The Analysis and Improvement of KEELOQ Algorithm

Dan Li*, Wenjun Xiao, Ziyi You, Yi Wang
Dept. of Physics & Electronic Science, Guizhou Normal University, Guiyang, China.

Corresponding author. Tel.:18583510456; email: 125433047@qq.com
Manuscript submitted July 17, 2017; accepted August 28, 2017.
doi: 10.17706/ijcee.2017.9.2.439-444

Abstract: Block cipher is used widely, as byte-orientation differential, cryptanalysis and linear cryptanalysis of block cipher, which is the security fatal blow. The KEELOQ algorithm is a block cipher algorithm designed by South Africa Willem Smit in the 1980s,in this thesis, based on the summary of the previous attack researches and the detailed rationale of KEELOQ algorithm, taking example by 3DES algorithm, the triple KEELOQ algorithm was proposed, and did the improvement on the key management, this further increased the capture and the difficulty of the crack, improved the safety performance, finally, made an experiments on the paper decode to keeloq, the experimental results show that the algorithm is more safe and more reliable.

Key words: Triple KEELOQ algorithm, difference analysis, paper decode.

1. Introduction

The KEELOQ algorithm [1] is a block cipher algorithm designed by South Africa Willem Smit in the 1980s, it includes 32-bit block cipher and 64 - bit key length, a block cipher is the nonlinear function of the five variables, it is now widely used in automobiles wireless door lock device. Although the KEELOQ algorithm has been proposed in early, but it was not until 2007 that Bogdanov [2] to use the speculation -decided and sliding technology to attacks the KEELOQ algorithm for the first time, the time complexity of 252,the space complexity of 16 GB. In 2008,Courtois[3] put forward four kinds of slide-algebraic attack methods, Its main idea is to use the difference of structure of the KeeLoq algorithm for 64 consecutive loops function structure and random permutation replacement and circle structure, First, attack the first 16 bits key, and then attack the rest of the 48 bits. Reduced computational complexity is about O(2^43) times at least encryption. In 2010,YouJianXiong [4] *et al* put forward three different byte-oriented differential fault attack methods, Among them the best way to attack efficiency, return 1 bit key information needs to be an average 0.707617 error, 8 byte keys just 46 error. In 2012, Nicolas T [5] *et al* put forward the self similar attacks on block cipher and applied to the KEELOQ algorithm, they point out that only need to select two clear, can decode the KEELOQ algorithm directly. From the above knowable, KEELOQ algorithm has made a lot of effective attack so fa, although reduces the computing time complexity largely, but at the same time increase the computing space complexity, and need a certain number of known premise, makes difficult in the process of actual crack, the safety enough to ensure, has been widely used in the practical application.

2. KEELOQ Algorithm Description

KEELOQ block cipher is an unbalanced Feistel structure [6], 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 [7], [8]. 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.

2.1. 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:

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

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

Type of NLF for nonlinear function

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

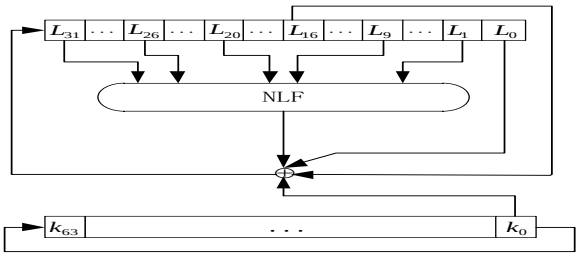


Fig. 1. KEELOQ encryption algorithm process.

2.2. KEELOQ Decryption Process

The method of decryption process and encryption process almost the same, KEELOQ decryption algorithm process is shown in the Fig. 2 below.

Mathematical expression of the decryption algorithm is as follows:

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

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

Type of NLF for nonlinear function

$$NLF(a,b,c,d,e) = abc \oplus abd \oplus ace \oplus ade \oplus de \oplus cd \oplus be \oplus bc \oplus ae \oplus ac \oplus e \oplus d \quad (2)$$

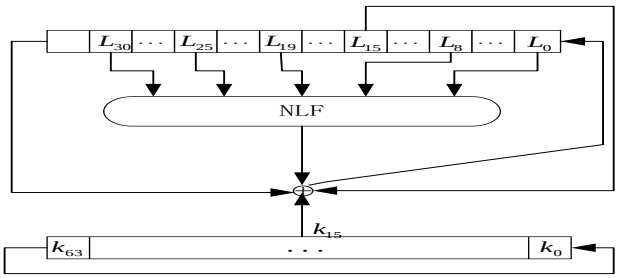


Fig. 2. KEELOQ decryption algorithm process.

