ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

KEELOQ Code Hopping Technology Development in Communciation Systems

[1] Arunkumar [2] Mamatha Dhananjaya [3]Dr. T.C.Manjunath [4] Pavithra G [5] Satvik M. Kusagur
[1]Ex. UG BE Student, New Horizon College of Engg., Bangalore
B.E., M.Tech.,
[2]Ex. Asst. Prof., New Horizon College of Engg., Bangalore
Ph.D. (IIT Bombay), FIETE, FIE, CE, SMIEEE
[3]Professor & HOD, ECE Dept., Dayananda Sagar College of Engg., Bangalore
B.E., M.Tech., [Ph.D.-VTU-Pursuing]
[4]Research Scholar, VTU – RRC, Belagavi, Karnataka
B.E., M.Tech.
[5]Visiting Faculty, Jain Inst. of Tech., Davanagere, Karnataka

Abstract:- **Keeloq code hopping technology incorporates high security, a small package outline and low cost. This technology is incorporated in keeloq encoders such as HCS300 family and keeloq decoders such as HCS500 family which makes these devices a perfect solution for unidirectional remote keyless entry systems and access controls systems. Keeloq encryption and decryption algorithms in encoders and decoders respectively generate a unique code for every new transmission, i.e. when the user presses a button. Thus rendering code capture and resend schemes useless Keeloq is used in majority of remote keyless entry systems by companies as Daewoo, fiat, Honda, GM, Toyota, Volvo etc. The light-weight architecture of the KeeLoq cipher allows for an extremely low-cost and efficient hardware implementation. This contributed to the popularity of the KeeLoq cipher among designers of remote keyless entry systems, automotive and burglar alarm systems, automotive immobilizers, gate and garage door openers, identity tokens, component identification systems. For instance, the KeeLoq block cipher is used in the HomeLink wireless control systems to secure communication with some garage door openers. The KeeLoq technology supplied by Microchip Technology Inc. includes the KeeLoq cipher and a number of authentication protocols.**

I. INTRODUCTION

A large portion of the block ciphers are built upon Fiestel networks. Such cryptographic algorithms as DES [22], Blowfish [26], Kasumi [6], Gost [32] or RC5 [25] are based on balanced fiestel networks. Other block ciphers use source heavy or target heavy unbalanced fiestel networks.
The most extreme case of a source heavy unbalanced fiestel network is a nonlinear feedback shift register (NLFSR), which can be applied in both the stream cipher and block cipher designs.

Keeloq is a block cipher based on the NLFSR with a nonlinear Boolean feedback function of 5 variables. The algorithm uses a 64 bit key and operates on 32 bit blocks.
Its architecture consists of two registers (a 32 bit text register and a 64 bit key register), which are rotated in each of 528 encryption cycles, and of a non linear (NLF) providing nonlinear feedback.

One bit of the key is added to the output of the NLF modulo 2 in each cycle.It was designed by William Smit PhD at Nanoteq (South Africa) in the mid 80's and sold to Microchip Technology Inc in 1995 for $10 million.
It's used in code hopping encoders and decoders such as NTQ105/106/115/125d/129D and HCS101/2XX/3XX/4XX/5XX.It is used in majority of remote keyless entry systems by companies as Chrysler, Daewoo, GM, Honda etc.

II. DESCRIPTION

Keeloq code hopping encoders encrypt a 0- filled 32 bit block with Keeloq cipher to produce a 32 bit hopping code.

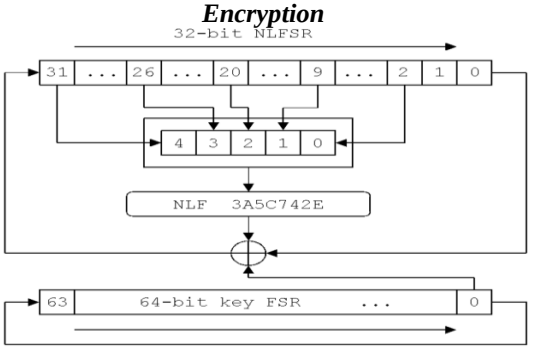
A 32 bit initialization vector is linearly added to the least significant 32 bits of the key prior to encryption to decryption.

Keeloq cipher accepts 64 bit keys and encrypts 32 bit blocks by executing its single bit NLFSR for 528 rounds. The NLFSR feedback function is 0x3A5C742E . It uses 2,9,20,26 and 31 of the NLFSR state as its inputs during encryption and bits 1,8,19,25, and 30 during decryption.

