韓國 컴퓨터情報學會 論文誌
第13卷 第4號, 2008. 7.

2008-13-4-3-8

대칭적인 블록 암호화 알고리즘을 기반으로 한 효율적인 다이내믹 네트워크 보안 방법

송 병 호*, 양 성 기*, 배 상 현**

An Efficient Dynamic Network Security Method based on Symmetric Block Cipher Algorithms

Byoung-Ho Song*, Sung-Ki Yang*, Sang-Hyun Bae**

요 약

현재의 블록 암호화 알고리즘은 암호화키 값을 변환하지 않고 설계되며, 각각의 블록의 라운드 함수들을 적용하며 암호화 한다. 그러므로, 반복적인 라운드 구조의 블록암호화 기법을 위한 가장 강력한 방법들인 차분 암호 분석법 또는 선형 암호 분석법에 의해 평문이나 암호화키는 쉽게 노출 된다는 취약점을 가지고 있다. 다이내믹 암호는 키의 크기, 라운드의 수, 그리고 평문의 길이가 동시에 측정될 수 있는 특성을 가지고 있다. 다이내믹 네트워크는 대칭적 블록 암호들에 대한 네트워크들 속에서 이러한 특성들을 만족시키는 독특한 네트워크이다. 우리는 중간 결과에 의한 공격, 선형 암호 분석법, 그리고 차분 암호 분석법에 대한 다이내믹 네트워크의 강력함을 분석한다. 또한, 본 논문에서 대칭적인 블록 암호를 위한 다이내믹 네트워크라 불리는 새 네트워크 방식을 제안한다.

Abstract

The existing block encryption algorithms have been designed for the encryption key value to be unchanged and applied to the round functions of each block, and enciphered. Therefore, it has such a weak point that the plaintext or encryption key could be easily exposed by differential cryptanalysis or linear cryptanalysis, both are the most powerful methods for decoding block encryption of a round repeating structure. Dynamic cipher has the property that the key-size, the number of round, and the plaintext-size are scalable simultaneously. Dynamic network is the unique network satisfying these characteristics among the networks for symmetric block ciphers. We analyze the strength of Dynamic network for meet-in-the-middle attack, linear cryptanalysis, and differential cryptanalysis. Also, In this paper we propose a new network called Dynamic network for symmetric block ciphers.

▸ Keyword : Dynamic network, linear cryptanalysis, differential cryptanalysis, Dynamic cipher

• 제1저자 : 송병호 교신저자 : 배상현
• 접수일 : 2008. 5. 5, 심사일 : 2008. 7. 6, 심사완료일 : 2008. 7. 25.
* 조선대학교 컴퓨터통계학과 박사 ** 조선대학교 컴퓨터통계학과 교수

www.kci.go.kr

Ⅰ. Introduction

The need for good cipher algorithm is spreading rapidly as more people use computer networks to exchange confidential documents, buy products, and access sensitive data. There are two general types of key-based algorithms: symmetric key and public key [8,11]. In symmetric key algorithm, the encryption key and the decryption key are same. Public key algorithm is designed so that the key used for encryption is different from the key used for decryption. Symmetric algorithm and public key algorithm cannot be compared on an equal footing because each has its own advantages and disadvantages. The existing block encryption algorithms have been designed for the encryption key value to be unchanged and applied to the round functions of each block, and enciphered. Therefore, it has such a weak point that the plaintext or encryption key could be easily exposed by differential cryptanalysis or linear cryptanalysis, both are the most powerful methods for decoding block encryption of a round repeating structure. There are two types of symmetric key algorithms: block cipher and stream cipher [8, 11]. Block cipher operates on blocks of plaintext and ciphertext. Stream cipher operates on streams of plaintext and ciphertext one bit or byte at a time. Feistel network is well known network for block cipher design [5,8,12]. And most block ciphers are based on Feistel network [8,10]. Feistel ciphers include DES, RC5, IDEA, and so on. Also, there have been many researches for the attack on Feistel ciphers. Differential cryptanalysis and linear cryptanalysis are well known attacks of Feistel ciphers [1,2,3,4,6,7,9]. We note that these type of cryptanaysis are possible in Feistel ciphers because Feistel ciphers involve the operation that operate on for round key and round block. In this paper we propose a new network, called Dynamic network, for symmetric block ciphers. Dynamic cipher consists of a series of round functions. In the ith round function, i-1 round block is converted to i round block by a sequence of operations that are specified in i round key and operate on only the bits of i-1 round block.

