Design of RKE System Based on KEELOQ Encryption Technology

Yue-li HU*
1. College of Mechatronics Engineering and Automation, Shanghai Key Laboratory of Power Station Automation Technology, Shanghai University
2. Key Laboratory of Advanced Display and System Applications(Shanghai University), Ministry of Education,Shanghai, China
*huyueli@shu.edu.cn

Yan ZHANG, Bin SUN
1. College of Mechatronics Engineering and Automation, Shanghai Key Laboratory of Power Station Automation Technology, Shanghai University
2. Key Laboratory of Advanced Display and System Applications(Shanghai University), Ministry of Education,Shanghai, China
zhangyan55@sohu.com

***Abstract*—KEELOQ code hopping technology is a nonlinear anti-encryption algorithm designed for secure Remote Keyless Entry (RKE) systems. It combines a 66-bits transmission length, so as to prevent the system from code predicting, code grabbing and code scanning. Because of its feature of high-security, it effectively overcomes the disadvantages of the traditional fixed code technology. This paper researched on KEELOQ encryption algorithm and presented a designed RKE system based on KEELOQ technology. When the software and hardware were designed, the whole RKE system was afterwards made as a prototype for the functionality tests. The experimental results showed that the design achieved the anticipative effects.**

Keywords-KEELOQ encryption algorithm; Remote Keyless Entry(RKE); Decoding method; Avalanche effect; System design

I. INTRODUCTION

Nowadays, the Remote Keyless Entry (RKE) system has been widely used for automotive applications since its practicality and convenience. Thus, where the system performs the data transmission is in the public channel. As known to all, data transmitted in the public channel is available completely to anyone and could be grabbed and scanned, which induces the potential danger of information security and is inevitable however. In order to prevent data grabber from identifying the actual contents of information, what we need do is to encrypt the transmitted data. This paper researches on the KEELOQ encryption algorithm that is designed for secure Remote Keyless Entry (RKE) systems and afterwards presents a designed RKE system based on KEELOQ encode technology.

II. RESEARCH ON SECURITY OF KEELOQ ENCRYPTION TECHNOLOGY

KEELOQ is a kind of patent code encryption technology and the core of it is the private key algorithm that encrypts the 32-bit data block based on 64-bit encryption key[1]. KEELOQ is such a non-linear formula for estimation that output is the only result and unrepeatable one to input. Compared to DES (Data Encryption Standard), KEELOQ technology greatly improves the security level, therefore it is suitable to the antitheft system of data transmission and Remote Entry System.

A. Data Encryption Standard (DES)

DES (Data Encryption Standard) was adopted as the forty-sixth Federal Information Processing Standard by National Bureau of Standards (now is named as NIST, National Institute of Standards and Technology) in 1977[2]. In DES, 64-bit data is separated as several groups to be encrypted and the crypt key is the 56-bit-length information which is the same as the one in decoding process. All the details of DES algorithm is public[3]. As a result, the information security totally depends on the security of crypt key.

B. KEELOQ algorithm principle

The algorithm principle of KEELOQ technology is discussed in detail as follows based on the encode chip HCS301.