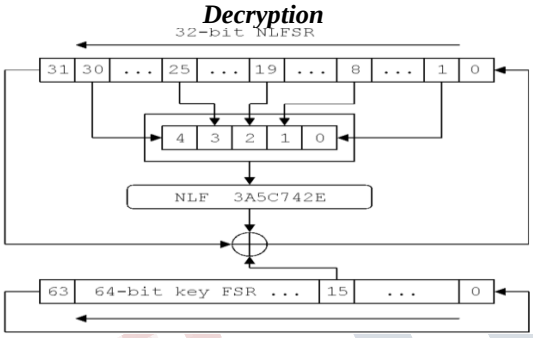
ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

Its output is linearly combined with one of its bits of the NLFSR state and with a key bit and is fed back into the NLFSR state on every round.

Encryption



Decryption



III. KEELOQ ENCODERS

The encoders rage from the HCS101, a fixed encoder designed for remote control systems, to HCS2XX and HCS3XX products, which utilize Microchips patented Keeloq code hopping technology. The devices incorporates a small package outline, are low cost and have minimal external components making them well suited for unidirectional RKE, remote control and access control systems.

The code hopping encoders combine a 32 bit code hopping code generated by a non linear encryption algorithm, with a 32 bit serial number and information bits to create transmission stream of up to 69 bits. The length of the transmission eliminates the threat of code scanning, and the code hopping mechanism makes each transmission unique, thus rendering code capture and resend schemes useless.

IV. KEELOQ DECODERS

The HCS5XX decoders offer a standard solution when used with the Keeloq encoders to implement unidirectional remote and access control systems.

The HCS5XX decoders operate over a wide voltage range and can be used as stand alone decoders in conjunction with PIC MCUs through a serial of parallel interface.
Microchip also offers a variety of software decoders that allows the system designer to integrate the Keeloq decoding functions with their applications on to a single PIC MCU.

The software decoders come as part of a licensing package (DS40038) and include the decoding algorithm, receive routines and support various learning schemes to reduce development time and get the product to market faster.

The Keeloq HCS4XX family of transponder and encoder combinations provides a single chip solution that brings together uni directional code hopping and bi-directional transponder identification (IFF).

The HCS4XX devices integrate the transponder circuitry needed to perform electronic verification of authenticity.

The HCS4XX family forms a complete line of products ranging from HCS410 for short range battery less operation, the HCS412 for longer range single antenna applications and HCS473 providing three sensitive antenna inputs for long range Omni directional communication

KEELOQ CODE HOPPING ENCODER - HCS301

Security

- Programmable 28 bit serial number
- Programmable 64 bit encryption key
- Each transmission is unique
- Encryption keys are read protected
- 32 bit hopping code
- 66 bit transmission code length

Operating

- 5V to 15V
- Four button inputs
- No additional circuitry required
- 15 functions available
- Selectable baud rate
- Automatic code word protection
- Battery low signal transmitted to receiver

typical applications

- Automotive remote keyless entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks
- Identity tokens
- Burglar alarm systems

ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

V. DESCRIPTION

The HCS301 from Microchip Technology Inc is a code hopping encoder designed for secure remote keyless entry (RKE) systems. The HCS301 utilizes the Keeloq code hopping technology, which incorporates high security, a small package outline and low cost, to make this device a perfect solution for unidirectional remote keyless entry systems and access control systems.

The HCS301 combines a 32 bit hopping code, generated by a nonlinear encryption algorithm, with a 28 bit serial number and 6 information bits to create a 66 bit code word. The code word length eliminates the threat of code scanning and code hopping mechanisms makes each transmission unique, thus rendering code capture and resend schemes useless.

The crypt key, serial number and configuration data are stored in an EEPROM array which is not accessible via any external connection. The EEPROM data is programmable but read protected. The data can be verified only after an automatic erase and programming operation. This protects against attempts to gain access to keys or manipulate synchronization values. The HCS301 provides an easy- to- use serial interface for programming the necessary keys, system parameters and configuration data.

System Overview

The HCS301 code hopping encoder is designed specifically for keyless entry systems; primarily vehicles and home garage door openers. The encoder portion of a keyless entry system is integrated into a transmitter, carried by the user and operated to gain to a vehicle or restricted area. The HCS301 is meant to be cost effective yet secure solution to such systems, requiring very few external components. Most low end keyless entry transmitters are given a fixes identification code that is transmitted every time a button is pushed. The number of unique identification codes in a low end system is usually a relatively small number.

