thereby improving the capability to discern the direct path.

6.4.4.2 Advantage 2: Alleviating Antenna Orientation Sensitivity Issues

As previously stated, under a single-antenna configuration, the relative orientation of the device's antenna significantly impacts ranging performance—certain orientations generate frequency-dependent null points, resulting in IQ data distortion. Multi-antenna devices, by arranging multiple antennas in different orientations, can exchange phase-based data from different spatial directions. Even if a certain orientation produces a null point, antennas in other orientations may still provide distortion-free IQ data, thereby significantly improving system robustness. Distortion-free IQ data is the core prerequisite for achieving high-precision distance estimation.

6.4.4.3 Advantage 3: Dual Enhancement of Accuracy and Robustness

The multi-antenna configuration not only enhances the anti-interference capability of the system but also translates directly into an improvement in ranging accuracy. The Bluetooth Channel Sounding standard supports up to four antenna paths, and the accuracy of distance estimation can be further optimized through multi-antenna measurements. Experience from industry engineering practices shows that deploying multiple antennas on at least one side of the devices makes ranging more robust—although the accuracy of a single measurement does not necessarily increase, a more reliable ranging result can be obtained by filtering out some interfered "bad" measurements. Furthermore, the dual-antenna architecture can provide a two-fold accuracy improvement over typical configurations by reducing fading and multipath effects.

6.4.4.4 Disadvantages: Increased Hardware Complexity and Cost

The primary cost of the multi-antenna configuration lies in the escalation of hardware complexity. First, it requires deploying multiple antennas on the device and designing an RF Switch to achieve switching between different antenna paths, which increases PCB area and BOM costs. Second, multiple antennas mean that more RF paths need to be calibrated to eliminate phase deviations introduced by circuit differences between the paths. In addition, because IQ data needs to be collected and exchanged from multiple antenna paths during the Channel Sounding process, a larger volume of data needs to be exchanged between devices to complete distance estimation. Finally, the multi-antenna configuration places higher demands on antenna layout and isolation design, which requires careful trade-offs in compact products.

6.4.5 Precautions for Dual-Antenna Design

From the above analysis, it is not difficult to see that introducing a dual-antenna configuration in Bluetooth Channel Sounding is a key design decision to enhance ranging accuracy and system robustness. However, the introduction of dual antennas is not a simple hardware superposition; it involves collaborative design across multiple levels, including antenna layout, RF switch selection, switching timing, channel calibration, and software configuration.

In addition to optimizing the characteristic metrics (efficiency, directivity, etc.) of each antenna, ideally, the following should be satisfied:

- **Antenna Orientation**: It is recommended to arrange the two antennas orthogonally at 90 degrees. Orthogonal placement allows the two antennas to cover different polarization directions—when antenna A is at a null point in a certain polarization direction, antenna B can still maintain good reception in the orthogonal polarization direction. This design fundamentally alleviates the signal attenuation problem caused by the uncontrollable relative orientation of devices.
- **Antenna Spacing**: The spacing between antennas is one of the core parameters determining the spatial diversity effect; it is recommended to set the distance between the two antennas to 31.1mm. This value corresponds to 1/4 wavelength of a 2.4GHz signal; at this spacing, the wireless channels experienced by the two antennas have sufficient decorrelation, thereby achieving effective spatial diversity gain. If the 1/4 wavelength spacing cannot be guaranteed due to size constraints, the performance benefit of dual antennas remains very pronounced. Maximize it as much as possible within the existing board layout.
- **Routing Symmetry**: The RF front-end routing for the dual antennas should be kept as symmetric as possible. Channel Sounding is essentially a phase-based measurement technique; any asymmetry in the RF paths—including differences in trace length, matching network discrepancies, and variations in via counts—will introduce additional phase offsets, thereby superimposing systematic errors onto the distance estimation. Therefore, the traces from the RF switch output to the antenna feed points should maintain equal lengths and consistent structures.
- **Antenna Type Selection**: To ensure the comparability of signals, the types of the two antennas should remain consistent. It is recommended to use the Inverted-F Antenna (IFA) as the preferred antenna form for dual-antenna design. IFA offers advantages such as a compact structure, high radiation efficiency, and ease of implementation on PCBs, along with stable performance in the 2.4GHz band. Specific antenna dimensions and matching network designs can be referenced in TI application manual [43]. If other types, such as

ceramic chip antennas, are chosen, it should also be ensured that the models and matching circuits of the two antennas are completely identical to minimize the phase difference between the paths.

