VNU Journal of Mathematics – Physics, Vol. 29, No. 1 (2013) 59-65

High Security RF Remote Controller

Pham Manh Thang*, Nguyen Van Quyen

Faculty of Engineering Mechanics and Automation-University of Engineering and Technology, VNU,
144 Xuan Thuy, Cau Giay, Hanoi, Vietnam

Received 15 January 2013
Revised 25 February 2013, accepted 20 March 2013

Abstract: Remote control via RF or IR is popular for many applications, including vehicle alarms and automatic garage doors. Conventional remote control systems are based on unidirectional transmission and have limited security. More sophisticated devices based on bi-directional transmission are also available but, because of their high cost and certain practical disadvantages, they are not widely used in commercial remote control devices. The popular unidirectional transmission systems currently have two very important security shortcomings: the codes they transmit are usually fixed and the number of possible code combinations is relatively small.Either of these shortcomings can lead to unauthorizedaccess. 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.

In this paper, an application of code hopping technology will be introduced, in 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.

Keywords: KeeLoq block cipher, cryptanalysis, slide attacks, guess-and-determine attacks

1. Introduction

The fact is that electric door system which uses a simple remote controller is easy to face to a hazard from code-grabbing. Suppose that, your existing garage door remote control transmits the same digital code every time you press the button. Thieves now use a code-grabber, a device that literally records, from hundreds of feet away, the code sent by your garage door transmitter. When you have left, they just use the code-grabber to retransmit the code and activate your garage door open. So, a high security remote control system is very necessary. The system must use reliable encryption algorithm (KEELOQ algorithm)[1].

It is apparent that secure remote control systems can only be implemented if two conditions are met. The KEELOQ code hopping system meets both these conditions.

[*] Corresponding author. Tel.: 84- 4-37549667
E-mail: thangpm@vnu.edu.vn

• A large number of possible combinations must be available. A 66-bit transmission code is used to make scanning impossible. The 32-bit encrypted portion provides for more than 4 billion code combinations. A complete scan would take 17 years! If the 34-bit fixed portion is taken into account, the time required for a complete scan jumps to 5,600 billion years!

• The system may never respond twice to the same transmitted code. The random code algorithm will never respond to the same code twice over several lifetimes of a typical system. Every time a remote control button is pushed, the system will transmit a different code. These codes appear random to an outsider – there is no apparent relationship between any code and the previous or next code [2].

Once the system has responded to a valid code, about 65,000 valid codes will have to be received before the same code will be used again. If the remote control is used eight times daily, 22 years will pass before the system responds to the same code again - once! Therefore, a retransmitted code (like when a code grabber is used) will never activate the system.

2. Materials and methods

2.1. Materials

KEELOQ is a proprietary block cipher based on a block length of 32 bits and a key length of 64 bits. The algorithm is characterized by a very economical hardware implementation, while retaining a level of security comparable to Data Encryption Standards (DES). This level of security makes it eminently suitable for code communication applications such as code hopping antitheft or access control devices [3].

Information regarding transmitter identity and synchronization is encoded so as to render it unintelligible to an outsider. For decoding, it is necessary to have the same 64-bit key originally used for encoding. Therefore, even though the decoder (which has the key) can identify the transmitter unambiguously, an outsider (who does not have access to the key and/or the algorithm) can glean no information at all from the transmissions. As it is impossible to insert information into the system from outside, strategies used to attack FEAL and other DES-like ciphers are not usable against this system.

The KEELOQ algorithm is designed to make it impossible for a potential assailant to predict the next code that will be transmitted by a valid transmitter. Even if the assailant makes a reasonable guess regarding the way in which transmitted information changes with each transmission, the algorithm obscures this information sufficiently that the next code can not be anticipated. In particular, even if the transmitted information (before encoding) differs only in one bit from the information in the previous transmission, the next transmission will be totally different. Checks exist that can be used to verify the security characteristics of an encoding algorithm and, in this instance, to determine whether the next transmitted code is predictable to any degree. The Avalanche Effect and a subset thereof, the Strict Avalanche Criterion, have been tested on the KEELOQ algorithm. The results give a good indication of the security offered by the system.

