동적 네트워크를 이용한 대칭블록암호 알고리즘

박종민*

Symmetric Block Cipher Algorithms Using the Dynamic Network

Jong-Min Park*

요 약

동적 암호는 키의 크기, 라운드의 수 그리고 평문의 크기가 동시에 측정될 수 있는 특성을 갖고 있다. 본 논문에서는 동적 네트워크에 기반한 대칭적인 블록 암호 알고리즘을 제안한다. 제안하는 동적 암호는 중간충돌공격과 선형 암호 해독 법에 대해서 안전하다. 또한 동적 암호에 대한 미분 분석이 힘든 것을 보여준다.

ABSTRACT

Dynamic cipher has the property that the key-size, the number of round, and the plain text-size are scalable simultaneously. In this paper we propose the block cipher algorithm which is symmetrical in the dynamic network. We present the method for designing secure Dynamic cipher against meet-in-the-middle attack and linear cryptanalysis. Also, we show that the differential cryptanalysis to Dynamic cipher is hard.

키워드

동적 네트워크, 대칭 블록 암호, 동적 암호

Key words

Dynamic network, symmetric block ciphers, Dynamic cipher

* 정회원 : 조선이공대학 사이버보안과 교수

접수일자 : 2011. 02. 28
심사완료일자 : 2011. 04. 14

Ⅰ. 서 론

오늘 날 인터넷 사용자의 증가는 더 많은 사람들이 은밀한 기록 자료들을 교환하고, 제품을 구매하고, 그리고 민감한 자료를 접근하기 위해 컴퓨터 망들을 사용하기 때문에 좋은 암호 알고리즘에 대한 필요는 급속히 퍼지고 있다.

암호시스템은 대칭적 키와 비대칭 키[1],[2]의 두 가지 일반적인 타입들의 키에 근거한 알고리즘이 있다. 대칭적인 키 알고리즘에서는 부호 매김 키와 암호 해독 키는 같다.

비대칭 키 알고리즘은 암호화를 위하여 사용된 키가 해독을 위하여 사용된 키와 다르게 하기 위해서 고안 되었다. 대칭 알고리즘과 비대칭 키 알고리즘은 각자가 자신의 장점과 단점을 가지고 있기 때문에 동등한 근거에서 비교될 수 없다.

여기에는 블록암호와 스트림 암호[1],[2] 두 가지 대칭 키 알고리즘이 존재한다. 블록암호는 평문과 암호문의 블록에서 작동한다.

스트림 암호는 한 번에 평문과 암호문의 1개의 비트 또는 바이트를 흐름상에서 작동한다.

Feistel 네트워크는 블록암호의 고안으로 잘 알려진 네트워크이다[1],[3],[4] 그리고 대부분의 블록암호들은 Feistel 네트워크상에 근거를 두고 있다[1],[5].

Feistel 암호들은 DES, RC5, IDEA 기타 등등을 포함한다. 또한 Feistel 암호들에 대한 공격에 관해 많은 연구들이 있었다. 미분 암호 분석과 선형 암호 분석들은 Feistel 암호들에 있어 잘 알려진 공격들이다[6],[7],[8],[9],[10],[11],[12].

Feistel 암호들이 라운드 키와 라운드 블록들에 영향을 끼치는 작동을 포함하고 있기 때문에 이러한 암호 분석들이 Feistel 암호들에서 가능하다.

동적 암호는 라운드 함수로 이루어져 있다. i번째 라운드 함수에서 i-1 의 라운드 블록은 i 라운드 키에 조건이 명시되어있고 i-1 라운드블록의 조각들에 영향을 미치는 조작 과정에 의해 i 라운드 블록으로 바뀐다. 라운드 블록의 생성 방법을 사용함에 따라 평문 사이즈, 라운드의 수, 그리고 동적 암호들이 동시에 측정 될 수 있다. 중간충돌공격(meet-in-the-middle), 미분 암호 분석법, 그리고 선형 암호 해독법에 대해서 동적 암호의 강도를 분석한다. 그 결과로 중간충돌공격과 선형 암호 해독법에 대한 안전한 동적 암호를 고안하는 방법들을 나타낸다. 또한, 동적 암호에 대한 미분 암호 해독법의 적용이 어렵다. 제안하는 대칭블록암호 알고리즘이 만족하는 성질들을 분석한다.

본 논문에서는 동적 네트워크를 이용한 대칭적인 블록 암호 알고리즘을 제안한다.

