TB043

KEELOQ® CRC Verification Routines

Author: Lucio Di Jasio
Microchip Technology Inc.

OVERVIEW

All of the KEELOQ Encoders share the same standard code word format composed of a basic set of 65 bits of information. Although, the Advanced Encoders (e.g. HCS360, HCS361) supplement that set with extra bits of information along with a pair of CRC bits (Cyclic Redundancy Check). This Technical Brief presents a routine in PICmicro® microcontroller (MCU) assembly language that implements the CRC polynomial as used by Advanced KEELOQ Encoders and allows a KEELOQ receiver to verify the received code word.

KEELOQ CRC EQUATIONS

The CRC bits are calculated on the 65 previous transmitted bits using the following equations:

$CRC[1]_{n+1} = CRC[0]_n \text{ xor } Di_n$

and

$CRC[0]_{n+1} = (CRC[0]_n \text{ xor } Di_n) \text{ xor } CRC[1]_n$

with

$CRC[0]_0 = 0; CRC[1]_0 = 0;$

where Di_n represents the *n*th transmission bit of the code word with 0<n<64

PICmicro® MCU IMPLEMENTATION

The CRC calculation would be ideally done on the fly by the same routine that is receiving the data from the radio input. Therefore, it would compute a new CRC value as every data bit gets shifted in. After receiving the first 65 bits, the computed CRC value is ready to be compared with the transmitted CRC bits that are following in the data stream. If the CRC calculation is further extended to include the transmitted CRC bits too (all first 67 bits), a valid transmission will result in a CRC value of `00`.

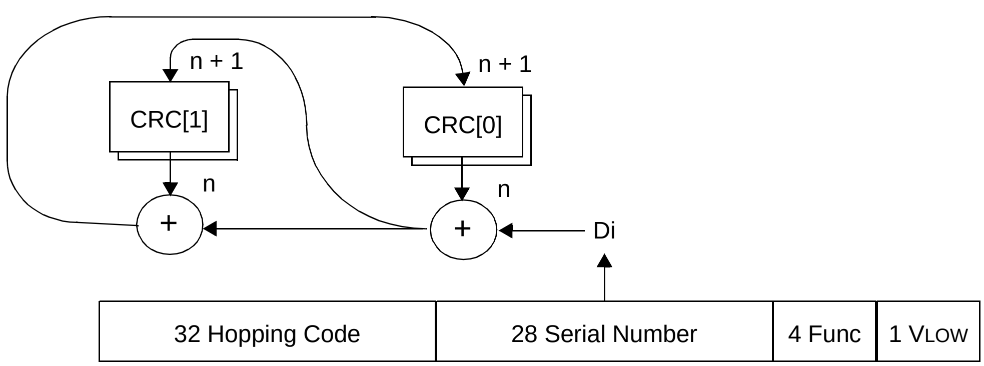
The assembler implementation of the CRC equations can be optimized by the use of the decrement instruction. The core code segment can be expressed simply as follows:

Listing 1:

```
DECF        CRC,W
BTFSC       CRC,1
XORLW       3
BTFSS       STATUS,C
XORLW       3
MOVWF       CRC
```

For completeness and testing purposes, the code presented in Appendix A shows a complete stand-alone routine implementing the CRC calculation on a buffer containing 9 bytes (65 + 2 bits) of data.

FIGURE 1: CRC FLOW GRAPH



The core segment is composed of the few lines of code from Listing 1 and is therefore suitable for inline insertion in any standard receive routine.

The stand-alone version includes a brief initialization code and a loop (67 times) around the CRC code, while shifting all the bits out of the buffer. The return value in the CRC variable (2 LSb) contains the CRC check result.

The source code presented in Appendix A can be compiled using MPASM™ 2.50 for any PICmicro MCU with 12-bit and 14-bit cores (PIC16C5X and PIC16CXXX family).

The only modification required for use with PIC17CXXX and PIC18CXXX families (16-bit and enhanced PICmicro MCU cores) is related to the use of the RRF instruction whose mnemonic changes in RRCF.

C LANGUAGE IMPLEMENTATION

Using the C programming language, the CRC equations can be effectively expressed in the following three lines of code:

```
TEMP = CRC1;
CRC1 = CRC0 ^ Di;
CRC0 = CRC1 ^ TEMP;
```

where `Di` represent the *n*th transmission bit of the code word and `TEMP` is a temporary variable.

