AN1323

PIC® MCU KEELOQ®/XTEA Receiver System with Acknowledge

Author: *Cristian Toma*
Microchip Technology Inc.

INTRODUCTION

A number of remote access applications rely on the user verifying if the access point (gate, door, vehicle, etc.) has been properly closed or opened. This application note describes a system by which the access point (receiver) responds back to the remote transmitter with a status message.

SYSTEM OVERVIEW

The system is implemented using the KEELOQ® 3 base station board. To add the described functionality to the KEELOQ 3 Development Kit, an add-on kit is used, consisting of a PICtail™ daughter board module, which features the MRF49XA transceiver and a key fob transmitter module. Both of these modules feature an integrated PCB loop antenna. The system uses a two-way key fob with open and close functions, which simulates the basic functions of a garage door or vehicle lock system. In addition, the key fob has the ability to query the receiver status over-the-air and display the status via the onboard LEDs.

The KEELOQ 3 receiver decodes the key fob transmission and displays the command issued by the key fob. The receiver will respond back to the key fob with the operation result (opened or closed).

RECEIVER FUNCTIONALITY

The receiver implements the main part of the system. It receives commands from the transmitter and sends back Acknowledges or response messages. It implements standard Open and Close functions, plus an additional Status function, which reports back to the transmitter the last known status of the receiver.

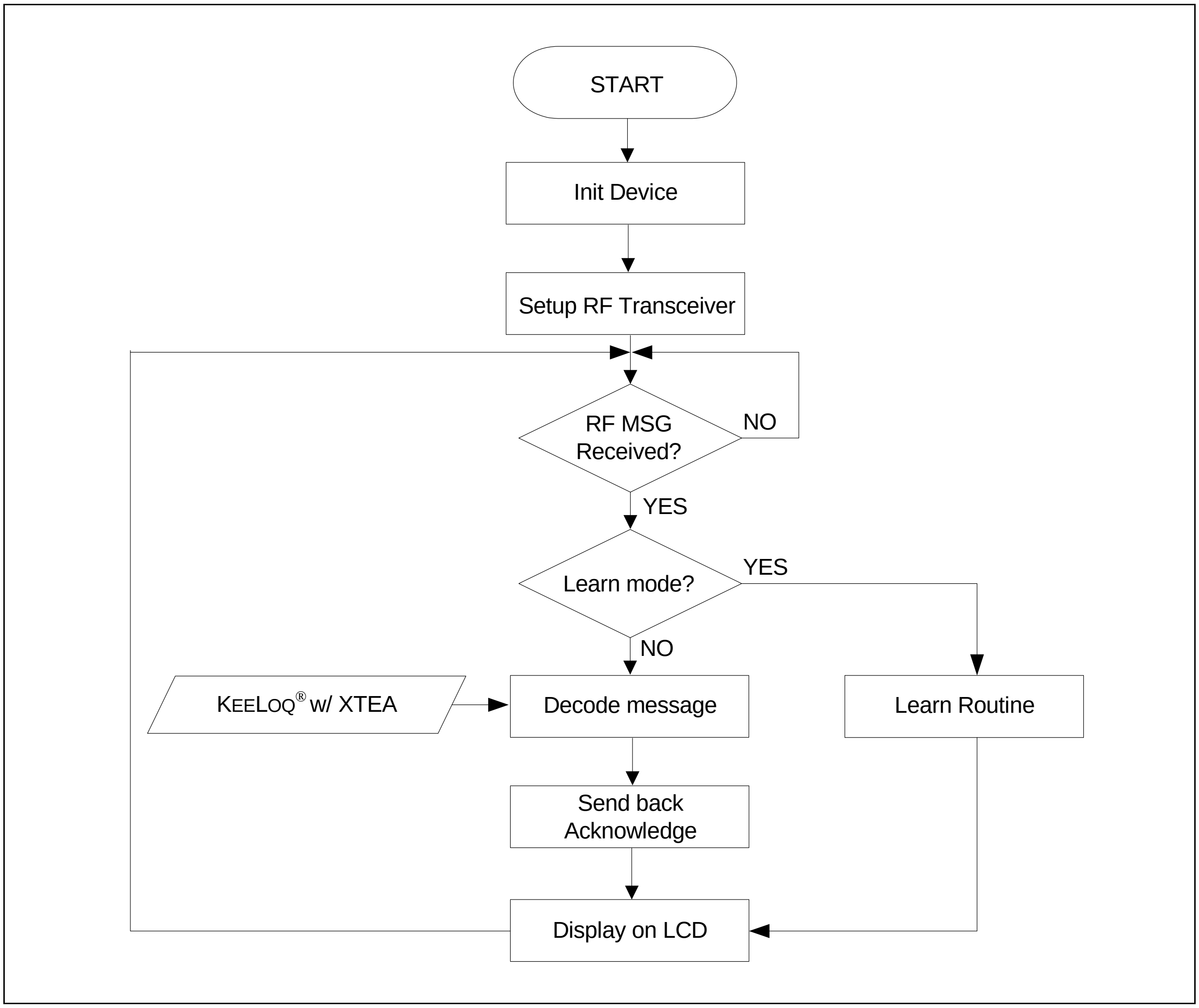
Upon receiving a data packet from the transmitter, the receiver will first verify if it is a known (learned) transmitter. If it is a known transmitter, the data packet is then decrypted. The receiver will acknowledge the received command or send a response.

