

Introduction

This application note describes a KeeLoq® garage door opener application using the ATA8510 and the WBZ451 devices. The application is equipped with hardware modules and software for both the keyfob and the base station.

The keyfob includes both devices, the WBZ451 Bluetooth® Low Energy controller and the ATA8510 Sub-GHz device. This configuration enables communication with either a Bluetooth Low Energy base station or a classic Sub-GHz base station.

The application implements the Microchip's KeeLoq crypto key generation and the communication protocol. It supports the following three KeeLoq variants:

- Classic
- Advanced
- Ultimate

Table of Contents

Introduction.....	1
1. Quick References.....	3
1.1. Reference Documentation.....	3
1.2. Software Prerequisites.....	3
1.3. Hardware Prerequisites.....	3
1.4. Acronyms and Abbreviations.....	3
2. Hardware Setup.....	4
3. Getting Started.....	5
3.1. Setting Up the Garage Opener Project.....	5
3.2. Tools and Development Environments.....	5
4. KeeLoq Technology.....	6
4.1. Classic KeeLoq Technology.....	6
4.2. Advanced KeeLoq Technology.....	7
4.3. Ultimate KeeLoq Technology.....	7
5. Software.....	9
5.1. Keyfob.....	9
5.2. Base Station.....	9
6. Document Revision History.....	11
Microchip Information.....	12
The Microchip Website.....	12
Product Change Notification Service.....	12
Customer Support.....	12
Microchip Devices Code Protection Feature.....	12
Legal Notice.....	12
Trademarks.....	13
Quality Management System.....	14
Worldwide Sales and Service.....	15

1. Quick References

1.1 Reference Documentation

- *Introduction to Ultimate KEELOQ Technology* (DS00001683)
- *MCS3142 Dual KEELOQ Technology Encoder Data Sheet* ([DS40001747](#))
- *MCS3122 Advanced KEELOQ Technology Encoder Data Sheet* ([DS40001762](#))
- *UHF ASK/FSK Transceiver User Manual* ([DS50003142](#))
- *WBZ451 Curiosity Board User's Guide* ([DS50003367](#))

1.2 Software Prerequisites

- MPLAB® X Integrated Development Environment ([MPLAB X IDE v6.10](#))

1.3 Hardware Prerequisites

- WBZ451 Curiosity Board (Bluetooth Low Energy Connection)
- ATAB5831C Board (Sub-GHz Connection)