6.5 Test results

The author conducted line-of-sight (LOS) distance tests at 60cm, 100cm, and 200cm using TI's reference design at close range.

The schematic diagram of the post-processing flow is shown in Figure 6-2:

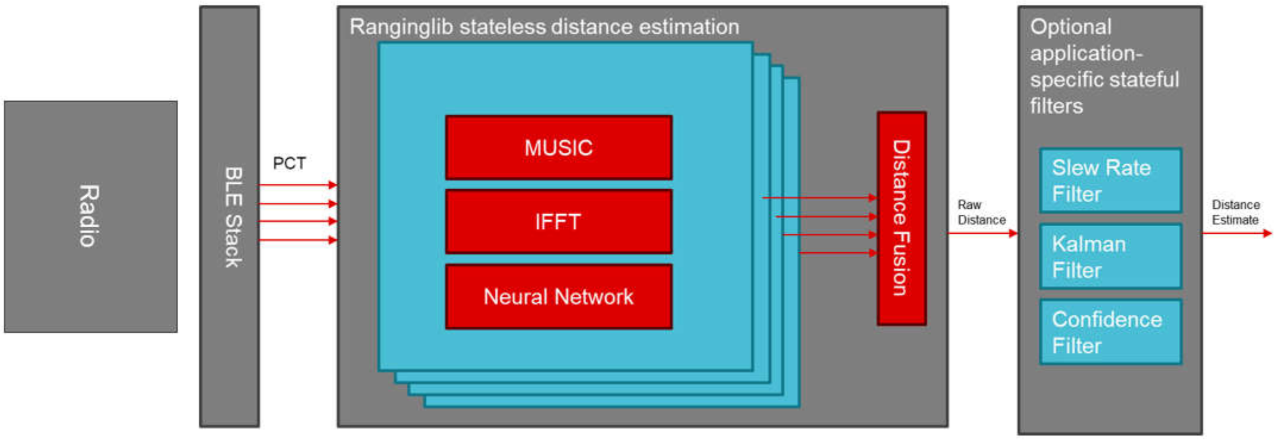


Figure 6-2. Fusion Post-Processing Flow Based on Phase-Based Ranging (PBR)

- Multi-Algorithm Advantages: Fuses the advantages of neural networks, Fast Fourier Transform (FFT), and MUSIC (Multiple Signal Classification) algorithms.
- **Error Compensation**: The disadvantages of each algorithm can be offset by the advantages of other algorithms.
- **Multipath Suppression**: The MUSIC algorithm performs particularly prominently in decoupling multipath interference.
- **Spectral Precision**: FFT provides frequency-domain insights to enhance resolution.
- **Real-Time Processing**: The fusion mechanism reduces computational overhead.
- **Performance in Obstacle Scenarios**: Performs better under Non-Line-of-Sight (NLOS) conditions or in high-reflection/interference scenarios.

6.5.1 Hardware configuration

- TI dual-antenna reference board + XDS110 interface board.
- The Initiator side is powered by a PC and captures data, running a Python script for display.
- The Reflector side is powered by a mobile power bank.

6.5.2 Software Configuration:

- SIMPLELINK-LOWPOWER-F3-SDK - CC27xx devices.
- Version: 9.14.02.16

6.5.3 Environment Setup:

Utilizing an open space, multi-scenario testing was conducted using a ground grid (20cm/15 degrees), with the test board elevated to a height of 1.3m.