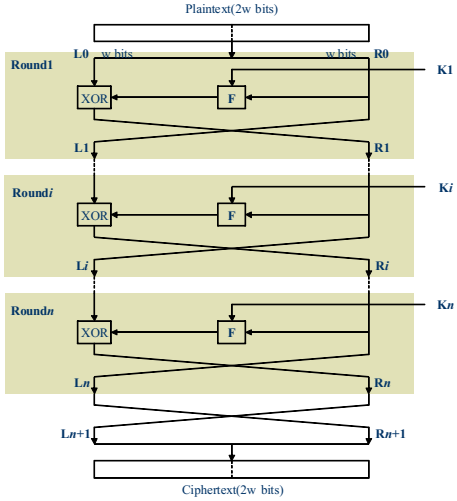

Fig 1. Feistel encryption structure
그림 1. Feistel 암호화 구조

By using the generating-method of round block, we show that the plaintext-size, the number of round, and the key-size of Dynamic cipher are scalable simultaneously. We analyze the strength of Dynamic cipher against meet-in-the-middle attack, differential cryptanalysis, and linear cryptanalysis. As the results, we present the methods for designing secure Dynamic cipher against meet-in-the- middle attack and linear cryptanalysis. Also, we show that applying of differential cryptanalysis to Dynamic cipher is hard. Our paper is organized as follows: Dynamic network is defined in section 2. Section 3 includes the characteristics of Dynamic cipher. The strength of Dynamic network against some attacks is analyzed in section 4. Section 5 includes conclusion and further researches.

Ⅱ. Related Works

2.1 DES(Data Encryption Standard)

DES (Data Encryption Standard) is symmetric

www.kci.go.kr

key encryption system publicized by NIST (National Institute of Standard Technology) in 1977. One of the advantages of DES is fast processing time due to the substitution, transposition, and XOR operators. DES is applied to "crypt" UNIX password encryption and to electronic fund transfer (EFT) system for financial institutions of USA and Europe. DES uses a 64 bit encryption key and transits normal text 64 bits to encrypted text 64 bits. The encryption key includes parity bit in every 8 bits and 56 bit encrypted data field. The operators of DES algorithm basically use transposition and contraposition, and mod 2.

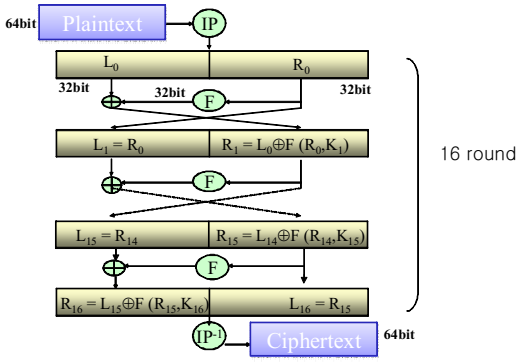

Fig 2. DES encryption algorithm
그림 2. DES 암호화 알고리즘

The transposition has parallel, expansion, and abbreviation operators. The contraposition operator is processed using S-Box system.

2.2 AES(Advandced Encryption Standard)

AES (Advanced Encryption Standard) substituted DES encryption algorithm in 1997. NIST opened the public for development of AES encryption algorithm and finally adopted Rijndael encryption algorithm. This algorithm has better efficiency and safety features than triple-DES. AES is very powerful symmetric key block encryption algorithm of SPN structure that can allow a flexible encryption key length selection from 128, 192, 256 bits according to the individual needs or specific system environment. Since AES code is simple and design is uncomplicated, AES has a fast processing time in the various platforms, has a strong merit for the various well-known viruses, and encrypts using addition, multiplication, XOR operators by GF(28).