TRANSMITTER LEARNING

The receiver will respond only to known transmitters. This means that, before a transmitter can be used with a receiver, it must be learned. By learning, we define the process by which the receiver gathers and stores information about a transmitter. This will typically include the serial number and the synchronization counter. If the receiver has this information, then it will be able to generate the key required to decrypt the received message.

Learning is done in two phases. The first phase needs a simple press of a button on the transmitter. This is to get information regarding the serial number and the synchronization counter. A second transmission is required in order to check the validity of the first transmission. If the two synchronization values are consecutive numbers, the transmitter is valid and its data is stored into the EEPROM transmitter database. Starting with the next transmission, the receiver will respond to the transmitter commands. Please note that the receiver will not send any Acknowledge during the learning phase, since the receiver has not yet learned the transmitter. If the automatic retry is enabled, then the second button press is not necessary, since the transmitter will retry automatically. If the feature is not enabled, a second button press is necessary.

FIGURE 1: RECEIVER FIRMWARE FLOWCHART



RECEIVER ACKNOWLEDGE

After receiving a valid packet, the receiver will respond with another data packet. This will consist of either an Acknowledge or a response message. The receiver will send an Acknowledge message to commands, such as OPEN or CLOSE. The command that reads the last known status will cause the receiver to respond with the appropriate information, such as (successfully) OPENED or CLOSED. The receiver must respond to the transmitter as soon as possible. After the transmitter has sent a command, it goes to Reception mode and waits for a period of time for a valid response. As soon as the receiver decodes and validates the data packet, it sends back an Acknowledge packet to the transmitter. If a valid response is received by the transmitter, it is displayed using the onboard LEDs. It is important that this wait period be as short as possible, because keeping the transceiver in Reception mode adds to the overall power consumption. The time needed for encryption/decryption must also be taken into account. The Acknowledge data format is slightly different from the one used by the transmitter.

