Application Of KEELOQ Algorithm In PEPS System

Dan Li
Dept. of Physics & Electronic Science
Guizhou Normal University
Guiyang,Guizhou,China
e-mail:125433047@qq.com

Wenjun Xiao[1,2]
1.Key Laboratory of special Automotive Electronics technology of the Education Department of Guizhou Province
Guiyang,Guizhou,China
2. Dept.of Physics & Electronic Science,Guizhou Normal University
Guiyang,Guizhou,China
e-mail:258552578@qq.com

Yi Wang[1,2] *
1.Key Laboratory of special Automotive Electronics technology of the Education Department of Guizhou Province
Guiyang, Guizhou, China
2. Dept.of Physics & Electronic Science,Guizhou Normal University
Guiyang,Guizhou,China
e-mail:wyigz@126.com
*Corresponding Author

Abstract—Passive Entry Passive Start(PEPS) because its high security and easy to use which has become the main development trend in the field of the automotive electronics.For the security and reliability of PEPS system,my paper proposed a encryption and decryption method based on KEELOQ algorithm.Compared with other encryption algorithms,the proposed method increases the synchronization,which makes each transmitted data is unique and does not repeat,and also increasing the difficulty of data decoding and interception,improving the security of the system.This paper mainly use the KEELOQ algorithm encryption and decryption principle and process,the working princeple of PEPS system,those program to discuss the design of the intelligent key and the application of KEELOQ algorithm in PEPS system.in the end,the paper also made a encoding and decoding experiments.The result show that as long as the sended data made one change,the result is changed more than half after the encryption of KEELOQ algorithm.therefore,the method I researched in this paper can effectively improve the security and reliability of PEPS system.

Keywords-PEPS;KEELOQ;intelligent key;KEELOQ tool; encryption algorithm

I. INTRODUCTION

With the continuous improvement of people's living standard, People have higher requirements to property security,For example,the safety of the entrance guard system[1]. Now in order to let people use more convenient,therefore,the security and reliability of the entrance guard system has been the subject of the researchers study[2]. Entrance guard system including visual entrance guard system, alarm,entrance guard system,fingerprint entrance guard system and entrance guard system of remote control,etc.,especially in the remote access system has been widely used,such as the home gateway,garage door,door, corridor to the highway toll station,etc[3].Passive Entry Passive Start(PEPS) system is developed on the basis of the remote access system is the latest security technology,it integrates the remote access system and anti-theft lock check system (Immobilizer, IMMO) function,to a great extent,it satisfies the people to the requirements of access control system security, The KEELOQ algorithm proposed in this paper to implement the encryption and decryption of PEPS system, so as to ensure the safety of the car.KEELOQ algorithm is a block cipher algorithm designed by South Africa WilleSmit,in the 1980s,it includes 32-bit block cipher and 64-bit key length,it is now widely used in automobiles wireless door lock device[4].

II. KEELOQ ALGORITHM PRINCIPLE

KEELOQ block cipher is an unbalanced Feistel structure[5], the packet length is 32 bit,encryption for 528 times,Each circle only change 1 bit,encryption key length is 64 bits,and recycling in the encryption process.the core idea KEELOQ algorithm is to use KEELOQ encryption algorithm with 64 bit encryption key to encrypt 32 bit plaintext, finally get a 32 bit cipher text,at the receiving end use the KEELOQ decryption algorithm decryption 32 bit cipher text,and restore the 32 bit plaintext,when decrypting need to learn the serial number, identification number and synchronization of the encoder count,can decod the encoded information effectively[6-7].The key of KEELOQ algorithm is the synchronous counter,because in the receiver receives the data after decryption,to determine whether the synchronous counter match,only the synchronous counter after the match,will process the received information.KEELOQ algorithm process has two steps they are encryption and decryption.

A. KEELOQ encryption process

It needs to define a data registers and key registers before encryption,used to store the 32 bit plaintext and 64 bit key, respectively.The encryption process is:(1)Define a

nonlinear table has five input code, 1 output code;(2) In the data register of evenly spaced take five: $L_{31}, L_{26}, L_{20}, L_9, L_1$ Through the type(1) nonlinear operation (NLF) to produce an output code;(3) Get the output code L_{16}, L_0 and the key k_0 in the register through an exclusive or operation to get the first output;(4) Each generates an output code,data registers and the key registers to do shift processing, respectively,then repeat the process above 528 times,can get a 32-bit cipher text.KEELOQ encryption algorithm process is shown in the Fig .1 below.

