PICmicro™ Midrange MCU Code Hopping Decoder

Author: Vivien Delport
Microchip Technology Inc.

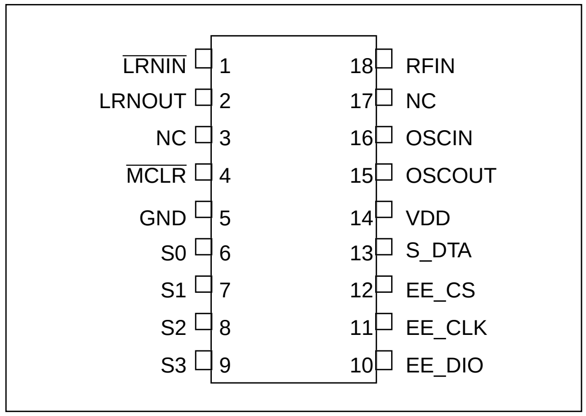
OVERVIEW

This application note describes the working of a KEELOQ® code hopping decoder implemented on a Microchip Midrange MCUs (PIC16C6X, PIC16C7X, PIC16C62X) The software can be used to implement a stand alone decoder or be integrated with the user application. The decoder supports the Microchip's HCS200, HCS201, HCS300, HCS301, HCS360, and HCS361 KEELOQ hopping code encoders. The decoder supports normal and secure learning. Two manufacturers codes allow different manufacturers to share a public key, but retain their own private keys.

KEY FEATURES

- Supports two manufacturer's codes
- Compatible with Microchip's HCS200, HCS201, HCS300, HCS301, HCS360 and HCS361 encoders.
- PIC16C6X, PIC16C7X and PIC16C62X platforms
- Automatic baud rate detection
- Automatic Normal or Secure learn detection
- Four function outputs
- Six learnable transmitters
- RC Oscillator
- Serial interface

FIGURE 1: MICROCHIP MIDRANGE DECODER



FUNCTIONAL INPUTS AND OUTPUTS

TABLE 1: MICROCHIP DECODER FUNCTIONAL INPUTS AND OUTPUTS

Mnemonic	Pin Number	Input / Output	Function
RF IN	18	I	Demodulated PWM signal from RF receiver. The decoder uses this input to receive encoder transmissions.
LEARN INIT	I	1	Input to initiate learning.
LEARN INDICATION	2	O	Output to show the status of the learn process (in an integrated system this will be combined with the system status indicator).
S_DTA	13	O	Serial data string output which contains the function code, VLOW bit and function code match bit.
S0, S1, S2, S3	6, 7, 8, 9	O	Function outputs, correspond to encoder input pins.
EE_CS EE_CLK EE_DIO	10,11,12	I/O	External Serial EEPROM Interface lines.

PUBLIC AND PRIVATE MANUFACTURER'S CODE

The decoder supports two manufacturer's codes, called the public manufacturer's code and private manufacturer's code. This feature allows two manufacturers to share one public manufacturer's code, but retain their own private manufacturer's code. The decoder uses the public manufacturer's code first to drive the encoder's decryption key, but if learn fails, it will retry using the private manufacturer's code.

PROGRAM FLOW

The decoder software will run on any PIC6C6X/7X with 1K program memory. The operating frequency is 4 MHz. The clock speed is important as the reception routine (`RECEIVE`) has some critical timing specifications. Other decoder functions that rely on a 4 MHz clock speed are the hold times of the various outputs, time-outs, etc. The compiler used is MPASM.

A high-level description of the main program flow, the transmission validation flow, and the transmitter learn flow are described in the following sections. More detailed descriptions of the other modules can be found in Application Note AN642.

MAIN PROGRAM FLOW

After reset, the decoder enters the main loop where it spends most of the time. The main loop checks the learn button and if pressed (`TST_LEARN`) enters the learn mode. The microcontroller checks transmissions from the encoders (`RECEIVE`). Once 65 bits are received, the microcontroller validates the transmission. When a valid transmission is received from a learnt encoder, the decoder sends out a serial data string containing the function code (`TX_FUNC`) and sets the appropriate function outputs (`M_BUT`).

