



Chipsmall Limited consists of a professional team with an average of over 10 year of expertise in the distribution of electronic components. Based in Hongkong, we have already established firm and mutual-benefit business relationships with customers from,Europe,America and south Asia,supplying obsolete and hard-to-find components to meet their specific needs.

With the principle of “Quality Parts,Customers Priority,Honest Operation,and Considerate Service”,our business mainly focus on the distribution of electronic components. Line cards we deal with include Microchip,ALPS,ROHM,Xilinx,Pulse,ON,Everlight and Freescale. Main products comprise IC,Modules,Potentiometer,IC Socket,Relay,Connector.Our parts cover such applications as commercial,industrial, and automotives areas.

We are looking forward to setting up business relationship with you and hope to provide you with the best service and solution. Let us make a better world for our industry!



## Contact us

Tel: +86-755-8981 8866 Fax: +86-755-8427 6832

Email & Skype: info@chipsmall.com Web: www.chipsmall.com

Address: A1208, Overseas Decoration Building, #122 Zhenhua RD., Futian, Shenzhen, China





**MICROCHIP**

---

**Wireless Security Remote Control  
Development Kit  
User's Guide**

---

---

**Note the following details of the code protection feature on Microchip devices:**

- Microchip products meet the specification contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is one of the most secure families of its kind on the market today, when used in the intended manner and under normal conditions.
- There are dishonest and possibly illegal methods used to breach the code protection feature. All of these methods, to our knowledge, require using the Microchip products in a manner outside the operating specifications contained in Microchip's Data Sheets. Most likely, the person doing so is engaged in theft of intellectual property.
- Microchip is willing to work with the customer who is concerned about the integrity of their code.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of their code. Code protection does not mean that we are guaranteeing the product as "unbreakable."

Code protection is constantly evolving. We at Microchip are committed to continuously improving the code protection features of our products. Attempts to break Microchip's code protection feature may be a violation of the Digital Millennium Copyright Act. If such acts allow unauthorized access to your software or other copyrighted work, you may have a right to sue for relief under that Act.

---

Information contained in this publication regarding device applications and the like is provided only for your convenience and may be superseded by updates. It is your responsibility to ensure that your application meets with your specifications. MICROCHIP MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WHETHER EXPRESS OR IMPLIED, WRITTEN OR ORAL, STATUTORY OR OTHERWISE, RELATED TO THE INFORMATION, INCLUDING BUT NOT LIMITED TO ITS CONDITION, QUALITY, PERFORMANCE, MERCHANTABILITY OR FITNESS FOR PURPOSE. Microchip disclaims all liability arising from this information and its use. Use of Microchip devices in life support and/or safety applications is entirely at the buyer's risk, and the buyer agrees to defend, indemnify and hold harmless Microchip from any and all damages, claims, suits, or expenses resulting from such use. No licenses are conveyed, implicitly or otherwise, under any Microchip intellectual property rights.

**Trademarks**

The Microchip name and logo, the Microchip logo, dsPIC, KEELOQ, KEELOQ logo, MPLAB, PIC, PICmicro, PICSTART, PIC<sup>32</sup> logo, rPIC and UNI/O are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.


FilterLab, Hampshire, HI-TECH C, Linear Active Thermistor, MXDEV, MXLAB, SEEVAL and The Embedded Control Solutions Company are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Analog-for-the-Digital Age, Application Maestro, chipKIT, chipKIT logo, CodeGuard, dsPICDEM, dsPICDEM.net, dsPICworks, dsSPEAK, ECAN, ECONOMONITOR, FanSense, HI-TIDE, In-Circuit Serial Programming, ICSP, Mindi, MiWi, MPASM, MPLAB Certified logo, MPLIB, MPLINK, mTouch, Omniscient Code Generation, PICC, PICC-18, PICDEM, PICDEM.net, PICkit, PICtail, REAL ICE, rLAB, Select Mode, Total Endurance, TSHARC, UniWinDriver, WiperLock and ZENA are trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

SQTP is a service mark of Microchip Technology Incorporated in the U.S.A.

All other trademarks mentioned herein are property of their respective companies.

© 2012, Microchip Technology Incorporated, Printed in the U.S.A., All Rights Reserved.

 Printed on recycled paper.

ISBN: 9781620764145

**QUALITY MANAGEMENT SYSTEM  
CERTIFIED BY DNV  
= ISO/TS 16949 =**

*Microchip received ISO/TS-16949:2009 certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona; Gresham, Oregon and design centers in California and India. The Company's quality system processes and procedures are for its PIC<sup>®</sup> MCUs and dsPIC<sup>®</sup> DSCs, KEELOQ<sup>®</sup> code hopping devices, Serial EEPROMs, microperipherals, nonvolatile memory and analog products. In addition, Microchip's quality system for the design and manufacture of development systems is ISO 9001:2000 certified.*

**Object of Declaration: Wireless Security Remote Control Development Kit**

EU Declaration of Conformity

Manufacturer: Microchip Technology Inc.  
2355 W. Chandler Blvd.  
Chandler, Arizona, 85224-6199  
USA

This declaration of conformity is issued by the manufacturer.

The development/evaluation tool is designed to be used for research and development in a laboratory environment. This development/evaluation tool is not intended to be a finished appliance, nor is it intended for incorporation into finished appliances that are made commercially available as single functional units to end users. This development/evaluation tool complies with EU EMC Directive 2004/108/EC and as supported by the European Commission's Guide for the EMC Directive 2004/108/EC (8<sup>th</sup> February 2010).

This development/evaluation tool complies with EU RoHS2 Directive 2011/65/EU.

For information regarding the exclusive, limited warranties applicable to Microchip products, please see Microchip's standard terms and conditions of sale, which are printed on our sales documentation and available at [www.microchip.com](http://www.microchip.com).

