TB086

PIC12F635/PIC16F636/PIC16F639 Cryptographic Module General Overview

Author: *Ken Dietz*
Microchip Technology Inc.

INTRODUCTION

This application note describes the general use of the PIC12F635/PIC16F636/PIC16F639 Cryptographic module. Technical Brief TB076, "*Using the KEELOQ® Compatible Cryptographical Module*" (DS91076) and the corresponding KEELOQ® Encoder License Agreement are needed to use the Cryptographic module.

Obtaining TB076 requires the completion of a licensing agreement that must be obtained through the Microchip Technology Inc. web site (www.microchip.com) and approved by the Microchip Technology Inc. Legal Department. The agreement form is located under the KEELOQ® Authentication Products section of our web site (www.microchip.com/keeloq).

Technical Brief TB076 describes how to implement cryptography on these products using the hardware peripheral. The Cryptographic module is capable of handling KEELOQ® compatible encoding/decoding, as well as application specific encoding/decoding.

After receiving approval by the Microchip Technology Legal Department, customers will receive Application Note AN249, "*KEELOQ® Transmitter Shell Using the PIC12F6XX*" (DS00249) as well as the TB076 Technical Brief on a CD ROM. Additionally, the disk includes firmware implementations of the KEELOQ encryption algorithm for PIC12, PIC16 and PIC18 devices with minor modifications, the algorithms for the PIC12 and PIC16 devices can be adapted to the PIC10 series of PICmicro® microcontrollers.

Note:	If the PIC12F635/PIC16F636/PIC16F639 devices are designed into a system without using the KEELOQ Compatible Cryptographic module, then a licensing agreement is not required.

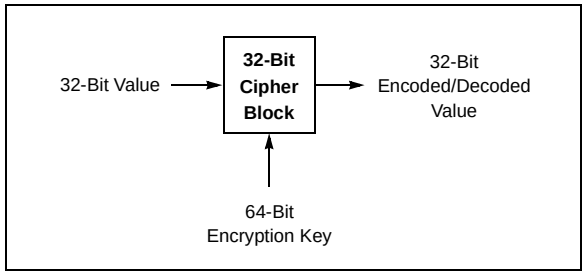
Additionally, firmware libraries for implementing decoding routines on PICmicro microcontrollers are also available by ordering the KEELOQ CD-ROM (DS40038). Please contact your local Microchip Technology sales office to order this CD-ROM.

CRYPTOGRAPHIC MODULE FEATURES

The PIC12F635/PIC16F636/PIC16F639 devices can be used as encoders or decoders based on the configuration settings of the peripheral. The cryptographic peripheral only does the actual data encryption and decryption. The peripheral requires that the following internal RAM locations are initialized before starting a KEELOQ compatible conversion:

1. Load a 64-bit encryption/decryption key into KEY<7:0>. This is completed in two 32-bit steps through the use of the CRCON and CRDAT<3:0> registers.
2. Load the Iteration Counter (ICR). This is also loaded through the CRCON and CRDAT0 register.
3. Load of the actual 32 bits of data using the CRCON and CRDAT<3:0> registers.

FIGURE 1: CRYPTOGRAPHIC MODULE



The conversion is then started by setting the GO/$\overline{\text{DONE}}$ bit in CRCON register and waiting for it to be cleared by the hardware. The peripheral can also generate an interrupt if enabled, which can also be used to poll for the end of the cryptographic process.

A main program in the C language will typically look like Example 1.

EXAMPLE 1:

```
void main(){
    .
    .
    .
Load_Encryption_Key()
Load_ICR()
Load_CSR()
//Start conversion by setting GO/DONE bit
//Wait for interrupt or GO/DONE to be cleared
     .
     .
     .
}
```

SUPPORTING FIRMWARE REQUIREMENTS

Encryption keys and serial numbers can be stored either in program memory or in data memory, which is up to the user to decide. The remaining code can be customized to implement KEELOQ compatible decoders and encoders as required by system specifications. This includes, but is not limited to:

- Keeping track of the 16-bit synchronization counter; storing the counter in EEPROM, adding EEPROM write error recovery schemes, and incrementing the counter before transmitting any new data.
- Reading and debouncing button inputs.
- Controlling actual transmission output. (Transmissions need to be firmware controlled on any of the available I/O pins.)
- Monitoring the battery voltage (i.e., using PLVD) and generating user feedback (i.e., LEDs, successful transmission or reception, etc.).
- Loading the pertinent information into the Code Shift Register (CSR), such as the function code, discrimination bits, and the synchronization counter data.