TRANSMISSION VALIDATION FLOW

After reception of a code, the decoder will first check if the transmitter is learnt on the decoder. This is done by calculating the checksum on the received transmission's serial number and then searching through the transmitter blocks stored in EEPROM to find a match. If a match is found, the decoder reads the decryption key stored for that transmitter and decrypts the hopping code portion. The 10 LSBs of the discrimination value are compared to the 10 LSBs of the serial number. The 16-bit synchronization counter is validated by checking if the received counter is in the blocked window. The decoder then checks if the counter is in the double operation window. If this is the case, the decoder will wait for the next sequential transmission to synchronize. If the counter is within the single operation window, the decoder updates the EEPROM counters and then generates the appropriate function output.

TRANSMITTER LEARN FLOW

To be able to use a transmitter with the decoder, the transmitter must first be learned into the decoder. Adding a transmitter is done by pressing the learn button. If the button is pressed for longer than 10 seconds, the decoder executes an "erase all" function, which will remove all the transmitters learned.

Normal Secure Learn Selection: In learn mode, the decoder monitors transmissions for 4 seconds. If two codes are received with different serial numbers, the first code is used as the hop code and the second as the seed for the secure learn algorithm. If the two serial numbers are the same, the first received code will be used for the normal learn algorithm.

Manufacturer's Code Selection: The decryption key is derived using the public manufacturer's code stored in a ROM table. The received hopping code is validated by comparing the received transmission's discrimination bits with the lower bits of the serial number. If the decryption validation fails, the decoder will derive the decryption key again by using the private manufacturer's code, also store in a ROM table. If the decryption validation was successful, the decoder will calculate a checksum value on the transmission's serial number. All of the information is then stored in an unused block in the EEPROM. The same memory block will be used if the transmitter was already learned. The result of the learn sequence is displayed on the LED.

COMPILER OPTIONS

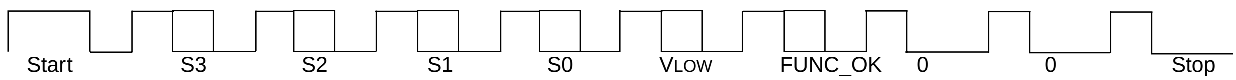
Delayed Increment: When this option is enabled, the decoder will automatically increment the synchronization counter by twelve, 30 seconds after the last valid reception. The synchronization window is increased from 16 to 256 in this mode. Delayed increment is used to defeat jamming code grabbers in single button transmitters. This option is enabled by setting the define variable `DLY_INC` to 1 and recompiling the code.

SERIAL FUNCTION STRING OUTPUT

The decoder's serial output sends out a function byte which consists of the function code, battery low status flag, and a function code match bit. After the last bit was clocked out, the line will go high for 500 ms. Repeated transmissions will, as with the binary function outputs, extend this 500 ms time-out. Start bit is one and the stop bit is zero.