The compiler specific efficiency might actually turn out to have quite an impact on the performance results of such implementation depending on the compiler ability to manipulate bit variables.

MEMORY USAGE

(Assembly implementation only)

Program memory: 6 words

RAM: 1 byte

REFERENCES

HCS360 Data Sheet	DS40152
HCS361 Data Sheet	DS40146
HCS362 Data Sheet	DS40189
HCS365 Data Sheet	DS41109
HCS410 Data Sheet	DS40158
HCS412 Data Sheet	DS41099
HCS473 Data Sheet	DS40035
AN730 CRC Generating and Checking	DS00730
TB001 Secure Learning RKE Systems using KEELOQ Technology	DS91000
TB003 Introduction to KEELOQ Technology	DS91002
TB030 KEELOQ Decryption & IFF Algorithms	DS91030
TB041 KEELOQ Decryption Routines in C	DS90041
TB042 Interfacing a KEELOQ Encoder to a PLL Circuit	DS90042

KEYWORDS

KEELOQ, CRC, Receiver

APPENDIX A: SOURCE CODE

```
;------------------------------------------------------------
; Keeloq CRC verification routine
;
; version 1.0  01/10/2001 Lucio Di Jasio, Myron Loewen
;
; INPUT:
;       Buffer[0..8]    67+ bit HCS code word (left aligned)
; OUTPUT:
;       CRC             computed CRC check result (two lsb bits only)
; USES:
;       FSR             indirect pointer
;       Aux             shift out data bits
;       Count           loop counter
;
CRCcheck
            clrf    CRC         ; start with 0,0
            movlw   Buffer0
            movwf   FSR         ; point to first byte
            clrf    Count       ;
            movf    INDF,W
            movwf   Aux         ; load first data byte
CRCLoop
            rrf     Aux,F       ; rotate data bit in CARRY
;
;---- this segment can be inline in receive routine
;
            decf    CRC,W       ; apply the CRC equations
            btfsc   CRC,1
            xorlw   3
            btfss   STATUS,C
            xorlw   3
            movwf   CRC
;-----------
;
            incf    Count,F     ; count the bit
            movlw   7
            andwf   Count,W     ; every eight
            BNZ     CRCLE
            incf    FSR,F       ; increase Buffer pointer
            movf    INDF,W
            movwf   Aux         ; load new data byte
CRCLE
            movlw   .67         ; repeat 65 times
            subwf   Count,W
            SKPZ
            goto    CRCLoop
            retlw   0
```

NOTES:

NOTES:

NOTES:

MICROCHIP

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: 480-792-7627
Web Address: http://www.microchip.com

Rocky Mountain
2355 West Chandler Blvd.
Chandler, AZ 85224-6199
Tel: 480-792-7966 Fax: 480-792-7456

Atlanta
500 Sugar Mill Road, Suite 200B
Atlanta, GA 30350
Tel: 770-640-0034 Fax: 770-640-0307

Austin
Analog Product Sales
8303 MoPac Expressway North
Suite A-201
Austin, TX 78759
Tel: 512-345-2030 Fax: 512-345-6085

Boston
2 Lan Drive, Suite 120
Westford, MA 01886
Tel: 978-692-3848 Fax: 978-692-3821

Boston
Analog Product Sales
Unit A-8-1 Millbrook Tarry Condominium
97 Lowell Road
Concord, MA 01742
Tel: 978-371-6400 Fax: 978-371-0050

Chicago
333 Pierce Road, Suite 180
Itasca, IL 60143
Tel: 630-285-0071 Fax: 630-285-0075

Dallas
4570 Westgrove Drive, Suite 160
Addison, TX 75001
Tel: 972-818-7423 Fax: 972-818-2924

Dayton
Two Prestige Place, Suite 130
Miamisburg, OH 45342
Tel: 937-291-1654 Fax: 937-291-9175

Detroit
Tri-Atria Office Building
32255 Northwestern Highway, Suite 190
Farmington Hills, MI 48334
Tel: 248-538-2250 Fax: 248-538-2260

Los Angeles
18201 Von Karman, Suite 1090
Irvine, CA 92612
Tel: 949-263-1888 Fax: 949-263-1338