Signed for and on behalf of Microchip Technology Inc. at Chandler, Arizona, USA



Derek Carlson  
VP Development Tools

05-DEC-2011  
Date

# Wireless Security Remote Control Development Kit User's Guide

---

---

NOTES:





# WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT USER'S GUIDE

---

---

## Table of Contents

---

---

<b>Preface</b> .....	<b>7</b>
<b>Chapter 1. Overview</b>	
1.1 Introduction .....	13
1.2 Wireless Security Remote Control Development Kit Contents .....	13
1.3 Getting Started .....	13
<b>Chapter 2. Getting Started</b>	
2.1 Introduction .....	15
2.2 Hardware Requirements .....	15
2.3 Software Requirements .....	15
2.4 Demo Setup .....	15
2.5 Demo Operation .....	16
2.6 Embedded Security Development Board Hardware Self-Check .....	19
<b>Chapter 3. PIC12LF1840T39A Wireless Remote Key Fob</b>	
3.1 Introduction .....	21
3.2 Hardware Description .....	21
3.3 Printed Circuit Board Description .....	21
3.4 PCB Antenna Description .....	22
<b>Chapter 4. SX1239 Receiver PICtail™ Daughter Board</b>	
4.1 Introduction .....	25
4.2 Hardware Description .....	25
<b>Chapter 5. Embedded Security Development Board</b>	
5.1 Introduction .....	27
5.2 Hardware Description .....	28
<b>Chapter 6. Developing with the Wireless Security Remote Control Development Kit</b>	
6.1 Introduction .....	31
6.2 Developing with a Key Fob as Transmitter .....	31
6.3 Developing with the Embedded Security Development Board as Receiver .....	32
<b>Appendix A. PIC12LF1840T39A Wireless Remote Key Fob Schematics</b>	
<b>Appendix B. SX1239 Receiver PICtail™ Daughter Board Schematics</b>	
<b>Appendix C. Embedded Security Development Board Schematics</b>	
<b>Worldwide Sales and Service</b> .....	<b>50</b>

# Wireless Security Remote Control Development Kit User's Guide

---

NOTES:



# WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT USER'S GUIDE

---

---

## Preface

---

---

### NOTICE TO CUSTOMERS

All documentation becomes dated, and this manual is no exception. Microchip tools and documentation are constantly evolving to meet customer needs, so some actual dialogs and/or tool descriptions may differ from those in this document. Please refer to our web site ([www.microchip.com](http://www.microchip.com)) to obtain the latest documentation available.

Documents are identified with a “DS” number. This number is located on the bottom of each page, in front of the page number. The numbering convention for the DS number is “DSXXXXA”, where “XXXX” is the document number and “A” is the revision level of the document.

For the most up-to-date information on development tools, see the MPLAB® IDE online help. Select the Help menu, and then Topics to open a list of available online help files.

## INTRODUCTION

This chapter contains general information that will be useful to know before using the Wireless Security Remote Control Development Kit User's Guide. Items discussed in this chapter include:

- [Document Layout](#)
- [Conventions Used in this Guide](#)
- [Warranty Registration](#)
- [Recommended Reading](#)
- [The Microchip Web Site](#)
- [Development Systems Customer Change Notification Service](#)
- [Customer Support](#)
- [Revision History](#)

## DOCUMENT LAYOUT

This document describes how to use the Wireless Security Remote Control Development Kit (WSRCDK) to evaluate and experiment with Microchip KEELOQ® Remote Keyless Entry (RKE) solutions. The main layout is as follows:

- **Chapter 1. “Overview”** – This chapter describes the WSRCDK and how it works.
- **Chapter 2. “Getting Started”** – This chapter describes the procedures to demonstrate Microchip KEELOQ RKE solution on WSRCDK.
- **Chapter 3. “PIC12LF1840T39A Wireless Remote Key Fob”** – This chapter provides the hardware details of the wireless key fob.
- **Chapter 4. “SX1239 Receiver PICtail™ Daughter Board”** – This chapter provides the hardware details of the Receiver PICtail Daughter Board.
- **Chapter 5. “Embedded Security Development Board”** – This chapter provides the hardware details of the Embedded Security Development Board.



# Wireless Security Remote Control Development Kit User's Guide

- **Chapter 6. “Developing with the Wireless Security Remote Control Development Kit”** – This chapter provides suggestions on the development based on Microchip RKE solution.
- **Appendix A. “PIC12LF1840T39A Wireless Remote Key Fob Schematics”** – This appendix provides the PCB layout, BOM and schematics.
- **Appendix B. “SX1239 Receiver PICtail™ Daughter Board Schematics”** – This appendix provides the PCB layout, BOM and schematics.
- **Appendix C. “Embedded Security Development Board Schematics”** – This appendix provides the PCB layout, BOM and schematics.

## CONVENTIONS USED IN THIS GUIDE

This manual uses the following documentation conventions:

### DOCUMENTATION CONVENTIONS

Description	Represents	Examples
<b>Arial font:</b>		
Italic characters	Referenced books	<i>MPLAB® IDE User's Guide</i>
	Emphasized text	...is the <i>only</i> compiler...
Initial caps	A window	the Output window
	A dialog	the Settings dialog
	A menu selection	select Enable Programmer
Quotes	A field name in a window or dialog	"Save project before build"
Underlined, italic text with right angle bracket	A menu path	<u><i>File&gt;Save</i></u>
Bold characters	A dialog button	Click <b>OK</b>
	A tab	Click the <b>Power</b> tab
N'Rnnnn	A number in verilog format, where N is the total number of digits, R is the radix and n is a digit.	4'b0010, 2'hF1
Text in angle brackets < >	A key on the keyboard	Press <Enter>, <F1>
<b>Courier New font:</b>		
Plain Courier New	Sample source code	#define START
	Filenames	autoexec.bat
	File paths	c:\mcc18\h
	Keywords	_asm, _endasm, static
	Command-line options	-Opa+, -Opa-
	Bit values	0, 1
	Constants	0xFF, 'A'
Italic Courier New	A variable argument	<i>file.o</i> , where <i>file</i> can be any valid filename
Square brackets [ ]	Optional arguments	mcc18 [options] <i>file</i> [options]
Curly brackets and pipe character: {   }	Choice of mutually exclusive arguments; an OR selection	errorlevel {0 1}
Ellipses...	Replaces repeated text	var_name [, var_name...]
	Represents code supplied by user	void main (void) { ... }

## WARRANTY REGISTRATION

Please complete the enclosed Warranty Registration Card and mail it promptly. Sending in the Warranty Registration Card entitles users to receive new product updates. Interim software releases are available at the Microchip web site.

## RECOMMENDED READING

This user's guide describes how to use the Wireless Security Remote Control Development Kit User's Guide. Other useful documents are listed below. The following Microchip documents are available and recommended as supplemental reference resources.

### Readme Files

For the latest information on using other tools, read the tool-specific Readme files in the Readme subdirectory of the MPLAB<sup>®</sup> IDE installation directory. The Readme files contain update information and known issues that may not be included in this user's guide.