Mathematical expression of the encryption algorithm is as follows:

$$\Phi^i = NLF(L_{31}^{\ i}, L_{26}^{\ i}, L_{20}^{\ i}, L_9^{\ i}, L_1^{\ i}) \oplus L_{16}^{\ i} \oplus L_0^{\ i} \oplus k_{i \bmod 64}$$

$$L^{i+1} = (\Phi^i, L_{31}^{\ i}, ..., L_1^{\ i}) \quad i \text{ from 0 to 527}$$

Type of NLF for nonlinear function

$$NLF(a,b,c,d,e) = abc \oplus abd \oplus ace \oplus ade \oplus de \oplus cd \oplus be \oplus bc \oplus ae \oplus ac \oplus e \oplus d \quad (1)$$

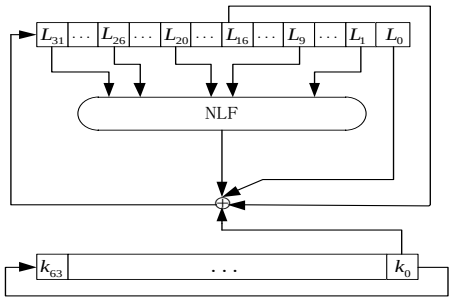

Figure 1. KEELOQ encryption algorithm process

B. KEELOQ decryption process

The method of decryption process and encryption process almost the same,just bits of operational data changed.Decryption process is:(1)Define a nonlinear table has five input code,1 output code;(2)In the data register of evenly spaced take five: $L_{30}, L_{25}, L_{19}, L_8, L_0$ Through the type (1) nonlinear operation (NLF) to produce an output code;(3)Get the output code L_{31}, L_{15} and the key k_{15} in the register through an exclusive or operation to get the first output;(4) Each generates an output code,data registers and the key registers to do shift processing, respectively,then repeat the process above 528 times,can get a 32-bit plaintext.KEELOQ decryption algorithm process is shown in the Fig .2 below.

Mathematical expression of the decryption algorithm is as follows:

$$\theta^i = NLF(L_{30}^{\ i}, L_{25}^{\ i}, L_{19}^{\ i}, L_8^{\ i}, L_0^{\ i}) \oplus L_{15}^{\ i} \oplus L_{31}^{\ i} \oplus k_{i\text{-}1 \bmod 64}$$

$$L^{i\text{-}1} = (L_{30}^{\ i}, ..., L_0^{\ i}, \ \theta^i) \quad i \text{ from 528 to 1}$$

Type of NLF for nonlinear function

$$NLF(a,b,c,d,e) = abc \oplus abd \oplus ace \oplus ade \oplus de \oplus cd \oplus be \oplus bc \oplus ae \oplus ac \oplus e \oplus d \quad (1)$$

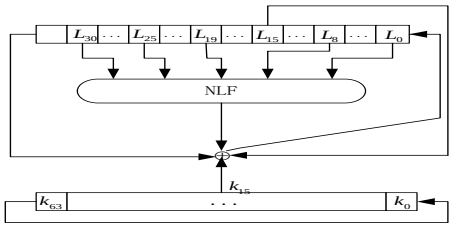

Figure 2. KEELOQ decryption algorithm process

III. PEPS SYSTEM COMPOSITION AND WORKING PRINCIPLE

A. PEPS system structure

The development of the car door,has experienced three stages,total mechanical locks,remote control door lock and PEPS system so far.

PEPS system consists of PEPS ECU、Electrical Steering Colum Lock(ESCL)、SWITCH、Immobilizer(IMMO)、ANTENNA、intelligent key、body control module(BCM)、engine control moduleand the inductive switch and other components.Very high requirements for hardware and security and it is very expensive,abroad mainly in high middle-grade automobile and domestic development of low cost and high security of PEPS system[8], The system removes trouble is that start the vehicle by inserting the key,improve the ride comfort[9-10].