1.4 Acronyms and Abbreviations

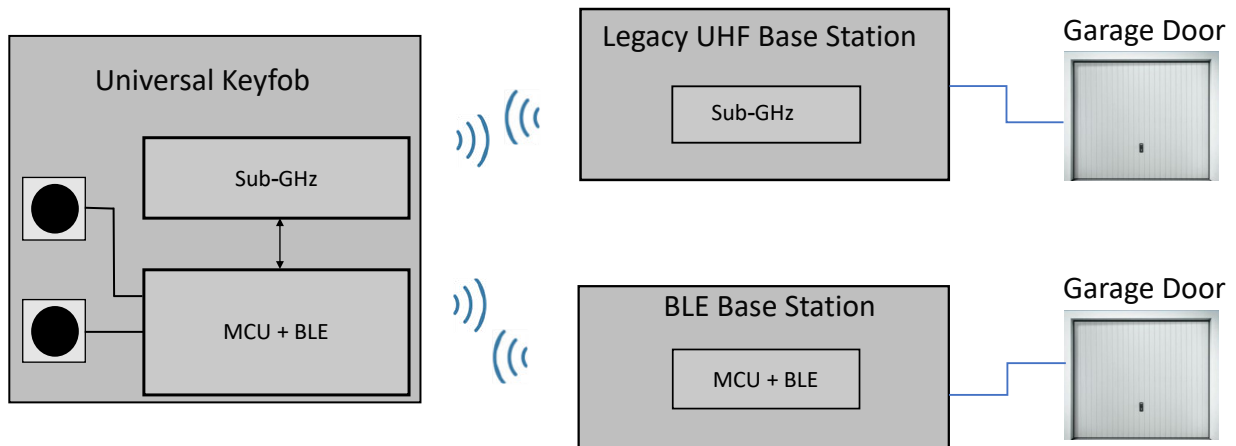
Table 1-1. Acronyms and Abbreviations

Acronyms and Abbreviations	Description
AES	Advanced Encryption Standard
LE	Low Energy
COM	Communication
EEPROM®	Electrical Erasable Programmable Read-Only Memory
ISP	In-System Programming
LED	Light Emitting Diode
LSb	Least Significant bit
NLFSR	Non-Linear Feedback Shift Register
PKOB4	PICKit On-Board 4
QSPI	Quad Serial Peripheral Interface
RF	Radio Frequency
SW	Software
UART	Universal Asynchronous Receiver Transmitter
UHF	Ultra-High Frequency
USB	Universal Serial Bus

2. Hardware Setup

The keyfob software includes a special feature for automatically detecting old Sub-GHz and Bluetooth Low Energy base stations. Depending on the type of base station, the software utilizes the corresponding Radio Frequency (RF) mode for communication.

Figure 2-1. Hardware Setup



The software contains all the services for a simple keyfob function, such as interrupt services for the buttons, communication type detection, as well as key pairing functions. It also contains the appropriate software for a Bluetooth Low Energy base station.

3. Getting Started

The following chapters provide more details about getting started with the sample code and a description of the code and the software interfaces.

3.1 Setting Up the Garage Opener Project

The delivered source directory contains two project files:

- Keyfob
- Base station Flash software

The user can open the project files using the MPLAB X IDE.

3.2 Tools and Development Environments

3.2.1 USB Connectivity Using Microchip USB 2.0 Hub Controller

The WBZ451 Curiosity Board has two Universal Serial Bus (USB) end devices:

- PICkit™ On-board 4 (PKOB4)
- MCP2200

Both of these USB devices are accessible to the upstream PC via a common USB connector. The PKOB4 serves as an integrated programmer and debugger, eliminating the need for additional programming or debugging tools. On the other hand, the MCP2200 functions as a USB-to-Universal Asynchronous Receiver Transmitter (UART) converter with hardware flow control support, allowing users to establish a serial UART connection to the Host PC.

3.2.2 MPLAB X Integrated Development Environment (IDE)

The MPLAB X Integrated Development Environment (IDE) is an expandable, highly configurable software program that incorporates powerful tools to help the user discover, configure, develop, debug and qualify embedded designs for most of the microcontrollers and digital signal controllers. MPLAB X IDE works seamlessly with the MPLAB development ecosystem of software and tools, many of which are completely free.

3.2.3 ATA5831 Configuration Tool

The EEPROM within the ATA8510 device stores the configuration settings of the RF transceiver. The ATA5831 configuration tool operates on a Java runtime engine providing significant assistance in managing configuration settings. For EEPROM® programming, use the *.hex file to export with the programming tools.

4. KeeLoq Technology

Microchip Technology stands as a major supplier in the security industry. Our use of the proprietary KeeLoq technology is instrumental in enhancing security across various applications for leading manufacturers worldwide.

KeeLoq technology is a code-hopping technology, which means that each transmission is unique with changes occurring at every button press. The core of this technology involves a counter that increments with each button press, followed by the addition of an encryption layer to the packet. This system operates on an event-driven basis, where the event corresponds to the pressing of a button on the transmitter. In the extended implementation of the ultimate KeeLoq technology, a timer replaces the counter. This timer runs at the same rate as a corresponding timer on the receiver side.

The following shows a comparison table with all available KeeLoq technology implementations.