### Application Notes

There are several application notes available from Microchip that help in understanding Microchip KEELOQ applications. These include:

- AN1259 *"KEELOQ<sup>®</sup> Microcontroller-based Code Hopping Encoder"*
- AN1265 *"KEELOQ<sup>®</sup> with AES Microcontroller-based Code Hopping Encoder"*
- AN743 *"Modular PIC<sup>®</sup> Mid-Range MCU Code Hopping Decoder"*
- AN745 *"Modular Mid-Range PIC<sup>®</sup> Decoder in C"*
- AN1275 *"KEELOQ<sup>®</sup> with AES Receiver/Decoder"*

## THE MICROCHIP WEB SITE

Microchip provides online support via our web site at [www.microchip.com](http://www.microchip.com). This web site is used as a means to make files and information easily available to customers. Accessible by using your favorite Internet browser, the web site contains the following information:

- **Product Support** – Data sheets and errata, application notes and sample programs, design resources, user's guides and hardware support documents, latest software releases and archived software
- **General Technical Support** – Frequently Asked Questions (FAQs), technical support requests, online discussion groups, Microchip consultant program member listing
- **Business of Microchip** – Product selector and ordering guides, latest Microchip press releases, listing of seminars and events, listings of Microchip sales offices, distributors and factory representatives

## DEVELOPMENT SYSTEMS CUSTOMER CHANGE NOTIFICATION SERVICE

Microchip's customer notification service helps keep customers current on Microchip products. Subscribers will receive e-mail notification whenever there are changes, updates, revisions or errata related to a specified product family or development tool of interest.

To register, access the Microchip web site at [www.microchip.com](http://www.microchip.com), click on Customer Change Notification and follow the registration instructions.

The Development Systems product group categories are:

- **Compilers** – The latest information on Microchip C compilers, assemblers, linkers and other language tools. These include all MPLAB C compilers; all MPLAB assemblers (including MPASM™ assembler); all MPLAB linkers (including MPLINK™ object linker); and all MPLAB librarians (including MPLIB™ object librarian).
- **Emulators** – The latest information on Microchip in-circuit emulators. This includes the MPLAB REAL ICE™ and MPLAB ICE 2000 in-circuit emulators.
- **In-Circuit Debuggers** – The latest information on the Microchip in-circuit debuggers. This includes MPLAB ICD 3 in-circuit debuggers and PICKit™ 3 debug express.
- **MPLAB® IDE** – The latest information on Microchip MPLAB IDE, the Windows® Integrated Development Environment for development systems tools. This list is focused on the MPLAB IDE, MPLAB IDE Project Manager, MPLAB Editor and MPLAB SIM simulator, as well as general editing and debugging features.
- **Programmers** – The latest information on Microchip programmers. These include production programmers such as MPLAB REAL ICE in-circuit emulator, MPLAB ICD 3 in-circuit debugger and MPLAB PM3 device programmers. Also included are nonproduction development programmers such as PICSTART® Plus and PICKit 2 and 3.

### CUSTOMER SUPPORT

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Field Application Engineer (FAE)
- Technical Support

Customers should contact their distributor, representative or field application engineer (FAE) for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in the back of this document.

Technical support is available through the web site at:

<http://www.microchip.com/support>.

### REVISION HISTORY

#### Revision A (July 2012)

- Initial Release of this Document.

NOTES:



# WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT USER'S GUIDE

---

---

## Chapter 1. Overview

---

---

### 1.1 INTRODUCTION

The Wireless Security Remote Control Development Kit is a demonstration and development platform for wireless security remote control applications. The kit demos two security protocols, KEELOQ<sup>®</sup> Classic and KEELOQ<sup>®</sup> AES.

The kit contains a four-button key fob transmitter based on the PIC12LF1840T39A, SX1239 Receiver PICtail™ Daughter Board, and the Embedded Security Development Board. The kits can be purchased in one of three transmit frequencies. See the next section for ordering part numbers.

- Wireless Security Remote Control Development Kit Contents
- Getting Started

### 1.2 WIRELESS SECURITY REMOTE CONTROL DEVELOPMENT KIT CONTENTS

The Wireless Security Remote Control Development Kits have three frequency choices:

- Wireless Security Remote Control Development Kit – 433.92 MHz (DM182017-1)
- Wireless Security Remote Control Development Kit – 868 MHz (DM182017-2)
- Wireless Security Remote Control Development Kit – 915 MHz (DM182017-3)

Each kit contains:

- PIC12LF1840T39A Wireless Remote Key Fob ([Chapter 3. “PIC12LF1840T39A Wireless Remote Key Fob”](#), [Appendix A](#))
- SX1239 Receiver PICtail Daughter Board ([Chapter 4. “SX1239 Receiver PICtail™ Daughter Board”](#), [Appendix B](#))
- Embedded Security Development Board ([Chapter 5. “Embedded Security Development Board”](#), [Appendix C](#))
- USB Cable
- CR2032 Coin Cell Battery

### 1.3 GETTING STARTED

[Chapter 2. “Getting Started”](#) provides a getting started tutorial to familiarize users with the Wireless Security Remote Control Development Kit.



# Wireless Security Remote Control Development Kit User's Guide

---

---

NOTES:

---

---

## Chapter 2. Getting Started

---

---

### 2.1 INTRODUCTION

This chapter provides a getting started tutorial to familiarize users with the Wireless Security Remote Control Development Kit.

The following topics are discussed in this chapter:

- Hardware Requirements
- Software Requirements
- Demo Setup
- Demo Operation

### 2.2 HARDWARE REQUIREMENTS

The following hardware is required to run the pre-programmed demo application:

- PIC12LF1840T39A Wireless Remote Key Fob
- SX1239 Receiver PICtail™ Daughter Board
- Embedded Security Development Board
- USB A to Mini-B Cable (to power the Embedded Security Development Board or power can also be provided by a bench power supply)

### 2.3 SOFTWARE REQUIREMENTS

The PIC12LF1840T39A Key Fob and Embedded Security Development Board are pre-programmed with a remote control demo program. The demo setup and operation are explained in the following sections.