3. Difference Analysis of the KEELOQ Algorithm

3.1. Differential Properties of the Nonlinear Boolean Function (NLF)

Depending on the relationship between the NLF output difference and the input difference, set $z = NLF(l_{31}, l_{26}, l_{20}, l_9, l_1)$,if the value of $\Delta z, l_{31}, l_{26}, l_{20}, l_9$ and $\Delta l_{31}, \Delta l_{26}, \Delta l_{20}, \Delta l_9, \Delta l_1$ are know, and the l_1 unkonw, according to the relationship between the input and output difference the l_1 can be find out the solution in the following.

(1)When the difference in input(0, 0, 0, 0, 0) ,(0, 0, 0, 0, 1) ,(0, 1, 1, 1, 0) or (0, 1, 1, 1, 1), the output difference Δz is 0 and $l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{31} \oplus l_{26} \oplus l_9 \oplus 1$,at this time l_1 do not ask.

(2) When the difference in input (0, 0, 0, 1, 0), (0, 0, 0, 1, 1), (0, 1, 1, 0, 0) or (0, 1, 1, 0, 1), the output difference Δz is $l_{31}l_{26} \oplus l_{31}l_1 \oplus l_{20} \oplus l_1 \oplus 1$ and $l_{31}l_{26} \oplus l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{31}l_1 \oplus l_{26} \oplus l_{20} \oplus l_9 \oplus l_1 \oplus 1$,if $l_{31} = 0$,the l_1 can only work out.

(3) When the difference in input (0, 0, 1, 0, 0)， (0, 0, 1, 0, 1), (0, 1, 0, 1, 0) or (0, 1, 0, 1, 1), the output difference Δz is $l_{31}l_{26} \oplus l_{31}l_1 \oplus l_{31} \oplus l_{26} \oplus l_9$ and $l_{31}l_{26} \oplus l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{31}l_1 \oplus l_{31} \oplus 1$, if $l_{31} = 1$,the l_1 can only work out.

(4) When the difference in input (0, 0, 1, 1, 0), (0, 0, 1, 1, 1), (0, 1, 0, 0, 0) or (0, 1, 0, 0, 1), the output difference Δz is $l_{31} \oplus l_{26} \oplus l_{20} \oplus l_9 \oplus l_1$ and $l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{20} \oplus l_1$, the l_1 can only work out.

(5) When the difference in input (1, 0, 0, 0, 0), (1, 0, 0, 0, 1), (1, 1, 1, 1, 0) or (1, 1, 1, 1, 1), the output difference Δz is $l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{20}l_1 \oplus l_{20} \oplus l_9l_1 \oplus l_1$ and $l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{31} \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{26} \oplus l_{20}l_1 \oplus l_9l_1 \oplus l_1$, if $l_{20} \oplus l_9 = 0$, the l_1 can only work out.

(6) When the difference in input (1, 0, 0, 1, 0), (1, 0, 0, 1, 1), (1, 1, 1, 0, 0) or (1, 1, 1, 0, 1), the output difference Δz is $l_{31}l_{26} \oplus l_{31}l_1 \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{26} \oplus l_{20}l_1 \oplus l_9l_1 \oplus l_1 \oplus 1$ and $l_{31}l_{26} \oplus l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{31}l_1 \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{20}l_1 \oplus l_{20} \oplus l_9l_1 \oplus l_1 \oplus 1$, if $l_{31} \oplus l_{20} \oplus l_9 = 0$, the l_1 can only work out.

(7) When the difference in input (1, 0, 1, 0, 0), (1, 0, 1, 0, 1), (1, 1, 0, 1, 0) or (1, 1, 0, 1, 1), the output difference Δz is $l_{31}l_{26} \oplus l_{31}l_1 \oplus l_{31} \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{20}l_1 \oplus l_{20} \oplus l_9l_1 \oplus l_9 \oplus 1$ and $l_{31}l_{26} \oplus l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{31}l_1 \oplus l_{31} \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{26} \oplus l_{20}l_1 \oplus l_9l_1 \oplus l_9$, if $l_{31} \oplus l_{20} \oplus l_9 = 1$, the l_1 can only work out.

(8) When the difference in input (1, 0, 1, 1, 0), (1, 0, 1, 1, 1), (1, 1, 0, 0, 0) or (1, 1, 0, 0, 1), the output difference Δz is $l_{31} \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{26} \oplus l_{20}l_1 \oplus l_9l_1 \oplus l_9 \oplus 1$ and $l_{31}l_{20} \oplus l_{31}l_9 \oplus l_{26}l_{20} \oplus l_{26}l_9 \oplus l_{20}l_1 \oplus l_{20} \oplus l_9l_1 \oplus l_9$, if $l_{20} \oplus l_9 = 1$, the l_1 can only work out.

4. Make an Improvement in KEELOQ Algorithm

KEELOQ algorithm under the NLF algorithm, the output more than half of the change can be caused by a small change of input, this will increase the difficulty of the crack and the KEELOQ algorithm has the characteristics of high security [9]. KEELOQ algorithm has obtained many effective attack so far, therefore, in order to further improve the security of the Keeloq algorithm, in this paper, from two aspects to improve the KEELOQ algorithm, first, improve the encryption process; second, improve the key management.