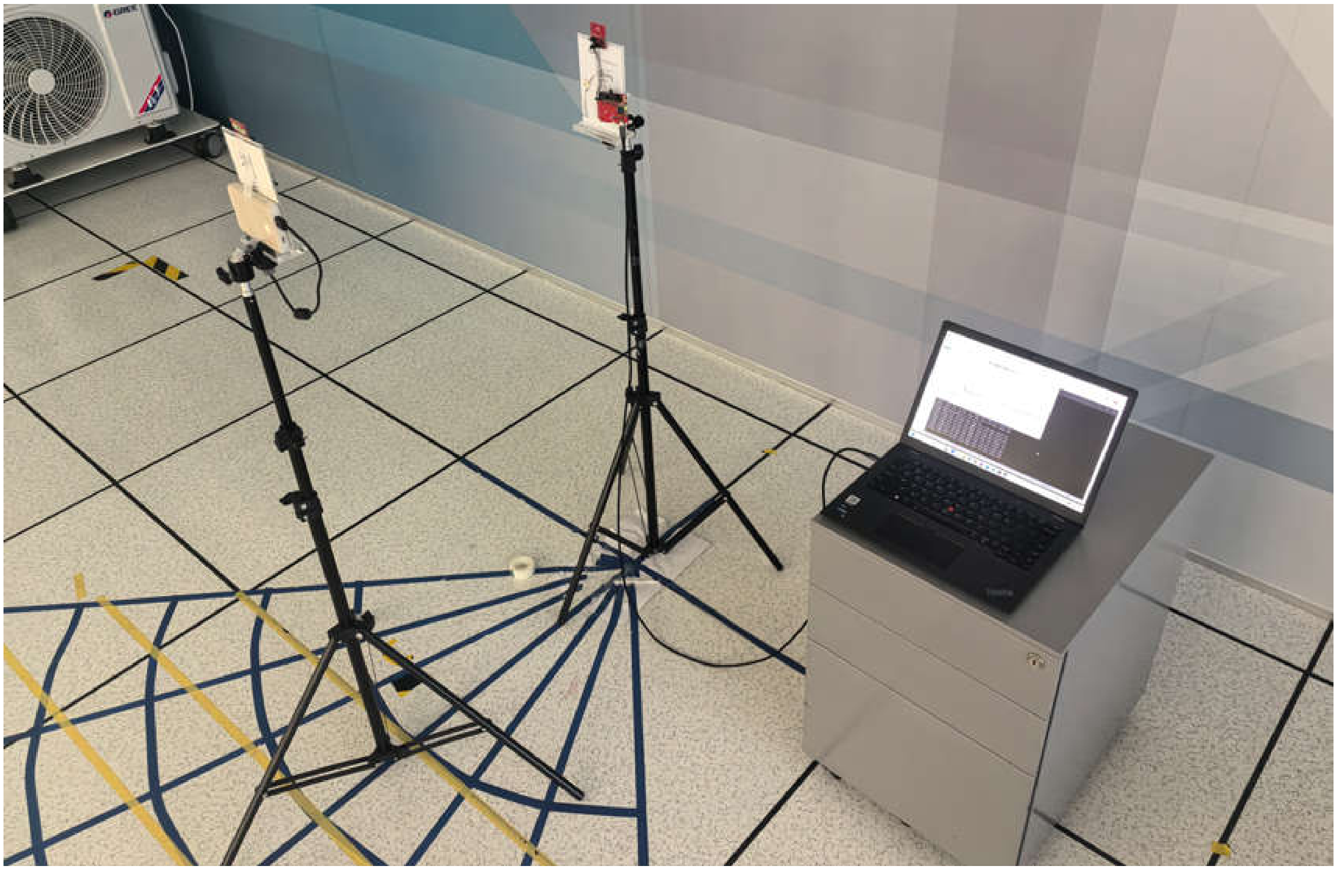


Figure 6-3. Actual View of the Test Environment

The results are shown in Figure 6-4, Figure 6-5, and Figure 6-6. They basically conform to expectations.