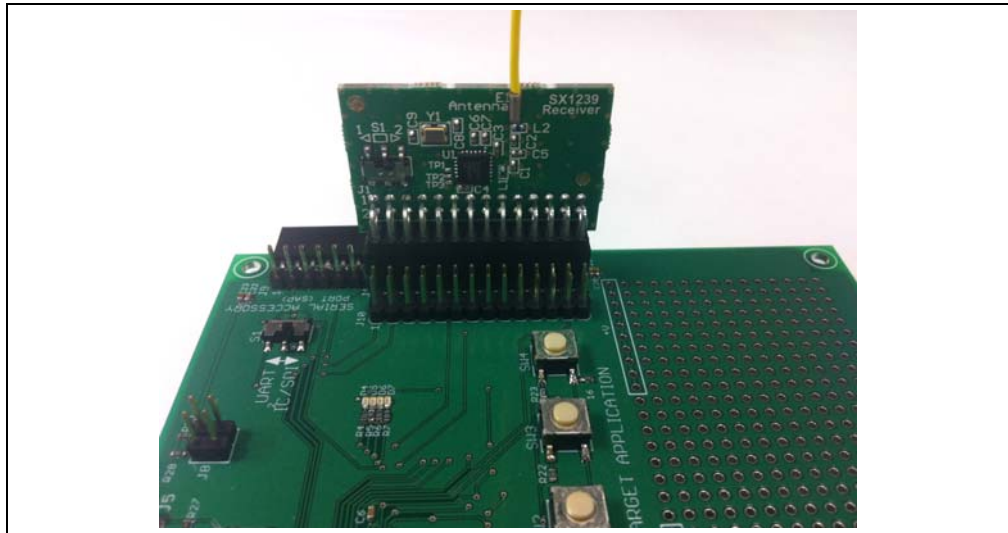
The source code for the demo is available from the Wireless Security Remote Control Development Kit product web page at <http://www.microchip.com/security>.

### 2.4 DEMO SETUP

This section describes how to set up the kit contents to operate the remote control demo program.

1. Obtain a CR2032 coin battery (if not included in the development kit)
2. Open the plastic enclosure of the red key fob by carefully prying apart the two halves. Remove the PCB board from the plastic enclosure carefully. Observe the correct battery polarity and insert the CR2032 coin battery into the battery holder. Put the PCB board back in the plastic enclosure and close the enclosure.
3. To verify that the key fob is properly installed, press any button and the LED should be flashing when the button is pressed.
4. Plug in the RF receiver daughter board on the PICtail slot of the Embedded Security Development Board. Make sure that the RF receiver daughter board has the side with RF receiver chip face the center, as shown in [Figure 2-1](#).

**FIGURE 2-1: PLUG THE SX1239 RECEIVER PICtail™ DAUGHTER CARD INTO THE EMBEDDED SECURITY DEVELOPMENT BOARD**



**5. Power-up the Embedded Security Development Board.**

To power the Embedded Security Development Board from the USB port, connect the USB A to mini-B cable to the development board and an available USB port or USB power source. Set jumper J6 to pins 1-2. When using a USB port for power, there is no requirement to load the USB drivers.

To power the Embedded Security Development Board from an external power supply, connect test points labeled +VEXT and GND to a bench power supply set to 3.3 VDC. Place jumper J6 to pins 2-3.

## 2.5 DEMO OPERATION

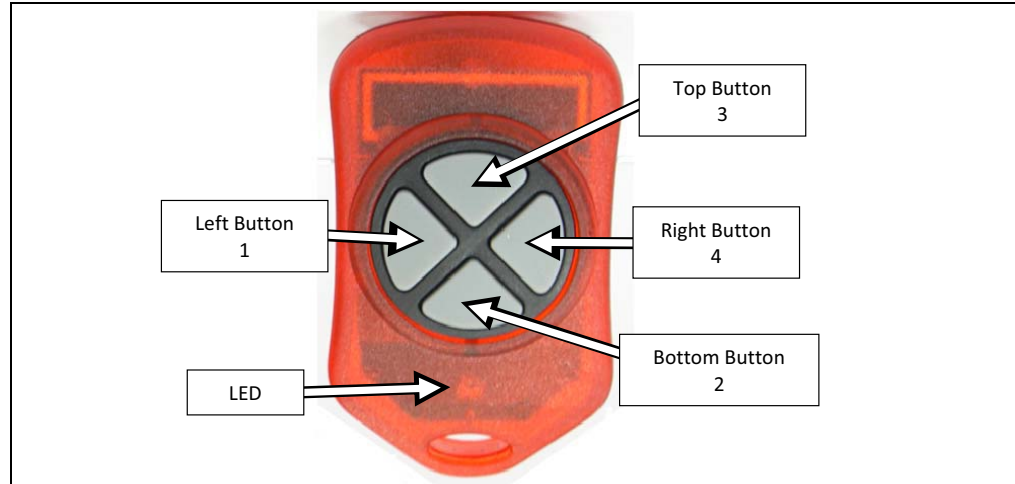
The pre-programmed demo is used to demonstrate the basic operation of Microchip Remote Keyless Entry (RKE) solutions. The demo highlights capabilities of transmitting and receiving data that is secured over the air. Two different methods, KEELOQ® Classic and KEELOQ® AES, are used in this demo.

### 2.5.1 Key Fob as Transmitter

The pre-programmed demonstration shows how to secure information during data transmission. Pressing any one of four buttons on the red key fob, the information about the pressed button will be encrypted and transmitted. When data is being transmitted, the LED on the key fob will flash. Two ways to secure the information have been shown in this demo: KEELOQ Classic and KEELOQ AES. When button 1 or 2 (see [Figure 2-2](#)) is pressed, the information is secured with KEELOQ Classic before the transmission; when button 3 or 4 (see [Figure 2-2](#)) is pressed, the information is secured with KEELOQ AES before the transmission.

For details on KEELOQ Classic and KEELOQ AES, please refer to Microchip application notes AN1259, “*KEELOQ® Microcontroller-Based Code Hopping Encoder*” and AN1265 “*KEELOQ® with AES Microcontroller-Based Code Hopping Encoder*”.

The key fob has four push buttons and is powered by a CR2032 coin battery. The key fob is shown in [Figure 2-2](#), where the four buttons are labeled individually.

