A Key Delay Design Operation Model of Block Cipher Algorithm in Networks

Lan Luo Zhiguang Qin Shaoquan Jiang Jian Wang

Computer Communication & Network Security Group, School of Computer Science and Technology University of Electronic Science Technology of China, ChengDu 610054, P. R. China

Abstract

For the published block cipher algorithm, the key design is an important part to a cryptographic system. Block ciphers used in networks environment take more risks than ever before because of their initialization key's distribution in internet openly. But key algorithm and block cipher algorithm combined with model has been ignored for a long period. If the key delay technology is used, the speed of algorithm will be promoted and the chip's area will be decreased with very low value. This article proposed an approach in block cipher's key design against only known ciphertext attack. Furthermore, we discussed this design's provable security according to information theory.

Keywords: Block cipher algorithm, Ａ key delay module, Operation model, Provable security

1. Introduction

A block cipher algorithm is a type of cryptographic system that usually strengthens the security of internet network and wireless networks. It is one of most active direction in published cipher algorithm and symmetric key encryption.

The most important design principle of block cipher algorithm is that algorithm security depends on the cipher's key absolutely and algorithm itself should be published openly. There are two kind of round encryption structures which denominated Feistel network and SP（Substitution-Permutation） network. Horst Feistel invented the Feistel network when he designed the Lucifer cipher. The Data Encryption Standard used the Feistel structure and many other block cipher systems such as GOST, FEAL, RC5. CAMELLIA used this structure too. The SP network round includes two layers. The first layer is confusion layer that is a non-linear substitution controlled by the key and usually is implemented with S-box [1]. The second layer is diffusion layer that is implemented by the reversible linear transform independent to key. SP network has the ability to avoid linear attack and differential attack. Furthermore this kind of ability can be evaluated easily.

Some famous block cipher algorithms have taken SP network as their structure because of both strong security and highly operating speed, such as AES[2]（Advanced Encryption Standard）.

Another merit of SP network is that its cryptographic structure is simpler than Feistel network. The rest of this paper is organized as follows. Section 2 contains necessary mathematic preliminaries related to block cipher and some design principal in block cipher. A delay module in key design and our test result are given in section 3. Section 4 contains information theory conclusion about the design.

2. The block cipher module design

A block cipher can be expressed a function E:$\{0,1\}^k\times\{0,1\}^l\rightarrow\{0,1\}^l$, k stand for k - -bit key K and l stand for l -bit "plaintext" P , to return an l -bit "ciphertext" $C=E(K,P)$, here $\{0,1\}^x\in GF_2{}^x$.

2.1. Mathematic preliminaries about block cipher

When x is suitable the $\{0,1\}^x$ also can express as a number in $GF_2{}^x$. The key-length and the block length are parameters different in kinds of block ciphers. Sometimes we define a function E_k:$\{0,1\}^l\rightarrow\{0,1\}^l$, so E_k (P) $=E$ (K,P) . E_k^{-1}can be define as its inverse and the function also maps $\{0,1\}^l$ to $\{0,1\}^l$. Of course,$E_k^{-1}(E_k\ (p\ )\ )=P$ and E_k^{-1} (E_k (c) $)=C$ for all $P,C\in\{0,1\}^l$. The inverse cipher to E is a function E^{-1} $(K,C\ )=E_k^{-1}$ (C) and E^{-1} :$\{0,1\}^k\times\{0,1\}^l\rightarrow\{0,1\}^l$. In a security communication of two parties a same random key used both in encryption and decryption. The adversary may see input-output examples of E_k, meaning pairs of the form (P,C) where $C=E_k$ (P) = E (K,P) and its security relies on the secrecy of the key.

We define the H as information entropy, so

$$H = -\sum_{\forall i} E_k(P_i)\log(E_k(P_i)) \quad (1)$$

E_k is the function that can change plaintext to ciphertext with key K.

2.2. The main principal on block cipher design

The block cipher design principles depend on information theory that was put forward by Shannon in 1949. The design includes both confusion and diffusion. The plaintext characters are concealed by encryption algorithm that made the simple round cryptographic structure complicated (figure 1).