4.1. Encryption Process Improvement

The encryption process improvement reference the Triple data encryption process improvement [10],put forward the triple keeloq encryption algorithm. The 3DES encryption process is $C = E_{K3}(D_{K2}(E_{K1}(P)))$, The decryption process is $P = D_{K1}(E_{K2}(D_{K3}(D)))$, Among them, $E_K()$ and $D_K()$ on behalf of the DES algorithm encryption and decryption process, P represent plaintext, C represent the ciphertext, K represent the key[11].In the same way the triple KEELOQ encryption process using three different keys K_1, K_2, K_3, as shown in figure one encrypt the plaintext, the encryption process for the first time get cipher, and the second to get the cipher respectively, and then get the final 32 bits ciphertext. Decryption process is the decryption process as shown in Fig. 2 with the third key to decrypt the ciphertext eventually get the second ciphertext, use the second key to decrypt the cipher for the second time to get the first cipher text, in the end, the first key to decrypt the cipher text for the first time to get plaintext .This process is by increasing the KEELOQ key lengths to further improve the safety, is showing in Fig. 3 below.

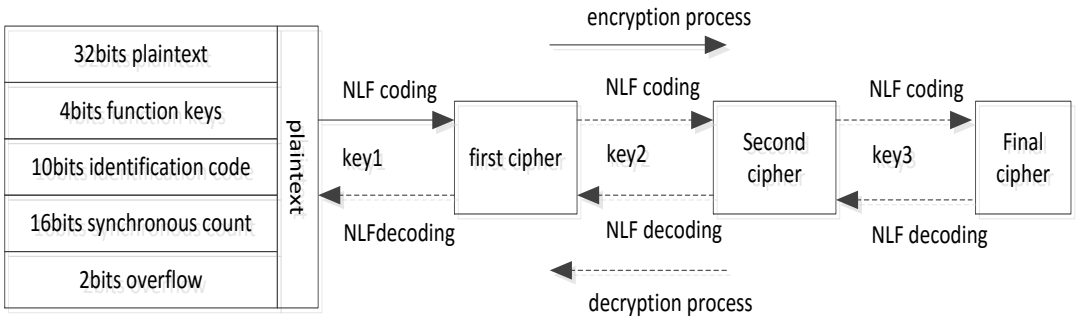


Fig. 3. Triple Keeloq encryption diagram.

4.2. Key Management Improvement

Microchip company put forward three learning modes, namely simple learning, normal learning and security learning model, Using this learning mode to manage the keys. The hightest safety of three kinds of learning is the safe learning. The security of simple learning mode depend on the key is not lost, once the key leak entirely, results cannot be redeemed; the security of normal learning mode depend on the key and the serial number is not at the same time lost; The security of safety learning mode depend on the key, seed code and serial number is not lost at the same time. The improving method of the key management is to make a random generator, this seed code can be randomly generated, once seed code is random, we don't

have to worry about it will leak or in which link leak, because everyone don't know how it is, it is further increased the safety of the KEELOQ.

4.3. Paper Decoding Experiment

KEELOQ algorithm has three learning mode: simple learning model, normal model and safe learning mode. The password of simple mode easy to steal, normal mode can ensure the system security, safe mode more secure than the norm model, but at the time of decoding more trouble than normal and easy to go wrong, so normal learning model is widely used, this thesis study triple KEELOQ encryption in the normal mode. We set Manufacturer's Code as 0123456789ABCDEF, Serial Number as 00001234, Encoder Data as 000012342166B791,in normal operation model, we get the result is shown in the Fig. 4 and Fig. 5 below.

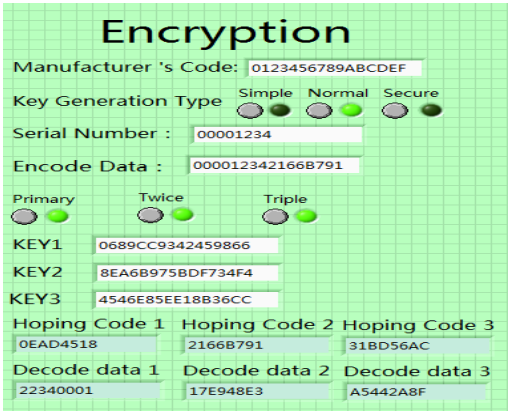


Fig. 4. Triple Keeloq encryption.

