블록 암호 알고리즘을 위한 Dynamic-네트워크

박 승 배
초당대학교 전자계산학과

Dynamic Network for Block Cipher Algorithm

Seung-Bae Park
Dept. of Computer Science, Chodang University

요 약

본 논문에서는 블록 암호 알고리즘을 위한 새로운 네트워크인 Dynamic-네트워크를 제시한다.

Dynamic-네트워크는 좋은 confusion과 diffusion 메카니즘을 제공한다. 어떠한 Dynamic-네트워크도 2^n-비트($n \geq 1$) 길이를 갖는 모든 평문을 입력으로 할 수 있으며, 일정 길이 이상의 모든 비트 스트링을 키로 사용할 수 있다.

1. 서 론

지금까지 제안된 대부분의 블록 암호 알고리즘들은 Feistel 네트워크이다 [9,12]. Feistel 네트워크는 $2t$-비트 평문을 t-비트 블록쌍 (L_0, R_0)로 나누고, 서브키 K_i와 함수 f를 이용하여 (L_i, R_i) $(1 \leq i \leq r,\ r \geq 1)$를 $L_i = R_{i-1}$과 $R_i = L_{i-1} \oplus f(R_{i-1}, K_i)$ ($\oplus$: Exclusive-OR)에 의해 구한 후, 최종 라운드에서 얻어진 (L_r, R_r)을 암호문으로 한다 [9,12]. Feistel 네트워크 개념을 이용한 블록 암호 알고리즘으로는 DES, Lucifer, FEAL, LOKI, GOST, CAST, Blowfish 등이 있다 [5,9,10,11,12].

Feistel 네트워크는 라운드 함수에 관계없이 역변환이 가능하고, 알고리즘의 수행속도가 빠르며 두 번의 수행으로 블록간의 완전한 diffusion이 가능하다는 등의 장점을 가지고 있다 [12]. 그러나, 1990년대에 들어와서 대부분의 Feistel 네트워크를 brute-force 공격 방법보다 효율적으로 공격할 수 있는 differential cryptanalysis [2,3,4,7,13]와 linear cryptanalysis [1,6,8,13]가 제시되었다. 이러한 공격 방법들의 결과로 Feistel-네트워크의 비도를 높이기 위하여 키 길이를 늘리거나 대체 알고리즘을 개발하고자하는 노력들이 활발히 진행되고 있다.

본 논문에서는 블록 암호 알고리즘을 위한 새로운 네트워크인 Dynamic-네트워크를 제시한다.

Dynamic-네트워크는 두 개의 키 스케줄링 함수를 사용하며, 주어진 블록으로부터 새로운 블록을 생성하기 위하여 하나의 함수를 사용한다.

Dynamic-네트워크는 좋은 confusion과 diffusion 메카니즘을 제공한다. 어떠한 Dynamic-네트워크도 2^n-비트($n \geq 1$) 길이를 갖는 모든 평문을 입력으로 할 수 있으며, 일정한 길이 이상의 모든 비트 스트링을 키로 사용할 수 있다.

논문의 구성은 다음과 같다. 2장에서는 Dynamic-네트워크에 대하여 정의하고, Dynamic-네트워크의 성질들을 살펴본다. 3장에서는 앞으로의 연구방향에 대하여 언급하고 결론을 맺는다.

2. Dynamic-네트워크

이 장에서는 Dynamic-네트워크에서 사용하는 함수들의 종류에 대하여 살펴보고, Dynamic-네트워크를 정의한다.

2.1 Dynamic-네트워크의 함수

블록에 적용하고자 하는 연산자를 원소로 하는 집합을 N이라 하자. 그러면, $\lceil \log_2|N| \rceil$-비트 비트 스트링을 사용하여 N의 원소들을 구분할 수 있다.

Dynamic-네트워크에서 $\log_2|N|$은 양의 정수이며, $\log_2|N|$-비트 비트 스트링을 이용하여 블록에 적용하고자 하는 연산자를 나타낸다.

bs_o를 $\log_2|N|$-비트 비트 스트링이라 하자. 함수 F_O는 bs_o를 이용하여 블록에 적용할 연산자를 결정하는 함수이다. $F_O(bs_o)$의 결과를 O라 할 때, $O = F_O(bs_o)$로 나타낸다.