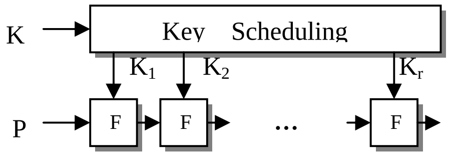

Figure 1: block cipher iterate structure

One of block cipher's merits is that keys can keep stable during a certain period meanwhile it must change every time in the other cryptographic system, such as stream cipher. This character of block cipher makes key distribution easier and avoids unnecessary information leak. A block cipher algorithm consists of key expand module and encryption algorithm module. The key expansion module changes only b bits key to r groups sub-key of users. The encryption module iterates a weak function in cryptography named f and r groups sub-key r times. Confusion and diffusion are representative block cipher algorithm design's basic principles. That the key length and blocks are changeable is an important character that the cipher algorithm is avoided both plaintext linear attack and differential attack. Because block cipher algorithm can be used in networks environments, it has been paid attention to performance speed as well as security. But for the economic factors of hardware, key expand generation usually depend on some functions related encryption itself. The performance model can offset shortages of block cipher algorithm and improve encrypting performance in both speed and security.

There are two basic directions in block cipher algorithm design. The first one is design based on security. The factors relate to securities include length of block and key length etc. The essence principals also are confusion and diffusion. The confusion principle requests enough complicity relationship among key, plaintext and ciphertext. So this relationship cannot be used in cryptanalysis. The diffusion principle is that every key bit should effect the ciphertext as much as possible to avoid slide attack the same as to make ciphertext's frequency becoming random. The second is that design should face to implementation. Block cipher algorithm can operate with both software and hardware.

3. The delay module in block cipher's key design

Block cipher algorithm belongs to symmetric cryptosystem. Symmetric cryptosystem is the encryption in which sender and receiver share the same key for both encryption and decryption. Key length is related to the security of a block cipher directly. With the block cipher algorithm used in internet network and wireless networks more popular, key length select issue and key generation become more concerned. Because internet TCP/IP protocol data block length is 128 bits, the new generation block cipher's group and key length at least need 128 bits. The block cipher's speed is a very crucial issue about key length and generation.

3.1. Block cipher algorithm key design

The key module design is one of two parts in block cipher in Feistel network or SP network. The key expand generator is based on the function has been used in encryption module. For example, AES's key module has used the S-box and affine function that is the same as the encryption module.

During encryption and decryption procedure generate key stream from a published initialization vector securely is the purpose of key scheduling. For example, *r*-rounds AES algorithm requires total $4\times(r+1)$ round keys of 32bits. These keys are generated from a user key of 128+32*k* (*k*=0,1, ⋯, 6) bits.

The round keys that are derived from the cipher key by means of the key schedule include two components that are the key expansion component and the round key selection component respectively. According to the AES encryption system, the total number of round key bits is equal to the block length multiplied by the number of rounds plus 1. The initialize key is expanded into an expanded key from which round keys are taken. AES's key design principle is the main trend of block cipher design. That the security degree of a block cipher algorithm is controlled by both the length of the initiative key schedule and key lengths is often powers of two or small multiples thereof.

Because the key expand generator cannot make the key stream at random at first, there is a result react the weakness in statistical values at first round. If key delay were used, the regular of the initialization vector would be concealed in some extent.

3.2. The delay design in key module

Because block cipher algorithm's security is depending on the key module, the key module must be researched as well as the performance model of key and encryption. As far, the key design principle has been focused on key algorithm itself. The key algorithm design usually use affine function and s-box, but has not used delay technology in published block cipher algorithm design ever before.

For more security in using the block cipher algorithm in networks environment, the protocol also is an important offset to algorithm [3]. This article put forward a method take delay scheme in key design and proof it security. Furthermore, the article presents the design to delay key module to combine with encryption module (figure 2). This design can conceal the relation information between key algorithm stream and initialization vector.

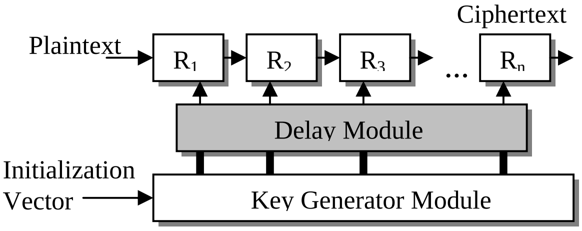

Figure 2: A key delay cryptosystem design.

When hardware is implement, the delay module and key expand generator module can be combined into one module. In this way, the space of hardware is decreased. The delay module is included in cryptographic system.

Key expand generator is a function about initialization vector. *R* bits initialization vectors can be represented as:

$$IV = (IV_0, IV_1, \ldots IV_{r-1})$$

Hence, if H stands for the relationship between *i* group key and every bit of initialization vectors and according to shannon's information theory, H can be leak the information value as:

$$H = -\sum_{\forall i} E^n(P_i)\log(E^n(P_i)) \quad （2）$$

3.3. A proof of security about the design

3.3.1 An analysis based on information theory to key delay module

As the expressions （1）, the information lead of initial key is decreased with the key generation. According to the block cipher algorithm by the value D which react the relationship between the information leak and bit key delay when the initialization operation can express as:

$$D = （\sum_{\forall i} E\ (P_i)\log(E\ (P_i))）/$$
$$（\sum_{\forall i} E^n(P_i)\log(E^n(P_i))）= O(2^{-nN}) \quad (3)$$

There is another standard to indicate a cryptographic system's security level that usually is expressed by computing times 2^{μ}. A certain security level offers an amount of protection in a promised environment. There are two factors change the security level. One of the factors is that changes in the computational environment that against the lowest attack. Another factor is that the algorithm security level itself is changed.