These shortcomings provide an opportunity for a sophisticated thief to create a device that grabs a transmission and retransmits it later, or a device that quickly scans all possible identification codes until the correct one is found. The HCS301, on the other hand, employs the Keeloq code hopping technology coupled with a transmission length of 66 bits to virtually eliminate the use of code grabbing and code scanning. The high security level of the HCS301 is based on the patented Keeloq technology.

It is a block cipher based on a block length of 32 bits and a key length of 64 bits is used. The algorithm obscures the information in such a way that even if the transmission information (before encoding) differs by only one bit from that of the previous transmission, the next coded transmission will be completely different. Statistically, if only one bit in the 32 bit string of information changes, greater than 50 percent of the coded transmission bits will change.

As indicated in the block diagram the HCS301 has a small EEPROM array which must be loaded with several parameters before use; most often programmed by the manufacturer at the time of production. The most important of these are:

- A 28 bit serial number, typically unique for every encoder.
- A crypt key
- An initial 16 bit synchronization value
- A 16 bit configuration value.

The 16 bit synchronization counter is the basis behind the transmitted code word changing for each transmission; it increments each time a button is pressed. Due to the code hopping algorithm's complexity, each increment of the synchronization value results in greater than 50% of the bits changing in the transmitted code word. Figure (8.5.2) shows how the key values in thee EEPROM are used in the encoder. Once the encoder detects a button press, it reads the button inputs and updates the synchronization counter. The synchronization counter and the crypt key are input to the encryption algorithm and the output is 32 bits of encrypted information. This data will change with every button press, its value appearing externally to 'randomly hop around'; hence it is referred to as the hopping portion of the code word.

The 32 bit hopping code is combined with the button information and the serial number to form the code word transmitted to the receiver. A receiver may use any type of controller as a decoder, but it is typically a microcontroller with compatible firmware that allows the decoder to operate in conjunction with the HCS301 based transmitter. The crypt key generation typically inputs the transmitter serial number and a 64 bit manufacturer's code into the key generation algorithm. The manufacture's code is chosen by the Same system manufacturer and must be carefully controlled as it is a pivotal part of the overall system security

A transmitter must be first learned by the receiver before its use is allowed in the system. Learning includes

ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

calculating the transmitters appropriate crypt key, decrypting the received hopping code and storing the serial number, synchronization counter value and crypt key in the EEPROM. In the normal operation, each received message of valid format is evaluated. The serial number is used to determine if it is from a learned transmitter. If from the learned transmitter, the message is decrypted and the synchronization counter is verified. Finally, the button status is checked to see what operation is requested.

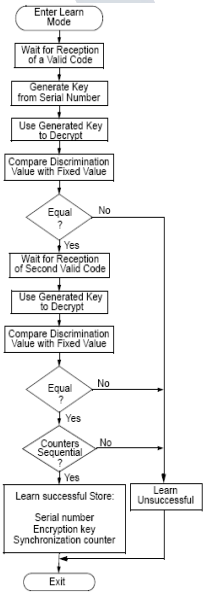
It is a simple device to use. It requires only the addition of buttons and RF circuitry for use as the transmitter in your security application. The HCS301 will wake up upon detecting a button press and delay approximately 10ms for button debounce. The synchronization counter, discrimination value and the button information will be encrypted to form the hopping code. The hopping code portion will change every transmission, even if the same button is pushed again. A code word that has been transmitted will not repeat for more than 64K transmissions. This provides more than 18 years of use before a code is repeated; based on 10 operations per day. Overflow information sent from the encoder can be used to extend the number of unique transmissions to more than 192K. If in the transmit process it is detected that a new button(s) has been pressed, a reset will immediately Occur and the current code word will not be completed

EEPROM Memory Organization

The HCS301 contains 192bits of EEPROM memory.

WORD ADDRESS	MNEMONIC	DESCRIPTION
0	KEY_0	64-bit encryption key (word 0) LSb's
1	KEY_1	64-bit encryption key (word 1)
2	KEY_2	64-bit encryption key (word 2)
3	KEY_3	64-bit encryption key (word 3) MSb's
4	SYNC	16-bit synchronization value
5	RESERVED	Set to 0000H
6	SER_0	Device Serial Number (word 0) LSb's
7	SER_1(Note)	Device Serial Number (word 1) MSb's
8	SEED_0	Seed Value (word 0)
9	SEED_1	Seed Value (word 1)
10	RESERVED	Set to 0000H
11	CONFIG	Config Word

Note: The MSB of the serial number contains a bit used to select the Auto-shutoff timer.



