2000년 한국정보처리학회 추계 학술발표논문집 제7권 제2호

Dynamic Cipher의 설계 및 분석

손선경*, 박승배**, 임형석*
*전남대학교 전산통계학과
**초당대학교 컴퓨터과학과
e-mail:sgsohn@cs.chonnam.ac.kr

The Design and Analysis of Dynamic Cipher

Seon-Gyoung Sohn*, Seung-Bae Park**, Hyeong-Seok Lim*
*Dept. of Computer Science, Chonnam National University
**Dept. of Computer Science, Chodang University

요약

Dynamic Network은 블록 크기와 키 크기, 라운드 수가 동시에 가변이며, 각 라운드에서 서브 블록과 서브 키 사이에 연산이 이루어지지 않는 대칭키 블록 암호 알고리즘을 위한 기본구조이다. 본 논문에서는 Dynamic Network에 기반한 대칭키 블록 암호 알고리즘을 제안한다. 제안하는 Dynamic Cipher는 임의의 비트 스트링을 키로서 사용할 수 있다. 제안하는 Dynamic Cipher에 차분 분석법과 선형 분석법의 적용이 어려움을 보이고, 대칭키 블록 암호 알고리즘이 만족하여야 할 성질들에 대한 실험 결과들을 제시한다.

1. 서론

컴퓨터 보급의 확대와 인터넷 사용자의 증가는 정보 보호의 중요성을 증대시키고 있다. 정보 보호는 기밀성, 무결성, 인증 등과 같은 정보 보호 서비스들의 제공에 의해 이루어지며, 정보 보호 서비스를 제공하는 가장 일반적인 방법은 암호 시스템을 사용하는 것이다.

암호 시스템은 대칭키 암호 시스템과 비대칭키 암호 시스템으로 구분된다. 대칭키 암호 시스템은 암호화와 복호화에 사용되는 키가 같은 암호 시스템이고, 비대칭키 암호 시스템은 암호화와 복호화에 사용되는 키가 다른 암호 시스템이다. 대칭키 암호 시스템은 암호화 단위에 의해 스트림 암호 알고리즘과 블록 암호 알고리즘으로 구분된다. 스트림 암호 알고리즘은 비트 또는 바이트 단위로 암호화하고, 블록 암호 알고리즘은 블록 단위로 암호화한다[8].

지금까지 대칭키 블록 암호 알고리즘을 위한 많은 기본구조들이 제안되었다. Feistel Network[3, 11]은 가장 많이 사용되는 기본 구조이며, 지금까지 제안된 대부분의 대칭키 블록 암호 알고리즘은 Feistel Network에 기반하고 있다. Feistel Cipher에 대한 다양한 분석방법들이 제안되었다[1, 3, 4]. 차분분석법과 선형분석법은 가장 많이 알려진 공격 방법들로, Feistel Cipher의 각 라운드에서 서브 블록과 서브키 사이에 연산이 이루어진다는 성질을 이용하고 있다[1, 4, 5].

Feistel Cipher들의 공격 방법들을 고려한 변형된 Feistel Network들이 제안되고 있지만, Feistel Network 부류의 기본 구조들은 서브 블록과 서브키 사이에 연산이 이루어진다[3, 11].

최근에 블록 크기와 키 크기, 라운드 수가 동시에 가변이며 각 라운드에서 서브 블록과 서브 키 사이에 연산이 이루어지지 않는 대칭키 블록 암호 알고리즘을 위한 기본구조인 Dynamic Network이 제안되었다. 하지만 아직까지 Dynamic Network에 기반한 암호 알고리즘은 제안되지 않고 있다.

본 논문에서는 임의의 비트 스트링을 키로서 사용 가능한 Dynamic Cipher를 제안한다. 제안하는 Dynamic Cipher에 차분 분석법과 선형 분석법의 적용이 어려움을 보인다. 제안하는 Dynamic Cipher가 대칭키 블록 암호 알고리즘이 만족하여야 하는 성질들을 만족하는지를 모의 실험을 통하여 분석한다.

논문의 구성은 다음과 같다. 2장에서는 대칭키 블록 암호 알고리즘을 위한 네트워크들과 대칭키 블록 암호 알고리즘의 분석 방법들에 대하여 살펴본다. 3장에서는 Dynamic Network에 기반한 대칭키

본 논문은 한국과학재단의 특정기초연구 (98-0102-11-01-3) 지원에 의한 것임

블록 암호 알고리즘을 제안한다. 4장에서는 제안하는 알고리즘에 대한 강도를 분석하고, 대칭키 블록 암호 알고리즘이 만족해야하는 성질들에 대한 모의 실험 결과들를 제시한다. 5장에서는 논문의 결론을 맺는다.