• Avalanche Effect (AE)

A block cipher satisfies the AE if changing one bit of the information causes, on average, half of the bits in the transmission to change. In the KEELOQ algorithm, this implies that changing one bit in the function and/or synchronization information will cause an average of 16 of the 32 bits in the transmitted code to change.

• Strict Avalanche Criterion (SAC)

The SAC requires that, if one bit of the encoded information is changed, each bit in the output must have a chance of 0.5 of changing as well.

Consequently, the probability of guessing any one bit correctly is 0.5, and the probability of guessing an entire 32-bit string correctly is one in about 4,300,000,000!

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 (XORed) to the 32 least significant bits of the key prior to encryption and after decryption [4].

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 or F(a,b,c,d,e) = d ⊕ e ⊕ ac ⊕ ae ⊕ bc ⊕ be ⊕ cd ⊕ de ⊕ ade ⊕ ace ⊕ abd ⊕ abc. It uses bits 1, 9, 20, 26 and 31 of the NLFSR state as its inputs during encryption and bits 0, 8, 19, 25 and 30 during decryption. Its output is linearly combined (XORed) with two of the bits of the NLFSR state (bits 0 and 16 on encryption and bits 31 and 15 on decryption) and with a key bit (bit 0 of the key state on encryption and bit 15 of the key state on decryption) and is fed back into the NLFSR state on every round [5].

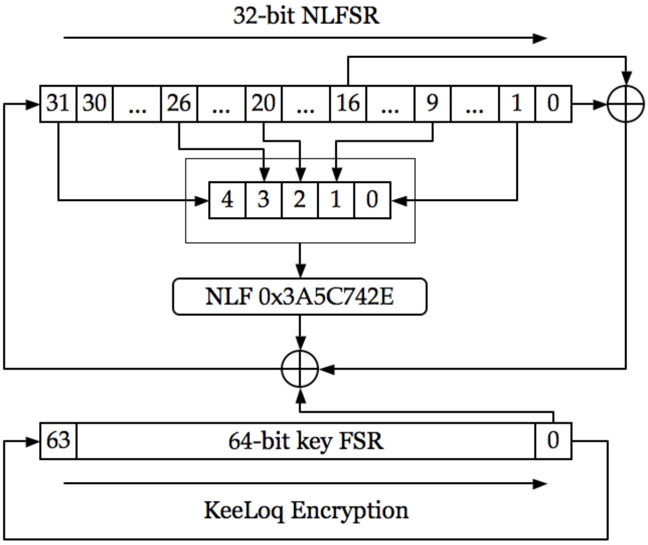

Figure 1. Keeloq Encrytion.

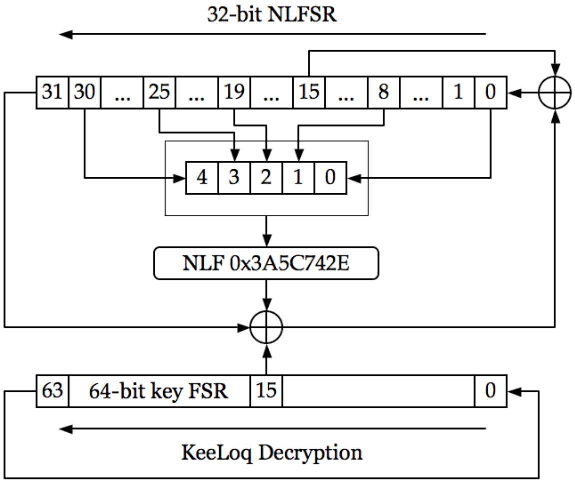

Figure 2. Keeloq Decrytion.

2.2. Methods

The transmitter 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 crypt key generation typically inputs the transmitter serial number and 64-bit manufacturer's code into the key generation algorithm (Figure 3). The manufacturer's code is chosen by the system manufacturer and must be carefully controlled as it is a pivotal part of the overall system security [6].