Ⅱ. 관련 연구

샤논은 대입(substitution) 암호법과 전송(transposition) 암호법 반복을 시행하는 블록암호는 강력한 암호가 될 수 있음을 보여준다. tishs의 정리에 바탕을 둔 대칭적 블록암호들에 대한 많은 네트워크들이 소개된다[1],[3],[4].

substitution-permutation 네트워크는 대입과 교환들을 포함하는 많은 단계들로 구성된다[1].

블록암호의 라운드는 적어도 한 개의 대입 암호와 적어도 한 개의 전송 암호[1]의 구성이다. 그리고 라운드 함수는 대칭 블록암호에서 기술되는 방법으로 전송 암호법과 전송 암호법을 실행하는 함수이다.

반복되는 연속적인 라운드 함수를 포함하고 있다. i번째 되풀이 된 라운드 함수는 i-1 라운드 블록과 그리고 i 라운드 키라 부르는 키들인 두 가지 입력들을 가지고 있다. 그리고 I번째 반복되는 라운드 함수의 산출은 i 라운드 블록이다.

Feistel 암호는 n 라운드 과정[1]을 통하여 암호문(Rn, Ln)에 대한 t-bit 블록 L0와 R0에 관해 2t-bit 평문(L0, R0)을 기록할 수 있는 반복되는 암호이다.

Feistel 암호의 i번째 라운드 블록은 f가 임의의 라운드 함수가 되고, Ki가 라운드 키가 되고, bit-wise eXclusive-OR를 의미하는 것은 Li=Ri-1 과 Ri=Li-1 f(Ri-1, Ki)을 사용하는 것에 의해 결정된다.

Feistel 암호의 i번째 라운드 블록은 대용을 위해 i-1 라운드 블록과 i 라운드 키 사이에서 실행된 작업과 i 라운드 사용하지 않고 전환을 위한 안정된 치환방법을 포함한다.

중간충돌공격은 키 K가 K1과 K2의 연속이 되고, E가 암호화 알고리즘이 되고, d가 암호해독 알고리즘이 되

며, p는 평문이 되고, c는 p[1]과 대응되는 암호문 E_{K_1}(p)= D_{K_2}(c) 수식을 사용한다. 중간충돌공격은 $2^{|K_1|}\times 2^{|K_2|}$ 을 대신해서 $2^{|K_1|}+2^{|K_2|}$에 대한 키 공간을 확보한다.

선형 암호 분석법은 선형의 근사적 표현[9],[10],[11],[12]을 사용한다. 선형의 근사적 표현은 비선형으로 고안된 라운드 기능의 입력과 출력사이에서 비선형으로 나타난다. 선형 근사치가 유지될 때 확률값은 가장 최적 표현을 찾는데 계산된다. 최상의 표현은 표출된 주제와 평문과 상호교류를 하는 알려진 평문과 암호문 쌍들을 포함한 약간의 통계적 특징들을 사용하여 키 비트들을 결정하는데 사용된다.

차분 암호 분석법은 차분[6],[7]을 규정했던 두 개의 암호문의 차이와 마지막 라운드 두 개의 입력 블록들의 차이를 계산한다.

Ⅲ. 동적 네트워크의 성질

O1, O2, …, Ol 가 블록 오퍼레이션 세트가 되도록 한다. Oj의 크기는 블록 오퍼레이션 세트들이 동적 암호(1≤j≤l)에서 설정되어지기 때문에 고정되어야 한다. 이것은 키 블록의 크기가 또한 고정된다.

m을 키 블록의 크기가 되도록 하고 k를 키가 되도록 한다. |K|가 키의 완전 검색에 대해 충분할 정도로 크다. 그리고 2m 요소를 갖는 블록 오퍼레이션 세트의 설계가 |K|m에 관해 실용적이지 못하기 때문에 |K|는 항상 m 보다 크다.

m≤|K|의 경우에, 키 같은 비트 스트링의 다양한 크기를 사용할 수 있는 키 스케줄링 알고리즘이 존재한다. 예를 들어 키 블록 kb와 키 K=k0k1…k|kb|×n-1에 관해, 키 블록 세트 {ki×|kb|ki×|kb|+1ki×|kb|+|kb|-1 | 0≤i≤n-1}를 생성하는 키 스케줄링 알고리즘 키로서 |kb|의 다중 크기의 모든 비트 선들을 사용할 수 있다. 키 K=k0k1…kn-1에 관해, 키 블록 세트 {ki mod n k(i+1) mod n…k(i+|kb|-1) mod n | 0≤i≤n-1}를 생성하는 알고리즘을 계획하는 키는 키로서 어떤 크기라도 비트 스트링을 사용할 수 있다. 따라서 동적 네트워크의 키 사이즈가 측정될 수 있다.