Table 4-1. KeeLoq Technologies

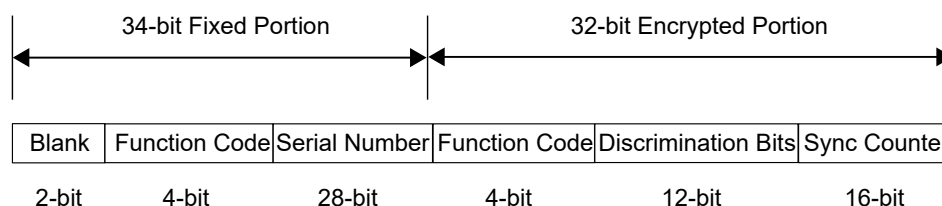
KeeLoq® Technology	Security Level	Encryption/Decryption Engine	Encryption/Decryption Key Length	Transmission Length	Synchronization
Classic KeeLoq technology	Medium	Non-linear Feedback Shift Register (NLFSR)	64 bits	66 bits	Counter
Advanced KeeLoq technology	High	Advanced Encryption Standard (AES)	128 bits	168 bits	Counter
Ultimate KeeLoq technology	High	AES	128 bits	192 bits	Counter + Timer

4.1 Classic KeeLoq Technology

The classic KeeLoq packet consists of two parts:

- Sent in plain text
- Sent in encrypted

Figure 4-1. Classic KeeLoq Technology



4.1.1 Encrypted Code Portion

The encrypted portion of the classic KeeLoq packet contains:

- 16-bit synchronization counter. This value is used to create the hopping code. This value is incremented after each button press.
- 12 discrimination bits. These are the 12 LSb of the serial number. This value is used as post decryption check.
- 4-bit function code. Indicating the buttons pressed on the encoder. This value is also sent in the fixed portion and can be used for post decryption check.

4.1.2 Fixed Code Portion

The fixed portion of the classic KeeLoq packet contains:

- 28-bit serial number. This value must be specific to each individual encoder.
- 4-bit function code. Also sent in encrypted portion.
- 2-bit blanks

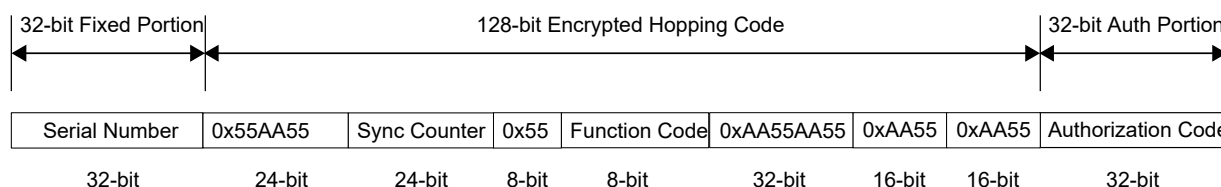
4.1.3 Secure Key Generation

The secure key generation scheme uses a random number (called a seed) and a manufacturer's code (stored at the encoder and decoder) to generate the encryption/decryption key. The 60-bit seed value is sent together with the function code, indicating that this is a seed transmission, and the 2-bit blanks.

4.2 Advanced KeeLoq Technology

Advanced KeeLoq technology is similar to classic KeeLoq technology, except that it provides a higher level of security due to the stronger AES (in comparison to NLFSR) encryption algorithm.

Figure 4-2. Advanced KeeLoq Technology



4.2.1 Authorization Code Portion

The AES encryption algorithm generates the authorization code. The calculation takes place over the entire code word, including the encrypted hopping code and the fixed portion, using the authorization key as input. The authorization code portion consists of the least significant 32 bits of the calculated authorization code.

4.2.2 Hopping Code Portion

The system calculates the hopping code portion by encrypting the padded values, function code and synchronization counter with the AES key.

4.2.3 Fixed Code Portion

The fixed code portion consists of the 32-bit serial number. This serial number is unique to a system.

4.2.4 Secure Key Generation

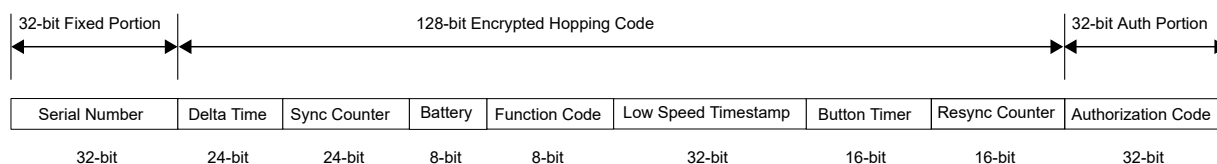
Use the seed word when pairing the transmitter to a receiver using a secure learn methodology.