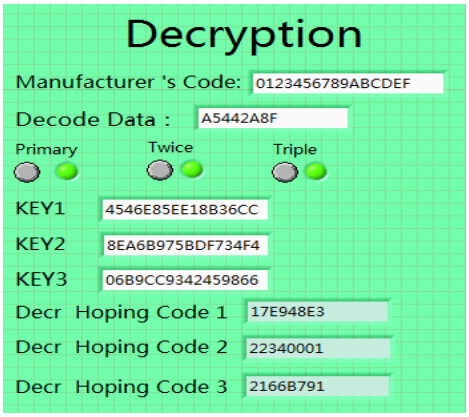


Fig. 5. Triple Keeloq decryption.

5. Conclusion

In this thesis, taking example by 3DES algorithm, the triple KEELOQ algorithm was proposed, in order to improve the reliability and security of the keeloq algorithm. And introduces the KEELOQ algorithm principle and process in detail, made a difference analysis, the nature of the two rounds of difference are analyzed in detail, by increasing the length of the secret key to improvement the keeloq algorithm, at the same time has also made improvements to key management, finally, made an experiments on the paper decode to KEELOQ, analyze the result, the KEELOQ algorithm after the improvement, the security and reliability are further increased greatly, therefore, indicates the triple KEELOQ algorithm has good popularization value and potential market application prospect.

Acknowledgement

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)，by Science& Technology Foundation of Guizhou Province(Grant No. J word [2013] 2228).

Reference

[1] Microchip. (2010). AN642: Code hopping decoder using a PIC16C56 [EB/OL]. Retrieved April 10, 2010, from http://www.keeloq.boom.ru/decryption.pdf

[2] Bogdanov, A. (2007). Linear slide attacks on the Keeloq block cipher. *Proceedings of the 3rd SKLOIS Conference on Information Security and Cryptology: LNCS 4586* (pp. 1-10). Heidelberg: Springer-Verlag.

[3] Courtois, N. T., Bard, G. V., & Wagner, D. (2008). Algebraic and slide attacks on Keeloq. *Proceedings of*

Fast Software Encryption 2008: LNCS 5086 (pp. 97-115). Heidelberg: Springer-Verlag.

[4] Jianxiong, Y., Ruilin, L., & Chao, L. (2010). Lightweight block cipher Keeloq fault attack. *Journal of Peking University: Natural Science, 46(5),* 756-762.

[5] Nicolas, T. C. (2012). Self-similarity attacks on block ciphers and application to Keeloq. *Springer Berlin Heidelberg (6805), 5*5-66.

[6] Qiuyan, W., & Chenhui, J. (2009). Improvement of first kinds of sliding and algebraic attacks on KeeLoq. *Computer Engineering, 35(16),* 133-137.

[7] Microchip Technology Inc. (2011). HCS301 KEELOQ code hopping encoder (DS21143C) [EB/OL]. Retrieved August 6, 2013, from http://www.microchip.com

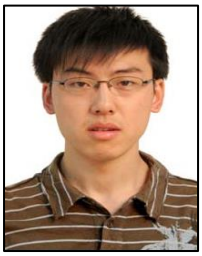
[8] Microchip Technology Inc. (2007). Use KEELOQ to generate code hopping password (DS00665A-CN) [EBOL]. Retrieved August 6, 2013, from http://www.mirochip.com

[9] Feng, Z. (2011). Research on the security of KEELOQ encryption algorithm. *Network Security, (8),* 29-31.

[10] Weijiang, Z. (2014). Research on network information encryption based on 3DES-ECC algorithm. *Bulletin of Science and Technology, 30(4),* 229-231.

[11] Zhang J., Ren, H. G., & Chen, Y. (2014). *Principles and Applications of Cryptography.* Beijing: Tsinghua University Press.

Dan Li is with the Dept. of Physics & Electronic Science, Guizhou Normal Uinversity, Guiyang, 550025, China. He was born in November 6, 1991, and she is a master graduate student. Her research direction is the research and design of computer network control system. She used to give college students a class, she didn't work at present, the current and previous research interests are same, that is the computer network control.



Wenjun Xiao is with the Dept. of Physics & Electronic Science, Guizhou Normal Uinversity, Guiyang, 550025, China. He was born in May 12, 1985, and he is a professor. His research direction is the study of embedded systems. He used to give college students a class, he is teaching at Guizhou Normal University at present, the current and previous research interests are same, that is the study of embedded systems.

Ziyi You is with the Dept. of Physics & Electronic Science, Guizhou Normal Uinversity, Guiyang, 550025, China. He was born in September 8, 1982. He is a professor. His research direction is the study of automobile network. He used to give college students a class, he is teaching at Guizhou Normal University at present, the current and previous research interests are same, that is the study of automobile network.

Yi Wang is with the Dept. of Physics & Electronic Science, Guizhou Normal Uinversity, Guiyang, 550025, China. He was born in July 25, 1957. He is a professor. His research direction is the study of automotive electronics. He used to give college students a class, he is teaching at Guizhou Normal University at present, the current and previous research interests are same, that is the study of automotive electronics.