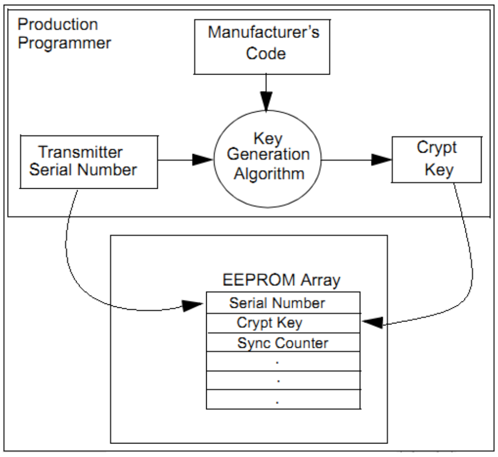

Figure 3. Creation and storage of crypt key during production.

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 4 shows how the key values in 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 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 serial number to form the code word transmitted to the receiver.

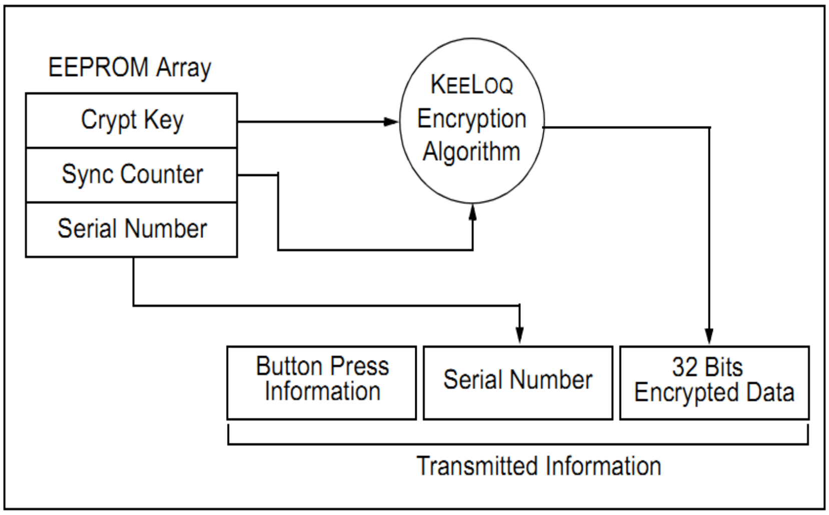

Figure 4. Building the transmitted code word (encoder).

A transmitter must first be 'learned' by the receiver before its use is allowed in the system. Learning includes calculating the transmitter's appropriate crypt key, decrypting the received hopping code and storing the serial number, synchronization counter value and crypt key in EEPROM. In 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 a learned transmitter, the message is decrypted and the synchronization counter is verified. Finally, the button status is checked to see what operation is requested. Figure 5 shows the relationship between some of the values stored by the receiver and the values received from the transmitter.

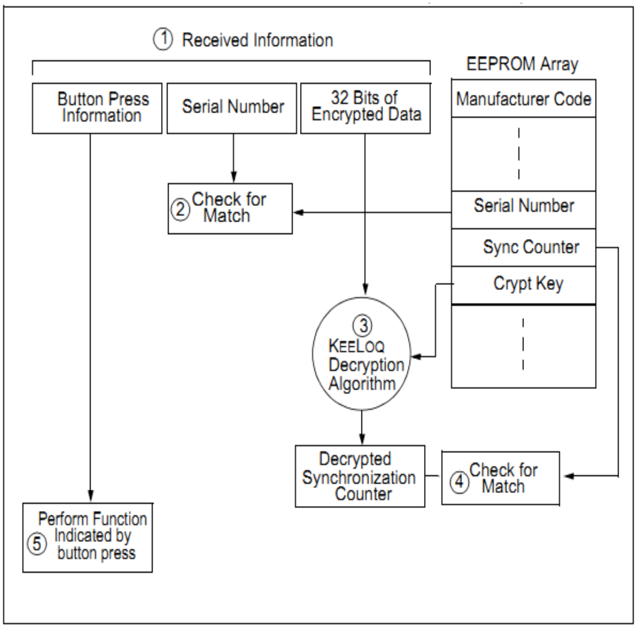

Figure 5. Basic operation of receiver (Decoder).
(Note: Circled numbers indicate the order of execution)