Among them, UD represents data processed by NPU/APU algorithms, and FD represents the result after applying additional filtering and smoothing at the application layer.

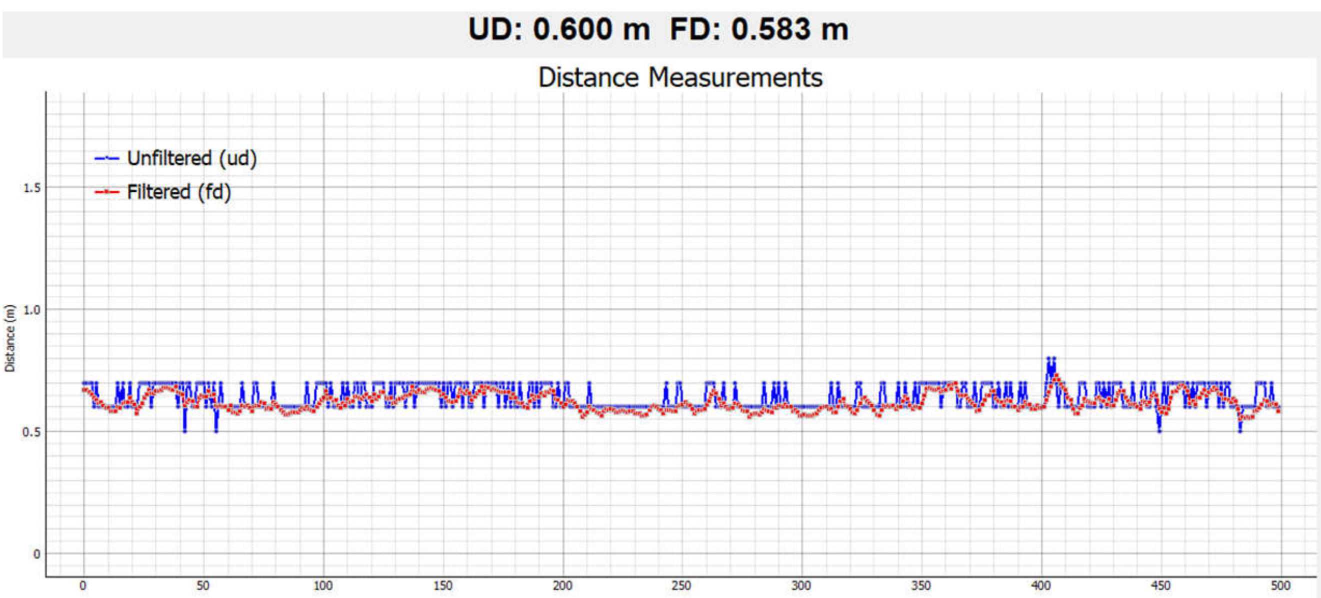


Figure 6-4. Actual 60cm Test Distance

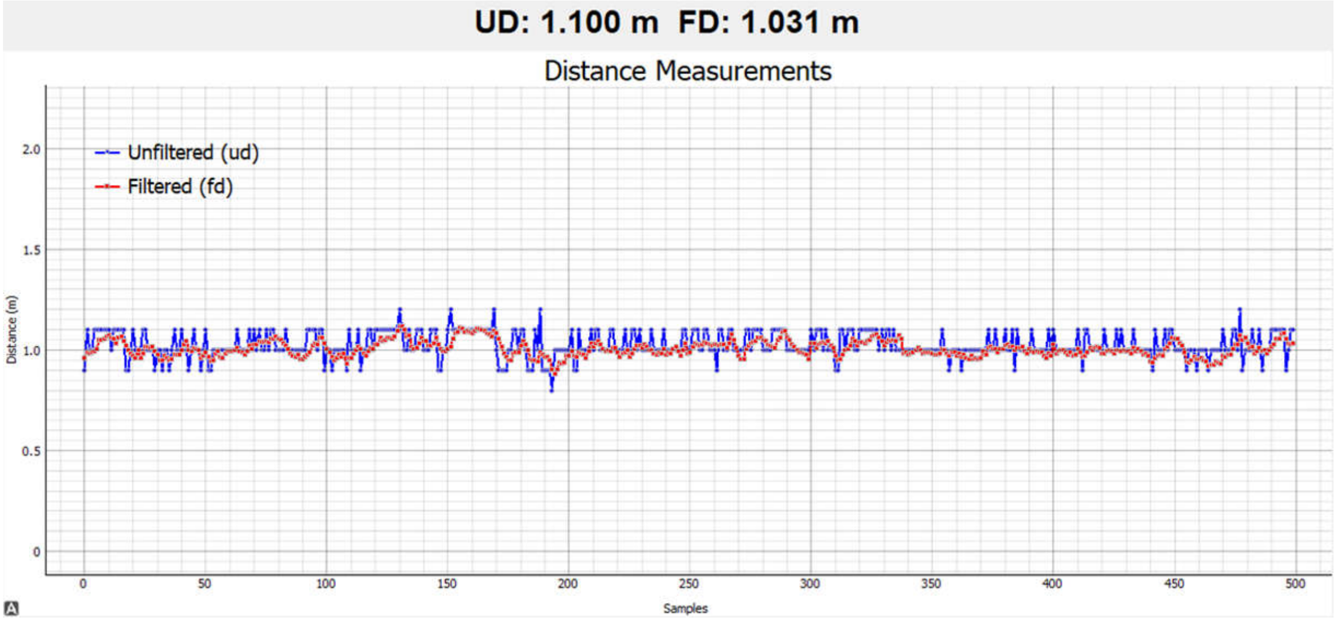