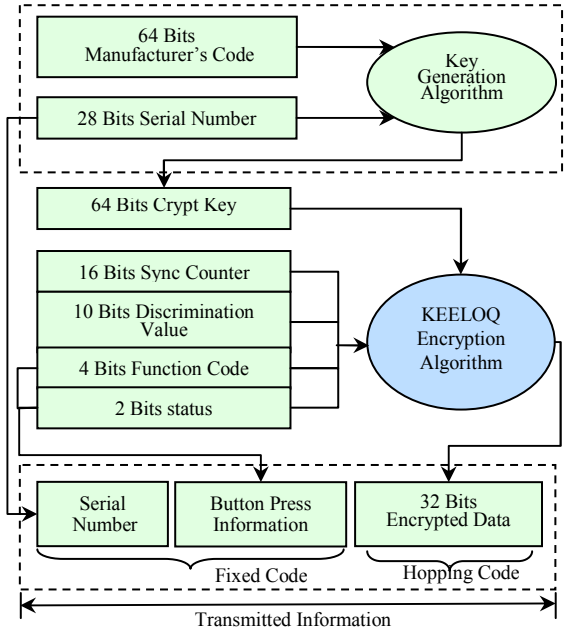


Figure 1. Structure diagram of encoding based on KEELOQ encryption algorithm

978-0-7695-3816-7/09 $26.00 © 2009 IEEE
DOI 10.1109/AICI.2009.99

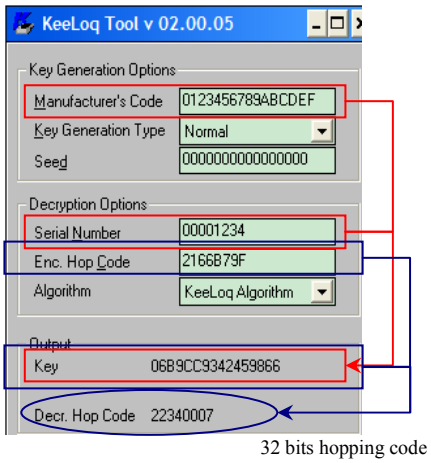
IEEE computer society

Figure 1 shows the structure diagram of encoding based on KEELOQ encryption algorithm. The Synchronization Counter is used to protect the code from being grabbed. Once the encoder detects a button press, it reads the button input and increments the Synchronization Counter value. The Synchronization Counter and 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 hopping around', hence it is referred to as the hopping portion of the code word[4]. The 32-bit hopping code is combined with the 34-bit fixed portion consists of button information and Serial Number to form the code word transmitted to the receiver.

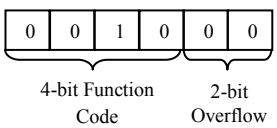
C. *Experiments of manual decoding*

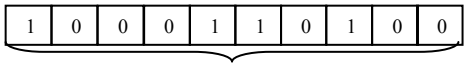
Figure 2 illustrates two experiments of manual decoding using a series of operating software including encoding and decoding provided by Microchip Technology Inc. On the assumption that Manufacturer's Code, Serial Number, Encrypted Hop Code which consists of 16 bits Synchronization Counter values, 10 bits Discrimination Code, 2 bits Overflow and 4 bits function values, are separately set to be 0123456789ABCDEF, 00001234 and 2166B79F, and button S0 is active.

After filling in the information, we get 64 bits Crypt Key 06B9CC9342459866, which is generated using the Key Generation Algorithm by the combination of Manufacturer's Code and Serial Number. Then Crypt Key combines Encrypted Hop Code to create the unique Decrypted Hop Code 22340007, which is a part of the transmission code. By decoding the hop code, we conclude that button S0 is active and the Discrimination Valves are accord with the lower order 10 bits of Serial Number (Default).

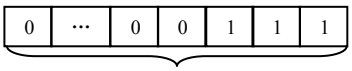


32 bits hopping code





10-bit Discrimination Key=234H



16-bit Sync Counter=0001H

Figure 2. Maunal decoding

Completing the first transmission, the encoder updates the Synchronization Counter and the Encrypted Hop Code is supposed to be 2166B7A0. Filling the value and others not changed, we acquire the new Decrypted Hop Code 1C314BF3 which is completely different.

Actually, KEELOQ algorithm obscures the information in such a way that even if the transmission information (before coding) 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[5].

D. *Avalanche Effect*

Avalanche Effect is the most marked security character of KEELOQ encoding technology.

The concept of Avalanche Effect is that each output bit and all the input bits are highly relevant. In other words, even if the whole input data differs by only one bit, more than half output bits will change[5]. With the introduction of Synchronization Counter in KEELOQ technology, the encrypted data will change with every button press since the Synchronization Counter value is updated before participating in creating the encrypted data, which is obvious an embodiment of Avalanche Effect.

The core principle of KEELOQ algorithm is to create 32 bits encrypted data using 32 bits CSR[31:0](Discrimination Key) which has been encrypted using 64 bits EN_KEY [63:0](Encrypting Key) previously[2][5].

First of all, we define a non-linear table in which there is one output NLF_OUT from 5 input bits NLF_IN[4:0] and function of it supposes f( ). The principle is introduced as follows.