블록 $B = b_0 b_1 b_2 \cdots b_{|B|-1}$에 대하여, $\lceil \log_2|B| \rceil$-비트 비트 스트링은 연산을 적용할 블록에서의 위치를 나타낼 수 있다.

Dynamic-네트워크에서 $\log_2|B|$는 양의 정수이며, $\log_2|B|$-비트 비트 스트링을 사용하여 연산이 적용되는

블록에서의 위치를 나타낸다.

bs_P가 $\log_2|B|$-비트 비트 스트링이고 연산이 적용되는 B에서의 위치를 나타낸다고 하자. 함수 F_P는 bs_p를 이용하여 연산이 적용되는 블록에서의 위치를 결정하는 함수이다. $F_P(bs_p)$의 결과를 P라 할 때, $P=F_P(bs_p)$로 나타낸다.

블록 $B=b_0b_1b_2\cdots b_{|B|-1}$에 대하여, $\log_2|B|$-비트 비트 스트링은 rotation left(right) shift 비트수를 나타낼 수 있다.

bs_s가 $\log_2|B|$-비트 비트 스트링이고 rotation left(right) shift 비트수를 나타낸다고 하자. 함수 F_S는 bs_s를 이용하여 rotation left(right) shift 비트수를 결정하는 함수이다. $F_S(bs_s)$의 결과를 S라 할 때, $S=F_S(bs_s)$로 나타낸다.

함수 F_O, F_P, F_S의 결과인 O, P, S를 이용하여 주어진 블록으로부터 새로운 블록을 생성할 수 있다.

예를 들어, $B=b_0b_1b_2b_3b_4b_5b_6b_7$=00111010, N=(보수, XOR, XNOR, addition modulo), 연산자를 나타내는 비트 스트링이 표 2.1과 같다고 하자. 그리고, O=00, P=100, S=100, $b_P=b_{100}(b_4)$에서부터 O=00(보수)를 적용한 후, S=100-비트(4-비트) 만큼 rotation left-shift 한다고 하자. 그러면, O, P, S를 이용하여, 주어진 블록 B=00111010으로부터 새로운 블록 B'=01011100을 생성할 수 있다.

N의 원소	연산자를 나타내는 $\log_2\|N\|$-비트 비트 스트링
보수	00
XOR	01
XNOR	10
addition modulo	11

표 2.1 : 연산자와 연산자에 대응하는 비트 스트링

함수 F_{NB}는 함수 F_O, F_P, F_S의 결과인 O, P, S를 이용하여 주어진 블록으로부터 새로운 블록을 생성하는 함수이다. 주어진 블록 B에 대하여, $F_{NB}(B, O, P, S)$의 결과를 NB라 할 때, $NB=F_{NB}(B, O, P, S)$로 나타낸다.

서브 키 K_i에 대하여, 함수 F_{SK}는 K_i를 이용하여 새로운 서브 키를 생성하는 함수이다. $F_{SK}(K_i)$의 결과를 K_{i+1}이라 할 때, $K_{i+1}=F_{SK}(K_i)$로 나타낸다.

예를 들어, $K_i=k_0k_1k_2k_3k_4k_5k_6k_7k_8k_9$=1100101001이라 하고, 함수 F_{SK}가 $k_j(0\le j\le 9)$의 보수를 취하는 함수라 하자 그러면, $K_{i+1}=F_{SK}(K_i)$=0011010110이 된다.

정의 : 함수 F_O, F_P, F_S의 파라미터인 bs_o, bs_p, bs_s를 접합 연산자 ·를 이용하여 접합한 $bs_o \cdot bs_p \cdot bs_s$를 키 블록(Key Block)이라 한다.

서브 키 K_i에 대하여, 함수 F_{KB}는 서브 키 K_i를 이용하여 키 블록을 원소로 하는 집합을 생성하는 함수이다 $F_{KB}(K_i)$의 결과를 KB_i라 할 때, $KB_i=F_{KB}(K_i)$로 나타낸다

예를 들어, $|B|=8$, $|N|=4$, $K_i=k_0k_1k_2k_3k_4k_5k_6k_7k_8k_9$= 1100101001, 함수 F_{KB}가 $k_jk_{j+1}\cdot k_{j+2}k_{j+3}k_{j+4}$ $(0\le j\le 5)$를 키 블록이 되도록하는 함수라 하자. 그러면, $KB_i=F_{KB}(K_i)$={11 · 001 · 001, 10 · 010 · 010, 00 · 101 · 101, 01 · 010 · 010, 10 · 100 · 100, 01 · 001 · 001}이 된다.