2. 관련연구

대칭키 블록 암호 알고리즘이 대치와 전이를 반복하면 좋은 비도를 갖는다는 사실이 Shannon의 정리에 의해 알려져 있다[12]. Shannon의 정리에 근거하여 대칭키 블록 암호 알고리즘을 위한 많은 기본 구조들이 제안되었다.

Feistel Network은 가장 많이 사용되어진 대칭키 블록 암호 알고리즘을 위한 기본 구조로, 평문 P를 왼쪽 절반 L_0와 오른쪽 절반 R_0로 나눈 후, 다음과 같은 과정을 반복적으로 수행하여 평문을 암호화한다[3, 11].

$$P = L_0 \| R_0$$
$$L_i = R_{i-1}$$
$$R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$$

최근에 제안된 대부분의 대칭키 블록 암호 알고리즘은 Feistel Cipher이며, 대표적인 Feistel Cipher들로는 DES[1, 3], Blowfish[9], RC5[6], RC6[7], Twofish[10], Mars[2] 등이 있다.

Feistel Cipher들을 분석하는 많은 방법들이 제안되었으며, 그 중 차분 분석법[1]과 선형 분석법[4]은 가장 잘 알려진 Feistel Cipher들에 대한 분석 방법들이다. 차분 분석법은 비선형 함수에서 서브 블록과 서브키가 연산되는 성질을 이용하여 비선형 함수의 입력쌍의 차분값과 출력쌍의 차분값을 가지고 키를 유추하는 공격 방법이다[1]. 선형 분석법은 비선형 함수의 입력 비트들을 연산한 결과와 출력 비트들을 연산한 결과를 사용하여 선형 근사식을 구하고, 이 선형 근사식을 이용하여 키를 유추하는 공격 방법이다[4].

Meet-in-the-Middle 공격[8]은 키 $K = K_1 \| K_2$와 평문 P, P에 대응하는 암호문 C에 대하여, $E_{K_1}(P) = D_{K_2}(C)$가 성립하는 성질을 이용하여 키를 유추하는 분석 방법이다.

Dynamic Network[5]은 블록 크기와 키 크기, 라운드 수가 가변이고 각 라운드에서 서브 블록과 서브 키 사이에 연산이 이루어지지 않는다는 사실이 알려져 있다. Dynamic Network은 주어진 블록의 비트들끼리 연산하여 새로운 블록을 생성하는 방법인 블록 생성 방법들과 블록 생성 방법들을 원소로 하는 집합의 부분 집합인 블록 연산 집합, 블록 연산 집합의 원소인 블록 연산으로 이루어진다. Dynamic Network의 키 스케줄링 알고리즘은 키를 이용하여 키 블록 집합을 생성하고, 키 블록 집합의 원소는 블록 연산 집합으로부터 하나의 블록 연산을 선택하는데 이용된다. Dynamic Cipher의 현재 라운드 블록은 이전 라운드 블록에 키 블록을부터 선택된 블록 연산을 적용하여 생성된다.

아직까지 Dynamic Network을 기반으로 한 대칭키 블록 암호 알고리즘은 제시되지 않고 있다.

3. Dynamic Cipher

본 논문에서 제안한 Dynamic Cipher는 다음과 같다.

Algorithm Dynamic Cipher
Input : Key K and Plaintext B_0^0;
Output : Ciphertext B_m^n;
$KB = Key\ Sceduling\ Algorithm(K)$;
Let $KB = \{kb_1, kb_2, \cdots, kb_n\}$;
if $(n/4)\%2 == 0$ **then**
  $rot = (n/4)\%2 + 1$;
else $rot = (n/4)\%2 + 2$;
end if
for $i = 1$ **to** n **do**
  $B_j^i = B_{j-1}^i \oplus K$;
  if $kb_i == 0$ **then**
    $B_j^i = B_j^i \otimes B_{n-j+1}^i$;
  else $B_j^i = B_j^i \otimes B_{\frac{n}{2}+j}^i$;
  end if
  while (k is prime number)
    $tmp = B_j^{i+1}$;
    $B_j^{i+1} = B_j^i$;
  end while
  if $kb_i = 1$ **then**
    $j = (j - |-\frac{n}{2}|)\%(n+1)$
  end if
  $B_j^i = B_{j-1}^i \oplus B_j^i$;
  $B_j^i = B_{(j+rot)\%n}^i$;
end for
End Dynamic Cipher

주 키 $K = K_1 K_2 \cdots K_n$에 대하여, 제안한 Dynamic Cipher의 키 스케줄링 알고리즘이 생성하는 키 블록 집합은 $\{K_1, K_2, \cdots, K_n\}$이다.

그림 1은 제안한 Dynamic Cipher의 1 라운드를 나타낸 것이다.