KEY_0 – KEY_3 (64 BIT CRYPT KEY)

The 64 bit crypt key is used to create the encrypted message transmitted to the the receiver. This key is calculated and programmed during [production using a key generation algorithm. While the key generation algorithm supplied from the microchip is the typical method used, a user may elect to create their own method of key generation.

SYNC (SYNCHRONIZATION COUNTER)

This is a 16 bit synchronization value that is used to create the hopping code for transmission. The value will increment after every transmission.

RESERVED

Must be initialized to 0000H.

TABLE (8.7.1): EEPROM MEMORY MAP

SER_0, SER_1 (ENCODER SERIAL NUMBER)

These are the lower and upper words of the device serial number. Although there are 32bits allocated for the serial number, only the lower order 28 bits are transmitted. The serial number is meant to be unique for every transmitter.

SEED_0, SEED_1 (SEED WORD)

The 2 word seed code will be transmitted when all the three buttons are pressed at the same time. This allows the system designer to implement the secure learn feature or use this fixed code word as part of a different key generation/ tracking process.

CONFIG (CONFIGURATION WORD)

The configuration word is a 16 bit word stored in EEPROM array that is used by the device to store information used during the encryption process, as well as the status of option configurations.

Transmitted Word

Code Word Format

The HCS301 code word format is made up of several parts. Each code word contains a 50% duty cycle preamble, a header, 32 bits of encrypted data and 34 bits of fixed data followed by a guard period before another code word can begin.

The HCS301 transmits a 66 bit code word when a button is pressed. The 66 bit word is constructed from a fixed portion and an encrypted code portion.

ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

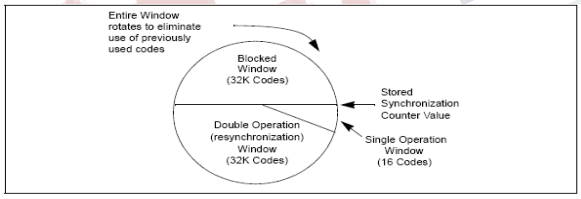
The 32 bits of encrypted data are generated from 4 button bits, 12 discrimination bits and the 16 bit sync value. The encrypted portion provides up to four billion changing code combinations. The 34 bits of fixed code data are made up of 2 status bits, 4 button bits and the 28 bit serial number. The fixed and encrypted sections combined increase number of code combinations to 7.38 x 10^19. Use of the HCS301 in a system requires a compatible decoder. This decoder is typically a microcontroller compatible firmware. A transmitter must first be learned by the decoder before its use is allowed in the system. The decoder receives and authenticates a first transmission; first button press. Authentication involves generating the appropriate crypt key, decrypting, validating the correct key usage via the discrimination bits and buffering the counter value.

A second transmission is received and authenticated.

A final check verifies that the counter values were sequential; consecutive button presses. If the learn sequence is successfully complete, the decoder stores the learned transmitters serial number, current synchronization counter value and appropriate crypt key.

Synchronization With Decoder

The Keeloq technology patent scope includes a sophisticated synchronization technique that does not require the calculation and storage of future codes. The technique securely blocks invalid transmissions while providing transparent resynchronization to transmitters inadvertently activated away from the receiver.



Figure(8.10.1): Synchronization Window

The figure shows a 3-partition, rotating synchronization window. The each time a transmission is authenticated, the intended function is executed and the transmission's synchronization counter value is stored in EEPROM. From the currently stored counter value there is an initial "single operation" forward window of 16 codes.

If the difference between a received synchronization counter and the last stored counter is within 16, the intended function will be executed on the single button press and the new synchronization counter value effectively rotates the entire synchronization window.

A "double operation" window further exists from the single operation window up to 32K codes forward of the currently stored counter value. It is referred to as "double operation" because a transmission with synchronization counter value in this window will require an additional, sequential counter transmission prior to executing the intended function.

Upon receiving the sequential transmission the decoder executes the intended function and stores the synchronization counter value. This resynchronization occurs transparently to the user as it is human nature to press the button a second time if the first on e was unsuccessful.

The third window is a "blocked window" ranging from the double operation window to the currently stored synchronization counter value. Any transmission with the synchronization value within this window will be ignored. This window excludes previously used, perhaps code grabbed transmissions from accessing the system.

VI. KEELOQ CODE HOPPING DECODER - HCS500

Security

- Encrypted storage of manufacturer's code
- Encrypted storage of crypt keys
- Up to seven transmitters can be learned.
- Keeloq code hopping technology
- Normal and secure learning mechanisms.