TABLE 1: XTEA ACKNOWLEDGE FORMAT

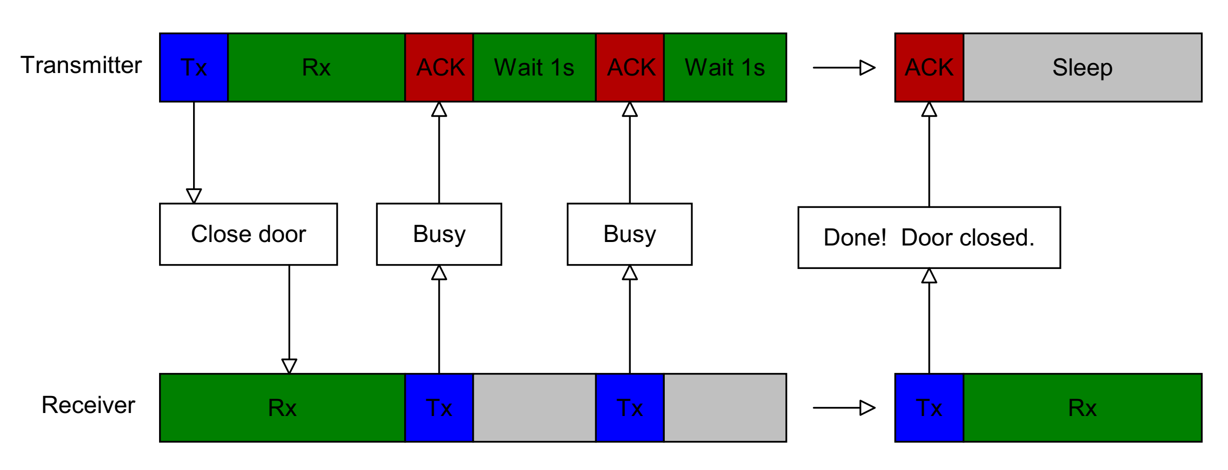
Non-encrypted Portion	Encrypted Portion		
32 bits Serial Code	Response 8 bits	Counter 32 bits	User Value 24 bits

WORK IN PROGRESS STATUS INDICATION

After the transmission of a packet, the transmitter will wait for Acknowledge within a specified time period. If it does not receive any Acknowledge from the receiver (the base unit), it will resend a new packet (if this feature is activated). There are times when the receiver needs time to complete an action (such as a garage door open/close, or an electric door lock). Thus, the Acknowledge cannot be sent immediately, since the receiver needs time to complete the action. During this time, the receiver will send a “work in progress” status indication to the transmitter. Upon receiving this status indication, the transmitter will prolong the time it waits for acknowledge before going to Sleep. After the open/close operation has completed, the receiver will send an OPEN/CLOSE Acknowledge.

For a more intuitive representation, refer to Figure 2.

FIGURE 2: WORK IN PROGRESS STATUS INDICATION



MRF49XA RADIO CONFIGURATION

The radio link parameters in the MRF49XA are set to a default configuration that is adequate for the majority of applications. The baud rate is 9600 bps, using an FSK modulation with deviation of 60 kHz. For a more detailed description on how to setup the MRF49xA, please refer to AN1252, “*Interfacing the MRF49XA Transceiver to PIC® Microcontrollers*”.

The following considerations were made to select the MRF49XA Configuration Words.

The configuration considers the use of standard 30ppm crystal accuracy. Such a crystal will generate a frequency error of:

EQUATION 1:

$$\Delta f_0 = \frac{30ppm}{10^6} * 915 * 10^6 = 27.45kHz$$

The deviation can now be calculated:

EQUATION 2:

$$\Delta f_{FSK} = 9600 + 2 * \Delta f_0 + 10 * 10^3$$

For the above values, we get a result of 74.5 kHz. The closest deviation supported by the MRF49XA transceiver is 75 kHz. For a maximum power output and a 75 Hz deviation, a value of 0x9840 is loaded into the TXCREG register.

Now, we can calculate the baseband bandwidth:

EQUATION 3:

$$BBBW = deviation*2 - 10 * 10^3\ Hz$$

For the above values, we get a result of 140 kHz. Picking a BBBW of 200 kHz, an RSSI of minus 97 dBm, and a maximum LNA gain, we get a value of 0x9481 to be loaded into the RXCREG register.

This code to configure the transceiver is contained in module `MRF49XA.c`.

KEY GENERATION

The KEELOQ encryption algorithm uses a 128-bit key to encrypt/decrypt 64 bits of message. The key generation algorithm uses the decryption routines to generate the key. Thus, the decryption routine has to be called twice, first for the MSB part of the key and then again for the LSB part of the key.

To generate the encryption key, the manufacturer key and the serial number (received in plain text) are used as inputs to the receiver. When calculating the XTEA encryption key, the serial number is padded with 0x55555555 for the MSB part of the key. Again, when calculating the LSB part of they key, it is padded with 0xAAAAAAAA (Equation 4).