The key delay design is according to the achievement of algorithm itself. When the initialization vector has been known, the key stream is easy generated. On the contrary, if only key stream has been known, to calculate the initialization vector is very difficult. Key algorithm itself is a part of whole cryptographic system so that a cryptographic system being completely attacked must include its key algorithm being recovery too. The block cipher design is based on the worst condition situation, so designers often ignore the best condition situation. If key delay technology has been used, only known plaintext attack will not have expected development because of the information leak decreased. According to the expressions (2), if delay 8 bits the information leak will be decreased 2^{8N}. So the delay technology used in block cipher algorithm and key algorithm juncture part improved the security level of algorithm effectively.

3.3.2. A operating provable security proof and related test result

Though the bit key delay design has reduced the algorithm's implement speed, ability of the algorithm against either linear attack or non-linear attack is achieved [4]. The key recover is the purpose of a block cipher algorithm analysis. The standard key schedule is at least 128 bits for SP network block cipher algorithm. There are kinds of methods to complement bit delay module in hardware such as Application Specific Integrated Circuit (ASIC) and Field Programmable Gate Arrays (FPGA). When complement in software with C language, C++ language and Java usually be used. In a large mount of volume data environment the hardware encryption is necessary because of the high-speed requirement. The merit of software encryption is that algorithm is very flexible and key management is easier. When encryption system operated in hardware, the effect of bit key delay can be compared among several types platform based on known algorithm AES.

The key length is related to the algorithm's security level. The longer the key length is, the more safety the block cipher algorithm will be. But the key length also is effected the speed of algorithm complement. Especially, the space of encrypt hardware is changed by the key length directly. The expressions （2） and the result of table1 shows that key module can effect algorithm request about its speed and security. If there is not key delay, the algorithm speed is about 200Mbytes/sec. The result shows that security level really is conflict with the algorithm performance speed.

	128 bit key	192 bit key	256 bit key
8bit	198.8M/Sec	198.6M/Sec	197M/Sec
16bit	197.7M/Sec	197.5M/Sec	195M/Sec
32bit	196.6M/Sec	196.2M/Sec	194M/Sec

Table1: Algorithm operation speed changed according to bitwise length

If the algorithm is used in Local Area Network (LAN), security level of algorithm is protected by isolated physical environment. So the speed issue sometimes is more important. In which situation the key delay technology should be adopted is a complexity question. There are kinds of protocols established by International Standard Organization (ISO). In this article the related protocol will not be discussed furthermore though it is a part of whole cryptographic system.

4. Conclusions

The block cipher algorithm is used popularity in networks environment. Due to off-line key distribution changing to on-line distribution, Initialization vector may be easily eavesdropping by attackers. According to international regulation, block cipher algorithm should be published through algorithm collection. The key expand module is the most important part in whole system. To enforce security effect of algorithm should be decreased in some situations. There is one economic method to promote the security through key bit delay design. The key bit delay also can decrease the weakness key attack more effectively. Furthermore, key delay design can reduce the rounds of iterates so that the speed performance is enhanced. This article did not discuss the relationship between iterate rounds and algorithm's complication effect particularly. The key delay design gives an approach to get more security encryption system through a kind of economic way based on some existing block cipher algorithms. Especially, key delay design can decrease the initialization vector information leak in only known ciphertext attack in some condition.

Acknowledgement

This work is partially supported by National Nature Science Foundation of China (Grant No. 60673075).

References

[1] K. Nyberg. Differentially uniform mappings for cryptography, Advances in Cryptology Proceedings Eurocrypt'93, *LNCS* 765, T.Helleseth.Ed, pp. 55-64, 1994.

[2] Joan Daemen, Vincent Rijmen *AES proposal*: *Rijndeal*, http://www.nist.gov/aes, 2004.

[3] B.Clifford Neuman and Theodore Ts'o. Kerberos : An Authentication Service for Computer Networks, *IEEE Communications*, 32(9):33-38, 1994.

[4] MATSUI.M, E *On correlation between the order of S-boxes and the strength of DES Advances in Cryptology:UROCRYPT'94, LNCS 950:* 366-375, 1995.