2.2 Dynamic-네트워크

Dynamic-네트워크는 키 스케줄링 함수로 F_{SK}와 F_{KB}를 이용하고, 주어진 블록으로부터 새로운 블록을 생성하기 위하여 함수 F_{NB}를 이용한다.

정의 : 입력 블록을 B_0, 키를 K_1, 서브 키의 수를 n이라 하자. 그러면, 다음과 같은 과정을 수행하는 블록 암호 알고리즘을 Dynamic-네트워크라 한다.

1) 현재의 서브 키를 $K_i(i\ge 1)$라 하자. 서브 키 $K_{i+1}=F_{SK}(K_i)$을 생성한다

2) 키 블록들의 집합 $KB_{i+1}=F_{KB}(K_{i+1})$을 생성한다.

3) $|KB_{i+1}|=l$, $KB_{i+1}=\{(K_{j_1}^{i+1}\cdot K_{j_2}^{i+1}\cdot K_{j_3}^{i+1})|(K_{j_1}^{i+1}\cdot K_{j_2}^{i+1}\cdot K_{j_3}^{i+1})\in F_{KB}(K_{i+1}),\ 1\le j\le l\}$이라 하자. $O_{j_1}^{i+1}=F_O(K_{j_1}^{i+1})$, $P_{j_2}^{i+1}=F_P(K_{j_2}^{i+1})$, $S_{j_3}^{i+1}=F_S(K_{j_3}^{i+1})$을 구한다 $(1\le j\le l)$.

4) 현재의 블록을 $B_m(m\ge 0)$이라 하자. $B_1=F_{NB}(B_m, O_{11}^{i+1}, P_{12}^{i+1}, S_{13}^{i+1})$, $B_2=F_{NB}(B_1', O_{21}^{i+1}, P_{22}^{i+1}, S_{23}^{i+1})$, …, $B_l'=F_{NB}(B_{l-1}', O_{l1}^{i+1}, P_{l2}^{i+1}, S_{l3}^{i+1})$를 차례로 생성한다

5) 단계 1) ~ 단계4)를 n-1번 반복한다.

6) B_l'을 암호문으로 한다.

함수 F_{KB}는 서브 키를 이용하여 키 블록 $bs_o \cdot bs_p \cdot bs_s$을 생성한다. 키 블록 $bs_o \cdot bs_p \cdot bs_s$에서, 비트 스트링 bs_P와 bs_S는 연산을 적용할 블록에서의 위치와 rotation left(right) shift 비트수를 나타내므로, Dynamic-네트워크는 2^n-비트$(n\ge 1)$ 길이를 갖는 모든 평문에 적용가능하다. 즉, 어떠한 Dynamic-네트워크도 2^n-비트$(n\ge 1)$ 길이를 갖는 모든 평문을 입력으로 할 수 있다

함수 F_{SK}는 주어진 서브 키로부터 새로운 서브 키만을 생성하고, 함수 F_{NB}가 주어진 블록으로부터 새로운 블록을 생성한다. 따라서, Dynamic-네트워크는 안전도가 보장되는 키 길이 이상의 모든 키를 키로 사용할 수 있다. 즉, 어떠한 Dynamic-네트워크도 일정 길이 이상의 모든 키를 키로 사용할 수 있다.

함수 F_{KB}는 서브 키를 이용하여 키 블록 집합을 생

성하고, 함수 F_{NB}는 키 블록이 가지고 있는 정보만을 이용하여 주어진 블록으로부터 새로운 블록을 생성한다. 따라서, 주어진 블록과 새로 생성된 블록 사이의 관계를 나타내는 정보는 키 블록 만이 가지고 있으며, 주어진 블록과 키 블록 사이에 어떠한 연산도 이루어지지 않는다. 그리므로, Dynamic-네트워크는 키와 블록간의 관계가 독립되어 있어 좋은 confusion 메카니즘을 제공한다.