2.3 Shannon's Theorem

Linear cryptanalysis uses linear approximate expression [4,6,7,9]. Linear approximate expression represents the linearity between an input and an output of the round function that is designed to be non-linear. And the probability, linear approximation to be hold, is calculated for finding the best expression. The best expression is used to determine key bits by using some statistical properties including Pilling-up lemma and the pairs of known plaintext and ciphertext corresponded by plaintext. Differential cryptanalysisuses the pairs of two chosen plaintexts having specified differential [1,2,3,4]. And differential cryptanalysis calculates differential of two ciphertexts corresponded by two plaintexts and of two input blocks of the last round. Many key bits of the last round key can be determined by comparing with calculated differentials. Shannon showed that symmetric block cipher, performing the repetition of a substitution and a transposition, has good strength [13]. Many networks, based on Shannon's theorem, for symmetric block ciphers have been presented [5,8,12].

A substitution-permutation network is composed of a number of stages each involving substitutions and permutations [8]. A round of a block cipher is the composition of at least one substitution and at least one transposition [8]. And a round function is a function performing the substitutions and transpositions by the ways described in symmetric block cipher. An iterated block cipher is a block cipher involving the sequential of a round function [8]. The ith repeatedround function has two inputs that are a block called i-1 round block and a key called i round key. And the output of the ith repeated round function is i round block.

www.kci.go.kr

A Feistel cipher is an iterated cipher mapping a $2t$-bit plaintext (L_0, R_0), for t-bit blocks L_0 and R_0, to a ciphertext (R_n, L_n), through an n-round process [8]. The ith round block of Feistel cipher is determined by $L_i=R_{i-1}$ and $R_i=L_{i-1} \oplus f(R_{i-1}, K_i)$ where f is an arbitrary round function, K_i is i round key, and $\oplus$ denotes bit-wise eXclusive-OR. And the ith round function of Feistel cipher involves the operation, performed between i-1 round block and i round key, for the substitutions and the settled permutation-method, without using i round key, for the transpositions.

Meet-in-the-middle attack uses an equation $E_{K_1}(P) = D_{K_2}(C)$ where the key K is the concatenation of K_1 and K_2,, E is an encryption algorithm, D is a decryption algorithm, P is a plaintext, and C is a ciphertext corresponding to P [8].

Meet-in-the-middle attack makes the key space to $2^{|K_1|}+2^{|K_2|}$ instead of $2^{|K_1|}\times 2^{|K_2|}$. But meet-in-the-middle attack is not proper attack to single encryption Feistel cipher.

III. Dynamic network

Dynamic network consists of a series of rounds. In ith round function of Dynamic network, an m-bits block is converted to another m-bits block by a sequence of operations that operate on only the bits of i-1 round block and specified in i round key.

Definition 1 A *block operation* is the operation that converts a block of plaintext to a ciphertext. A *block operation set of factor n* is the set that is composed of 2^n block operations.

Each block operation describes the method to map a m-bit block into another m-bit block. Dynamic cipher contains block operation sets that are classified by applying method of block operation or used operators. And the block operation setsinclude basically the block operation set for the substitutions and the block operation set for the transpositions.

Key scheduling algorithm of Dynamic cipher generates n-bit strings by using the key. Therefore, one n-bit string can be used to determine one block operation from a block operation set.

Definition 2 A *key block* is an n-bit string generated by the key scheduling algorithm. And a *key block set* is the set that is composed of key blocks.

Let l be the number of block operation set. Then the number of block operation, determined by any key block, is in the range from 1 to l.