B. PEPS system working principle

Principle of PEPS system are shown in Fig .3 below.Between PEPS ECU and BCM,ECM,ESCL through CAN bus communication,and the information obtained from the bus through CAN bus and the ECM,ESCL authentication.

It consists of Passive Entry Passive Start two parts,in PE section,when the user has a valid intelligent key near the door handle within one meter,PEPS controller by low frequency antenna to send instruction to intelligent key,and then validated, after verification the received information by the KEELOQ algorithm for data encryption,and the encrypted data is returned to the PEPS controller, the PEPS control will sent unlock instructions to BCM via CAN bus controller,and then complete the unlock door lock operation.In PS section,under the condition of the interior has a valid intelligent key,only requires the user to press the ignition switch,PEPS ECU send low frequency signal by low frequency antenna to intelligent key,Then intelligent key compare the received signal with the storing information and authentication,if authentication complete,t he PEPS ECU will connecte the powe immediately,with the ESCL,EMS through the CAN bus communication authentication and unlock,after unlocked,PEPS ECU will receive the brake pedal signal is connected with the ECM starter relay,so as to make the engine start.

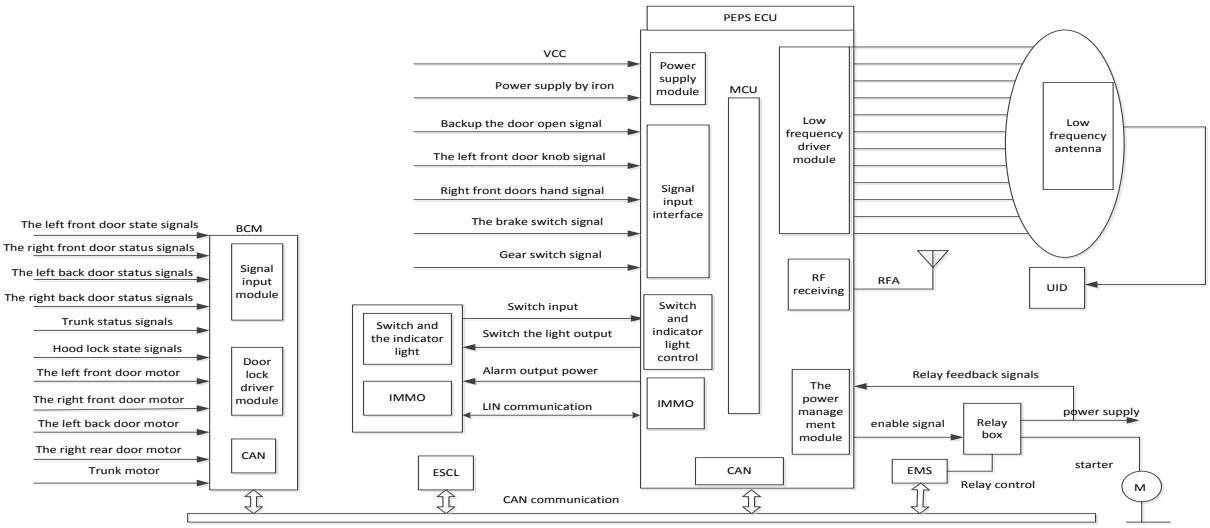

Figure 3. PEPS system schematic diagram

IV. THE DESIGN OF THE PEPS SYSTEMS' INTELLIGENT KEY

A. The working principle of intelligent key

Due to the block HCS365 built-in EEPROM,the PEPS system intelligent key work is under the principle of the HCS365 KEELOQ encoder.EEPROM is used to store a s-

erial number (SN),synchronization code (SYNC),SEED,c-

ode(SEED), encryption keys(EN_KEY),etc[11].SN is used for identifie different objects,EN_KEY use KEELOQ algorithm to encrypt data,and make the data is not easy to decipher,SYNC is used to prevent data be intercepted and each button press,synchronous counter value will be add 1,after the KEELOQ encryption algorithm,the outcome by the PWM serial output,SEED is used for users in learning KEELOQ encryption algorithm,to participate in the encryption key generation,intelligent key work flow chart are shown in Fig .4 below.