To indicate a seed transmission, the encoder sets the serial number to 0xFFFFFFFF. The upper 64-bit of the 128-bit seed value is padded with 0x12121212.

The encryption/decryption key is generated similarly to the classic KeeLoq technology using the seed value and manufacturer's code.

4.3 Ultimate KeeLoq Technology

Ultimate KeeLoq technology adds an on-board, free-running timer. When the user presses a button, the system captures a snapshot of its internal timer value and sends it inside the encrypted data packet. The receiver also has an on-board timer at its end. If pairing a transmitter to a receiver, the receiver stores relevant information, such as the timer value when synchronized, the last received timestamp and the resynchronization counter.

Figure 4-3. Ultimate KeeLoq Technology

4.3.1 Authorization Code Portion

The AES encryption algorithm generates the authorization code. The calculation takes place over the entire code word, including the encrypted hopping code and the fixed portion, using the authorization key as input. The authorization code portion consists of the least significant 32 bits of the calculated authorization code.

4.3.2 Hopping Code Portion

The hopping code portion is calculated by encrypting the resynchronization counter, button timer, low speed timestamp, function code, battery level, synchronization counter and the delta time with the AES key.

- The resynchronization counter is incremented in the transmitter or receiver side in case of power loss. If these counter values differ, the resynchronization will occur.
- The button timer represents the total time a button is pressed (not implemented).
- The low-speed timestamp contains a snapshot of the actual timer value.
- The function code represents the button pressed at the transmitter.
- The battery level indicates the battery level of the transmitter (not implemented).
- The synchronization counter is always incremented whenever a button is pressed and a new code word is prepared.
- The delta time represents the elapsed time since the previous code word is sent (not implemented).

4.3.3 Fixed Code Portion

The fixed code portion consists of the 32-bit serial number. This serial number is unique to a system.

4.3.4 Secure Key Generation

Use the seed word when pairing the transmitter to a receiver using a secure learn methodology.

To indicate a seed transmission, the encoder sets the serial number to 0xFFFFFFFF. The upper 64-bit of the 128-bit seed value is padded with 0x12121212.

The encryption/decryption key is generated similarly to the classic KeeLoq technology using the seed value and manufacturer's code.

5. Software

The keyfob and the base station Flash software offer several configurations through compiler defines. The primary function of the software is to enable the KeeLoq technology (classic/advanced/ultimate). In addition, it allows further debugging by enabling a virtual Communication (COM) port to the PC and some debug pins.

The Quad Serial Peripheral Interface (QSPI) serial Flash, which is soldered on the WBZ451 Curiosity Board, stores all the necessary variables required for the KeeLoq algorithm.

To establish a connection in the Pairing mode, the Bluetooth Low Energy address must be unique to a system. Otherwise, the keyfob switches to Ultra-High Frequency (UHF) communication.

When the keyfob/base station is powered up and the QSPI serial Flash is empty, the software assumes that this is the first power-up and proceeds to write a default EEPROM setting to the ATA8510 via In-System Programming (ISP).