이러한 유용성 때문에 키 블록 세트를 생성하는데 사용되지 않은 키 비트는 존재하지 않는다. K1과 K2와 대응하는 두 개의 키 블록 세트를 생성할 것이다. 그리고 K2에 의해 생성된 키 블록 세트의 크기는 K1을 사용하여 생성하는 키 블록 세트의 크기보다도 더 크다. 따라서 동적 암호의 라운드의 수는 측정할 수 있다.

O1, O2, …, Ol가 블록 오퍼레이션 세트가 되도록 선택하고, Ui이 블록 오퍼레이션 Oi (1il), U=LCM(U1, U2, …, Ul)의 적용되는 단위가 되도록 한다. 크기 U=Ui×mi를 갖는 라운드 블록은 선택된 블록 작업 Oi mi번의 연속적 적용에 의해 얻어질 수 있다. 따라서 동적 암호는 평문들로서 크기 U×n를 갖는 모든 비트 스트링들을 사용할 수 있다. (2)의 예1의 유닛에 의해 대치되는 두 블록 오퍼레이션들을 사용한다.

Ⅳ. 동적 암호의 강도

중간충돌공격은 이중 암호화 feistel 암호들[1]에서 키 공간을 줄여준다. 이중 암호화 feistel 암호들은 끊임없이 두 개의 다른 키들을 사용한다. 모든 키 비트들을 두 배로 사용하는 이중 암호화 feistel 암호들의 키 공간은 싱글 암호화 feistel 암호들의 키 공간과 동등하게 된다.

중간충돌공격에 대한 안전한 동적 암호를 설계하는 제안된 방법은 키 비트들을 두 배 이상으로 사용한다. 예문들은 모든 키 비트들을 사용하는 것에 의해 키 블록 하부 세트 KB를 만들어내고, 그런 후에 KB의 반복에 의해 키 블록 세트를 생성하는 키 알고리즘을 포함한다.

두 배 이상 키 비트들을 사용하는 것은 모든 키 비트들을 두 배로 사용하는 키 블록 세트의 크기가 모든 키 비트들을 정확하게 한 번 사용하는 키 블록 세트의 크기보다도 더 크기 때문에 동적 암호의 실행 시간에 영향을 줄 것이다.

선형암호 분석법에 대해서 안전한 동적 암호를 고안하기 위해서 선형암호 분석법을 동적 암호에 적용하려는 가능성을 실험해야 한다. KB가 키 블록 세트의 하부 세트가 되도록 하고, K가 KB를 만들어내는데 사용된 키 비트들의 세트가 되도록 한다. 비트들의 가치가 KB에 의한 특정 지어진 가치로 인식될 가능성이 존재한다. 이 사실은 KB에 의해 결정된 선택된 블록 작업 세트가 선형이라는 것을 의미한다. 이런 경우에 있어서, 더 적어지게 하기 위해서 동적 암호의 키 공간으로 될 가능성이 있다.

선형암호 분석법에 대한 안전한 동적 암호를 설계하는 방법들은 다음과 같다.

(1) 암호법을 시행하는 몇몇의 블록 오퍼레이션들은 i 라운드 블록의 어떤 비트가 i 라운드 블록의 비트들에 가능한 많은 영향을 미칠 수 있도록 하기 위해 설계 되어야 한다. 이런 특성은 약간의 조각들의 값들과 그에 대응하는 값을 비교하는 것에 의해 키 블록을 추론 것은 어려울 것이다.

(2) 키 블록 kb에 관해서, kb에 의해 결정된 선택된 블록 오퍼레이션 세트를 결정하는 키 블록 공간은 2|kb| 가 되어야만 한다. 이런 특성은 특성(1)을 포함하며, 선택된 블록 오퍼레이션 세트의 비선형성을 보장한다. 그리고 이 특성은 키 블록 세트의 하부 세트에 관해 만족되어야 할 것이다.

(1)의 예문들은 다음 블록 작업을 포함한다. b1b2 bn 들이 i-1 라운드 블록이 되도록 하고 eXclusive-OR를 나타낸다. 대치 암호법을 실행하는 블록 오퍼레이션은 b1b2 bn 3in과 b'1= b'n b1에 대해서 b'2=b1 b2, b'i=b'i-1 로 되는 곳에서 b'1b'2 b'n 으로 측정을 하게 된다. 이런 경우에 i-1 라운드 블록의 한 비트는 평균적으로 i 라운드 블록의 n/2 비트들에 영향을 미친다.