The data format and the communications protocol must also be customized by the end-user. Additionally, if end-users want to implement a solution similar to an existing KEELOQ device, such as any of the KEELOQ encoders, but with more features, they should reference the applicable KEELOQ device data sheet for information of what to store in EEPROM, how to transmit the actual data stream, how to setup the CSR registers, mapping how to sample and map of the input buttons and any outputs that exist.

As one can discern, the type of transmission can be implemented in any manner that is appropriate to system requirements such as Pulse Code Modulation (i.e., PWM, VPWM, PPM, Manchester, etc.). Validation and software testing are also left to customers, as is generating their own SQTP^{SM} data files. Microchip will handle all customer projects as either a standard QTP or SQTP (serialized) PICmicro microcontroller design with the same development tools and production support that are currently available.

CODE SPACE AND TIME RESOURCES

Since these PICmicro microcontrollers can implement the KEELOQ algorithm in a hardware module, the actual encoding and decoding process is typically 50 times faster than completing the algorithm in firmware with a processor running at the same speed (~500 µs vs. ~25 ms, with a 14-bit PICmicro microcontroller core running at 4 MHz).

In terms of resource space, the encryption/decryption routines typically utilize about 60 to 70 lines of code in a PICmicro microcontroller and about 14 RAM locations. All of these instructions and handling of volatile variables are now handled within the hardware peripheral after it is initialized, properly loaded and set into motion to complete the encryption/decryption process.

CONCLUSION

This document describes the general use of the Cryptographic module included on the PIC12F635/PIC16F636/PIC16F639. Additionally, a general description of the type of supporting firmware designers can expect to implement to effectively use the Cryptographic module was provided. An explanation of the necessity and process of obtaining a licensing agreement, the application note and technical brief relating to this module was included.

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.

Trademarks

QUALITY MANAGEMENT SYSTEM
CERTIFIED BY DNV
ISO/TS 16949:2002

Microchip received ISO/TS-16949:2002 quality system certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona and Mountain View, California in October 2003. The Company's quality system processes and procedures are for its PICmicro® 8-bit MCUs, 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://support.microchip.com
Web Address:
www.microchip.com

Atlanta
Alpharetta, GA
Tel: 770-640-0034
Fax: 770-640-0307

Boston
Westford, MA
Tel: 978-692-3848
Fax: 978-692-3821

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

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

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

Kokomo
Kokomo, IN
Tel: 765-864-8360
Fax: 765-864-8387

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

San Jose
Mountain View, CA
Tel: 650-215-1444
Fax: 650-961-0286

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

ASIA/PACIFIC

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

China - Beijing
Tel: 86-10-8528-2100
Fax: 86-10-8528-2104

China - Chengdu
Tel: 86-28-8676-6200
Fax: 86-28-8676-6599

China - Fuzhou
Tel: 86-591-8750-3506
Fax: 86-591-8750-3521

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

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 - Shunde
Tel: 86-757-2839-5507
Fax: 86-757-2839-5571

China - Qingdao
Tel: 86-532-502-7355
Fax: 86-532-502-7205

ASIA/PACIFIC

India - Bangalore
Tel: 91-80-2229-0061
Fax: 91-80-2229-0062

India - New Delhi
Tel: 91-11-5160-8631
Fax: 91-11-5160-8632

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

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

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

Taiwan - Kaohsiung
Tel: 886-7-536-4818
Fax: 886-7-536-4803

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

Taiwan - Hsinchu
Tel: 886-3-572-9526
Fax: 886-3-572-6459

EUROPE

Austria - Weis
Tel: 43-7242-2244-399
Fax: 43-7242-2244-393

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

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

Germany - Ismaning
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

England - Berkshire
Tel: 44-118-921-5869
Fax: 44-118-921-5820

10/20/04