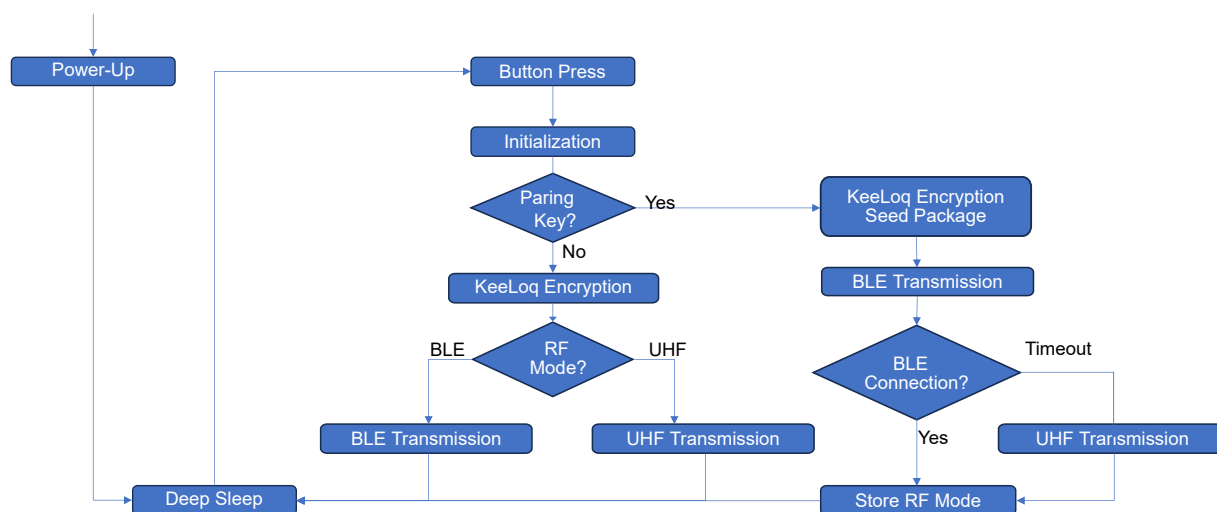
5.1 Keyfob

The keyfob software primarily operates in the Deep Sleep mode to reduce current consumption. Pressing a button initiates a wake-up along with a KeeLoq package transmission.

For debugging purposes, disable the Sleep mode by using a compiler define to interface with the keyfob via the virtual COM port. This is necessary to store the serial number and the seed value to the keyfob.

The two buttons SW1 and SW2 are currently configured for package transmission, reflected in the function code of the KeeLoq package. To transmit a seed package for pairing, hold down the SW2 button while pressing the SW1 button.

Figure 5-1. Flow Diagram



5.2 Base Station

The base station software is continuously monitoring for incoming packets via Bluetooth Low Energy and UHF. Upon receiving a packet, the system decodes and verifies its validity.

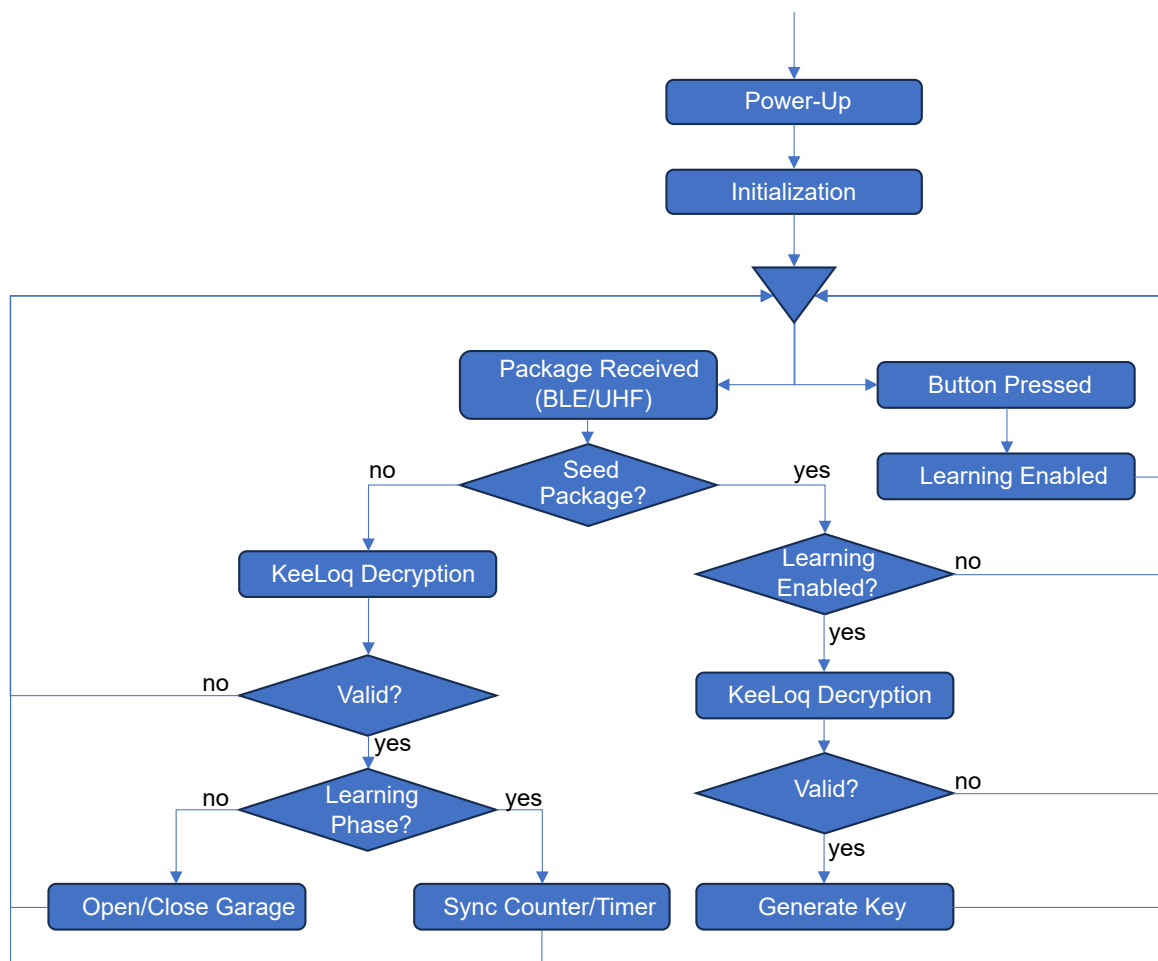
To monitor validity, observe the outputs on the virtual COM port or check the Light Emitting Diode (LED) indicators:

- Green LED indicates a valid packet

- Red LED indicates an invalid packet
- Blue LED indicates a learning state

To activate the Learning mode, press the SW2 button. Otherwise, the system considers the seed packages invalid.

Figure 5-2. Flow Diagram



6. Document Revision History

The revision history describes the changes that were implemented in the document. The changes are listed by revision, starting with the most current publication.

Table 6-1. Document Revision History

Revision	Date	Section	Description
A	03/2024	Document	Initial Revision

Microchip Information

The Microchip Website

Microchip provides online support via our website at www.microchip.com/. This website is used to make files and information easily available to customers. Some of the content available includes:

- **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 design partner 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

Product Change Notification Service

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

To register, go to www.microchip.com/pcn and follow the registration instructions.

Customer Support

Users of Microchip products can receive assistance through several channels:

- Distributor or Representative
- Local Sales Office
- Embedded Solutions Engineer (ESE)
- Technical Support

Customers should contact their distributor, representative or ESE for support. Local sales offices are also available to help customers. A listing of sales offices and locations is included in this document.

Technical support is available through the website at: www.microchip.com/support

Microchip Devices Code Protection Feature

Note the following details of the code protection feature on Microchip products:

- Microchip products meet the specifications contained in their particular Microchip Data Sheet.
- Microchip believes that its family of products is secure when used in the intended manner, within operating specifications, and under normal conditions.
- Microchip values and aggressively protects its intellectual property rights. Attempts to breach the code protection features of Microchip product is strictly prohibited and may violate the Digital Millennium Copyright Act.
- Neither Microchip nor any other semiconductor manufacturer can guarantee the security of its code. Code protection does not mean that we are guaranteeing the product is "unbreakable". Code protection is constantly evolving. Microchip is committed to continuously improving the code protection features of our products.

Legal Notice

This publication and the information herein may be used only with Microchip products, including to design, test, and integrate Microchip products with your application. Use of this information in any other manner violates these terms. Information regarding device applications 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. Contact your local Microchip sales office for additional support or, obtain additional support at www.microchip.com/en-us/support/design-help/client-support-services.

THIS INFORMATION IS PROVIDED BY MICROCHIP "AS IS". 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 ANY IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, AND FITNESS FOR A PARTICULAR PURPOSE, OR WARRANTIES RELATED TO ITS CONDITION, QUALITY, OR PERFORMANCE.