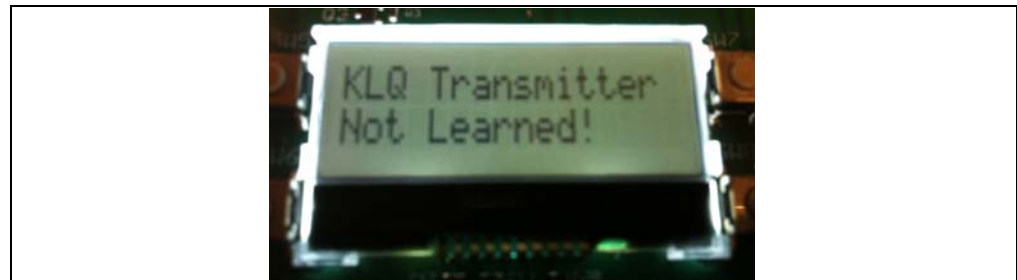
**FIGURE 2-2: KEY FOB WITH FOUR PUSH BUTTONS**

### 2.5.2 Embedded Security Development Board as Receiver

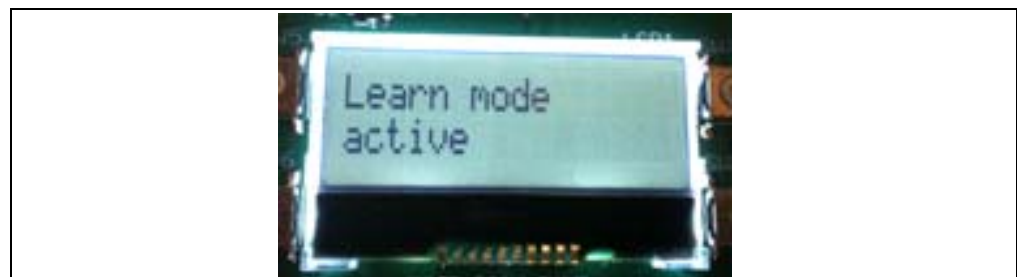
When the SX1239 Receiver PICtail Daughter Board receives a secured packet, the content of the packet is acquired by the target application microcontroller. Based on the length of the received packet, the target application microcontroller decides the cipher (KEELOQ Classic or KEELOQ AES) that is used to secure the data. The decryption process reveals the plain text, and the authentication process verifies whether the plain text is valid information.

#### 2.5.2.1 KEELOQ CLASSIC

For KEELOQ Classic, only a message from a known transmitter can be accepted by the receiver. If a packet is received from an unknown transmitter, the message **"KLQ Transmitter Not Learned"** will be displayed on the LCD, as shown in [Figure 2-3](#).

**FIGURE 2-3: ERROR MESSAGE OF RECEIVING PACKET FROM UNKNOWN TRANSMITTER**

To learn a transmitter, the receiver initiates the learning process by pressing button SW4. The learning procedure will be started and the message **"Learn mode active"** will be displayed on the LCD, as shown in [Figure 2-4](#).

**FIGURE 2-4: START LEARN MODE**

In the event no KEELOQ Classic packet from an unknown transmitter is received within 18 seconds, the KEELOQ Classic learn mode will time out and display the message “**Learn mode timeout**” on the LCD, as shown in [Figure 2-5](#).

**FIGURE 2-5: LEARN MODE TIMEOUT**



The known transmitters and their latest counters are stored in the Nonvolatile Memory (NVM) space of the microcontroller. When all slots in the NVM space for transmitters are taken, the learning process will fail. Pressing and holding button SW3 for a few seconds will erase all transmitter records from the NVM, and then the display message “**Memory Erased**” on the LCD, as shown in [Figure 2-6](#).

**FIGURE 2-6: ERASE TRANSMITTER RECORDS FROM MEMORY**



When a KEELOQ Classic packet is received from a known transmitter, the contents of the packet is displayed on the LCD, as shown in [Figure 2-7](#). The following information from the KEELOQ Classic packet are available:

- Encoder: KLQ that represents KEELOQ Classic
- Serial number of the transmitter: 28-bit serial number (according to [Figure 2-7](#)) in this transmission
- Counter: 16-bit number (according to [Figure 2-7](#)) in this transmission
- Function Code: A bitmap of the pressed buttons (it will be 3 if both KLQ buttons are pressed), depending on the button pressed on the key fob

**FIGURE 2-7: KEELOQ PACKET INFORMATION**



### 2.5.2.2 KEELOQ AES

For KEELOQ AES, there is no requirement that a transmitter must be known to the receiver before a packet can be accepted, so there is no learning process for a packet that is encoded with KEELOQ AES cipher. When a KEELOQ AES packet is received, the contents of the packet is displayed on the LCD, as shown in [Figure 2-8](#). The following information from the KEELOQ AES packet are available:

- Encoder: AES that represents KEELOQ AES
- Serial number of the transmitter: 32-bit serial number (according to [Figure 2-8](#)) in this transmission
- Counter: 32-bit counter (according to [Figure 2-8](#)) in this transmission
- Function Code: A bitmap of pressed buttons, depending on the button pressed on the key fob

**FIGURE 2-8:**



## 2.6 EMBEDDED SECURITY DEVELOPMENT BOARD HARDWARE SELF-CHECK

A hardware self-check can be performed to ensure the hardware integrity of the Embedded Security Development Board. The instruction of the hardware self-check is displayed on the LCD. The test result is either checked by firmware and display on the LCD, or verified by user observation.

To initiate the hardware self-check, press and hold push button SW1 before powering up the Embedded Security Development Board. SW1 can then be released when “**HDW Self Tests**” is displayed on the LCD screen. Four individual hardware self-tests will then be performed one by one.

### 2.6.0.1 BUTTON TESTS

“**Button Test**” will be displayed on the first line of the LCD display. Test instructions of pressing individual buttons will be displayed on the second line of the LCD display. Once a required push button is pressed, the test instruction message will be changed for the next push button. Once all push buttons have been tested, SW1 needs to be pressed to move forward to the LED test.

### 2.6.0.2 LED TESTS

There are two sets, ten LEDs, which can be controlled by the host and target application microcontroller separately. When LED tests start, the message “**LEDs Flashing**” will be displayed on the first line of the LCD display. During the tests, two sets of LEDs will be flashing separately, while LEDs from the same set should be flashing together. The user should observe that all LEDs are turned on and off with flashing intervals of roughly one second. Once the user has verified the LED test, SW1 needs to be pressed to move forward to the RTCC test.



## 2.6.0.3 RTCC TEST

When RTCC tests are initiated, the LCD display will show the clock and calendar. If no coin battery for RTCC has been installed, the time displayed will be close to the reset time of January 1, 2012. On the other hand, if a coin battery for RTCC is installed, the time displayed will be based on whatever is previously set, plus the time that has been passed. Observe that the clock is advancing. Once the RTCC test is done, SW1 needs to be pressed to move forward to the SPI test.

## 2.6.0.4 SPI TEST

The SPI test in hardware self-check is performed to the SPI bus that connects the target application microcontroller and the SX1239 Receiver PICtail Daughter Board. Therefore, the SX1239 Receiver PICtail Daughter Board must have been plugged in before this test starts. Once the SPI test starts, the target application microcontroller requests specific information from the SX1239 receiver through the SPI bus. If the expected response is received, then the **“Successful”** status will be displayed; otherwise, the **“Fail”** status will be displayed.