The data byte format for this output is shown in Figure 2

FIGURE 2: DATA BYTE FORMAT



Note: The serial data is clocked out with basic pulse width T_E = 200 µs

FIGURE 3: MAIN PROGRAM FLOW

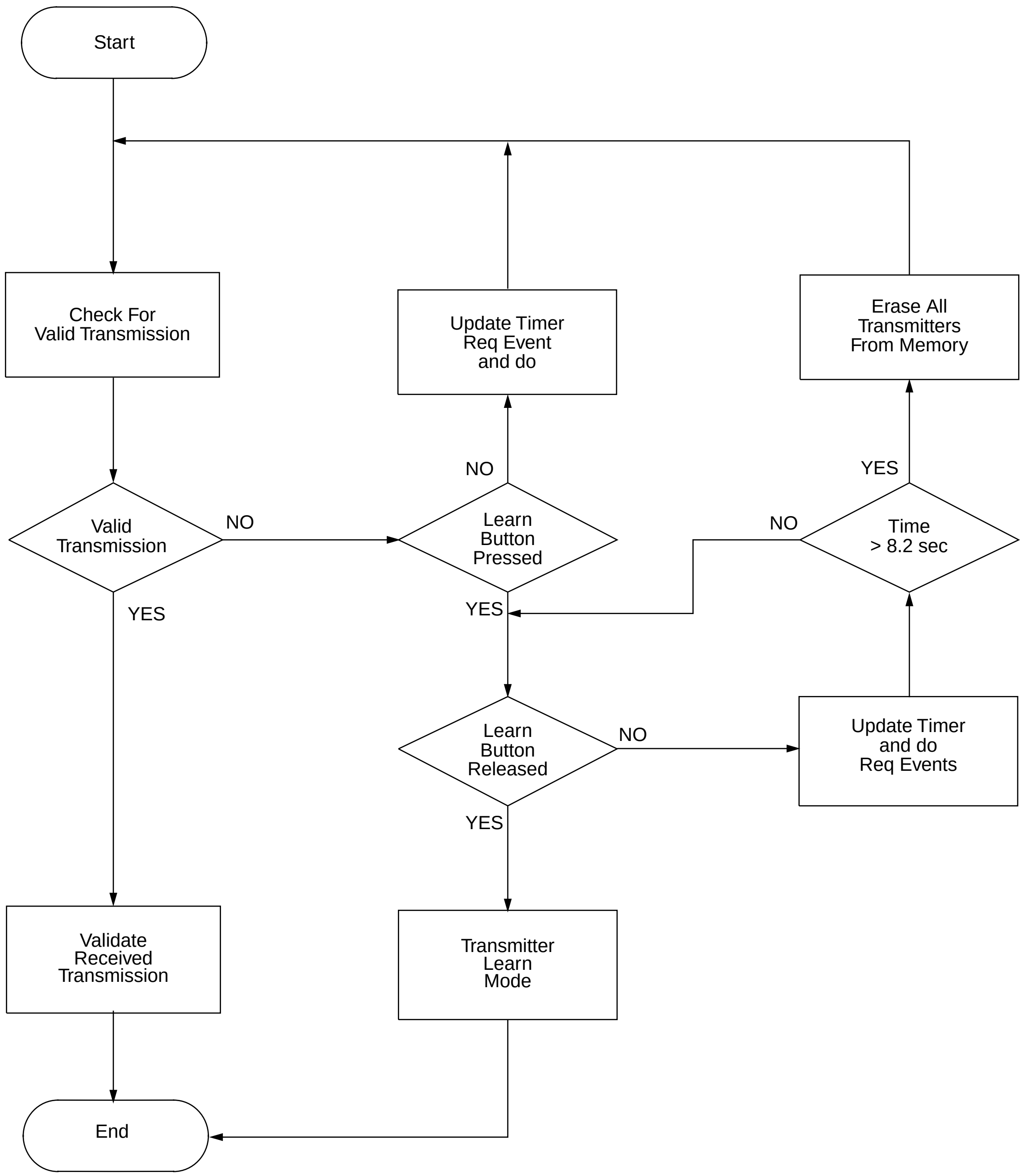