IN NO EVENT WILL MICROCHIP BE LIABLE FOR ANY INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, OR CONSEQUENTIAL LOSS, DAMAGE, COST, OR EXPENSE OF ANY KIND WHATSOEVER RELATED TO THE INFORMATION OR ITS USE, HOWEVER CAUSED, EVEN IF MICROCHIP HAS BEEN ADVISED OF THE POSSIBILITY OR THE DAMAGES ARE FORESEEABLE. TO THE FULLEST EXTENT ALLOWED BY LAW, MICROCHIP'S TOTAL LIABILITY ON ALL CLAIMS IN ANY WAY RELATED TO THE INFORMATION OR ITS USE WILL NOT EXCEED THE AMOUNT OF FEES, IF ANY, THAT YOU HAVE PAID DIRECTLY TO MICROCHIP FOR THE INFORMATION.

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 unless otherwise stated.

Trademarks

The Microchip name and logo, the Microchip logo, Adaptec, AVR, AVR logo, AVR Freaks, BesTime, BitCloud, CryptoMemory, CryptoRF, dsPIC, flexPWR, HELDO, IGLOO, JukeBlox, KeeLoq, Kleer, LANCheck, LinkMD, maXStylus, maXTouch, MediaLB, megaAVR, Microsemi, Microsemi logo, MOST, MOST logo, MPLAB, OptoLyzer, PIC, picoPower, PICSTART, PIC32 logo, PolarFire, Prochip Designer, QTouch, SAM-BA, SenGenuity, SpyNIC, SST, SST Logo, SuperFlash, Symmetricom, SyncServer, Tachyon, TimeSource, tinyAVR, UNI/O, Vectron, and XMEGA are registered trademarks of Microchip Technology Incorporated in the U.S.A. and other countries.

AgileSwitch, ClockWorks, The Embedded Control Solutions Company, EtherSynch, Flashtec, Hyper Speed Control, HyperLight Load, Libero, motorBench, mTouch, Powermite 3, Precision Edge, ProASIC, ProASIC Plus, ProASIC Plus logo, Quiet-Wire, SmartFusion, SyncWorld, TimeCesium, TimeHub, TimePictra, TimeProvider, and ZL are registered trademarks of Microchip Technology Incorporated in the U.S.A.

Adjacent Key Suppression, AKS, Analog-for-the-Digital Age, Any Capacitor, AnyIn, AnyOut, Augmented Switching, BlueSky, BodyCom, Clockstudio, CodeGuard, CryptoAuthentication, CryptoAutomotive, CryptoCompanion, CryptoController, dsPICDEM, dsPICDEM.net, Dynamic Average Matching, DAM, ECAN, Espresso T1S, EtherGREEN, EyeOpen, GridTime, IdealBridge, IGaT, In-Circuit Serial Programming, ICSP, INICnet, Intelligent Paralleling, IntelliMOS, Inter-Chip Connectivity, JitterBlocker, Knob-on-Display, MarginLink, maxCrypto, maxView, memBrain, Mindi, MiWi, MPASM, MPF, MPLAB Certified logo, MPLIB, MPLINK, mSiC, MultiTRAK, NetDetach, Omniscient Code Generation, PICDEM, PICDEM.net, PICKit, PICtail, Power MOS IV, Power MOS 7, PowerSmart, PureSilicon, QMatrix, REAL ICE, Ripple Blocker, RTAX, RTG4, SAM-ICE, Serial Quad I/O, simpleMAP, SimpliPHY, SmartBuffer, SmartHLS, SMART-I.S., storClad, SQI, SuperSwitcher, SuperSwitcher II, Switchtec, SynchroPHY, Total Endurance, Trusted Time, TSHARC, Turing, USBCheck, VariSense, VectorBlox, VeriPHY, ViewSpan, WiperLock, XpressConnect, 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.

The Adaptec logo, Frequency on Demand, Silicon Storage Technology, and Symmcom are registered trademarks of Microchip Technology Inc. in other countries.