Mountain View
Analog Product Sales
1300 Terra Bella Avenue
Mountain View, CA 94043-1836
Tel: 650-968-9241 Fax: 650-967-1590

New York
150 Motor Parkway, Suite 202
Hauppauge, NY 11788
Tel: 631-273-5305 Fax: 631-273-5335

San Jose
Microchip Technology Inc.
2107 North First Street, Suite 590
San Jose, CA 95131
Tel: 408-436-7950 Fax: 408-436-7955

Toronto
6285 Northam Drive, Suite 108
Mississauga, Ontario L4V 1X5, Canada
Tel: 905-673-0699 Fax: 905-673-6509

ASIA/PACIFIC

Australia
Microchip Technology Australia Pty Ltd
Suite 22, 41 Rawson Street
Epping 2121, NSW
Australia
Tel: 61-2-9868-6733 Fax: 61-2-9868-6755

China - Beijing
Microchip Technology Beijing Office
Unit 915
New China Hong Kong Manhattan Bldg.
No. 6 Chaoyangmen Beidajie
Beijing, 100027, No. China
Tel: 86-10-85282100 Fax: 86-10-85282104

China - Shanghai
Microchip Technology Shanghai Office
Room 701, Bldg. B
Far East International Plaza
No. 317 Xian Xia Road
Shanghai, 200051
Tel: 86-21-6275-5700 Fax: 86-21-6275-5060

Hong Kong
Microchip Asia Pacific
RM 2101, Tower 2, Metroplaza
223 Hing Fong Road
Kwai Fong, N.T., Hong Kong
Tel: 852-2401-1200 Fax: 852-2401-3431

India
Microchip Technology Inc.
India Liaison Office
Divyasree Chambers
1 Floor, Wing A (A3/A4)
No. 11, O'Shaugnessey Road
Bangalore, 560 025, India
Tel: 91-80-2290061 Fax: 91-80-2290062

Japan
Microchip Technology Intl. Inc.
Benex S-1 6F
3-18-20, Shinyokohama
Kohoku-Ku, Yokohama-shi
Kanagawa, 222-0033, Japan
Tel: 81-45-471- 6166 Fax: 81-45-471-6122

ASIA/PACIFIC (continued)

Korea
Microchip Technology Korea
168-1, Youngbo Bldg. 3 Floor
Samsung-Dong, Kangnam-Ku
Seoul, Korea
Tel: 82-2-554-7200 Fax: 82-2-558-5934

Singapore
Microchip Technology Singapore Pte Ltd.
200 Middle Road
#07-02 Prime Centre
Singapore, 188980
Tel: 65-334-8870 Fax: 65-334-8850

Taiwan
Microchip Technology Taiwan
11F-3, No. 207
Tung Hua North Road
Taipei, 105, Taiwan
Tel: 886-2-2717-7175 Fax: 886-2-2545-0139

EUROPE

Denmark
Microchip Technology Denmark ApS
Regus Business Centre
Lautrup hoj 1-3
Ballerup DK-2750 Denmark
Tel: 45 4420 9895 Fax: 45 4420 9910

France
Arizona Microchip Technology SARL
Parc d'Activite du Moulin de Massy
43 Rue du Saule Trapu
Batiment A - ler Etage
91300 Massy, France
Tel: 33-1-69-53-63-20 Fax: 33-1-69-30-90-79

Germany
Arizona Microchip Technology GmbH
Gustav-Heinemann Ring 125
D-81739 Munich, Germany
Tel: 49-89-627-144 0 Fax: 49-89-627-144-44

Germany
Analog Product Sales
Lochhamer Strasse 13
D-82152 Martinsried, Germany
Tel: 49-89-895650-0 Fax: 49-89-895650-22

Italy
Arizona Microchip Technology SRL
Centro Direzionale Colleoni
Palazzo Taurus 1 V. Le Colleoni 1
20041 Agrate Brianza
Milan, Italy
Tel: 39-039-65791-1 Fax: 39-039-6899883

United Kingdom
Arizona Microchip Technology Ltd.
505 Eskdale Road
Winnersh Triangle
Wokingham
Berkshire, England RG41 5TU
Tel: 44 118 921 5869 Fax: 44-118 921-5820

01/30/01