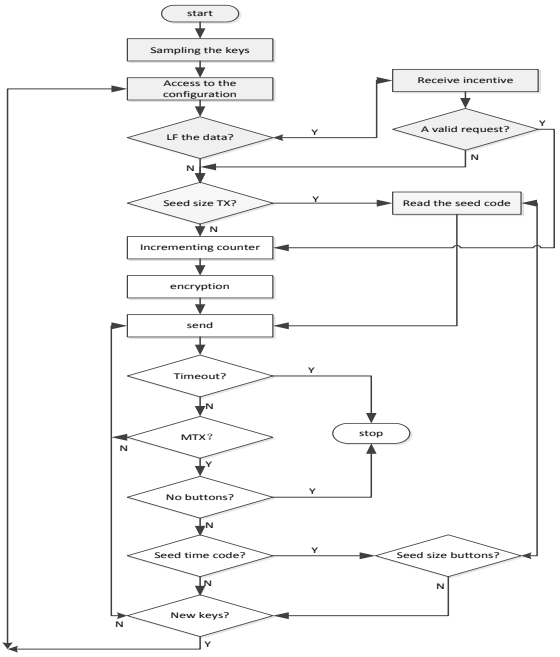

Figure 4. Intelligent key working flow chart

Intelligent key with four buttons,S0,S1,S2,S3.After combination can achieve 15 kinds of function,so each button press,will automatically generate KEELOQ encryption password.then the encrypted data is sent to the receiver,the receiver only through learning can get the decrypt key.KEELOQ algorithm has three kinds of learning methods,namely,simple to learn,normal and safety study.Simple learning results is that decode passwords is manufacturer code, normal learning needs two study can get the decode passwords, Safety study way and normal way to learn the decoding way actually is the same,just produce the decode passwords in a different way,it needs a SEED to decode passwords,through three steps can obtain 64 decoding password:

Step 1: First start the receiver in a safe learning model,then press the four key at the same time,and sent seeds code and serial number.

Step 2: Code for 32-bit LSB by seed.

Step 3: Use the method of 0 + serial number to generate 32-bit MSB.

Above use the decryption algorithm is through the KEELOQ algorithm for decoding,the decodingprocess is as follows[12]:

(1) Receive effective KEELOQ data;

(2) The fixed code and serial number in the database compared to see if the same;

(3) Take out the 64 decode passwords in the database;

(4) Decode the received information;

(5) Compares the 10 bit identification code and the serial number of the low 10 bit to see if the same;

(6)Compare fixed code and after decode their function keys to see if the same;

(7) Check the synchronization count change is correct.

B. The experiment of encryption and decryption

Fig .5 shows a paper decodes the demonstration experiment,this paper adopted the Microchip company offers a software that is use KEELOQ algorithm to encryption and decryption.Assumes that the manufacturer code is 0123456789ABCDEF,serial number is 01234567,t

he encryption hopping code is D4A34B0E,S1 button press (the order of the keys to S2 and S1, S0, S3),Fig .5 illustrates the 64 bit encryption key is 0516FBE989074278,and to send a 32bit hopping code is 41670001,After verification,found that 10 bit identification code and the fixed code of 28 serial number low 10 bit are same,while 4 bit key values for 0100 is S1 button press. Fig .6 shows the paper decodes the experiment of the second sending code,we can see synchronous count automatically add 1,become D4A34B0F,at the same time,the size of hopping code has completely changed(B7587ECD),so the uniqueness and the unrepeatable conclusion of KEELOQ algorithm mentioned above is verified,and showed the KEELOQ algorithm has high security and reliability.