**Note:** If a PICtail daughter board other than the SX1239 Receiver PICtail Daughter Board is plugged into the PICtail connector, even though the SPI bus may still work, the SPI test might show failure status. The reason is due to the expected values to be received from the SX1239.

---

---

**Chapter 3. PIC12LF1840T39A Wireless Remote Key Fob**

---

---

**3.1 INTRODUCTION**

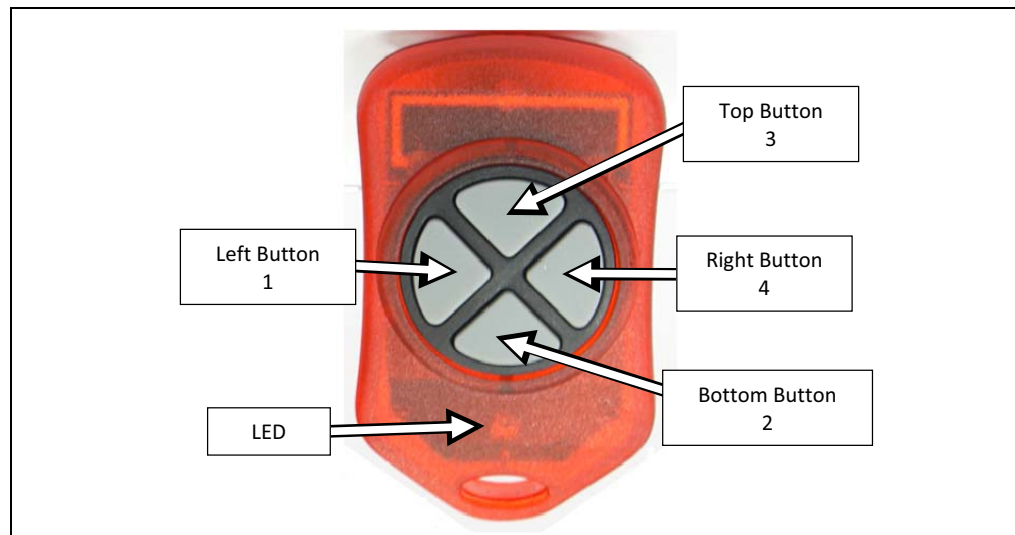
The PIC12LF1840T39A Wireless Remote Key Fob is a demonstration and development platform for wireless security remote control applications. This section gives a detailed description of the key fob.

**3.2 HARDWARE DESCRIPTION**

Figure 3-1 shows the key fob. The enclosure is an off-the-shelf key fob enclosure from Polycase (<http://www.polycase.com/>). The enclosure houses a two-sided Printed Circuit Board (PCB).

The schematic, PCB layout, and Bill of Materials are listed in [Appendix A. "PIC12LF1840T39A Wireless Remote Key Fob Schematics"](#).

**FIGURE 3-1: PIC12LF1840T39A WIRELESS REMOTE KEY FOB**

**3.3 PRINTED CIRCUIT BOARD DESCRIPTION**

The key fob PCB is a two-layer, plated through hole, 0.031 inches (0.7874 millimeters) thick, FR4 material. Figure 3-2 shows the top layer of the PCB. All components, except the LED, are on the top layer. A PCB antenna is employed in the design for reduced cost and compactness. The PCB antenna is explained in more detail below.

P1 is the ICSP™ programming port. See [Chapter 6. "Developing with the Wireless Security Remote Control Development Kit"](#) for suggestions on developing and programming the key fob.

FIGURE 3-2: PCB TOP LAYER PHOTO

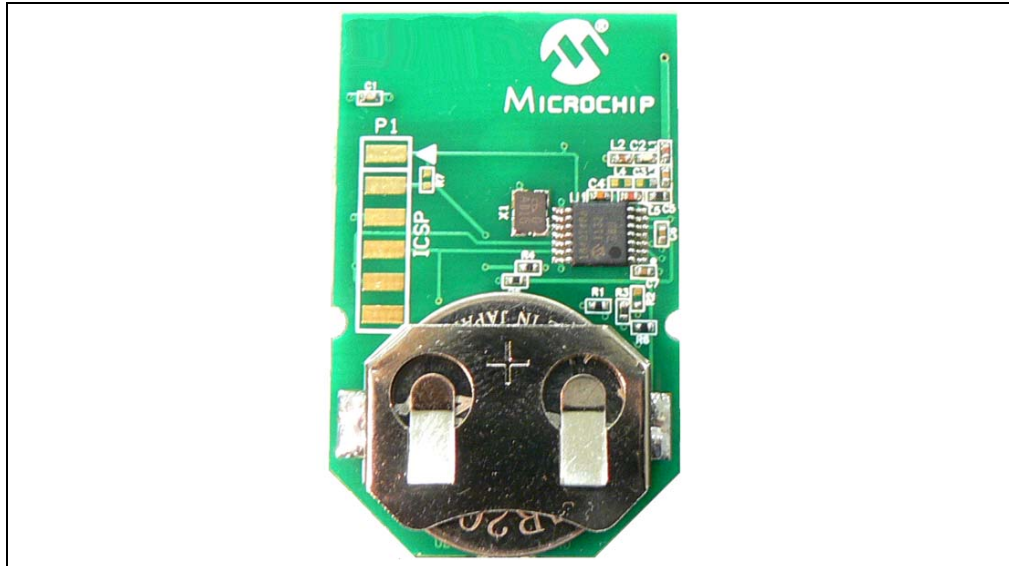
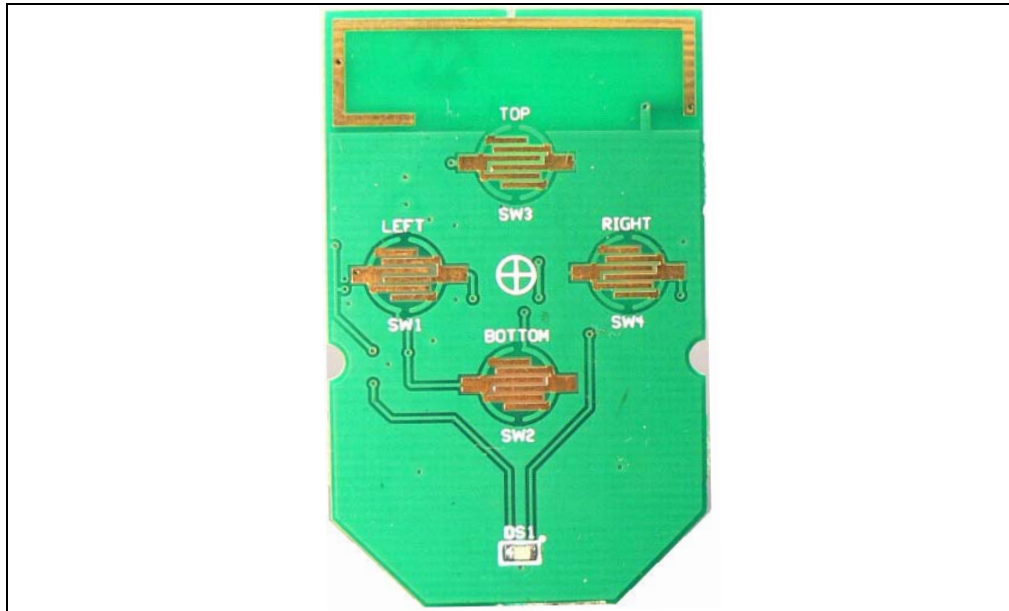