It generates an output code NLF_OUT utilizing non-linear algorithm by getting 5 fixed bits: I_0, I_1, I_2, I_3, I_4 from CSR[31:0] distantly and equably. The output is

$$\begin{aligned} NLF\_OUT_0 &= f[NLF\_IN(4:0)] \\ &= f[CSR_0(I_0, I_1, I_2, I_3, I_4)] \end{aligned} \quad (1)$$

It combines the fifteenth bit in EN_KEY and two bits in CSR to create the first output code CRYP [0].

$$CRYP[0] = NLF\_OUT_0 \ xor \ EN\_KEY_0[15]$$

$$
\begin{aligned}
&xor\ \ CSR_0[I_5]\ \ xor\ \ CSR_0[I_6] \\
&= f[CSR_0(I_0, I_1, I_2, I_3, I_4)] \\
&\ \ xor\ \ EN\_KEY_0[15]\ \ xor\ \ CSR_0[I_5] \\
&\ \ xor\ \ CSR_0[I_6]
\end{aligned} \tag{2}
$$

Then, EN_KEY and CSR shift separately. CRYP[0] acts as the input when CSR shifts.

$$
CSR_i = (CSR_{i-1} << 1) + CRYP[i-1] \tag{3}
$$

$$
EN\_KEY_i = EN\_KEY_{i-1} << 1 \tag{4}
$$

Repeat above steps till we get the 32 bits encrypted key CRYP [31:0]:

$$
\begin{aligned}
CRYP[i] = f[CSR_i(I_0, I_1, I_2, I_3, I_4)] \\
xor\ \ EN\_KEY_i[15] \\
xor\ \ CSR_i[I_5]\ \ xor\ \ CSR_i[I_6]
\end{aligned} \tag{5}
$$

From the discussions and formulas, we can find that the output of next round contains the results of previous round, while tiny changes of input data qua input information of next round will expand so rapidly that Avalanche Effect is formed.

Algorithm based on Avalanche Effect effectively prevents the risk that analyzers observe the output by altering the input slightly, therefore it greatly enhance the system security.

III. RKE SYSTEM DESIGN

In this paper, a typical RKE system using the encoder chip HCS301 is designed to realize the decoding solution based on KEELOQ encode technology.

A. System hardware design

Figure 3 shows the block diagram of the designed RKE system proposed in this paper, which consists of a receiver installed in the car and a remote wireless key as a transmitter carried by the driver. The receiver is composed of a RF receiver device, a microcontroller and the control module, while the wireless key portion consists of an encoder and the Surface Acoustic Wave circuit that generates RF signals.

It is a typical solution for Remote Keyless Entry system. The car doors can be controlled by sending a relevant control command from drivers. In figure 3, users press the button to start the communication between the receiver and transmitter. The encoder HCS301 encodes data composed of the function messages and synchronization values. Afterwards it creates a 66 bits code which will be transmitted to UHF frequency band through the SAW circuit. The receiver device MICRF002 acquires the 66 bits code and demodulates it. And then the microcontroller PIC16F689[6], which is in charge of the decrypting task, implements relevant control commands.

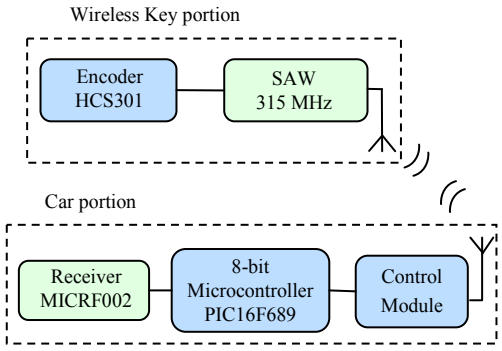


Figure 3. RKE system structure block diagram

ASK(Amplitude Shift Keying) modulation mode is adopted in the system to extend the battery life of transmitter.

B. System software design

Instead of the decoding chip of HCS series, a microcontroller PIC16F689 is applied to implement all the decoding and controlling module, which adds the difficulty for programming but acquires a greater feasibility for the system and also exceeds the limitations of hardware.