Operating

- 3.0V – 5.5V operation
- Internal oscillator
- Auto bit rate detection.
- Stand alone decoder chipset
- External EEPROM for transmitter storage
- Synchronous serial interface
- 1 Kbit user EEPROM
- 8 pin DIP/ SOIC package

Typical applications

- Automotive remote keyless entry systems
- Automotive alarm systems
- Automotive immobilizers
- Gate and garage openers
- Electronic door locks
- Identity tokens
- Burglar alarm systems

Compatible encoders

All Keeloq encoders and transponders configured for the following setting:

- PWM modulation format
- Te in the range from 100us to 400us
- 10x Te header

ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

- ♣ 28 bit serial number
- ♣ 16 bit synchronization counter
- ♣ Discrimination bits equal to serial number 8 LSbs
- ♣ 66 to 69 bit length code word.

Description

The Microchip Technology Inc HCS500is a code hopping decoder designed for secure remote keyless entry (RKE) systems. The HCS500 utilizes the patented Keeloq code hopping system and high security learning mechanisms to make this a canned solution when used with the HCS encoders to implement a unidirectional remote and access control systems. The HCS500 can be used as a stand alone decoder or in conjunct ion with a microcontroller

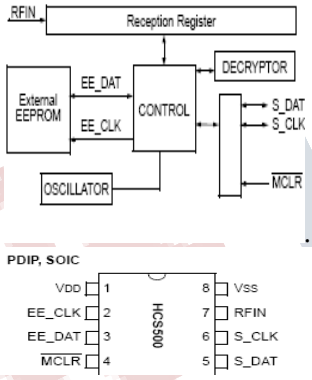


Figure (9.5.1): Internal Block Diagram Of Decoder Hcs500

The manufacturer's code, crypt keys, and the synchronization information are stored in encrypted form in external EEPROM.

The HC500 uses the S_DAT and S_CLK inputs to communicate with a host controller device

The HCS500 operates over a wide voltage range of 3.0 volts to 5.5 volts. The decoder employs automatic bit rate detection, which allows it to compensate for wide variations in transmitter data rate.The decoder contains sophisticated error checking algorithms to ensure only valid codes are accepted.

VII. ENCODERS PACKAGING INFORMATION

Figure (10.1): 8- Lead Plastic Dual In- Line (P) - 300 Mil (Pdip)

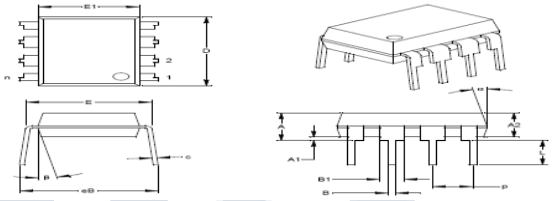
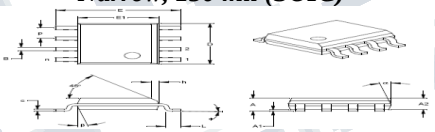


Figure (10.2): 8 – Lead plastic small outline (SN) – Narrow, 150 mil (SOIC)



VII. DECODERS PACKAGING INFORMATION

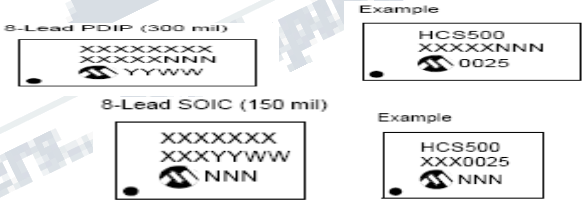


FIGURE (11.1): 8- Lead Plastic Dual In- Line (p) - 300 mil (PDIP)

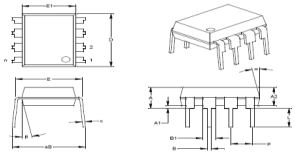
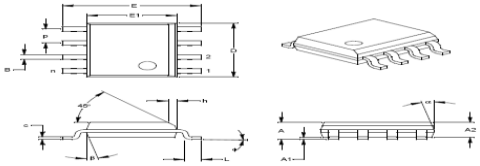


FIGURE (11.2): 8 – Lead plastic small outline (SN) – Narrow, 150 mil (SOIC)



11. TYPICAL APPLICATIONS

FIGURE(11.1): TYPICAL APPLICATIONS

ISSN (Online) 2456-1290
International Journal of Engineering Research in Mechanical and Civil Engineering (IJERMCE)
Vol 1, Issue 7, November 2016

Authentication
Remote keyless entry
Passive keyless entry
Odometer counter
Property identification
Garage door openers
Remote gate openers
User authorization
Immobilizers
Wireless home security
Remote control
Clone protection