Figure 3-3 shows the bottom layer of the PCB. The bottom layer shows the PCB loop antenna and the PCB traces for the conductive push buttons from the plastic enclosure.

FIGURE 3-3: PCB BOTTOM LAYER PHOTO



## 3.4 PCB ANTENNA DESCRIPTION

The PCB antenna is a combination of top and bottom PCB layer traces, as shown in Figure 3-4. The feed point from the transmitter is on the right side of the figure. It is a top layer trace shown in red. It taps into the PCB loop antenna on the bottom layer shown in blue. The antenna loops to the left side of the PCB and is terminated to ground by a capacitor.

The PCB antenna is an “electrically small loop antenna.” That is, the wavelength of the antenna is very much less than the one-quarter wavelength that antennas are normally designed to. This type of antenna has an extremely high quality factor (Q). Therefore, it is very susceptible to parasitic impedances and very challenging to impedance match to the transmitter.

Figure 3-4 is a design suggestion. The designer is cautioned that even though this design can be copied, the final product will require tuning. There are many factors that determine the performance of a PCB antenna: thickness of the copper layer, thickness of the PCB material, choice of the PCB material (e.g., FR4), and choice of the passive components used in the impedance matching circuit. The PCB antenna dimensions are not critical. Once the design has been tuned, what is important is the consistency of the manufacture.

**FIGURE 3-4: PCB ANTENNA DIMENSIONS**

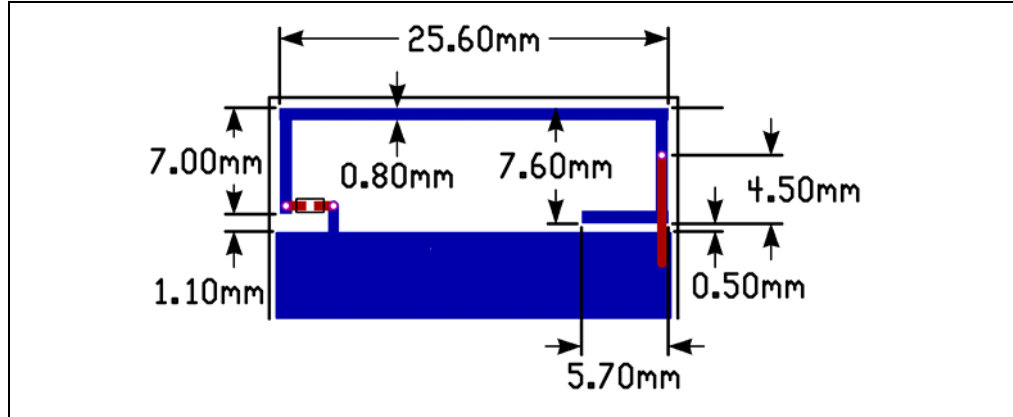
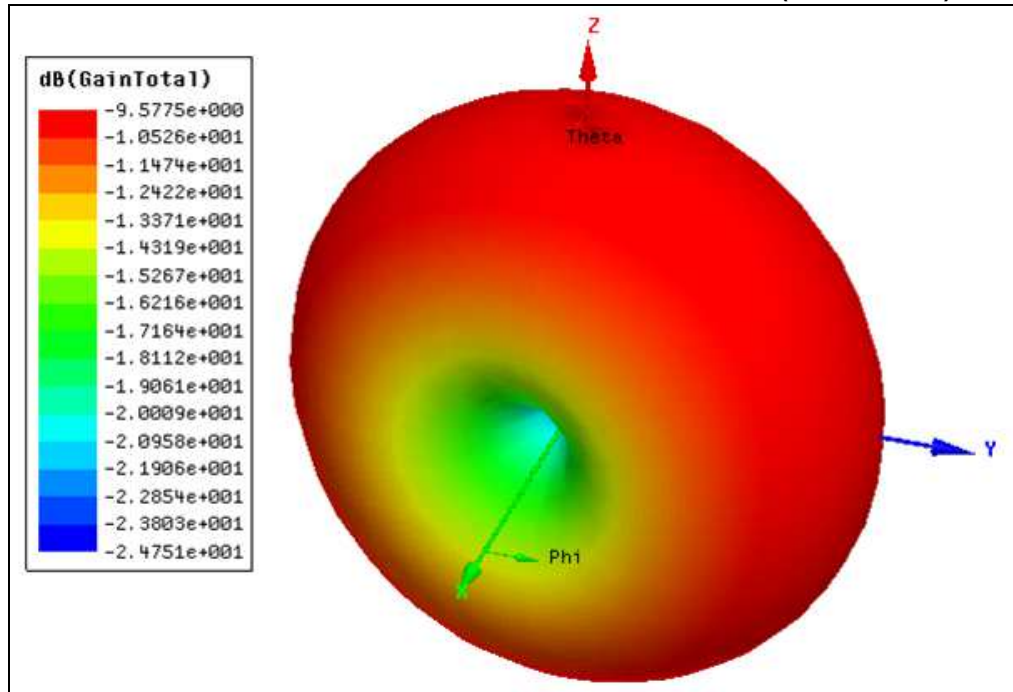
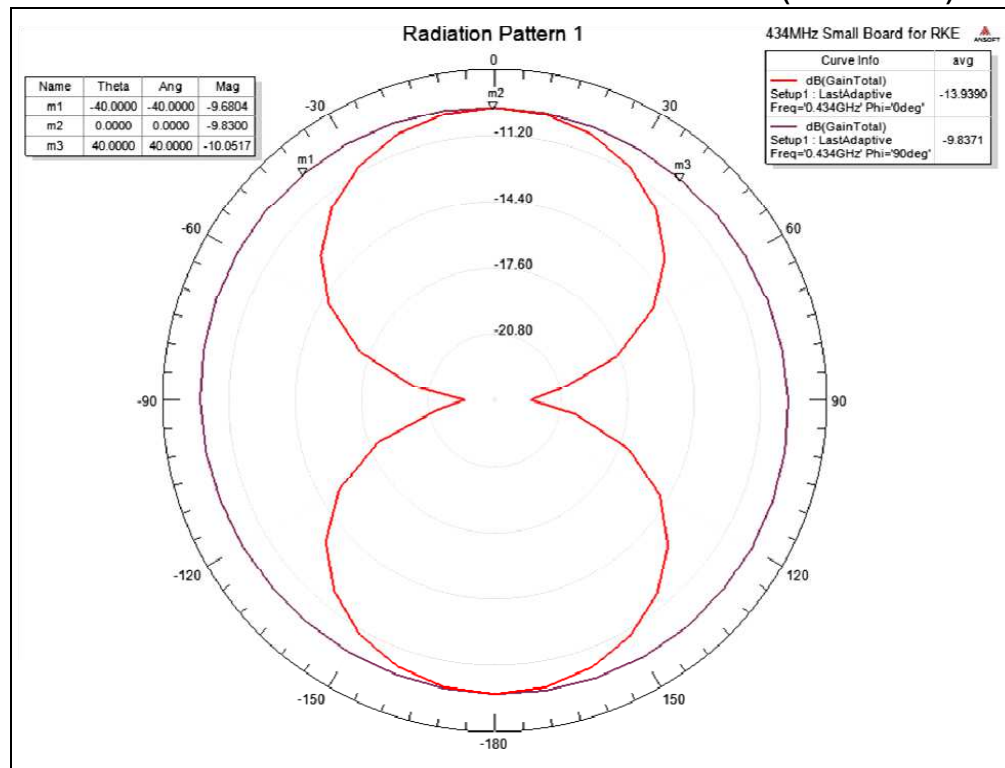