Figure 6-5. Actual 100cm Test Distance

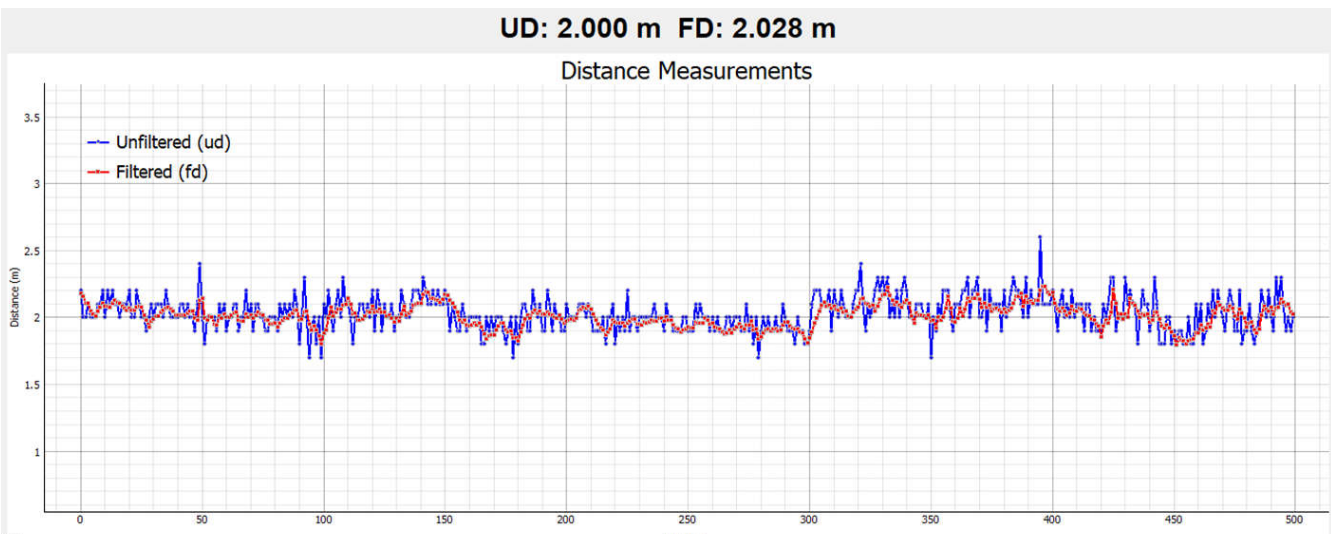


Figure 6-6. Actual 200cm Test Distance

6.6 Power consumption simulations

This paper only introduces the tools provided by TI that can be used for simulation. It does not offer recommendations for specific solutions.