GestIC is a registered trademark of Microchip Technology Germany II GmbH & Co. KG, a subsidiary of Microchip Technology Inc., in other countries.

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

© 2024, Microchip Technology Incorporated and its subsidiaries. All Rights Reserved.

ISBN: 978-1-6683-4068-4

Quality Management System

For information regarding Microchip's Quality Management Systems, please visit www.microchip.com/quality.

Worldwide Sales and Service

AMERICAS	ASIA/PACIFIC	ASIA/PACIFIC	EUROPE
Corporate Office 2355 West Chandler Blvd. Chandler, AZ 85224-6199 Tel: 480-792-7200 Fax: 480-792-7277 Technical Support: www.microchip.com/support Web Address: www.microchip.com	Australia - Sydney Tel: 61-2-9868-6733 China - Beijing Tel: 86-10-8569-7000 China - Chengdu Tel: 86-28-8665-5511 China - Chongqing Tel: 86-23-8980-9588 China - Dongguan Tel: 86-769-8702-9880 China - Guangzhou Tel: 86-20-8755-8029 China - Hangzhou Tel: 86-571-8792-8115 China - Hong Kong SAR Tel: 852-2943-5100 China - Nanjing Tel: 86-25-8473-2460 China - Qingdao Tel: 86-532-8502-7355 China - Shanghai Tel: 86-21-3326-8000 China - Shenyang Tel: 86-24-2334-2829 China - Shenzhen Tel: 86-755-8864-2200 China - Suzhou Tel: 86-186-6233-1526 China - Wuhan Tel: 86-27-5980-5300 China - Xian Tel: 86-29-8833-7252 China - Xiamen Tel: 86-592-2388138 China - Zhuhai Tel: 86-756-3210040	India - Bangalore Tel: 91-80-3090-4444 India - New Delhi Tel: 91-11-4160-8631 India - Pune Tel: 91-20-4121-0141 Japan - Osaka Tel: 81-6-6152-7160 Japan - Tokyo Tel: 81-3-6880-3770 Korea - Daegu Tel: 82-53-744-4301 Korea - Seoul Tel: 82-2-554-7200 Malaysia - Kuala Lumpur Tel: 60-3-7651-7906 Malaysia - Penang Tel: 60-4-227-8870 Philippines - Manila Tel: 63-2-634-9065 Singapore Tel: 65-6334-8870 Taiwan - Hsin Chu Tel: 886-3-577-8366 Taiwan - Kaohsiung Tel: 886-7-213-7830 Taiwan - Taipei Tel: 886-2-2508-8600 Thailand - Bangkok Tel: 66-2-694-1351 Vietnam - Ho Chi Minh Tel: 84-28-5448-2100	Austria - Wels Tel: 43-7242-2244-39 Fax: 43-7242-2244-393 Denmark - Copenhagen Tel: 45-4485-5910 Fax: 45-4485-2829 Finland - Espoo Tel: 358-9-4520-820 France - Paris Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79 Germany - Garching Tel: 49-8931-9700 Germany - Haan Tel: 49-2129-3766400 Germany - Heilbronn Tel: 49-7131-72400 Germany - Karlsruhe Tel: 49-721-625370 Germany - Munich Tel: 49-89-627-144-0 Fax: 49-89-627-144-44 Germany - Rosenheim Tel: 49-8031-354-560 Israel - Ra'anana Tel: 972-9-744-7705 Italy - Milan Tel: 39-0331-742611 Fax: 39-0331-466781 Italy - Padova Tel: 39-049-7625286 Netherlands - Druenen Tel: 31-416-690399 Fax: 31-416-690340 Norway - Trondheim Tel: 47-72884388 Poland - Warsaw Tel: 48-22-3325737 Romania - Bucharest Tel: 40-21-407-87-50 Spain - Madrid Tel: 34-91-708-08-90 Fax: 34-91-708-08-91 Sweden - Gothenberg Tel: 46-31-704-60-40 Sweden - Stockholm Tel: 46-8-5090-4654 UK - Wokingham Tel: 44-118-921-5800 Fax: 44-118-921-5820