3. Results and discussion

Applying the above method on a RF transmitting hardware:

- A main board with a microcontroller PIC 16F with a RF receiver

- A transmitting board

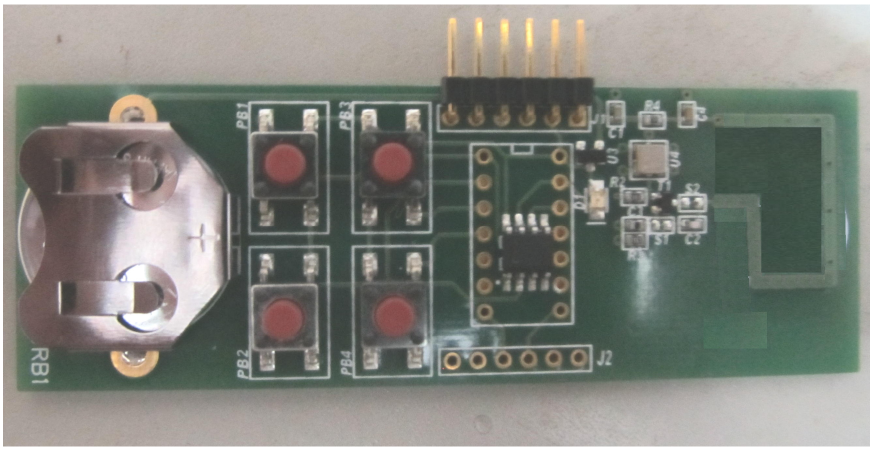

Figure 6. Transmitting board.

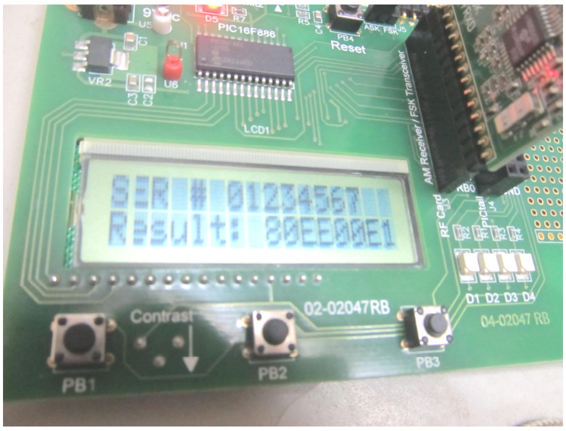

Figure 7. Main board [7].

After learning procedure, the main board receives the exact command from transmitting board. In this system, we can use four buttons on transmitting board. With a sending data, main board can recognize the pressed button, and then make a control to outside device.

4. Conclusion

The RF controller brings us a good performing with a high security and a reliable transmission, beside the price of this system is quite low. As a result, the system can be used globally at unidirectional remote keyless entry systems and access control systems. In addition, we can combine Keeloq with some advantaged algorithm such as: AES, XTEA to get a higher security system.

Acknowledgement

This work is supported by the research project No. KC03.DA12/11-15 granted by Ministry of Science and Technology of Vietnam.

References

[1] http://en.wikipedia.org/wiki/KeeLoq

[2] N.Courtois and G.V.Bard, Algebraic and Slide attacks on Keeloq.

[3] Andrey Bogdanov, Cryptanalysis of the KeeLoq block cipher

[4] Microchip Technology, An introduction to keeloq Code hopping

[5] Nicolas T. Courtois, Self-similarity Attacks on Block Ciphers and Application to Keeloq, February 2007

[6] Eisenbarth,T.Kasper,T.Moradi,A.Paar, C.Salmasizadeh, M. Manzuri Shalmani, M.T, On the power of power analysis in the real world: A complete break of the Keeloa code hopping scheme, In: Wagner, D(ed) Crypto 2008, LNCS, vol.5157, pp.343-350, Springer, Heidelber(2010)

[7] Microchip Technology, Keeloq programming system