Readers can use the tools to optimize relevant parameters based on actual user experiences (such as connection/broadcast intervals, CS measurement frequency and scenarios, sleep/wake duty cycles, etc.), which greatly saves debugging time.

Reference Tool: BT-POWER-CALC — Bluetooth Power Calculator for CC13xx, CC26xx, CC23xx, and CC27xx devices

7 Summary

This paper presents a detailed introduction to the design of a smart door lock keyless entry system based on the TI CC2755 wireless MCU.

Compared to traditional RSSI ranging solutions, Channel Sounding technology offers a qualitative leap in precision, stability, and security. The CC2755-based system can achieve centimeter-level ranging accuracy, providing a truly reliable and frictionless entry experience for smart door locks. It is recommended to adopt a dual-antenna design scheme to further enhance ranging accuracy and adaptation to complex environments.

Addressing the core engineering problem of distinguishing between the inside and outside of a room, this paper proposes practical schemes such as multi-level thresholds with hysteresis comparison, dual-antenna channel characteristic identification, a dual-Bluetooth module scheme, and proximity sensor assistance, and provides a fusion decision strategy to ensure the system can accurately differentiate whether the user is indoors or outdoors, effectively avoiding accidental unlock triggers.

TI provides a complete SimpleLink™ SDK, Channel Sounding reference designs, multi-antenna evaluation boards, and hardware PCB design references to help developers rapidly apply Channel Sounding technology to smart door lock products.