FIGURE 4: TRANSMITTER LEARN FLOW

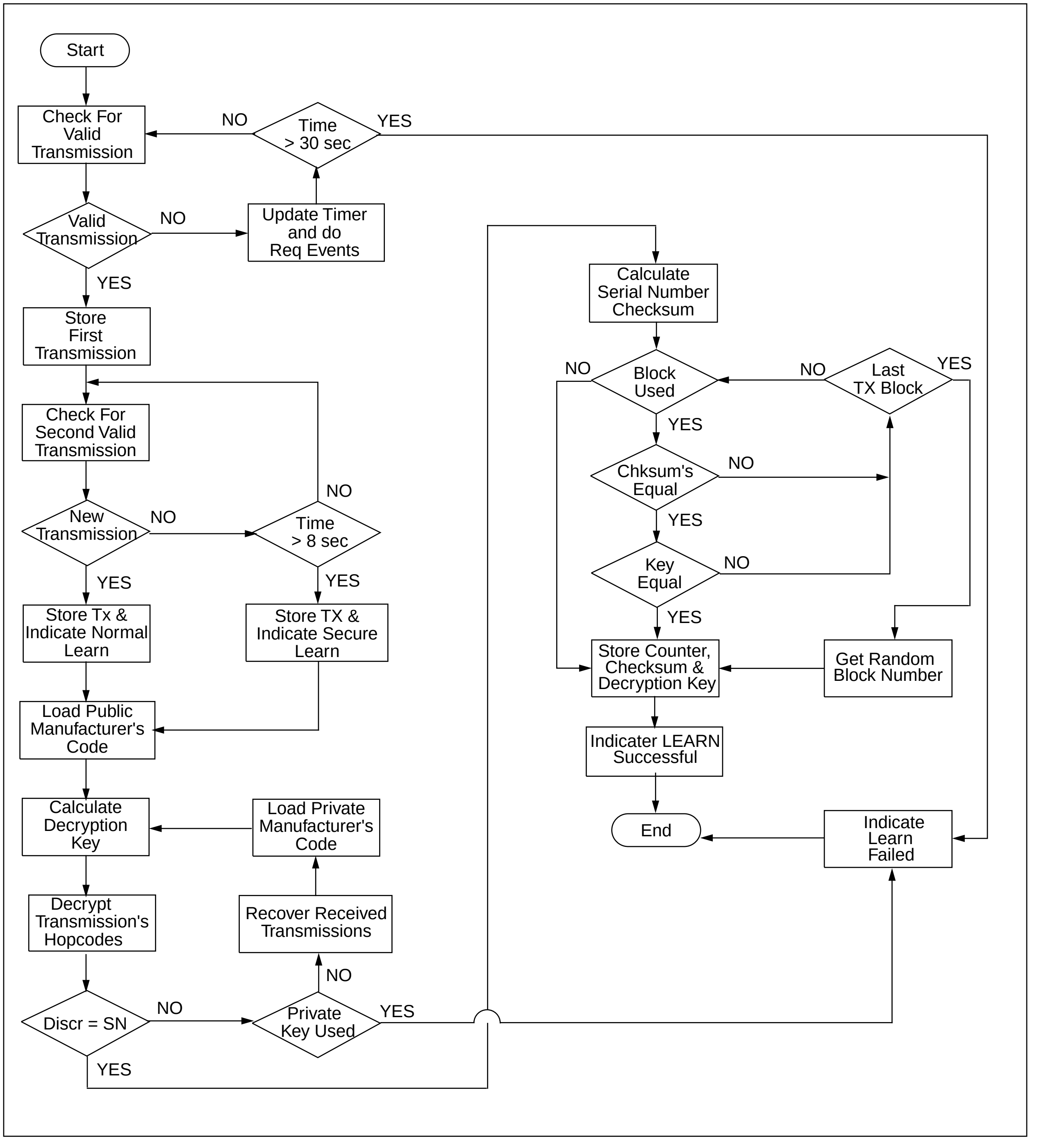
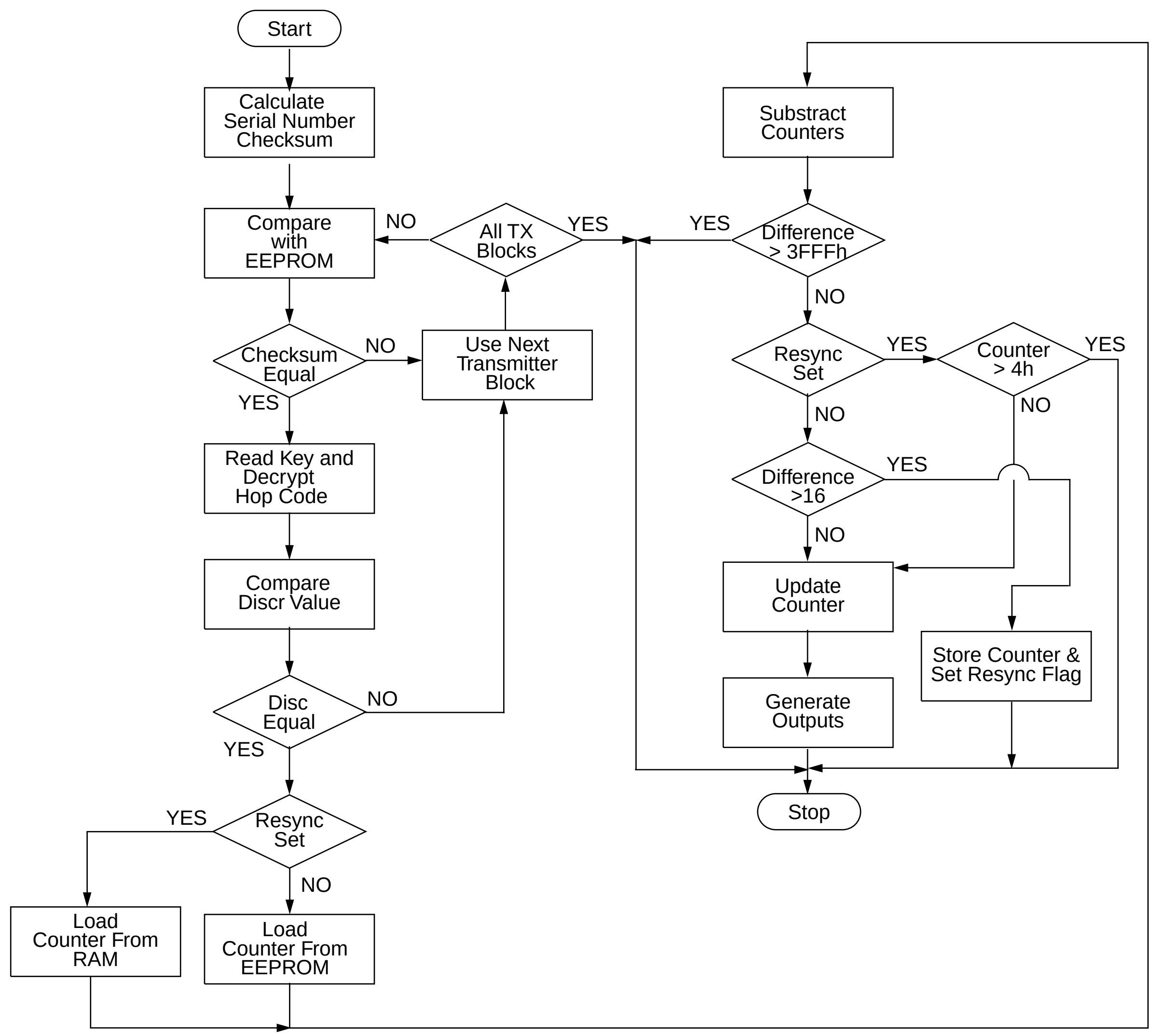