(2)의 예문들은 두 개의 대치 암호법들로 구성된 다음의 블록 오퍼레이션 세트들을 포함한다. 하나의 대치 방법은 (1)의 예문에서 언급된 방법이다. eXclusive-NOR로 나타내도록 한다. 또 다른 대치 방법은 b1b2 bn 3in과 b'1= b'n b1에 대해서 b'2=b1 b2, b'i=b'i-1 b'i로 되는 곳에서 b'1b'2 b'n 으로 측정한다. 이 경우에 있어서 키 블록의 크기는 1이고 정확하게 하나의 대치 방법을 결정하는 키 블록 공간은 2가 된다.

차분암호 분석법에 대한 안전한 동적 암호를 설계하는데 있어서, 차분암호 분석법을 대칭적 블록 암호에 적용하는 조건을 조사했다. 차분암호 분석법은 차분적인 [1],[2],[4]를 결정하여 왔던 두 개의 선택된 평문들의 쌍을 사용한다. 그리고 각 쌍의 선택된 평문들의 차별성은 한 쌍의 암호문들의 명기된 차별성들과 한 쌍의 마지막 라운드의 입력 블록들로 측정된다.

Feistel 암호들이 순환에서 많은 키 비트들을 사용하고 있고 라운드 키와 라운드 블록 사이에서 작업을 실행하고 있다. 따라서 많은 키 비트들은 두 개의 암호문들의 알려진 차별성과 마지막 라운드의 두 입력 블록들의 알려진 차별성을 비교하는 것에 결정된다. 그리고 동적 네트워크의 경우는 아니다. (2)의 예문들을 관찰하여 보면 동적 암호에서 두 i-1 라운드 블록들의 차별성은 다른 키 블록은 다른 라운드 블록을 생성하기 때문에 두 i 라운드 블록들의 다양한 차별성들로부터 온다. 이 사실은 동적 암호에 대한 차별적 암호 분석법의 적용이 어렵다.

V. 동적 네트워크

동적 네트워크는 연속된 라운드 연속으로 구성된다. 동적 네트워크의 i 번째 라운드 함수에서 m-bits 블록은 유일하게 i-1 라운드 블록의 비트들에서 작동하는 작업들의 과정에 의해 또 다른 m-bits 블록으로 변형되거나 i 순환키에서 특성화 된다.

정의**1:** 블록 오퍼레이션은 평문의 블록을 암호문으로 바꾸는 작업이다. factor n의 블록 오퍼레이션 세트는 2n 블록 오퍼레이션들을 구성하는 세트이다.

각각의 블록작업은 m-bit 블록을 또 다른 m-bit 블록으로 지정하는 방법으로 표현된다. 동적 암호는 블록 오퍼레이션의 적용된 방법 혹은 사용된 오퍼레이터들에 의해 정의된 블록 오퍼레이션 세트들을 포함하고 있다. 그리고 블록 오퍼레이션 세트들은 기본적으로 전송 암호들에 대한 블록 작업 세트와 전송 암호들에 대한 블록 오퍼레이션 세트를 포함한다.

동적 암호의 키 스케줄링 암호는 그 키를 사용하는 것에 의해 n-bit 문자열들을 만들어 낸다. 따라서 하나의 n-bit 문자열은 블록 오퍼레이션 세트로부터 하나의 블록 오퍼레이션을 결정한다.

정의**2:** 키 블록이라는 것은 키 스케줄링 알고리즘에 의해 생성되는 n-bit 문자열이다.

L이 블록 오퍼레이션 세트의 숫자가 되도록 한다. 어떤 키 블록에 의해 결정되는 블록 오퍼레이션의 숫자는 1부터 L에 이르는 범위에 존재한다.

m을 각각 블록 오퍼레이션 세트로부터의 블록 오퍼레이션들에 의해 결정할 키 블록들의 숫자가 되도록 하고, {kb1, kb2, ···, kbjm}이 키 블록 세트가 된다. 키 스케줄링 알고리즘 블록 세트 {kb1, kb2, ···, kbjm}를 사용하는 것에 의해 {kb1||···||kbm-1||kbm, ···, kb(j-1)(m+1)||···

||kbjm} 라는 새로운 키 블록 세트를 재생산 할 수 있다. 따라서 어떠한 키 블록이 각각 블록 오퍼레이션 세트로부터의 블록 작업들에 의해 결정된다.