EQUATION 4:

$$KEY_{MSB} = XTEADescription(|0x55555555|SerialCode|)$$

$$KEY_{LSB} = XTEADescription(|0xAAAAAAAA|SerialCode|)$$

RECEIVER I²C™ COMMAND INTERFACE

A standard I²C communication is provided. This allows the receiver to be controlled by an external master device. This allows the receiver to be integrated into a larger automation system. The receiver acts as a slave device on the I²C bus. A set of I²C registers is implemented to read and write data to the receiver (Table 2).

TABLE 2: I²C™ REGISTERS IMPLEMENTED BY THE RECEIVER

Register	Description
0x01	The last received data packet (decoded).
0x02	Sets the On/Off status of the LEDs.
0x03	The length of the last received data packet. Used to determine the type of encryption used.
0x04	Last error. This indicates the result of the most recent operation. Typical values will contain information such as: valid packet received, learn operation successful, learn operation fail, etc.

FIRMWARE MODULES

The following files make up the KEELOQ receiver firmware:

- `main.c`: contains the main loop routine, as well as the wake-up, debounce, read configuration, load transmit buffer and transmit functions.
- `lcd.c`: contains the LCD initialization and display functions.
- `I2C.c`: contains the I²C initialization functions.
- `MRF49XA.c`: contains all the functions that control the MRF49XA transceiver.
- `ProcessMessage.c`: contains the functions that implement the command processing.
- `EncoderDatabase.c`: contains the functions store and recall information about the learned transmitters.
- `encryption.c`: contains the functions that provide the encryption algorithm. Because of statutory export license restrictions on encryption software, the source code listings for the XTEA algorithms are not provided here.

These applications may be ordered from Microchip Technology Inc. through its sales offices, or through the corporate web site: www.microchip.com.

FIRMWARE CONFIGURATION

The transmitter firmware is fully configurable. The encryption algorithm can be changed very easily. All the necessary functions and definitions are contained in the `encryption.c` and `encryption.h` modules. Changing the encryption algorithm is as simple as replacing the above module and recompiling the source code.

XTEA (eXtended TEA) is an improvement of the original TEA algorithm. It was developed by David Wheeler and Roger Needham of the Cambridge Computer Laboratory. XTEA is practical both for its security and the small size of its algorithm. XTEA security is achieved by the number of iterations it goes through. The implementation in this KEELOQ Hopping receiver uses 32 iterations. If a higher level of security is needed, 64 iterations can be used.

CONCLUSION

The proposed receiver system enables a two-way communication for the Remote Keyless Entry systems. The receiver acknowledges every command by sending back data to the key fob transmitter. The system is very flexible and allows different encryption algorithms to be used within the same receiver. The interface with the radio transceiver is also flexible, allowing easy modifications to suit different devices. The receiver is also controllable via the I^2C port, enabling the receiver to be controlled by an external controller.

Also, the firmware is modular, allowing fast new encryption algorithms implementation, adding new features and changing for another radio transceiver.

ADDITIONAL INFORMATION

Microchip's Secure Data Products are covered by some or all of the following:

Code hopping encoder patents issued in European countries and U.S.A.

Secure learning patents issued in European countries, U.S.A. and R.S.A.

REVISION HISTORY

Revision B (June 2011)

- Added new section **Additional Information**
- Minor formatting and text changes were incorporated throughout the document

NOTES:

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.

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2009

Trademarks

Printed on recycled paper.

ISBN: 978-1-61341-269-5

Microchip received ISO/TS-16949:2002 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® MCUs and dsPIC® DSCs, KEELOQ® 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.

Worldwide Sales and Service

AMERICAS

Corporate Office
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7200
Fax: 480-792-7277
Technical Support:
http://www.microchip.com/support
Web Address:
www.microchip.com