FIGURE 5: TRANSMISSION VALIDATION FLOW



DECODER MEMORY MAPS

TABLE 2: MEMORY MAP ROM (8-BIT BYTES)

Word Address	Mnemonic	Description
42	MKEY1_0	64-Bit Public Manufacturers Code (Used to generate decryption keys)
43	MKEY1_1	
44	MKEY1_2	
45	MKEY1_3	
46	MKEY1_4	
47	MKEY1_5	
48	MKEY1_6	
49	MKEY1_7	
4A	MKEY2_0	64-Bit Private Manufacturers Code (Used to generate decryption keys)
4B	MKEY2_1	
4C	MKEY2_2	
4D	MKEY2_3	
4E	MKEY2_4	
4F	MKEY2_5	
50	MKEY2_6	
51	MKEY2_7	
52	EKEY_0	64-Bit EEPROM Key (Used to encrypt EEPROM data)
53	EKEY_1	
54	EKEY_2	
55	EKEY_3	
56	EKEY_4	
57	EKEY_5	
58	EKEY_6	
59	EKEY_7	

TABLE 3: MEMORY MAP EEPROM (16 BIT WORDS)

Address	Mnemonic	Address	Mnemonic
00	Scratch Pad #1 – First TX	20	CNT20
01	Scratch Pad #1 – First TX	21	CNT21
02	Scratch Pad #1 – First TX	22	DISC2
03	Scratch Pad #1 – First TX	23	CHKSUM2
04	Scratch Pad #2 – Seed TX	24	KEY20
05	Scratch Pad #2 – Seed TX	25	KEY21
06	Scratch Pad #2 – Seed TX	26	KEY22
07	Scratch Pad #2 – Seed TX	27	KEY23
08	Not Used	28	CNT30
09	Not Used	29	CNT31
0A	Not Used	2A	DISC3
0B	Not Used	2B	CHKSUM3
0C	Not Used	2C	KEY30
0D	Not Used	2D	KEY31
0E	Not Used	2E	KEY32
0F	Not Used	2F	KEY33
10	CNT00	30	CNT40
11	CNT01	33	CNT41
12	DISC0	32	DISC4
13	CHKSUM0	33	CHKSUM4
14	KEY00	34	KEY40
15	KEY01	35	KEY41
16	KEY02	36	KEY42
17	KEY03	37	KEY43
18	CNT10	38	CNT50
19	CNT11	39	CNT51
1A	DISC1	3A	DISC5
1B	CHKSUM1	3B	CHKSUM5
1C	KEY10	3C	KEY50
1D	KEY11	3D	KEY51
1E	KEY12	3E	KEY52
1F	KEY13	3F	KEY53

Note:

SCRATCHPAD: Temporary storage of transmission during learn.

CHKSUM: The encoder serial number checksum.

KEY: These bytes contain the decryption key for each encoder.

DIS: Discrimination values and function code storage.

CNT: Two copies of the synchronization counter are stored for each encoder to prevent loss of synchronization information due to EEPROM write failure.

TABLE 4: RAM MEMORY MAP (8-BIT BYTES)

Address	Mnemonic	Description
0C	FLAGS	Decoder flags
0D	ADDRESS	Address register – points to address in EEPROM
0E	TXNUM	Current transmitter's block index
0F	TX_CNT	Transmitter loop counter
10	OUTBYT	General data register, mask register used in decryption
11	CNT0	Loop counters
12	CNT2	
13	CNT3	
14	CNT_HI	16-bit event clock counter
15	CNT_LO	
16	RAM_HI	16-bit RAM counter (used in resynchronization)
17	RAM_LW	
18	TMP0	Temporary registers
19	TMP1	
1A	TMP2	
1B	TMP3	
1C	TMP4	
1D	TMP5	
1E	TMP6	
1F	TMP7	
20	CSR4	64-bit shift register Used in reception, decryption and key generation
21	CSR5	
22	CSR6	
23	CSR7	
24	CSR0	
25	CSR1	
26	CSR2	
27	CSR3	
28	KEY7	64-bit shift register holds decryption key
29	KEY6	
2A	KEY5	
2B	KEY4	
2C	KEY3	
2D	KEY2	
2E	KEY1	
2F	KEY0	

Many of the memory locations in RAM are used by multiple routines. A list of alternate names and functions are given in the table below.

Address	Mnemonic	Also Known As	Description
10	CNT2	OUTBYT	Temporary Loop Counter.
18	HOP1	CSR0	32-bit hop code register.
19	HOP2	CSR1	
1A	HOP3	CSR2	
1B	HOP4	CSR3	
OD	EHOP3	ADDRESS	Extended 32-bit buffer used during key generation as a 32-bit buffer.
1C	EHOP2	TXNUM	
1D	EHOP1	TX_CNT	
1E	EHOP0	CNT3	
17	SER_0	CSR7	28-bit serial number, stores received transmission open 32 bits.
16	SER_1	CSR6	
15	SER_2	CSR5	
14	SER_3	CSR4	
1B	FUNC	CSR3	Button code and user nibble of discrimination value.
1A	DISCR	CSR2	Discrimination value.
19	CNTR_HI	CSR1	16-bit received counter.
18	CNTR_LW	CSR0	

DEVICE PINOUTS

The device used in the application note is a PIC16C6X PDIP.