The decoding process is as follows. The decoder waits until a transmission is received. The received serial number is compared to the EEPROM table of learned transmitters to first determine if this transmitter's use is allowed in the system. If it is from a learned transmitter, the transmission is decrypted using the stored crypt key and authenticated via the discrimination bits for appropriate crypt key usage. If the decryption is valid the synchronization value is evaluated.

We designed for C coding to realize learning, decoding, and controlling sequences, which has been programmed into the microcontroller PIC16F689[6].

C. Implementation and display result

After the complete designing of software and hardware, the whole RKE system is then made as a prototype for the functionality tests.

The signal of transmitter is analyzed and checked by using the Real-Time Spectrum Analyzer and finally the transmitter is proved to function properly. Figure 4 shows the results of spectrum analysis.

TABLE 1. PARAMETERS SETTING

Num	***Name***	***Performance***
1	Center Frequency	315MHz
2	Span	36MHz
3	Acquisition Length	40ms

Since the centre RF of designed system is 315±0.5MHz, the parameter 'Center Frequency' and 'Span' is set to 315MHz, 36MHz respectively.

Taking account of the facts that the total transmission time is 17.6ms~44.6ms and the signals can be stably acquired, we set the 'acquisition length' to be 40ms and achieve ideal experimental results.

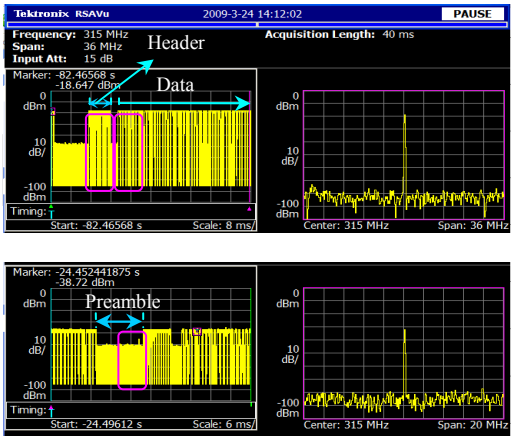


Figure 4. Spectrum analysis

In figure 4, the preamble, header and encrypted data of a code word are marked clearly as a standard format.[4] We can analyze the organization of a code word according to the transformation of electrical signals, from which the transmitter is proved to work properly.

Finally, the RKE system was proved to work stably and properly by connecting the receiver with the electrical motor. The function of opening/locking the door using wireless key and lock automatically was verified separately via positive and negative motor rotation.

IV. CONCLUSION

This paper researched on security of the KEELOQ encoding algorithm and designed a RKE system using the encoder HCS301 and the microcontroller PIC16F689. Moreover, the whole system was proved to work properly and stably by signal analysis via Real-Time Spectrum Analyzer and functionality tests via connecting the receiver to the motor.

ACKNOWLEDGMENT

The authors would like to thank "11th Five-Year Plan" 211 Construction Project supported by Shanghai University ,the National High Technology Research and Development Program of China (863 Program) （No. 2008AA03A336），National Natural Science Foundation of China (Foundation Number: 60773081)，IC Special Foundation of Shanghai Municipal Commission of Science and Technology (Grant No. 08706201800) and Innovation Fund of Shanghai University for financial support.

REFERENCES

[1] Wang Xiahua, Zhang Yongmei, System of Hopping Code Rmote Keyless Entry, Computer Measurement & Control, Vol10, 2002. 692-693

[2] Willian Stalling. Cryptography and Network and Security-Principles and Practice[M].Beijing: Electronic Industry Publishing House, 2004. 51, 57~58

[3] Yang Xiaoyuan, Wei Lixian, Computer cryptography[M]. Xi'an: Xi'an Jiaotong University Publishing House, 2007. 11~12, 23~25

[4] Microchip Technology Inc, KEELOQ Code Hopping Encoder HCS301, Data Sheet, 1996

[5] Wang Wenhu, Li Jiaoqi, Tao Zengjie, Application of KEELOQ hopping encode technology in the automobile security system[J], Electronic Measurement Technology, Vol30, No10. October 2007. 197~198

[6] Microchip Technology Inc, PIC16F685/687/689/690, Data Sheet, 2005