Let $m$be the number of key blocks to determine by block operations from each block operation set, and let $\{kb_1, kb_2, \cdots, kb_{jm}\}$ be the key block set. Key scheduling algorithm can reproduce a new key block set $\{kb_1||\cdots||kb_{m-1}||kb_m, \cdots, kb_{(j-1)(m+1)}||\cdots||kb_{jm}\}$ by using the key block set {kb1, kb2, ⋯, kbjm}. Therefore, we assume that any key block determines by block operations from each block operation set.

Definition 3 A selected block operation set is an ordered set of block operations, determined by a key block, from each block operation set. And a selected block operationis an element of the selected block operation set. An input of the ith selected block operation is an output-block of $(i-1)$th selected block operation. And the output is a block that is obtained by applying selected block operation to an input-block. Therefore, a key block is used to generate i round block by using i-1 round block. Dynamic cipher is a symmetric block cipher that encrypts a plaintext by the following way:

Algorithm Dynamic-Cipher

Input : Key block set KB and Plaintext B_0^0.

Output : Ciphertext B_0^n.

Let KB=$\{kb_1, kb_2, \cdots, kb_n\}$.

for i=1 **to** n **do**

www.kci.go.kr

Get the selected block operation set.
Let { A_1^i, ⋯, A_m^i } be the selected block operation set.
for j=1 **to** m **do**
Get a new block B_j^{i-1} by applying A_j^i to B_{j-1}^{i-1}.
endfor
$B_0^i = B_m^{i-1}$
endfor
end Dynamic-Cipher

We can see that the strength of Dynamic cipher depends on the design method of: (1) the key scheduling algorithm; (2) the block operation sets.

IV.The Properties of dynamic network

Let O_1, O_2, ⋯, O_l be the block operation sets. The size of O_j is fixed because the block operation sets are nested in Dynamic cipher ($1 \le j \le l$). This means that a size of key block is also fixed. Let m be a size of key block and K be the key. We assume that $|K|$ is sufficiently large for the exhaustive search of the key. And $|K|$ is always greater than $m$because the design of the block operation set having 2^m elements is not practical for $|K|m$. In case of $m \le |K|$, there exist key scheduling algorithms that can use the various sizes of bitstring as the key. As an example, for a key key block kb and the key $K=k_0k_1\cdots k_{|kb|\times n-1}$, the key scheduling algorithm, producing a key block set $\{ k_{i\times|kb|}k_{i\times|kb|+1}k_{i\times|kb|+|kb|-1} \mid 0 \le i \le n-1\}$, can use every bit strings of multiple size of $|kb|$ as the key. For a key $K=k_0k_1\cdots k_{n-1}$, the key scheduling algorithm, producing a key block set $\{ k_{i \bmod n}k_{(i+1) \bmod n}\cdots k_{(i+|kb|-1) \bmod n} \mid 0 \le i \le n-1\}$, can use any size of bit string as the key. Therefore, we conclude that the key-size of Dynamic network is scalable. There is no key bit not used to generate the key block set because of its usability. Let K_1 and K_2 be two keys with different sizes used in same key scheduling algorithm, and let assume that $|K_1|<|K_2|$. Then, key scheduling algorithm produces two key block sets corresponding to each K_1 and K_2. And the size of key block set generated by using K_2 is larger than the size of key block set generated by using K_1. Therefore, the number of round of Dynamic cipher is scalable. Let O_1, O_2, ⋯, O_l be the selected block operation set, U_i be the applying unit of a selected block operation O_i ($1il$), U=LCM(U_1, U_2, ⋯, U_l). A round block with size $U=U_i \times m_i$, can be obtained by sequential applying of a selected block operation O_i m_i times. Therefore, Dynamic cipher can use all of the bit strings with size $U \times n$ as plaintexts. Example of (2) uses two block operations that substitutes by the unit of 1.