Figure 3-5 shows the simulated three-dimensional plot of the radiation pattern from the antenna. Figure 3-6 shows the two-dimensional plots.

**FIGURE 3-5: PCB ANTENNA 3D RADIATION PATTERN (SIMULATED)**



**FIGURE 3-6: PCB ANTENNA 2D RADIATION PATTERN (SIMULATED)**



---

---

**Chapter 4. SX1239 Receiver PICtail™ Daughter Board**

---

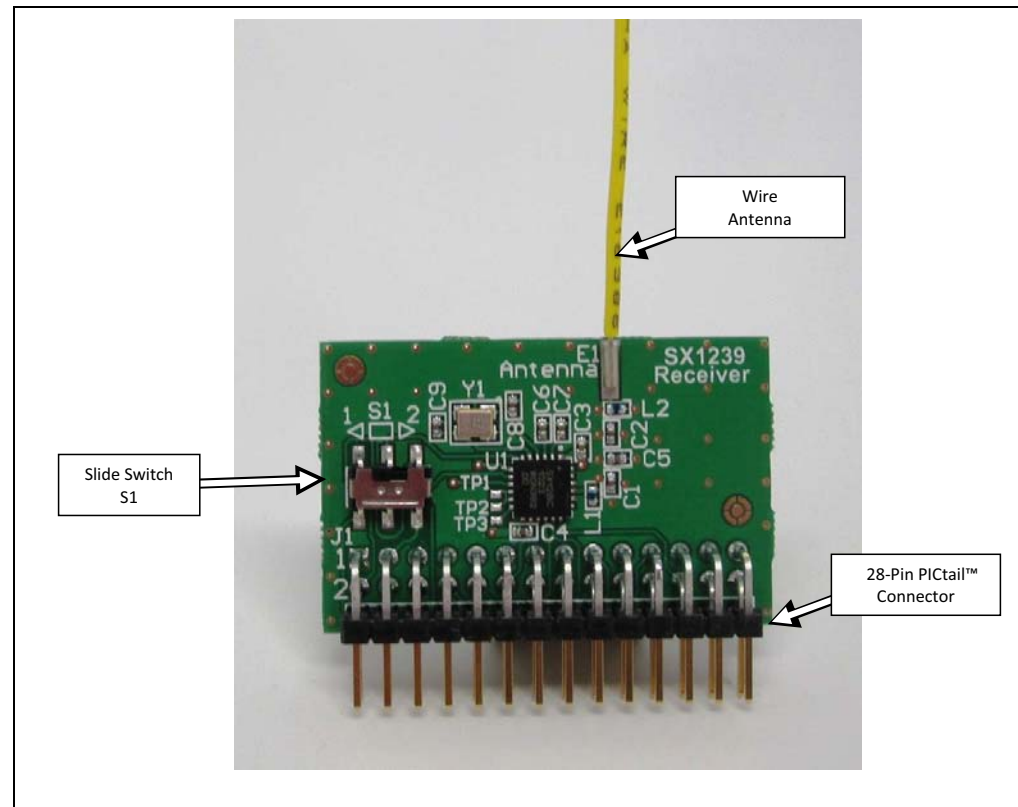
---

**4.1 INTRODUCTION**

The SX1239 PICtail™ Receiver Daughter Board is a demonstration and development platform for wireless security remote control applications. This section gives a detailed description of the receiver daughter board.

**4.2 HARDWARE DESCRIPTION**

Figure 4-1 shows the SX1239 Receiver PICtail Daughter Board. The schematic, PCB layout, and Bill of Materials are listed in [Appendix B. “SX1239 Receiver PICtail™ Daughter Board Schematics”](#).

**FIGURE 4-1: SX1239 PICtail™ DAUGHTER BOARD**

The daughter board features the Semtech SX1239 Low-Power Integrated UHF Receiver (<http://www.semtech.com/wireless-rf/rf-receivers/sx1239/>). The PICtail daughter board can plug into the 28-pin PICtail connector featured on many Microchip Technology development tools.

The antenna connection has a pin socket for plugging a wire antenna. This demonstrates a simple and low-cost antenna option. The length of the antenna should be approximately  $\frac{1}{4}$  wavelength of the frequency of interest.