8 References

1. Texas Instruments, CC2755x10 SimpleLink Series 2.4GHz High-Performance Wireless MCU Datasheet.
2. Texas Instruments, Enhancing Edge Intelligence with Embedded Processors White Paper.
3. Texas Instruments, TPS62745 Dual-Cell Ultra-Low IQ Buck Converter for Low-Power Wireless Applications Datasheet (Rev. A).
4. Texas Instruments, Smart Lock Reference Design Enabling 5+ Years of Battery Life with 4 AA Batteries (Rev. C).
5. Texas Instruments, TPS62745 Buck Converter Evaluation Board User's Guide.
6. Texas Instruments, TPS562202 4.3V to 17V Input, 2A Synchronous Buck Converter in SOT563 Package Datasheet.
7. Texas Instruments, TPS563202 4.3V to 17V Input, 3A Synchronous Buck Converter in SOT563 Package Datasheet (Rev. B).
8. Texas Instruments, TPS562202 Buck Converter Evaluation Module User's Guide (Rev. A).
9. Texas Instruments, TPS563202 Buck Converter Evaluation Module User's Guide (Rev. B).
10. Texas Instruments, Analog Front End for Arc Detection in Photovoltaic Applications Reference Design (Rev. B).
11. Texas Instruments, TPS62901 3V to 17V, High-Efficiency, Low IQ Buck Converter in a 1.5mm × 2mm QFN Package Datasheet (Rev. A).
12. Texas Instruments, TPS62902 3V to 17V, High-Efficiency and Low IQ Buck Converter in a 1.5mm × 2mm QFN Package Datasheet (Rev. A).
13. Texas Instruments, TPS62903 3V to 17V, High-Efficiency and Low IQ Buck Converter in a 1.5mm × 2mm QFN Package Datasheet (Rev. A).
14. Texas Instruments, TPS6290x Buck Converter Evaluation Module User's Guide (Rev. A).
15. Texas Instruments, High-Power Density 17V, 3A Buck Converter Reference Design.
16. Texas Instruments, TPS562211 4.2V to 18V Input, 2A Synchronous Buck Converter in SOT583 Package Datasheet (Rev. A).
17. Texas Instruments, TPS563211 4.2V to 18V Input, 3A Synchronous Buck Converter in SOT583 Package Datasheet (Rev. A).
18. Texas Instruments, TPS562211 Buck Converter Evaluation Module User's Guide (Rev. A).
19. Texas Instruments, TPS563211 Buck Converter Evaluation Module User's Guide (Rev. A).
20. Texas Instruments, TPS629203 300mA, 3V to 17V Low IQ Buck Converter with DCS-Control Topology Datasheet.
21. Texas Instruments, TPS629206 600mA, 3V to 17V Low IQ Buck Converter with DCS-Control Topology Datasheet.
22. Texas Instruments, TPS629210 3V to 17V, 1A Low IQ Buck Converter in a SOT-583 Package Datasheet (Rev. B).
23. Texas Instruments, TPS629203 Buck Converter Evaluation Module User's Guide.
24. Texas Instruments, 19W, 5V and 12V AC/DC Multi-Output, ZVS Flyback Reference Design for Server Applications.
25. Texas Instruments, TPS629206 Buck Converter Evaluation Module User's Guide.
26. Texas Instruments, TPS629210 Buck Converter Evaluation Module User's Guide.
27. Texas Instruments, DRV8210 11V H-Bridge Motor Driver with PWM, PH/EN, and Half-Bridge Control Interfaces and Low-Power Sleep Mode Datasheet (Rev. B).
28. Texas Instruments, DRV8210P 11V H-Bridge Motor Driver with PWM Interface and Low-Power Sleep Mode Datasheet.
29. Texas Instruments, DRV8212 11V H-Bridge Motor Driver with PWM, PH/EN, and Half-Bridge Control Interfaces and Low-Power Sleep Mode Datasheet (Rev. B).
30. Texas Instruments, DRV8212P 11V H-Bridge Motor Driver with PWM Interface and Low-Power Sleep Mode Datasheet (Rev. A).
31. Texas Instruments, DRV821x Low-Voltage H-Bridge Motor Driver Evaluation Module with Low-Power Sleep Mode.
32. Texas Instruments, Low-Cost Blood Pressure and Heart Rate Monitor Reference Design.
33. Texas Instruments, DRV8847 Dual-Channel H-Bridge Motor Driver Evaluation Module.
34. Texas Instruments, Blower and Valve Control Reference Design for Respiratory Applications.
35. Texas Instruments, DRV8832 Evaluation Module.

36. Texas Instruments, DRV8876 H-Bridge Motor Driver with Integrated Current Sensing and Regulation Datasheet (Rev. A).
37. Texas Instruments, DRV8876 Single-Channel H-Bridge Motor Driver Evaluation Module.
38. Texas Instruments, Advantages of Integrated Current Sensing.
39. Texas Instruments, 18V, 2A, 25mm Brushed DC Motor Driver Reference Design with Stall Detection and Speed Control.
40. Texas Instruments, DRV8213 4A Brushed DC Motor Driver with Integrated Current Sensing, Current Regulation, and Stall Detection Datasheet.
41. Texas Instruments, DRV8214 2A Brushed DC Motor Driver with Ripple Counting, Stall Detection, and Speed Regulation Datasheet.
42. Texas Instruments, DRV821x and DRV823x Evaluation Modules (Rev. A).
43. Texas Instruments, CC23xx and CC27xx Hardware Configuration and PCB Design Considerations (Rev. A).

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES "AS IS" AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you fully indemnify TI and its representatives against any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI's products are provided subject to TI's Terms of Sale, TI's General Quality Guidelines, or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI's provision of these resources does not expand or otherwise alter TI's applicable warranties or warranty disclaimers for TI products. Unless TI explicitly designates a product as custom or customer-specified, TI products are standard, catalog, general purpose devices.

TI objects to and rejects any additional or different terms you may propose.