V. The Design of Dynamic cipher

Meet-in-the-middle attack reduces the key space in the double encryption Feistel ciphers [8]. Double encryption Feistel ciphers use two different keys consecutively. We note that the key space of double encryption Feistel ciphers using every key bits twice will be equal to the key space of single encryption Feistel ciphers. Our method for designing secure Dynamic cipher against meet-in-the-middle attack is the use of key bits more than twice. Examples include the key scheduling algorithm which generates a key block subset KB by using every key bits, and then generates the key block set by repetition of KB. The use of key bits more than twice affects the execution time of Dynamic cipher because the size of the key block set using every key bits more than twice is greater than the size of the key block set using every key bits exactly once. Therefore, our strategy guarantees Dynamic cipher to be secure against meet-in-the-middle attack at the expense of execution time. For designing secure Dynamic cipher against linear cryptanalysis, we have to examine the possibility of applying linear

www.kci.go.kr

cryptanalysis to Dynamic cipher. Let *KB* be a subset of key block set and K be the set of key bits used for generating *KB*. There is the possibility that the values of some bits are mapped into the specified values by *KB*. This fact means that the selected block operation set determined by *KB*is linear. In this case, there is the possibility that becomes the key space of Dynamic cipher to be smaller. Our methods for designing secure Dynamic cipher against linear cryptanalysis are as follows:

(1) Some block operations doing the substitution should be designed so that any bit of *i* round block affects to bits of *i*round block as many as possible. This property makes hard to infer key blocks by comparing with the values of some bits and their corresponding values.

(2) For any key block *kb*, the key-block space for deciding the selected block operation set determined by *kb* must be $2^{|kb|}$. This property includes property (1) and guarantees the non-linearity of selected block operation set. And this property should be satisfied for a subset of the key block set. Examples of (1) include the following block operation: Let $b_1 b_2 \ldots b_n$ be *i*-1 round block and $\oplus$ denote eXclusive-OR. A block operation performing the substitution is to map $b_1 b_2 \ldots b_n$ into $b'_1 b'_2 \ldots b'_n$ where $b'_2 = b_1 \oplus b_n$, $b'_i = b'_{i-1} \oplus b'_i$ for $3 \le i \le n$, and $b'_1 = b'_n \oplus b_1$. In this case, one bit of *i*-1 round block affects *n*/2 bits of *i* round block in average.

Examples of (2) include the following block operation set that is composed of two substitution methods. One substitution method is a method described in example of (1). Let $\otimes$ denote eXclusive-NOR. Another substitution method maps $b_1 b_2 \ldots b_n$ into $b'_1 b'_2 \ldots b'_n$ where $b'_2 = b_1 \otimes b_2, b'_i = b'_{i-1} \otimes b'_i$ for $3 \le i \le n$, and $b'_1 = b'_n \otimes b_1$. In this case, a size of key block is 1 and the key-block space for determining exactly one substitution method is 2. For designing secure Dynamic cipher against differential cryptanalysis, we have investigated the condition for applying differential cryptanalysis to symmetric block ciphers. Differential cryptanalysis uses the pairs of two chosen plaintexts having determined differential [1,2,3,4]. And differential of each pair of chosen plaintexts is mapped into specified differentials of a pair of ciphertexts and a pair of input blocks of the last round. We note that Feistel ciphers use many key bits in a round and perform the operation between round key and round block. Therefore, many key bits can be determined by comparing known differential of two ciphertexts and known differential of two input blocks of the last round. And this is not the case of Dynamic network. See example of (2). In Dynamic cipher, differential of two *i*-1 round blocks come out various differentials of two i round blocks because different key block produces different round block. This fact leads that applying of differential cryptanalysis to Dynamic cipher is hard.