하나의 키 블록은 주어진 블록의 모든 비트에 영향을 미치고, 키 블록에 따라 $0 \sim 2^n$-비트 만큼을 rotation left(right) shift하므로 주어진 블록과 새로 생성된 블록의 관계를 유추하기 어렵다. 그러므로, Dynamic-네트워크는 좋은 diffusion 메카니즘을 제공한다.

3. 결론

본 논문에서는 블록 암호 알고리즘을 위한 새로운 네트워크인 Dynamic-네트워크를 제안하였다.

Dynamic-네트워크는 키 스케줄링 함수로 F_{SK}와 F_{KB}를 이용하며, 주어진 블록으로부터 새로운 블록을 생성하기 위하여 함수 F_{NB}를 이용한다.

함수 F_{SK}는 주어진 서브 키로부터 새로운 서브 키를 생성하는 함수이며, 함수 F_{KB}는 F_{SK}로부터 생성된 서브 키를 이용하여 키 블록 집합을 생성하는 함수이다.

함수 F_O, F_P, F_S는 F_{KB}에 의해 생성된 키 블록을 이용하여 블록에 적용할 연산자, 연산자를 적용할 블록에서의 위치, rotation left(right) shift 비트수를 결정하는 함수이다.

함수 F_{NB}은 F_O, F_P, F_S에 의해 결정된 정보만을 이용하여 주어진 블록으로부터 새로운 블록을 생성한다.

Dynamic-네트워크는 키와 블록간의 관계가 독립되어 있어 좋은 confusion 메카니즘을 제공하며, 주어진 블록과 새로 생성된 블록과의 관계를 유추하기가 어려우므로 좋은 diffusion 메카니즘을 제공한다.

Dynamic-네트워크는 2^n-비트($n \geq 1$) 길이를 갖는 모든 평문을 입력으로 할 수 있으며, 일정 길이 이상의 모든 비트 스트링을 키로 사용할 수 있다.

앞으로, Dynamic-네트워크가 가지고 있는 성질들을 분석하는 것과 Dynamic-네트워크가 가지고 있는 장점들을 잘 표현하는 블록 암호 알고리즘을 개발하는 것이 필요하다.

참고 문헌

[1] E. Biham, "On Matsui's linear cryptanalysis," Technical Report CS0813, Department of Computer Science, Technion-Israel Institute of Technology, Israel, 1994.

[2] E. Biham and A Shamir. "Differential cryptanalysis of DES-like cryptosystems," Journal of Cryptosystems, vol.4, no. 1, pp. 3-72, 1991.

[3] E Biham and A. Shamir, "Differential cryptanalysis of Snefru, Khafre, REDOC-II, LOKI, and Lucifer," Advances in Cryptology-CRYPTO '91 Proceedings, Springer-Verlag, pp. 156-171, 1992

[4] E. Biham and A. Shamir. Differential cryptanalysis of the Data Encryption Standard, Springer-Verlag, 1993.

[5] L. Brown. J.Pieprzyk, and J. Seberry, "LOKI A Cryptographic primitive for authentication and secrecy applications," Advances in Cryptology-AUSCRYPT '90 Proceedings, Springer-Verlag, pp. 229-236 1991

[6] B.S Kaliskijr and M.J.B. Robshaw, "Linear cryptanaysis using multiple approximations," Advances in Cryptology-CRYPTO '94 Proceedings, Springer-Verlag, pp 26-39. 1994

[7] B.S. Kaliskijr and Y.L. Yin, "On differential and linear cryptanalysis of the RC5 encryption algorithm," Advances in Cryptology-CRYPTO '95 pp. 171-184, 1995

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

[9] A.J. Menezes, P.C. van Oorschot, and S.A. Vanstone. Handbook of applied cryptography, CRC Press, 1997.

[10] B. Schneier. "Descryption of a new variable-length key, 64-bit block cipher (Blowfish)," Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer-Verlag, pp. 191-204, 1994.

[11] A. Shimizu and S. Miyaguchi, "Fast data encryption encipherment algorithm FEAL," Transaction of IEICE of Japan, vol. J70-D. no. 7, pp. 1413-1423. 1987.

[12] D R Stinson, Cryptography theory and practice, CRC Press, 1995.

[13] A.M. Youssef and S.E. Tavares, "Resistence of balanced s-boxes to linear and differential crypyanalysis," Information Processing Letters 56, pp. 249-252, 1995.