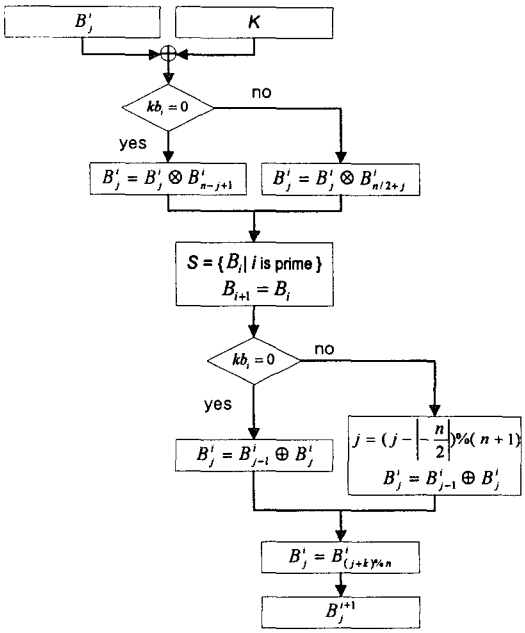

그림 1 Dynamic Cipher의 1 라운드

4. Dynamic Cipher의 분석

Feistel Cipher의 비선형 함수의 출력값은 입력값과 서브키의 연산으로 이루어진다. 따라서 비선형 함수의 출력쌍의 차분값은 입력쌍의 차분값과 서브키를 연산한 형태로 나타낼 수 있다. 이러한 성질을 이용하여 차분 분석법을 적용한다. 그러나, Dynamic Cipher의 라운드 함수에서는 서브 블록과 서브키 사이에 연산이 이루어지지 않으므로 함수의 입력 차분값과 출력 차분값을 키와 연산된 상태로 나타낼 수 없다. 그러므로 Dynamic Cipher에 차분 분석법을 적용하기가 어렵다.

Dynamic Cipher에 선형 분석법을 적용하기 위해서는 선형 근사식을 구해야 한다. 그런데 Dynamic Cipher는 키 블록에 따라 블록 연산을 선택하므로 키 블록에 따라 선형 근사식이 다르게 나타나게 된다. 따라서 어떤 선형 근사식을 적용해야 하는지 알 수 없으므로 Dynamic Cipher에 선형 분석법을 적용하기는 어렵다.

Meet-in-the-middle 공격은 라운드 함수가 순차적으로 구성되어 있는 Dynamic Cipher에 치명적일 수 있다. 키 블록 집합 $K=\{K_1, K_2, \cdots, K_n\}$에 대하여, 평문을 $K_1, \cdots, K_i$로 암호화한 결과와 암호문을 $K_n, \cdots, K_{i+1}$로 복호화한 결과가 같은 경우가 있다. Meet-in-the-middle 공격으로부터 안전한 Dynamic Cipher를 설계하는 방법은 키 비트를 두 번 이상 사용하는 방법과 서브 블록과 서브키 사이에 연산을 행하는 방법이 있다. 제안한 Dynamic Cipher는 알고리즘 초기 단계에서 서브 블록과 서브키 사이에 xor 연산을 함으로써 Meet-in-the-middle 공격에 대해 안전하도록 설계하였다.

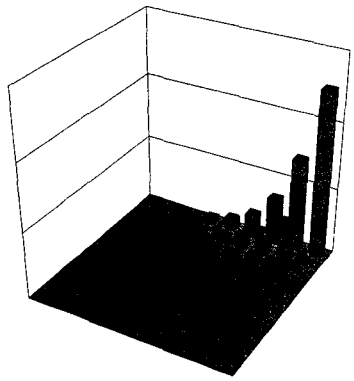

그림 2 제안한 Dynamic Cipher의 속도

Dynamic Cipher는 56비트의 키를 사용하여 초당 약 9.12Kbit의 속도로 암호화를 수행함을 알 수 있었다. 그림 2는 키 크기와 블록 크기를 증가시키면서 암호화 속도를 측정한 결과이다.

완벽하게 안전한(perfect secrecy) 암호 시스템은 다음의 두 가지 조건을 만족해야 한다.

$$E_{k_1}(P) \neq E_{k_2}(P) \quad \cdots\cdots \text{(식 1)}$$

$$E_k(P_1) \neq E_k(P_2) \quad \cdots\cdots \text{(식 2)}$$

서로 다른 두 평문을 같은 키로 암호화한 암호문은 서로 다르므로 제안한 Dynamic Cipher가 식 2를 만족함은 자명하다. 제안한 Dynamic Cipher가 식 1을 만족하는가에 대한 분석을 위해 분산을 구하는 다음 식을 사용하였다.

$$\frac{\sum(x-\bar{x})}{n} \quad \cdots\cdots \text{(식 3)}$$

식 3에서 x는 임의의 비트 스트링이 암호문으로 나타나는 횟수이고, $\bar{x}$는 평균으로 나오는 암호문의 수로 $\bar{x}$의 값은 1이다. n은 가능한 모든 키의 가짓수이다.