VI. Conclusion and further research

We presented Dynamic network for symmetric block cipher algorithms. Dynamic network encrypts plaintext by using of block operations that operate on only the bits of round block. And the key is used only for generating key blocks that are used to determine by block operations from each block operation set. This characteristic of Dynamic network distinguishes oneself in networks for symmetric block ciphers. We showed that the key-size, the number of round, and the plaintext-size of Dynamic cipher are scalable simultaneously. Dynamic network is the unique network satisfying these characteristics among the networks for symmetric block ciphers. We analyzed the strength of Dynamic network for meet-in-the-middle attack, linear cryptanalysis, and differential cryptanalysis. And we suggested the design-methods for designing secure Dynamic cipher against meet-in-the-middle attack and linear cryptanalysis. Also, we showed that Dynamic cipher is secure for differential cryptanalysis. We have

www.kci.go.kr

many research items for Dynamic network including: (1) analysis of the strength of Dynamic cipher for unanalyzed attacks; (2) design of Dynamic cipher that maximizes the advantages of Dynamic network; (3) search the application that use the characteristics of Dynamic network.

참고문헌

〔1〕 E. Biham and A. Shamir, "Differential Cryptanalysis of DES-like cryptosystems", Advances in Cryptology - CRYPTO '90, LNCS 537, pp. 2-21, 1990.

〔2〕 E. Biham and A. Shamir, " Differential Cryptanalysis of Feal and Hash", Advances in Cryptology - EUROCRYPT '91, LNCS 547, pp. 1-16, 1991

〔3〕 E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York, 1993.

〔4〕 B. S. Kaliski and Y. L. Yin, "On differential and linear cryptanalysis of the RC5 encryption", Advances in Cryptology - CRYPTO '95, LNCS 963, pp. 171-184, 1995.

〔5〕 L. R. Knudsen, "Practically Secure Feistel Ciphers, Fast Software Encryption", Cambridge Security Workshop Proceedings, pp. 211-221, 1994.

〔6〕 M. Matsui, "Linear Cryptanalysis Method for DES Cipher", Advances in Cryptology - EUROCRYPT '93, LNCS 765, pp. 386-397, 1993.

〔7〕 M. Matsui, "The first experimental cryptanalysis of the Data Encryption Standard", Advances in Cryptology - CRYPTO '94, LNCS 839, pp. 1-11, 1994.

〔8〕 A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, Applied Cryptography, CRC Press, 1997.

〔9〕 K. Ohta, S. Moriai, and K. Aoki, "Improving the Search Algorithm for the Best Linear Expression", Advances in Cryptology - EUROCRYPT '95, LNCS 963, pp. 157-170, 1995.

〔10〕 R. L. Rivest, "The RC5 encryption algorithm", Fast Software Encryption, Second International Workshop, LNCS1008, pp. 86-96, Springer-Verlag, 1995.

〔11〕 B. Schneier, Applied cryptography, John Wiley & Sons, 1996.

〔12〕 B. Schneier and J. Kelsey, "Unbalanced Feistel Networks and Block-Cipher Design", Fast Software Encryption, Cambridge Security Workshop Proceedings, pp. 121-144, 1996.

〔13〕 C.E. Shannon, "Communication theory of secrecy systems", Bell System Technical Journal, v. 27, n. 4, pp. 379-423, 1948.

〔14〕 Data Encryption Standard. "Fedral Information Processing Standards(FIPS)" Publication 46. National Bureau of Standards, U.S. Department of Commerce, Washington D.C. January, 1977.

〔15〕 NIST, "2nd AES Conference", AES Round2 Information, 1999.

"This study was supported by research funds from Chosun University, 2005"

저 자 소 개

송 병 호

2000년 2월 조선대학교 일반대학원 전산통계학과 이학석사

2008년~2 조선대학교 일반대학원 전산통계학과 이학박사

〈관심분야〉 정보보호, 인공지능, 영상처리

양 성 기

1999년 2월 조선대학교 일반대학원 전산통계학과 이학석사

2000년 2월 조선대학교 일반대학원 전산통계학과 이학박사

〈관심분야〉 영상처리, 인공지능

배 상 현

1988년 2월 동경 도립대학교 대학원 공학박사

1988년~현재 조선대학교 컴퓨터통계학과 교수

〈관심분야〉 인공지능, 멀티미디어, 영상처리, 컴퓨터비젼

www.kci.go.kr