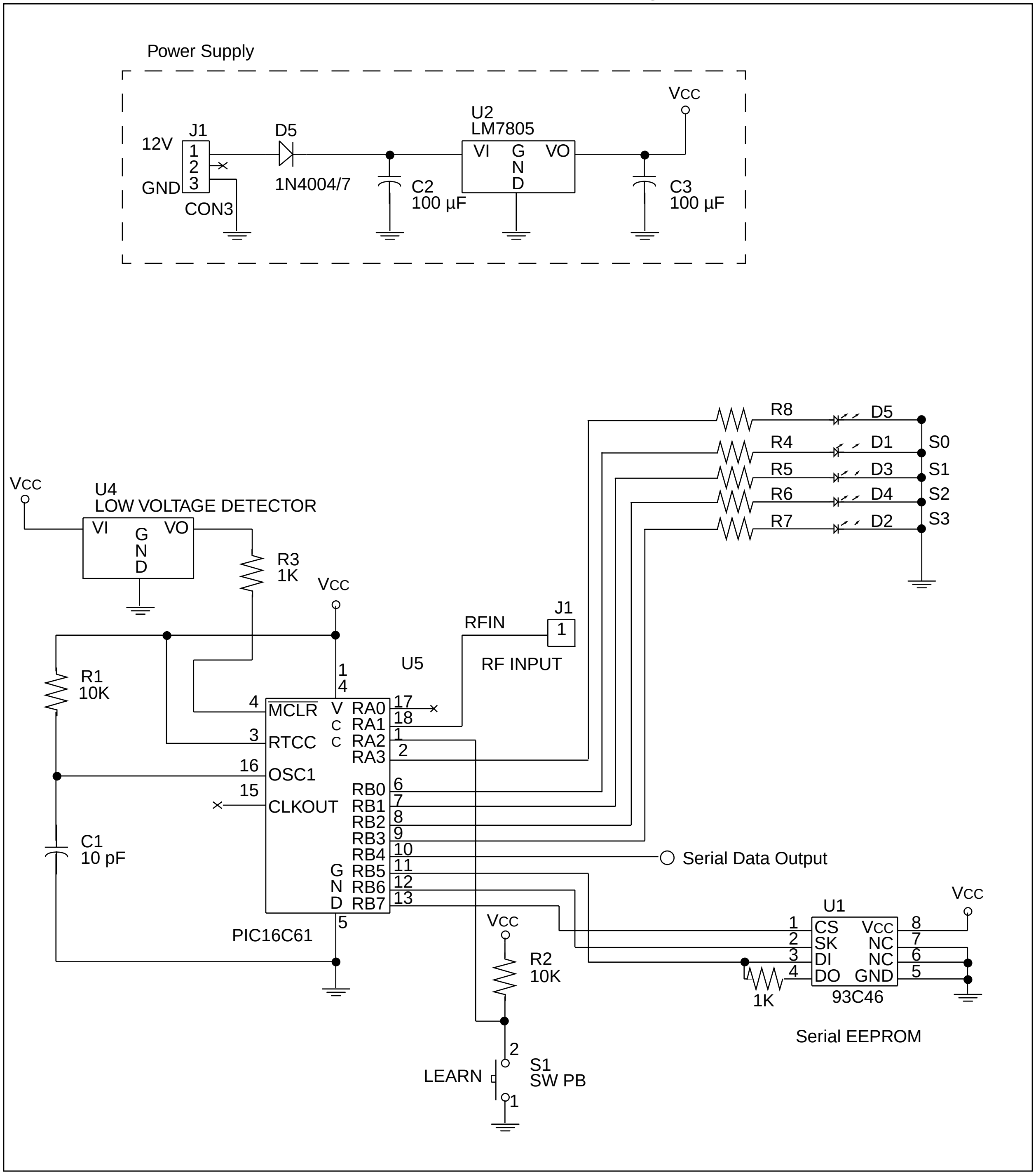
PIN	PICmicro Function	Decoder Function	PIN	PICmicro Function	Decoder Function
1	Port A Bit 2	LEARN Input Act Low	18	Port A Bit 1	RF Input
2	Port A Bit 3	LRN IND Output High	17	Port A Bit 0	Not Used
3	TIMER0	Connect to V_{DD}	16	OSC_{IN}	RC OSC (4 MHz)
4	$\overline{MCLR}$	Brown-out detect	15	OSC_{OUT}	—
5	GND	Ground	14	V_{DD}	+5V supply
6	Port B Bit 0	S0	13	Port B Bit 7	FUNC OK
7	Port B Bit 1	S1	12	Port B Bit 6	CS (1)
8	Port B Bit 2	S2	11	Port B Bit 5	CLK (2)
9	Port B Bit 3	S3	10	Port B Bit 4	DIO (3+4)