정의3: 선택된 블록 오퍼레이션 세트는 각 블록 오퍼레이션 세트로부터 하나의 키 블록에 의해 결정된 블록 오퍼레이션들의 선택된 세트이다.

i 번째로 선택된 블록 오퍼레이션의 입력은 (i-1)번째로 선택된 블록 오퍼레이션의 출력 블록이다. 출력은 선택된 블록 작업을 입력 블록에 적용하여 얻어지는 블록이다. 결과적으로 키 블록은 i-1 라운드 블록을 사용하는 것에 의해 i 라운드 블록을 만들도록 사용된다.

동적 암호는 다음 방법으로 평문을 암호화하는 대칭적 블록암호이다.

Algorithm Dynamic-Cipher

Input : Key block set *KB* and Plain text B_0^0.

Output : Cipher text B_0^n.

Let *KB*={*kb1, kb2, ···, kbn*}.
  for *i*=1 to *n* do
    Get the selected block operation set.
    Let {A1i, ···, A*mi*} be the selected block operation set.
  for *j*=1 to *m* do
    Get a new block B_j^{i-1} by applying Aji to B_{j-1}^{i-1}.
  end for
  $B_0^i = B_m^{i-1}$
end for
end Dynamic-Cipher

그림 1. 동적 암호 알고리즘
Fig. 1 Dynamic Cipher Algorithm

동적 암호의 강도는 다음의 (1)키 스케줄링 알고리즘 (2) 블록 오퍼레이션 세트들의 두 가지의 설계 방법에 좌우된다는 것을 알 수 있다.

서브블럭과 서브키 사이에 xor 연산을 함으로써 그림 2는 동적 암호의 강도를 나타내며 표 1은 모든 비트가 0인 평문을 가능한 모든 키로 암호화했을 때 나오는 암호문을 구한 후, 암호화한 암호문의 분산을 나타낸다.

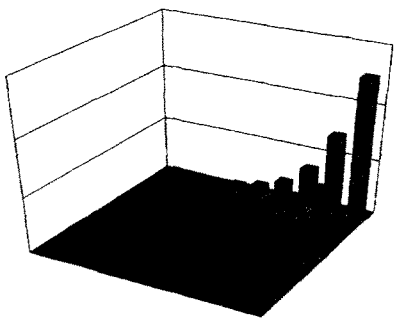

그림 2. 동적 암호의 강도
Fig. 2. Burglar of Dynamic Cipher

표 1. 암호화한 암호문의 분산
Table 1. Dispersion of the cipher text which encrypts

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

VI. 결 론

동적 암호는 키의 크기, 라운드의 횟수, 그리고 동적 암호의 평문 크기가 동시에 측정될 수 있다. 동적 네트워크는 대칭적 블록 암호들에 대한 네트워크들 속에서 이러한 특성들을 만족시키는 독특한 네트워크이다.

본 논문에서는 동적 네트워크에 기반한 대칭적인 블록 암호 알고리즘을 제안한다. 제안하는 동적 암호는 중간충돌공격, 선형암호 분석법, 차분암호 분석법에 관한 동적 네트워크의 강력함을 분석한다. 그리고 중간충돌 공격과 선형암호 분석법에 대해서 안전하다. 또한 동적 암호가 차분암호 분석법에 대해 안전하다.

참고문헌

[1] A. J. Menezes, P. C. Oorschot, and S. A. Vanstone, Applied Cryptography, CRC Press, 1997.

[2] B. Schneier, Applied cryptography, John Wiley Sons, 1996.

[3] 백진욱, 방정원, "동적 네트워크 환경하의 분산 에이전트를 활용한 병렬 유전자 알고리즘 기법," 한국컴퓨터정보학회 논문지 vol. 11, no. 4, pp. 1191-125, 2006.

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

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

[6] 김형식, 좌경룡, "동적 네트워크에서 최소 신장 트리를 유지하는 분산 알고리즘," 한국정보과학회 논문집 vol. 28, no. 1, pp. 739-741, 2001.

[7] 정치윤, 손선경, 장범환, 나중찬, "시각화 기반의 효율적인 네트워크 보안 상황 분석 방법," 한국정보보호학회 논문지 vol.19, no. 3, pp. 107-117, 2009.

[8] E. Biham and A. Shamir, Differential Cryptanalysis of the Data Encryption Standard, Springer-Verlag, New York, 1993.

[9] 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.

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

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

[12] 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.

저자소개

박종민(Jong-Min Park)

1988년 조선대학교 공학석사
2005년 조선대학교 공학박사
2008년 ~ 현재. 조선이공대학 사이버보안과 교수

※관심분야 : 바이오인식, 패턴인식, 인공지능, 정보보호 및 보안