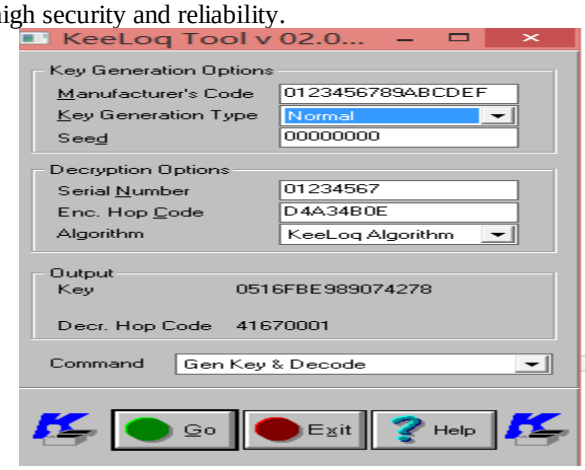

Figure 5. The paper decodeing the experiment

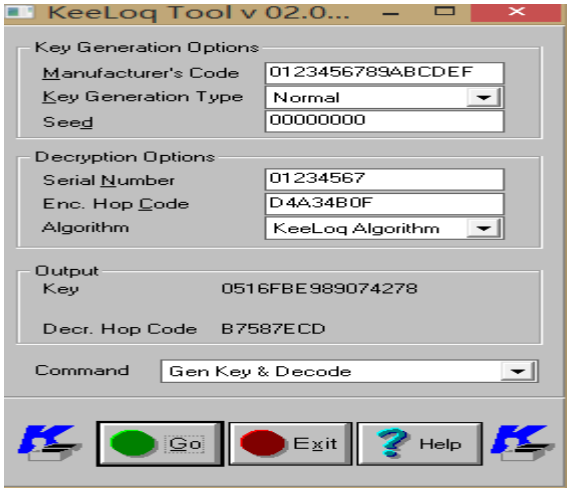

Figure 6. The second paper decodeing the experiment

V. CONCLUSIONS

This paper introduces the KEELOQ encryption algorithm principle and process,gives a detailed Passive Entry Passive Start (PEPS) schematic diagram,finally did KEELOQ encryption to decrypt the experiment on the paper,analyze the result,and it is concluded that the KEELOQ algorithm in decoding the uniqueness and the unrepeatable conclusion,through analyzing the KEELOQ technology,apply it to the PEPS system,make the system high confidentiality,low cost,and has a great practical value.

ACKNOWLEDGMENT

This work was supported by the National Natural Science Foundation of China (Grant No. 61262007，61462015), by International Science & Technology Cooperation Research Foundation of Guizhou Province (Grant No. [2014]7007), in part by Key Laboratory of Education Department of Guizhou Province (Grant No. KY word [2014] 213)

REFERENCES

[1] Liu J T.The development of multi-functional door,garage door, automatic door in China.China Construction Metal Structure,2006, pp.11-12.

[2] Wang K R.Reliable and secure password lock.Electronic Technology Application,2001,pp.14-16.

[3] Qiao P.DESIGN of remote control without a spoonful of entrance guard system based on the rolling code technology.Harbin:Northeast Forestry University Control Theory and Control Engineering,2014.

[4] Wang Y M,Zhang T,and Huang J W.Information hiding--Theory and technology.Beijing:Tsinghua University press,2006,pp.30-65.

[5] Wang Q Y and Jin C H.IMPROVEMENT of first kinds of sliding and algebraic attacks on Keeloq.Computer Engineering,2009,pp.133-137.

[6] Microchip Technology Inc.HCS301 KEELOQ code hopping encoder (DS21143C)[EB/OL].(2011)[2013-08-06].http://www.microchip.com.

[7] Microchip Technology Inc.Use the KEELOQ generate the hopping code(DS00665A-CN)[EB/OL].(2007)[2013-08-06].http://www.microchip.com

[8] Wikipedia.Advanced Encryption Standard[EB/OL].[2013-10-25].http://en.wikiped ia.org/wiki/ Advanced-Encryption-Standard.

[9] Wang S G and Li Xia Q S.Automotive electronics.Beijing:Tsingh-

ua University press,2011.

[10] Ke L P R.Starter motor integration technology.Beijing:Beijing institute of technology press,2008.

[11] Microchip Technology Inc.KEELOQ Code Hopping Encoder HCS365 Data sheet[EB/OL].[2002-12-10].http://www.microchip.com.

[12] Wang W H,Li J Q,and Tao Z J.Application of KEELOQ rolling encryption technology in the automobile anti-theft system.Electronic measurement technology,2007,pp.197-1.