TIMING PARAMETERS

Parameter	Typical	Unit
Output activation duration	524	ms
Output pause if new function code received	100	ms
Erase all duration	8.4	s
Learn mode time-out	33.6	s
Learn successful LED flash duration	4.2	s
Learn successful LED flash rate	3.8	Hz
Learn failure LED on duration	1	s

APPENDIX A: APPENDIX SCHEMATIC DIAGRAMS

FIGURE A-1: SCHEMATIC DIAGRAM OF MICROCHIP KEELOQ DECODER



Note the following details of the code protection feature on PICmicro® MCUs.

- The PICmicro family meets the specifications contained in the Microchip Data Sheet.
- Microchip believes that its family of PICmicro microcontrollers is one of the most secure products 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 PICmicro microcontroller in a manner outside the operating specifications contained in the data sheet. The person doing so may be 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 product.

If you have any further questions about this matter, please contact the local sales office nearest to you.

DNV Certification, Inc. USA
ANSI • RAB QMS ACCREDITED
DNV MSC The Netherlands Accredited by the RvA
ISO 9001 / QS-9000 REGISTERED FIRM

Microchip received QS-9000 quality system certification for its worldwide headquarters, design and wafer fabrication facilities in Chandler and Tempe, Arizona in July 1999. The Company’s quality system processes and procedures are QS-9000 compliant for its PICmicro® 8-bit MCUs, KEELOQ® code hopping devices, Serial EEPROMs and microperipheral products. In addition, Microchip’s quality system for the design and manufacture of development systems is ISO 9001 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: 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

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

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

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

Kokomo
2767 S. Albright Road
Kokomo, Indiana 46902
Tel: 765-864-8360 Fax: 765-864-8387

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

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 Consulting (Shanghai) Co., Ltd., Beijing Liaison Office
Unit 915
Bei Hai Wan Tai Bldg.
No. 6 Chaoyangmen Beidajie
Beijing, 100027, No. China
Tel: 86-10-85282100 Fax: 86-10-85282104

China - Chengdu
Microchip Technology Consulting (Shanghai) Co., Ltd., Chengdu Liaison Office
Rm. 2401, 24th Floor,
Ming Xing Financial Tower
No. 88 TIDU Street
Chengdu 610016, China
Tel: 86-28-6766200 Fax: 86-28-6766599

China - Fuzhou
Microchip Technology Consulting (Shanghai) Co., Ltd., Fuzhou Liaison Office
Unit 28F, World Trade Plaza
No. 71 Wusi Road
Fuzhou 350001, China
Tel: 86-591-7503506 Fax: 86-591-7503521

China - Shanghai
Microchip Technology Consulting (Shanghai) Co., Ltd.
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

China - Shenzhen
Microchip Technology Consulting (Shanghai) Co., Ltd., Shenzhen Liaison Office
Rm. 1315, 13/F, Shenzhen Kerry Centre,
Renminnan Lu
Shenzhen 518001, China
Tel: 86-755-2350361 Fax: 86-755-2366086

Hong Kong
Microchip Technology Hongkong Ltd.
Unit 901-6, 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 Japan K.K.
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

Korea
Microchip Technology Korea
168-1, Youngbo Bldg. 3 Floor
Samsung-Dong, Kangnam-Ku
Seoul, Korea 135-882
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 Nordic ApS
Regus Business Centre
Lautrup hoj 1-3
Ballerup DK-2750 Denmark
Tel: 45 4420 9895 Fax: 45 4420 9910

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

Italy
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

01/18/02