키 \ 블록	8bit	10bit	12bit	14bit	16bit
8bit	0.976562	0.804688	0.949219	0.992188	0.996094
10bit		0.949219	0.798828	0.943359	0.982422
12bit			1.040527	0.803955	0.941162
14bit				0.996460	0.807556
16bit					1.021881

표 1 평문을 모든 키로 암호화한 암호문의 분산

표 1은 모든 비트가 0인 평문을 가능한 모든 키로 암호화했을 때 나오는 암호문을 구한 후, 암호문이 분포하는 정도를 식 3을 이용하여 구한 것이다. 표 1에서 분산은 1에 근사하고, 분산이 1이라는 것은 하나의 평문을 암호문으로 대응시키는 키가 평균 두 개라는 것을 의미한다. 이러한 성질은 제안한 Dynamic Cipher의 암호 분석(Cryptanalysis)을 어렵게 한다.

평문, 키의 길이	평문만 1bit 차이날 때	키만 1bit 차이날 때
64bit	34bit	27bit
128bit	60bit	67bit
192bit	109bit	104bit
256bit	136bit	130bit

표 2 1bit가 다른 두 블록에 대한 쇄도효과

표 2는 첫 번째 비트만 다른 평문을 동일한 키로 암호화한 암호문과 동일한 평문을 첫 번째 비트만 다른 키로 암호화한 암호문을 각각 비교한 것이다. 첫 번째 비트만 다른 평문을 동일한 키로 암호화한 경우, 평문 길이의 약 절반 정도가 달라짐을 알 수 있다. 동일한 평문을 첫 번째 비트만 다른 키로 암호화한 암호문도 역시 약 절반이 다르다. 그리고 평문과 키의 크기가 커질수록 1비트의 차이가 암호문 블록 전체에 미치는 영향이 커짐을 알 수 있다. 모의 실험 결과는 제안한 Dynamic Cipher가 좋은 쇄도 효과를 가진다는 사실을 보여주고 있다.

5. 결론

Dynamic Network은 최근에 제안된 대칭키 블록 암호 알고리즘을 위한 기본 구조이지만 아직까지 Dynamic Cipher는 제안되어 있지 않다. 본 논문에서는 Dynamic Cipher를 제안하였다. 제안한 Dynamic Cipher는 임의 길이의 비트 스트링을 키로서 사용가능하고, 짝수 길이의 비트 스트링을 평문으로 사용가능하며, 키의 길이와 같은 라운드 수를 갖는다. 그러므로 제안한 Dynamic Cipher는 키의 길이, 평문의 크기, 라운드 수가 모두 가변이다.

제안한 Dynamic Cipher에 대한 차분 분석법과 선형 분석법, Meet-in-the-middle 공격의 강도를 분석하였다. 제안한 Dynamic Cipher에 차분 분석법과 선형 분석법을 적용하기는 어려운 이유들을 제시하였고, Meet-in-the-middle 공격으로부터 안전한 이유를 제시하였다.

제안한 Dynamic Cipher는 임의의 평문이 서로 다른 키에 의해 대응된 암호문의 분산이 평균 1이며, 좋은 쇄도 효과를 갖는다는 사실을 모의 실험을 통하여 분석하였다.

추후에 전수 검사와 취약키 문제, 보수 특성 존재 등 대칭키 블록 암호 알고리즘이 만족하여야 할 성질들 중에서 분석되지 않은 사항들에 대하여 분석할 필요가 있다.

참고문헌

[1] E. Biham, "Differential Cryptanalysis of DES-like Cryptosystems", Advances in Cryptology-CRYPTO '90, LNCS 537, pp. 2-21, 1990.

[2] E. Biham, V. Furman, "Impossible Differential on 8-Round MARS' Core", http://csrc.nist.gov/encryption/aes.

[3] L. R. Knudsen, "Practically Secure Feistel Ciphers, Fast Software Encryption", Cambridge Security Workshop Proceedings, pp. 211-221, 1994.

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

[5] S. B. Park, N. K. Joo, H. S. Lim, "Dynamic Network: A New Framework for Symmetric Block Cipher Algorithms", proceedings of ITC-CSCC, pp. 743-746, 2000.

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

[7] R. Rivest, M.J.B. Robshaw, R. Sidney, and Y. Yin, "The RC6 Block Cipher", a block cipher submitted for consideration as the new AES

[8] B. Schneier, "Applied Cryptography second edition", John Wiley & Sons, 1996.

[9] B. Schneier, "Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish)", Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, 1994, pp. 191-204.

[10] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, and N. Ferguson, "Twofish: A 128-Bit Block Cipher", 15 June 1998.

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

[12] C. E. Shannon, "Communication theory of secrecy systems", Bell System Technical Hournal, v. 27, n. 4, pp. 379-423, 1948.