Atlanta
Duluth, GA
Tel: 678-957-9614
Fax: 678-957-1455

Boston
Westborough, MA
Tel: 774-760-0087
Fax: 774-760-0088

Chicago
Itasca, IL
Tel: 630-285-0071
Fax: 630-285-0075

Cleveland
Independence, OH
Tel: 216-447-0464
Fax: 216-447-0643

Dallas
Addison, TX
Tel: 972-818-7423
Fax: 972-818-2924

Detroit
Farmington Hills, MI
Tel: 248-538-2250
Fax: 248-538-2260

Indianapolis
Noblesville, IN
Tel: 317-773-8323
Fax: 317-773-5453

Los Angeles
Mission Viejo, CA
Tel: 949-462-9523
Fax: 949-462-9608

Santa Clara
Santa Clara, CA
Tel: 408-961-6444
Fax: 408-961-6445

Toronto
Mississauga, Ontario, Canada
Tel: 905-673-0699
Fax: 905-673-6509

ASIA/PACIFIC

Asia Pacific Office
Suites 3707-14, 37th Floor
Tower 6, The Gateway
Harbour City, Kowloon
Hong Kong
Tel: 852-2401-1200
Fax: 852-2401-3431

Australia - Sydney
Tel: 61-2-9868-6733
Fax: 61-2-9868-6755

China - Beijing
Tel: 86-10-8569-7000
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8665-5511
Fax: 86-28-8665-7889

China - Chongqing
Tel: 86-23-8980-9588
Fax: 86-23-8980-9500

China - Hangzhou
Tel: 86-571-2819-3180
Fax: 86-571-2819-3189

China - Hong Kong SAR
Tel: 852-2401-1200
Fax: 852-2401-3431

China - Nanjing
Tel: 86-25-8473-2460
Fax: 86-25-8473-2470

China - Qingdao
Tel: 86-532-8502-7355
Fax: 86-532-8502-7205

China - Shanghai
Tel: 86-21-5407-5533
Fax: 86-21-5407-5066

China - Shenyang
Tel: 86-24-2334-2829
Fax: 86-24-2334-2393

China - Shenzhen
Tel: 86-755-8203-2660
Fax: 86-755-8203-1760

China - Wuhan
Tel: 86-27-5980-5300
Fax: 86-27-5980-5118

China - Xian
Tel: 86-29-8833-7252
Fax: 86-29-8833-7256

China - Xiamen
Tel: 86-592-2388138
Fax: 86-592-2388130

China - Zhuhai
Tel: 86-756-3210040
Fax: 86-756-3210049

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-3090-4444
Fax: 91-80-3090-4123

India - New Delhi
Tel: 91-11-4160-8631
Fax: 91-11-4160-8632

India - Pune
Tel: 91-20-2566-1512
Fax: 91-20-2566-1513

Japan - Yokohama
Tel: 81-45-471- 6166
Fax: 81-45-471-6122

Korea - Daegu
Tel: 82-53-744-4301
Fax: 82-53-744-4302

Korea - Seoul
Tel: 82-2-554-7200
Fax: 82-2-558-5932 or
82-2-558-5934

Malaysia - Kuala Lumpur
Tel: 60-3-6201-9857
Fax: 60-3-6201-9859

Malaysia - Penang
Tel: 60-4-227-8870
Fax: 60-4-227-4068

Philippines - Manila
Tel: 63-2-634-9065
Fax: 63-2-634-9069

Singapore
Tel: 65-6334-8870
Fax: 65-6334-8850

Taiwan - Hsin Chu
Tel: 886-3-6578-300
Fax: 886-3-6578-370

Taiwan - Kaohsiung
Tel: 886-7-213-7830
Fax: 886-7-330-9305

Taiwan - Taipei
Tel: 886-2-2500-6610
Fax: 886-2-2508-0102

Thailand - Bangkok
Tel: 66-2-694-1351
Fax: 66-2-694-1350

EUROPE

Austria - Wels
Tel: 43-7242-2244-39
Fax: 43-7242-2244-393

Denmark - Copenhagen
Tel: 45-4450-2828
Fax: 45-4485-2829

France - Paris
Tel: 33-1-69-53-63-20
Fax: 33-1-69-30-90-79

Germany - Munich
Tel: 49-89-627-144-0
Fax: 49-89-627-144-44

Italy - Milan
Tel: 39-0331-742611
Fax: 39-0331-466781

Netherlands - Drunen
Tel: 31-416-690399
Fax: 31-416-690340

Spain - Madrid
Tel: 34-91-708-08-90
Fax: 34-91-708-08-91

UK - Wokingham
Tel: 44-118-921-5869
Fax: 44-118-921-5820

05/02/11